МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Доржи Банзарова

И.С.Поломошнов

Администрирование локально-вычислительных сетей под управлением BaseALT Linux Server

Улан-Удэ
2026

УДК _____
ББК _____

Утверждено к печати Экспертным советом университета
Протокол № __ от «___» _____ 2026 г.

Рецензенты

А.А.Дубанов
Кандидат технических наук, доцент кафедры Информационной безопасности Института математики, физики и компьютерных наук БГУ

А.В.Лобанов
Доцент практики, начальник отдела Информационной безопасности ГБУ РБ «Информационно-Технологический Центр»

Поломошнов И.С.
Администрирование локально-вычислительных сетей под управлением BaseALT Linux Server: учебное пособие. — Улан-Удэ: Изд-во Бурятского госуниверситета, 2026. — 145 с.
ISBN

В учебном пособии рассмотрены процессы установки и конфигурирования сервера под управлением BaseALT Linux, а также настройка ключевых сетевых служб (DHCP, DNS, Samba DC, файлового сервера и прокси-сервера Squid). Особое внимание уделяется интеграции клиентских машин под управлением Windows и Linux в доменную инфраструктуру и управлению доступом к сетевым ресурсам. Пособие содержит подробные практические инструкции по созданию виртуальной лаборатории в среде Oracle VirtualBox и примеры выполнения типовых задач системного администратора. Материал направлен на формирование у обучающихся базовых навыков администрирования гетерогенных локально-вычислительных сетей.

Пособие предназначено для обучающихся по направлению подготовки 09.03.03 "Прикладная информатика" в рамках освоения дисциплины «Системное администрирование».

УДК _____
ББК _____

ПРЕДИСЛОВИЕ

В данном учебном пособии рассматриваются возможности развёртывания сервера на примере операционной системы BaseALT Server Linux. Выбор данной версии ОС обусловлен её относительно невысокими требованиями к аппаратным ресурсам: достаточно 256 МБ оперативной памяти и минимального свободного дискового пространства. Для сравнения: десктопная версия MS Windows Server 2019 требует 4 ГБ оперативной памяти, что может стать критичным при развёртывании в виртуальной среде с ограниченными ресурсами.

Основная цель пособия: сформировать у обучающихся базовые навыки администрирования локально-вычислительной сети (ЛВС) под управлением BaseALT Server Linux.

Для моделирования виртуальной среды используется бесплатное программное обеспечение Oracle VirtualBox. Актуальную версию программы можно скачать с официального сайта разработчика: https://www.virtualbox.org/wiki/Downloads .

В пособии представлена модель построения локально-вычислительной сети с использованием доменной архитектуры под управлением единого сервера. Сервер выполняет следующие ключевые функции:

1. Контроллер домена (Samba AD-DC).
2. DNS-сервер (BIND9 или внутренний DNS Samba).
3. DHCP-сервер (ISC DHCP-Server).
4. Файловый сервер (Samba).
5. Прокси-сервер (Squid).

Кроме того, в пособии рассмотрены вопросы:

- создание и настройка групповых политик на уровне домена;
- организация управляемого общего доступа в интернет с использованием программного прокси-сервера.

Оглавление

Технический словарь

1. DHCP (Dynamic Host Configuration Protocol) — протокол динамической конфигурации узла, позволяющий устройствам автоматически получать IP-адрес и другие параметры сети (маску, шлюз, DNS) от сервера.

2. DHCP-сервер — сервер, который в соответствии с протоколом DHCP автоматически назначает IP-адреса и сетевые настройки клиентским устройствам в сети.

3. DNS-сервер (Domain Name System Server) — сервер, который преобразует понятные человеку доменные имена (например, google.com) в машинные IP-адреса и наоборот.

4. Firewall (Брандмауэр) — система (программная или аппаратная), которая контролирует и фильтрует сетевой трафик между сетями (например, между локальной сетью и интернетом) на основе заданных правил безопасности.

5. FTP (File Transfer Protocol) — протокол передачи файлов между клиентом и сервером по сети.

6. GUI (Graphical User Interface) — графический пользовательский интерфейс, основанный на окнах, кнопках, меню и других визуальных элементах, управляемых с помощью мыши или сенсорного ввода.

7. IP-адрес (Internet Protocol Address) — уникальный числовой идентификатор устройства в сети, построенной по протоколу IP. Служит для адресации и маршрутизации данных.

8. Kernel (Ядро) — центральная часть операционной системы, обеспечивающая взаимодействие между приложениями и аппаратным обеспечением компьютера, управляющая ресурсами и процессами.

9. LAN (Local Area Network) — локальная вычислительная сеть, ограниченная небольшим географическим пространством (офис, дом, здание).

10. Маска сети (Subnet Mask) — битовая маска, которая определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу конкретного узла (хоста) в этой сети.

11. Маршрутизатор (Router) — сетевое устройство, которое пересылает пакеты данных между различными сетями (например, между локальной сетью и интернетом), определяя оптимальный путь на основе таблицы маршрутизации.

12. NAT (Network Address Translation) — технология преобразования сетевых адресов, позволяющая множеству устройств в локальной сети выходить в интернет под одним публичным IP-адресом маршрутизатора.

13. Port (Порт) — числовой идентификатор (от 0 до 65535) в транспортных протоколах (TCP/UDP), который определяет конкретное сетевое приложение или службу на устройстве для обработки входя8. щего или исходящего трафика.

14. Proxy-сервер (Прокси-сервер) — промежуточный сервер между клиентом и другими серверами. Он выполняет запросы от имени клиента, может кэшировать данные, фильтровать трафик, обеспечивать анонимность или контроль доступа.

15. RDP (Remote Desktop Protocol) — проприетарный протокол от Microsoft, обеспечивающий удалённое подключение к графическому рабочему столу другого компьютера.

16. SMB (Server Message Block) — сетевой протокол для совместного доступа к файлам, принтерам и другим ресурсам в локальной сети, широко используемый в системах Windows.

17. SSH (Secure Shell) — сетевой протокол для безопасного удалённого управления операционной системой и туннелирования TCP-соединений, использующий шифрование.

18. TUI (Text-based User Interface) — текстовый пользовательский интерфейс, который использует символы и псевдографику для создания интерактивных элементов (меню, кнопок) в текстовом режиме (например, Midnight Commander).

19. WAN (Wide Area Network) — глобальная вычислительная сеть, покрывающая большие географические регионы (например, интернет или корпоративная сеть между филиалами).

20. Виртуализация — технология создания виртуальных (эмулируемых) версий компьютерных ресурсов: серверов, рабочих станций, сетей, хранилищ или операционных систем, работающих на одном физическом оборудовании.

21. Виртуалбокс (VirtualBox) — популярное кроссплатформенное программное обеспечение для виртуализации от компании Oracle, позволяющее создавать и запускать виртуальные машины.

22. Домен (Domain) — 1) В контексте DNS — имя, идентифицирующее область в интернете или локальной сети (например, example.com). 2) В контексте

Windows Active Directory — группа компьютеров и пользователей, управляемая как единое целое с общими правилами и каталогом.

23. Клиент — компьютер или программное обеспечение, которое запрашивает и использует услуги, ресурсы или данные, предоставляемые сервером.

24. Рабочая станция (Workstation) — 1) Персональный компьютер пользователя в сети, предназначенный для выполнения прикладных задач. 2) Мощный компьютер для профессиональных задач (дизайн, программирование, инжиниринг).

25. Сервер — компьютер или специализированное устройство (а также программное обеспечение), предоставляющее услуги, ресурсы или данные другим компьютерам (клиентам) по сети.

26. Сеть (Network) — совокупность компьютеров и других устройств, соединённых каналами связи для обмена данными и совместного использования ресурсов.

27. Файловый сервер (File Server) — сервер, основная задача которого — централизованное хранение файлов и обеспечение доступа к ним для клиентов в сети.

28. ЦП (Центральный процессор) — это "мозг" компьютера, электронный блок, выполняющий все вычисления и управляющий работой остальных устройств. Основные характеристики: тактовая частота (скорость операций) и количество ядер (сколько задач может выполнять одновременно).

29. ОЗУ (Оперативное запоминающее устройство) — это временная память компьютера, в которой хранятся данные и программы, с которыми процессор работает прямо сейчас. При отключении питания все данные стираются. Объем ОЗУ напрямую влияет на количество задач, которые можно выполнять одновременно «без тормозов».

30. LVM (Logical Volume Manager) — это подсистема Linux для гибкого управления дисковым пространством, создающая уровень абстракции между физическими дисками и файловой системой.

Введение

Современное информационное общество немыслимо без надёжных и масштабируемых сетевых инфраструктур. Локально-вычислительные сети (ЛВС) с доменной архитектурой стали стандартом для организаций любого масштаба — от небольших офисов до корпораций. Ключевым элементом такой инфраструктуры выступает сервер, выполняющий функции управления ресурсами, аутентификации пользователей и контроля доступа к сервисам.

Актуальность изучения администрирования серверных операционных систем обусловлена следующими факторами:

- ростом числа распределённых информационных систем и облачных технологий;
- повышением требований к безопасности и отказоустойчивости корпоративных сетей;
- дефицитом квалифицированных специалистов по настройке и обслуживанию Linux-серверов в России, особенно на базе отечественных дистрибутивов;
- необходимостью импортозамещения в сфере системного программного обеспечения.

Цель пособия состоит в том, чтобы сформировать у обучающихся комплекс практических навыков, необходимых для:

- развёртывания сервера на ALT Server Linux;
- настройки ключевых сетевых служб (DNS, DHCP, файлового и прокси-сервера);
- организации доменной инфраструктуры с применением Samba AD-DC;
- управления доступом и применения групповых политик;
- диагностики и устранения типовых неполадок в виртуальной среде.

Настоящее методическое пособие посвящено практическому освоению развёртывания и администрирования ЛВС на базе операционной системы ALT Server Linux с использованием виртуальной среды Oracle VirtualBox. Выбор данной платформы продиктован сочетанием низких аппаратных требований, открытости исходного кода и соответствия промышленным стандартам сетевого администрирования.

Для успешного освоения материала достаточно базовых знаний по администрированию операционных систем и сетевым технологиям в объёме вводного курса. Все практические задания выполняются в виртуальной среде, что исключает риск повреждения рабочей инфраструктуры и позволяет многократно отрабатывать сценарии настройки.

Пособие адресовано студентам технических специальностей вузов, изучающим дисциплины «Администрирование компьютерных сетей», «Администрирование Linux/UNIX систем», «Системное администрирование», «Информационная безопасность», «Администрирование информационных систем», «Машинное обучение», «Компьютерные сети», «Введение в базы данных», «Базы данных» а также всем, кто желает получить практические навыки работы с серверными Linux-системами.

Раздел 1. Установка сервера.

В нашем примере в качестве сервера будет выступать операционная система Alt Server версии 11, образ которого можно загрузить с официального сайте https://www.altlinux.org в разделе «Alt Linux Сервер», где будет находится последняя версия серверной системы.

Выделить можно следующие преимущества AltServer: доступность, наличие стабильных репозиториев, дружелюбное сообщество администраторов, качественная техподдержка. Для реализации виртуальной среды будет использоваться бесплатное программное обеспечение Oracle VM VirtualBox. После установки оно практически сразу готово к работе и не требует настроек.

Если в процессе создания у вас не будут доступны некоторые функции, перекоючите режим работы VirtualBox из «Основой» в «Расширенный» (в некоторых версиях «Экспертный»). Для начала создадим виртуальную машину и разберем каждый этап ее создания:

1.1. Создание виртуальной машины.

Этап 1. Создание виртуальной среды. (ВС)

Запускаем приложение VirtualBox, затем нажимаем кнопку создать. (рис.1.1). У вас откроется окно создания виртуальной машины как показано ниже.

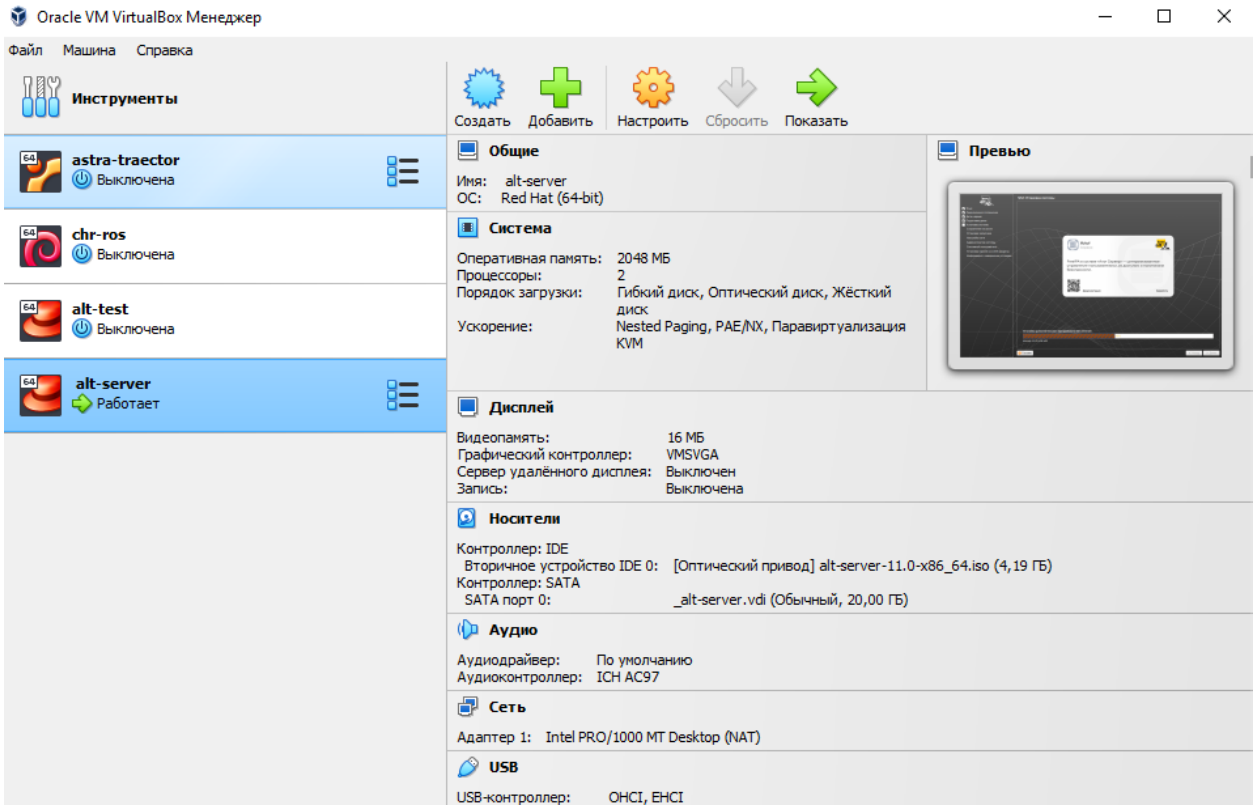

Рис.1.1. Рабочее окно Oracle VM VirtualBox

Примечание 1. Коротко об интерфейсе ВиртуалБокс:

- ***Создать*** *– клавиша вызывает команду создания новой виртуальной машины.*
- ***Добавить*** *– данная клавиша позволяет вам выполнить импорт ранее созданной ВМ или перенесенной с другого устройства.*
- ***Настроить*** *– данная команда вызывает окно настроек выбранной вами ВМ, в зависимости от состояния машины (включена или выключена) набор доступных настроек может меняться, так, например нельзя изменить количество ядер процессора или объём оперативной памяти на уже включенной машине, для внесения таких настроек нужно предварительно выключить ВМ.*
- ***Сбросить*** *– клавиша актуальна лишь в том случае, если вместо выключения вы сделали действие «Сохранить состояние ВМ», функция*

позволяет выполнить сброс сохраненного состояния и полностью выключит ВМ (методом грубой силы, «выдернуть из розетки»).

- ***Показать*** *– клавиша позволяет переключиться на окно с активной ВМ, доступна в том случае, когда машина включена.*

Этап 2. Виртуальная машина. (ВМ)

На данном этапе от вас требуется: задать имя виртуальной машине; указать расположение рабочей папки виртуальной машины, выбрать тип и версию.

В нашем примере название, папка, тип и версия уже указаны в необходимых для этого полях. (рис.1.2)

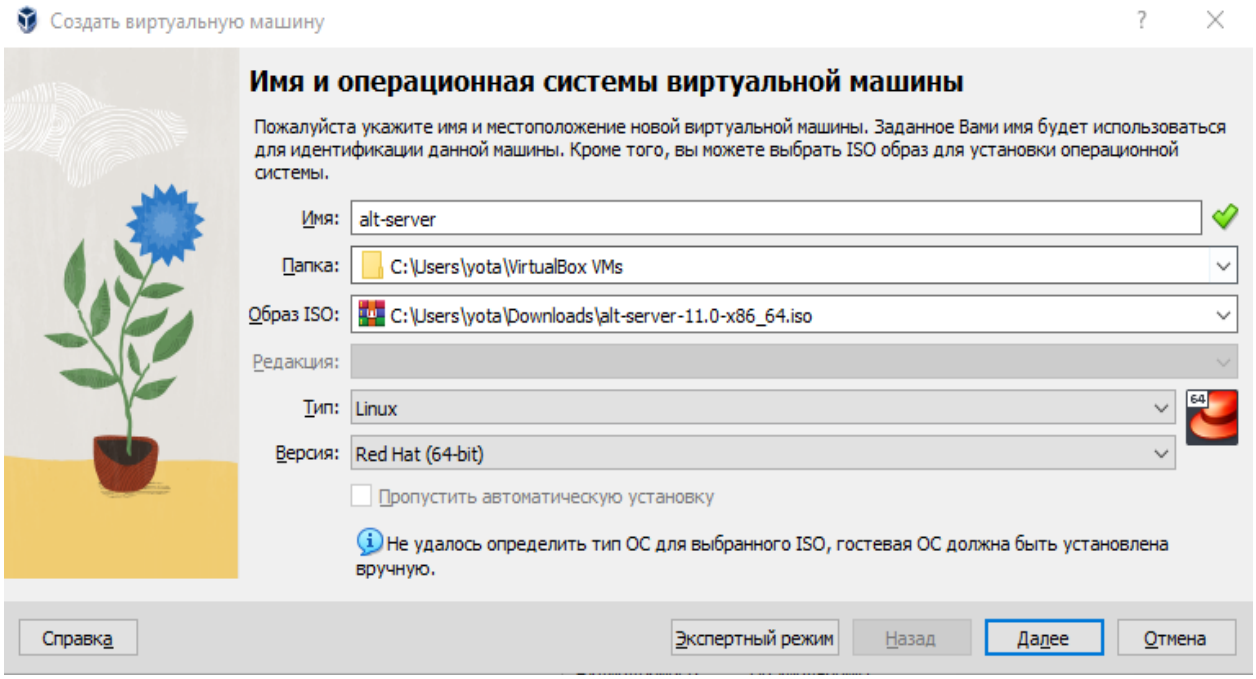

Рис. 1.2. Создание новой виртуальной машины

Этап 3. Оперативная память. (ОЗУ)

Затем от вас требуется задать необходимый для виртуальной машины объем оперативной памяти и количество ядер центрального процессора. Рекомендуемый объем — 2 ядра ЦП и 512 МБ ОЗУ, но для повышения производительности следует указывать с запасом.

Так, например, в нашем случае объем взят с запасом (*в связи с использование графической оболочки и веб-интерфейса*) и равен 2 ядра ЦП и 2048 МБ ОЗУ, что составляет 2ГБ физической оперативной памяти. (рис.1.3)

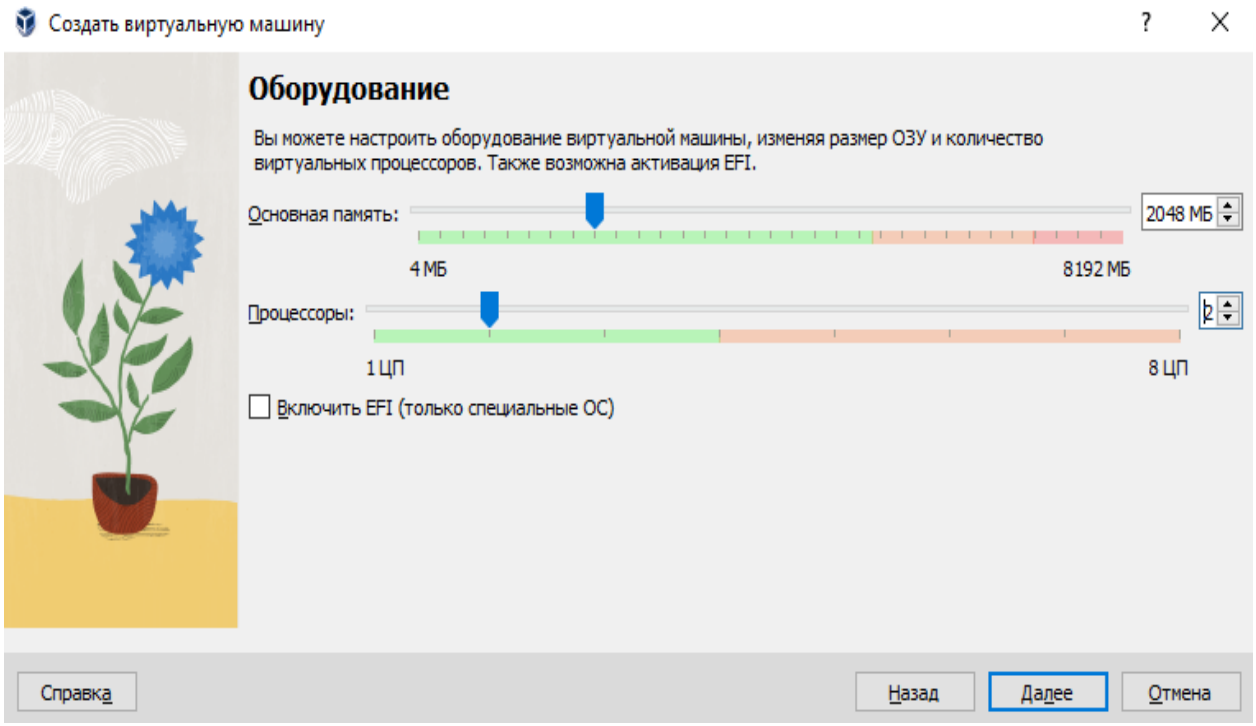

Рис. 1.3. Определение ресурсов виртуальной машины

Примечание 2. Следует принимать во внимание тот факт, что в данном случае используется полноценная операционная система и гипервизор ВМ ВиртуалБокс и для их нормального функционирования следует также оставлять свободными несколько ядер ЦП и ОЗУ, поэтому не рекомендуется отдавать все ресурсы виртуальной машине, и оставлять «холостыми» несколько ГБ ОЗУ и ядер ЦП.

После чего можно перейти к следующему окну.

Этап 4. Жесткий диск. (ЖД)

На данном этапе от вас требуется указать имеющийся у вас виртуальны жесткий диск или создать новый. *(рис.1.4)*

Выбираем «Создать новый виртуальный жесткий диск», затем жмем на кнопку «Далее».

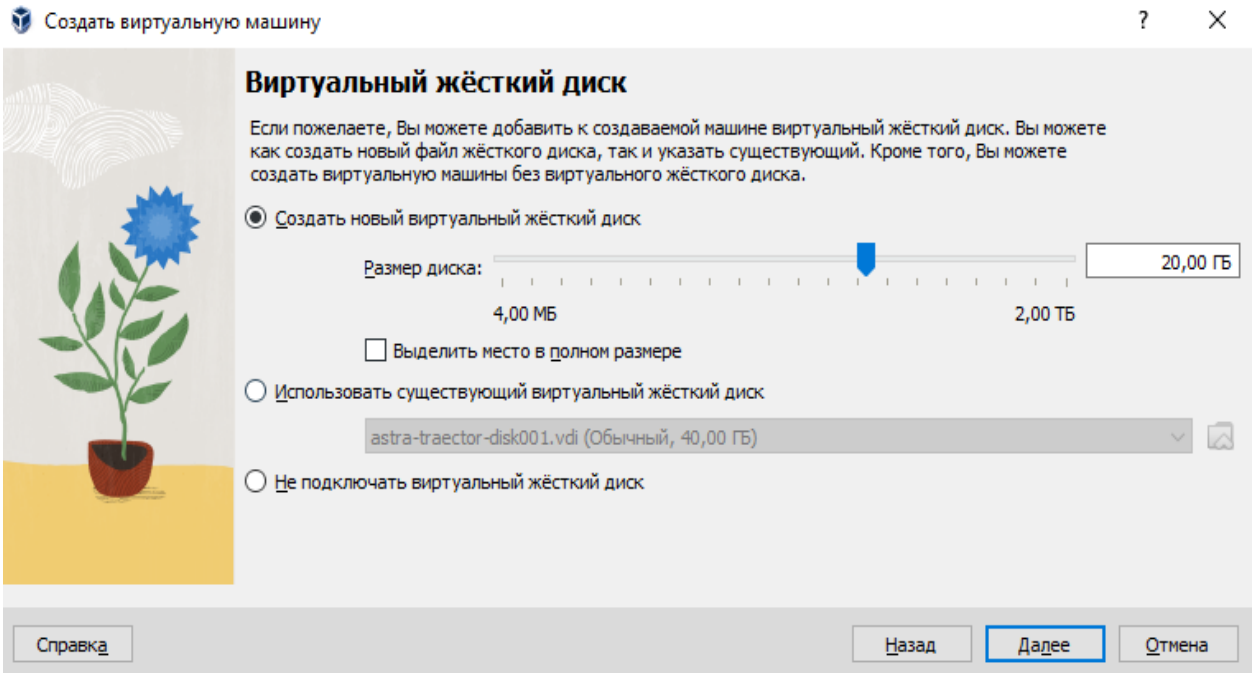

Рис.1.4. Определение размера жесткого диска

Этап 5. Тип виртуального жесткого диска. (ВЖД) (опционально)

Примечание 3. Данные этап является опциональным и строго необходим лишь в случае, если вам критически важна совместимость вашей ВМ с другими гипервизорами, например ATL Виртуализация, ProxmoxVE, Hyper-V и др.

Формат следует выбирать из соображений совместимости ВЖД с другими платформами виртуализации, так например:

- **формат VDI** используется исключительно в рамках программы VirtualBox;
- **формат VHD** может быть инициализирован в основной среде Windows, что позволит использовать его параллельно на ВС и на Windows;
- **формат VMDK** может быть использован не только вышеупомянутыми средствами, а также и в других программах виртуализации, например в VMware Workstation.

Пример выбора типа ВЖД представлен на рис 1.5.

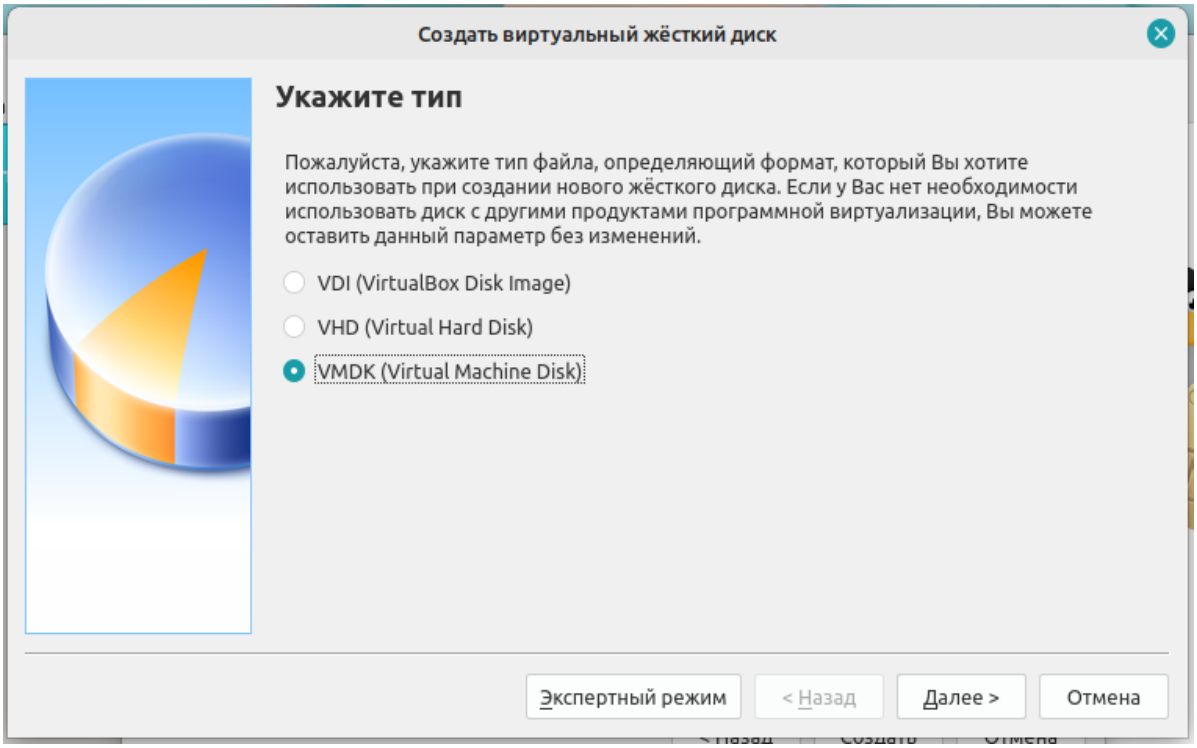

Рис. 1.5. Выбор типа жесткого диска

Этап 5.1. Формат хранения данных на ВЖД. (опционально)

На данном этапе ВМ задаст вопрос о выборе формата хранения данных на ВЖД. (рис.1.6)

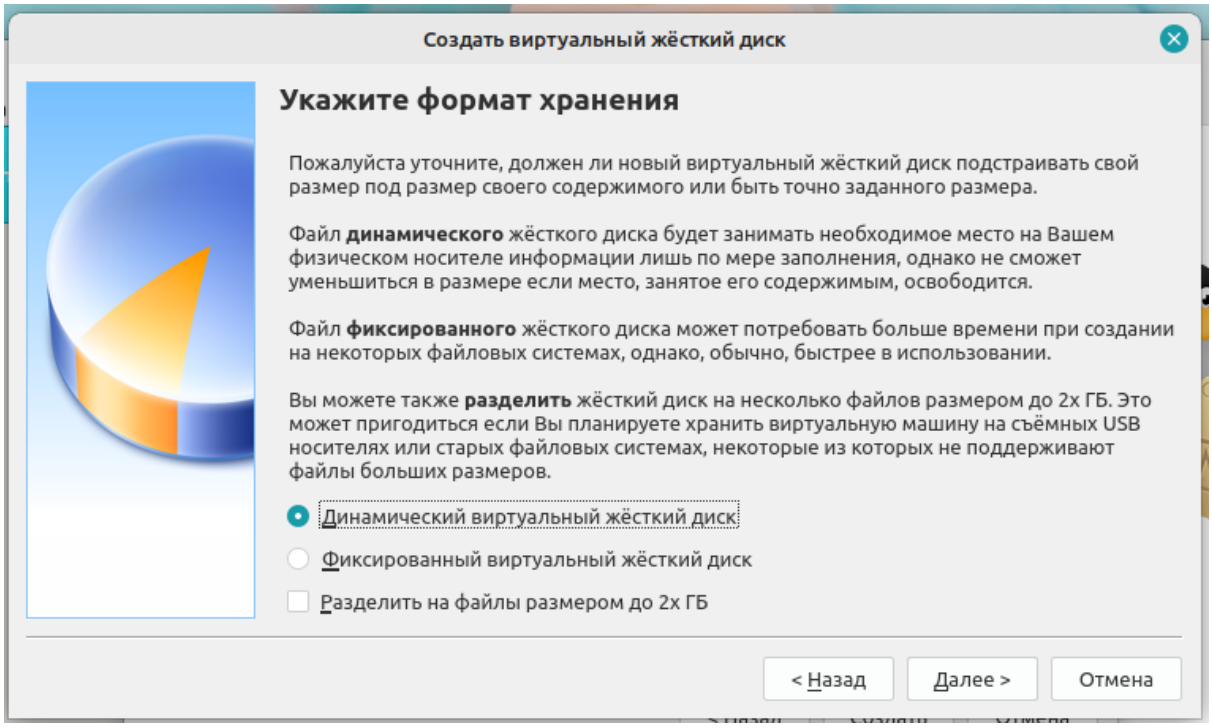

Рис. 1.6. Выбор формата хранения

Мы рекомендуем использовать динамический, т.е. размер файла диска будет напрямую зависеть от размера данных, хранящихся на нем, фиксированный же, сразу займет выделенный для него объем свободного пространства, а также процесс выделения займет некоторое количество времени. Определившись с выбором, вы можете продолжить.

Этап 6. Размер дискового пространства.

Если говорить на простом языке, то на данном этапе от вас требуется выделить некое количество места на диске для вашей машины. (рис.1.7)
Для данной операционной системы рекомендуется выбрать 10ГБ или более.

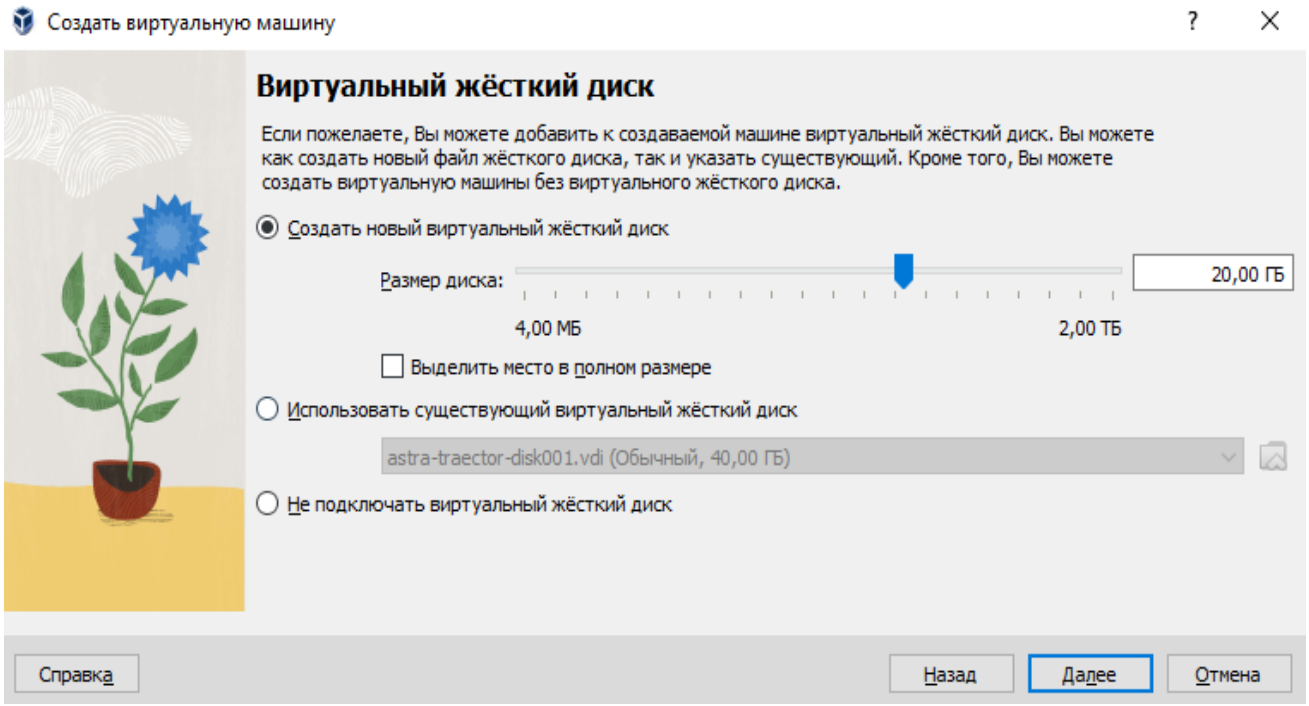

Рис. 1.7. Выбор объема жесткого диска

После того, как вы определились с объем нового виртуального жесткого диска, вы можете перейти к следующему этапу создания ВМ.

Примечание 4. Объем жесткого диска следует выбирать, ориентируясь на свободное место на вашей физическом (реальном) жестком диске или ssd, т.к. в случае выделения избыточного объема для ВМ, на вашей реальной машине (компьютере или ноутбуке) будет занято достаточно большое количество свободного места.

После выделения дискового пространства, гипервизор завершит создание ВМ и вам останется лишь подтвердить завершение создания ВМ. (рис. 1.8)

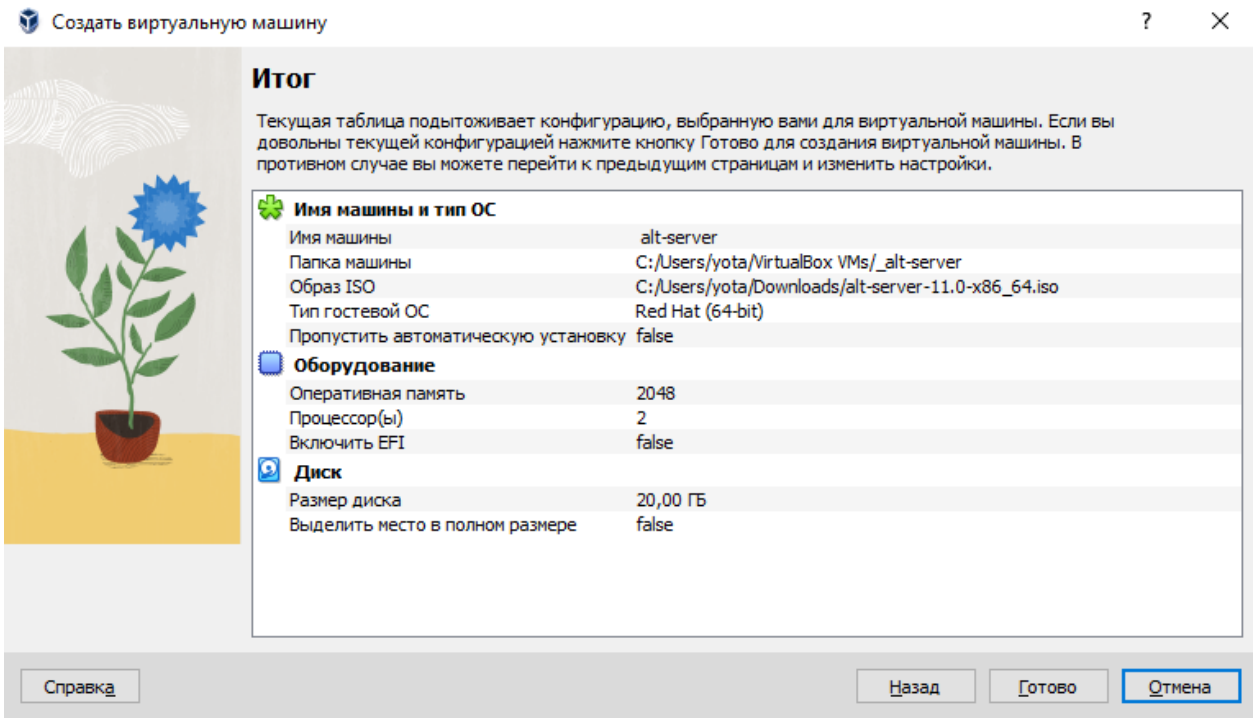

Рис.1.8. Сводная информация о созданной виртуальной машине

Затем жмем кнопку «Готово». Таким образом у вас завершится процесс создания виртуальной машины.

1.2. Предварительная настройка виртуальной машины.

Этап 1. Настройка внутренней сети виртуальной машины.

После проделанных выше действий можно считать, что виртуальная машина создана и готова к первому запуску, однако, перед запуском следует подключить в настройках машины еще одну важную деталь. Ниже приведена последовательность действий:

Шаг 1. Перейдите в настройки виртуальной машины; (рис.1.9)

Шаг 2. Перейдите на вкладку «Сеть»;

Шаг 3. Перейдите в раздел «Адаптер 2»;

Шаг 4. Активируйте сетевой адаптер;

Шаг 5. Задайте тип подключения «Внутренняя сеть» и задайте имя внутренней сети «intnet». (рис.1.10)

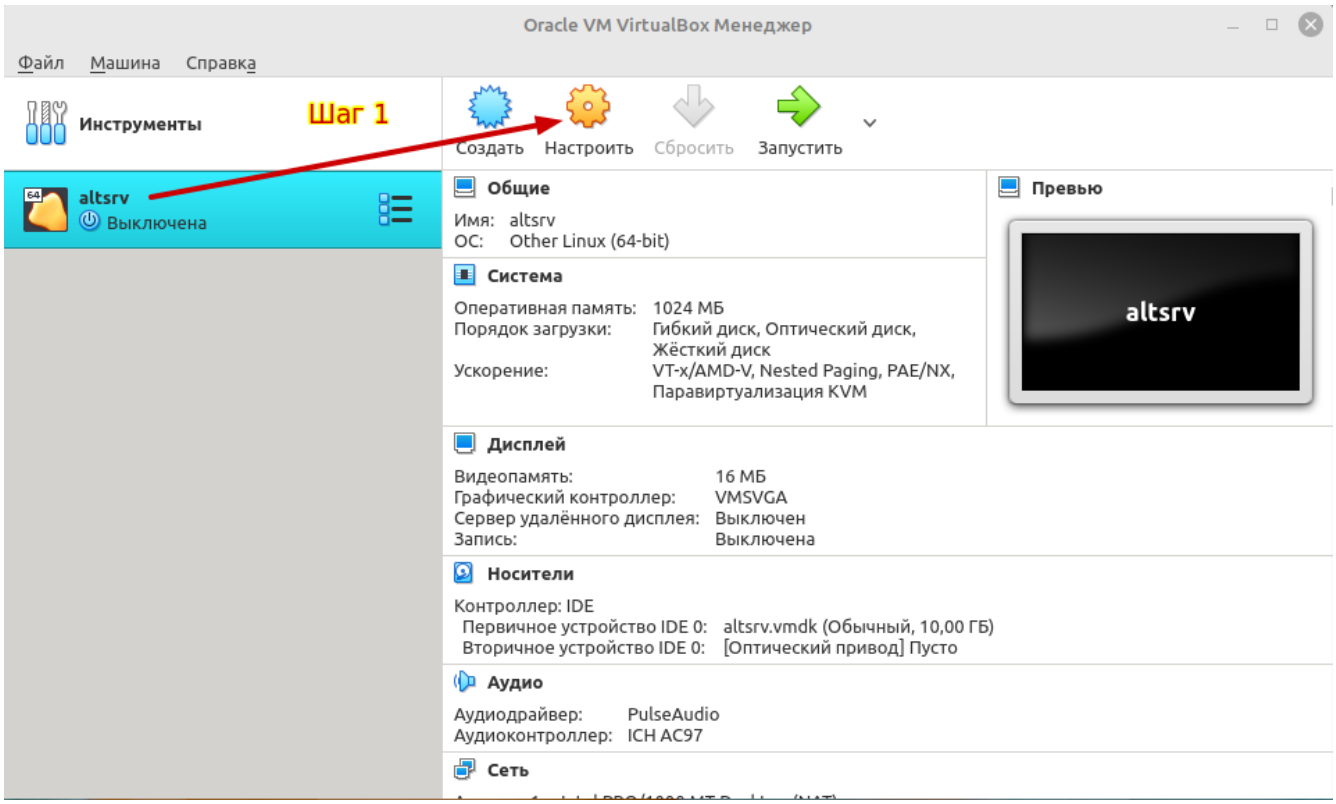

Рис. 1.9. Главное окно Oracle VM VirtualBox

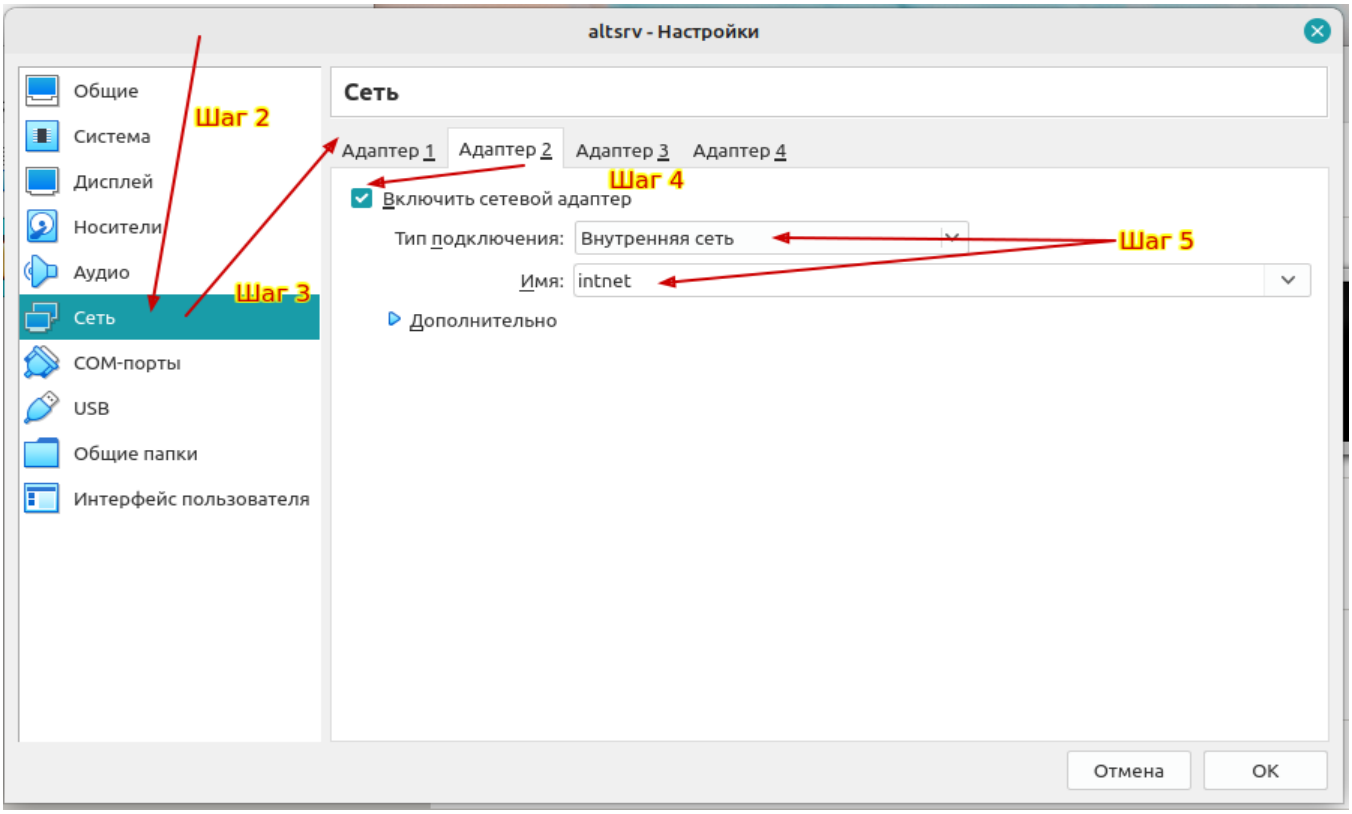

Рис. 1.10. Настройка сетевых интерфейсов гипервизора

1.3. Установка операционной системы.

Этап 1. Первый запуск, указание загрузочного диска.

При первом включения машина предложит вам выбрать образ загрузочного диска, после чего вы сможете приступить к установке ОС. Укажите путь до вашего загрузочного образа диска и нажмите кнопку «Продолжить».

Примечание 5. В нашем случае используется загрузочный образ alt-server-11. (рис.1.11)

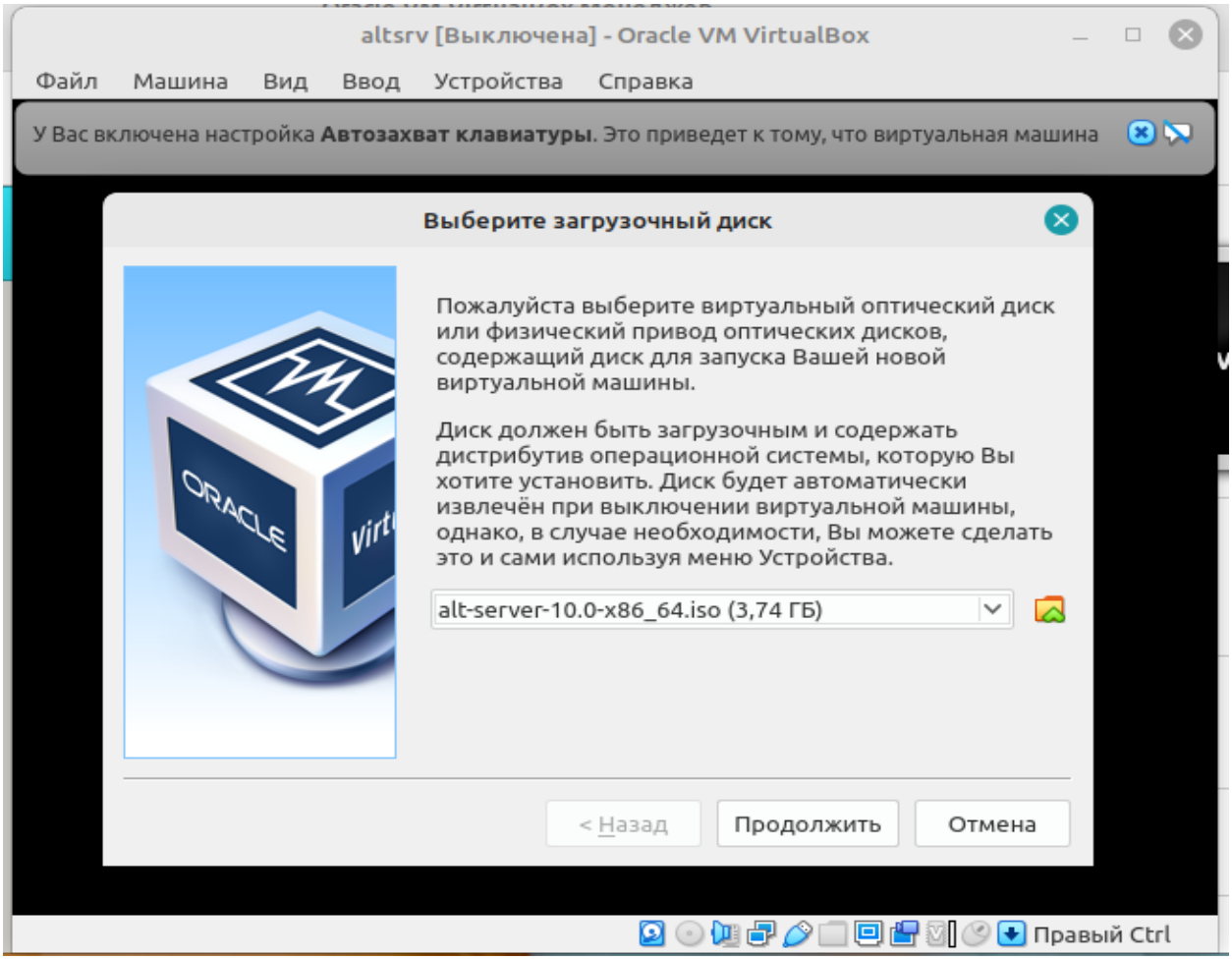

Рис. 1.11. Выбор диска загрузки операционной системы

Этап 2. Загрузка из образа диска.

При помощи клавиш со стрелками выберите пункт меню «Install ALT Server» и нажмите клавишу «Enter», чтобы запустить установщик ОС. Также в этом меню для вас предоставляется возможность загрузки с жесткого диска, если ранее была установлена другая операционная система или выполнить проверку оперативной памяти компьютера на возможность появления сбоев. (рис.1.12)

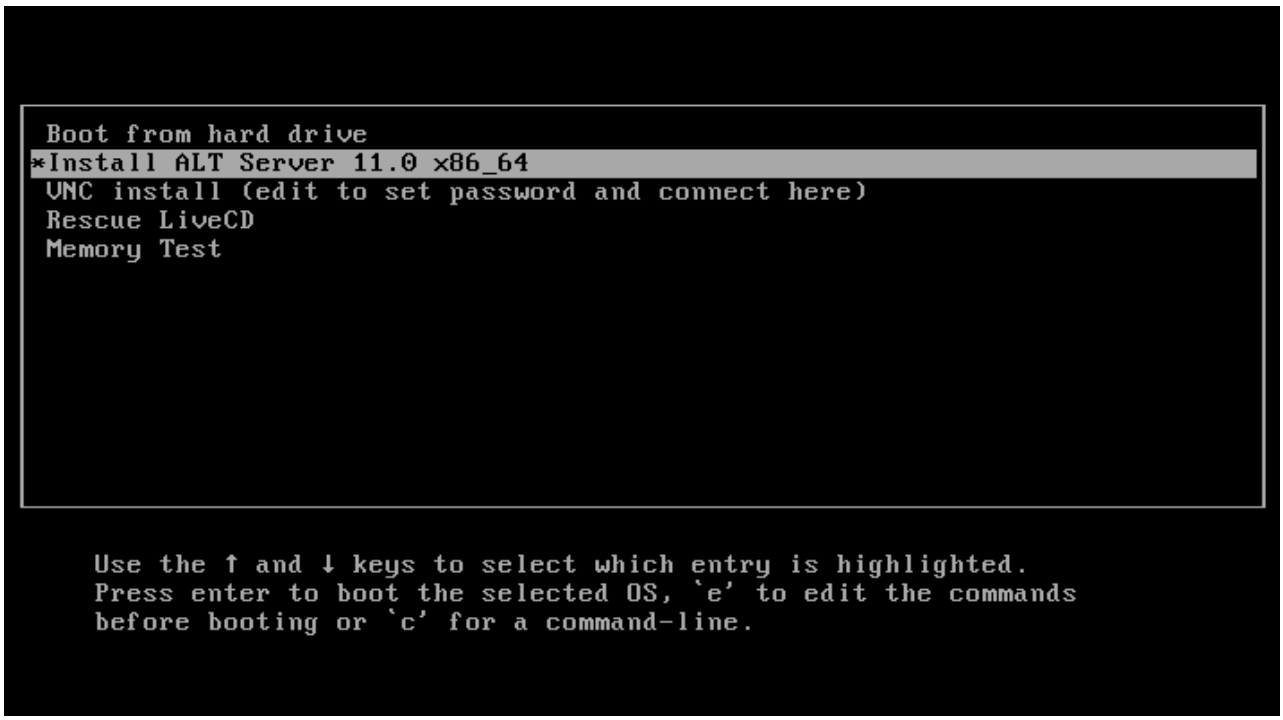

Рис 1.12. Загрузочное меню

Этап 3. Начало установки.

На данном этапе перед вами открывается окно установщика операционной системы, здесь присутствует возможность выбора языка устанавливаемого продукта, а также комбинации клавиш для возможности переключения раскладки клавиатуры, что в сравнении с другими операционными системами (например Windows), очень удобно. (рис.1.13)

Также внизу окна установщика есть возможность изучить справочные материалы Base ALT Linux при нажатии на кнопку «Справка» или переключиться между этапами установки нажав на логотип компании «BaseALT» в левом нижнем углу экрана. (Эта функция зачастую необходима, например, в случае если вам нужно восстановить загрузчик уже установленной ранее системы, но удаленный или испорченный в результате тех или иных действий. Рис 1.14)

Выбираем нужное и переходим дальше.

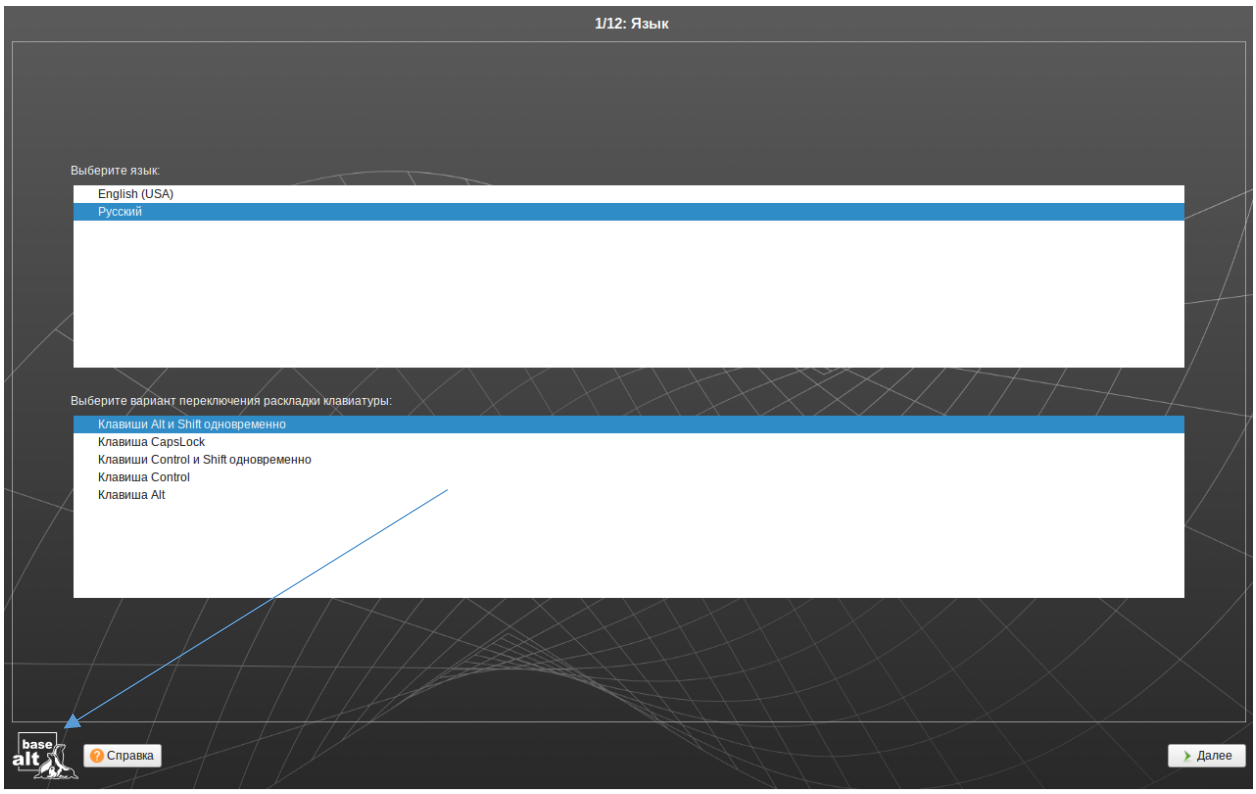

Рис. 1.13. Окно начала установки Alt Linux Server 11

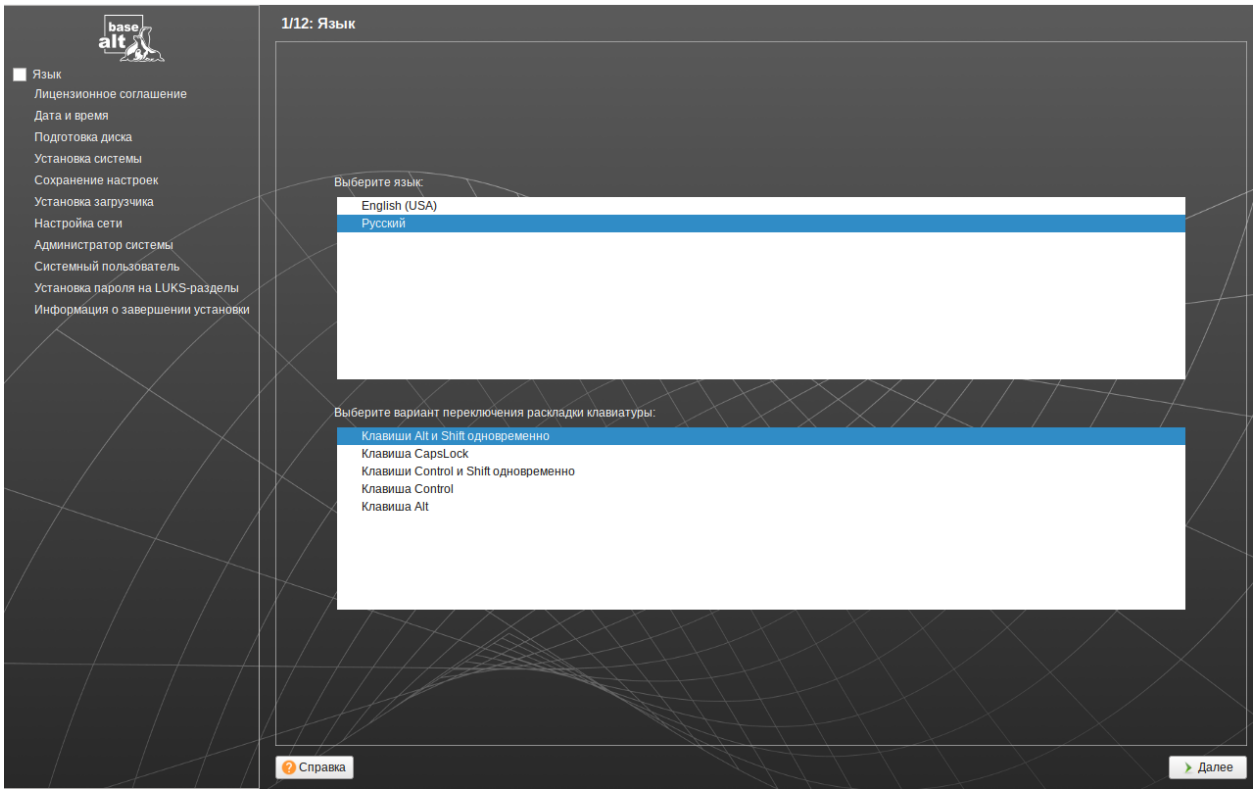

Рис 1.14 Окно выбора языка

Этап 4. Лицензионное соглашение.

Далее следует внимательно изучить условия лицензии, возможности устанавливаемого дистрибутива, а также возможные ошибки. (рис.1.15)

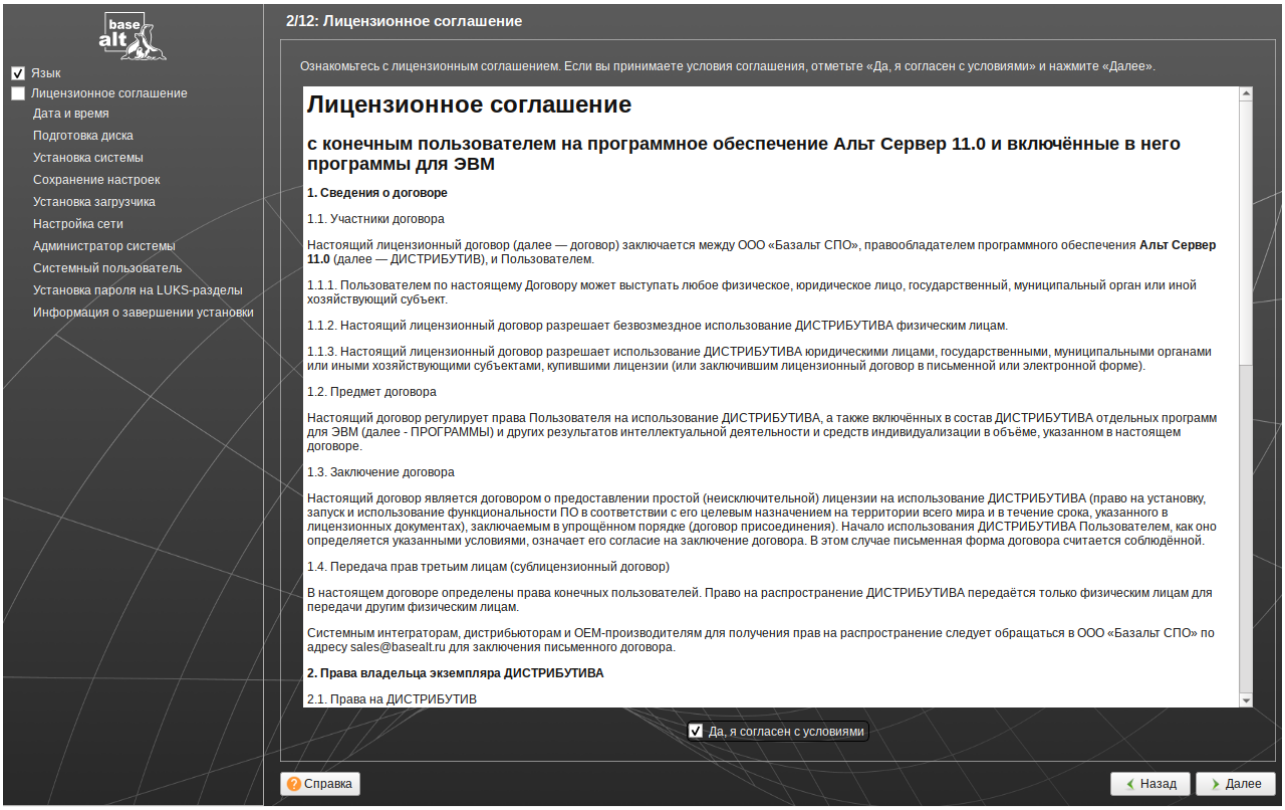

рис.1.15. Лицензионное соглашение

Примечание 6. Если лицензионный договор вас устраивает, ставьте галочку напротив параметра «Да, я согласен с условиями» и переходите к следующему этапу.

Этап 5. Выбор временной зоны (часовой пояс).

На данном этапе указываете свой регион и часовой пояс, после чего можно продолжить установку ОС. (рис.1.16)

Указание корректного часового пояса очень важный момент установки, т.к. от правильности указанного времени будет зависеть работа Сетевых служб сервера, а в дальнейшем и вся клиентская сеть.

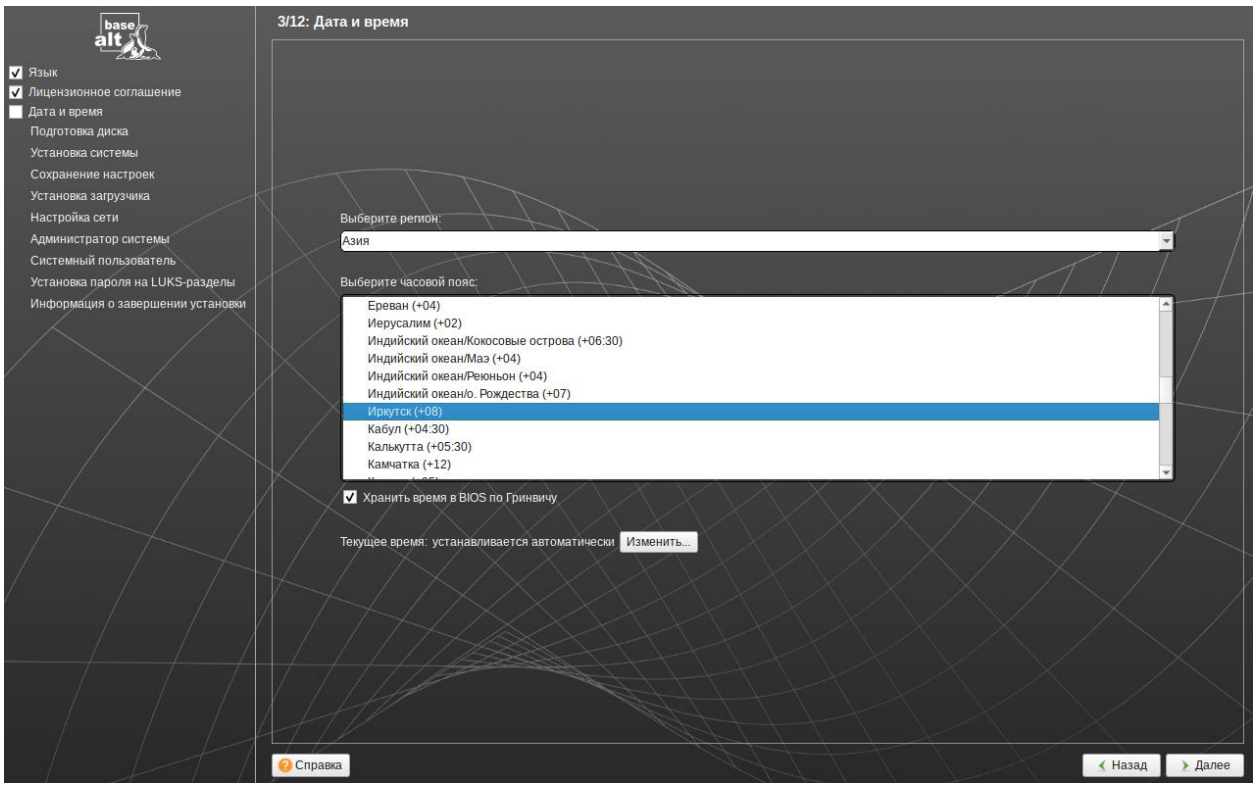

Рис. 1.16. Часовой пояс

Этап 6. Подготовка диска.

После установки временной зоны, установщик потребует от вас указать место для установки ОС, а также произвести (если это необходимо) разметку разделов жесткого диска.

Выбираете ваше запоминающее устройство, а затем можно выбрать установку сервера в автоматическом режиме или же перейти в ручной режим установки.

Мы рекомендуем ставим галочку напротив команды «Очистить выбранные разделы перед изменением профиля», а сам профиль установки указывать «Вручную», т.к. это дает больше гибкости при установке серверной системы. (рис.1.17)

Примечание 7. Так, например: установка сервера в автоматическом режиме займет около 26 ГБ свободного места на диске, в то время как корректно выполненная ручная установка займет всего 8-10 ГБ свободного места, а это ощутимая экономия ресурсов как компьютера, так сервера в дальнейшем

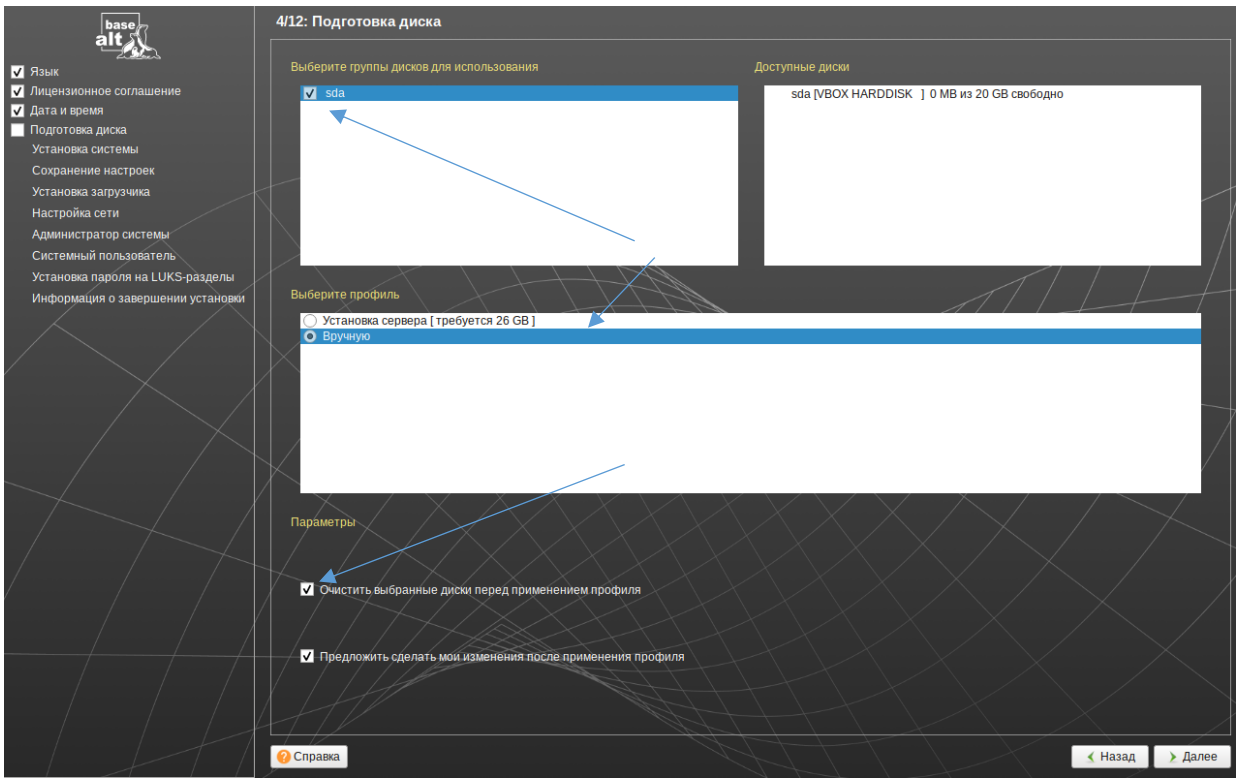

Рис. 1.17. Выбор диска для установки

Этап 7. Разметка дискового пространства.

После проделанных выше действий, программа разметки дисков откроет перед вами окно, как показано на рис.1.18. Чтобы приступить к разметке диска, нажмите на имя вашего устройства (sda 20GB).

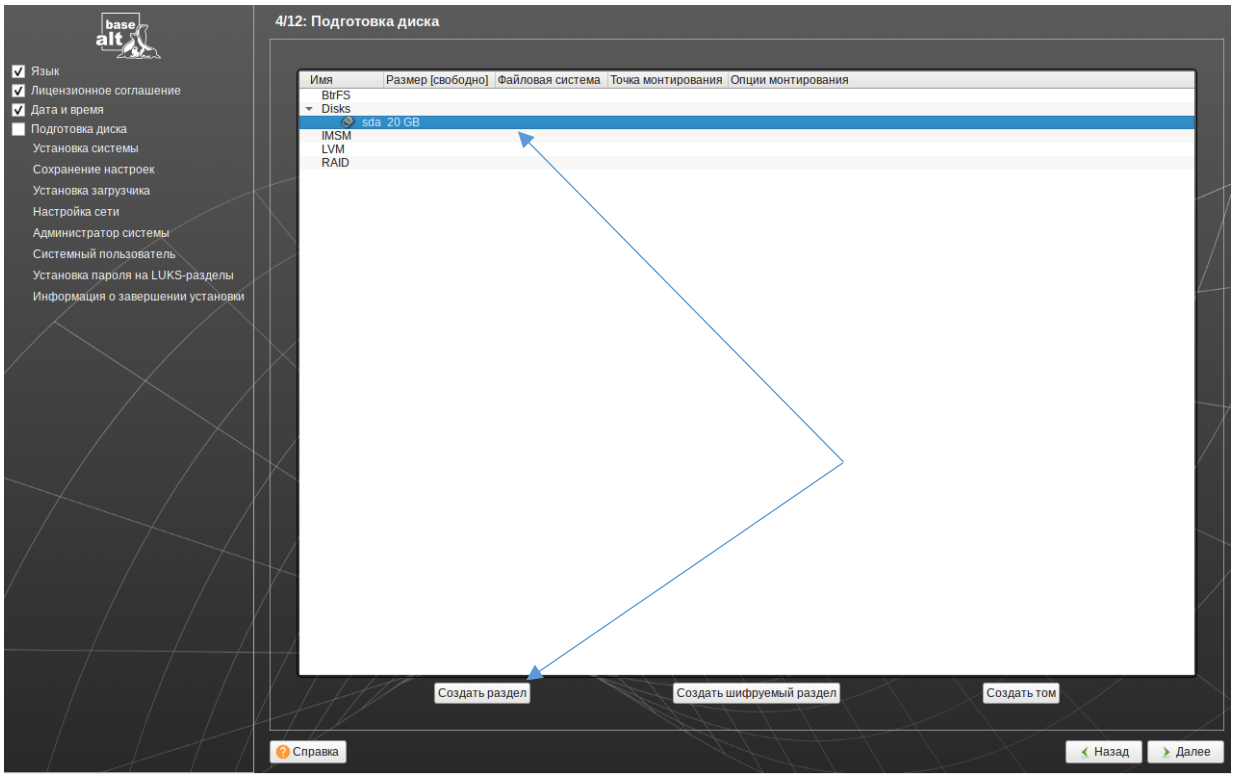

Рис. 1.18. Разметка дискового пространства

Если вы планируете в системе использовать группы томов LVM или программный RAID (mdadm) массив, то именно здесь вы можете подключить к нему диски, задать тип (raid0, raid1, raid5, raid10 и др.), выбрать точки монтирования при необходимости

Этап 8. Создание раздела.

На данном этапе вам следует поставить галочку напротив значения «Показать дополнительные параметры» чтобы перейти в более расширенное меню выбора ФС и в меню выбора точки монтирования раздела, от чего напрямую будет зависеть работа вашего сервера. (рис.1.19), после чего нажать кнопку «ОК»

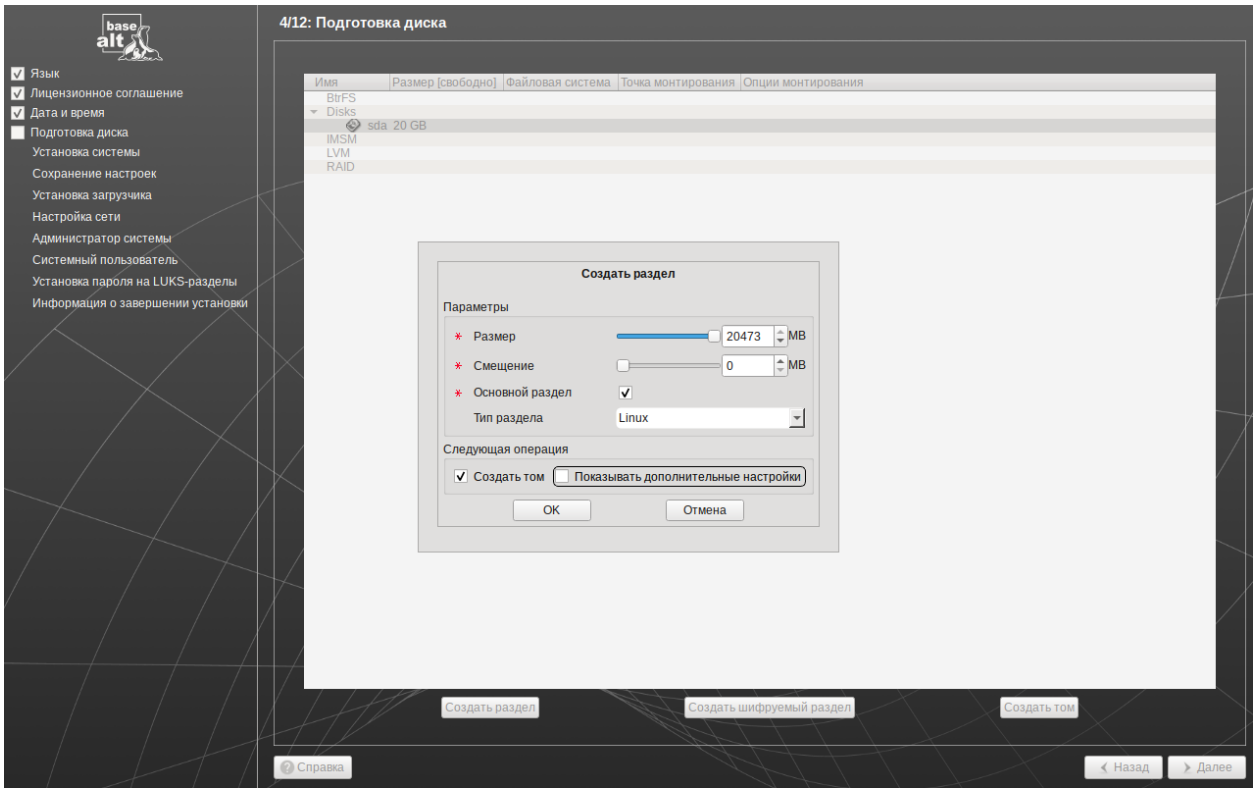

Рис. 1.19. Создание нового раздела

Этап 9. Создание файловой системы. (ФС)

Важный этап уставки любой ОС — выбор файловой системы, и если в windows он ограничен лишь NTFS, то Linux может похвастаться поддержкой различных ФС для установки системы. (рис. 1.20)

Мы рекомендуем выбрать файловую систему Ext4, в том случае, если таковая имеется, в ином случае следует указать Ext3. Разница между ними

заключается в конечном размере хранимого файла, если ext3 может хранить файлы размером до 2х терабайт, то ext4 файлы размером до 1 экзабайта (1 экзабайт = 1 000 000 терабайт).

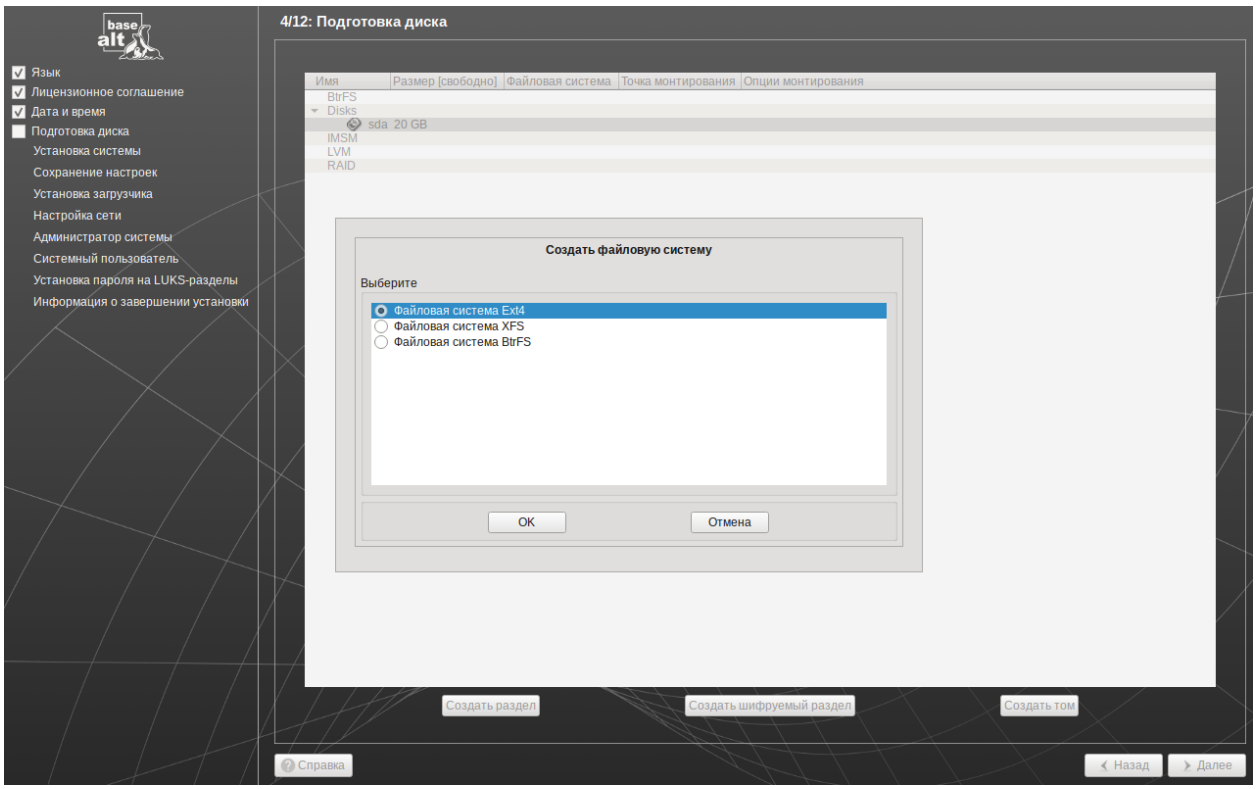

Рис. 1.20. Выбор файловой системы

Примечание 8.

***EXT4** — Четвертая расширенная файловая система, стандартная для многих дистрибутивов Linux. Надежная, стабильная и отлично подходит для большинства повседневных задач (системные разделы, документы, медиафайлы). Хорошо справляется с мелкими файлами.*

***XFS** — Высокопроизводительная 64-битная журналируемая ФС, разработанная Silicon Graphics. Оптимизирована для работы с очень большими файлами и высокой параллельной нагрузкой. Идеальна для серверов баз данных, видеомонтажа и медиасерверов.*

***Btrfs (B-Tree FS)** — Современная ФС, работающая по принципу «копирование при записи» (Copy-on-Write). Включает встроенные функции: создание снапшотов, сжатие на лету, контроль целостности данных (суммы checksum) и управление томами (встроенный LVM).*

Этап 10. Указание точки монтирования раздела.

В этом окне можно оставить все как есть, если вас интересует простая установка в один раздел, в ином случае вам стоит задать несколько дисковых разделов с разными точками монтирования. (рис.1.21)

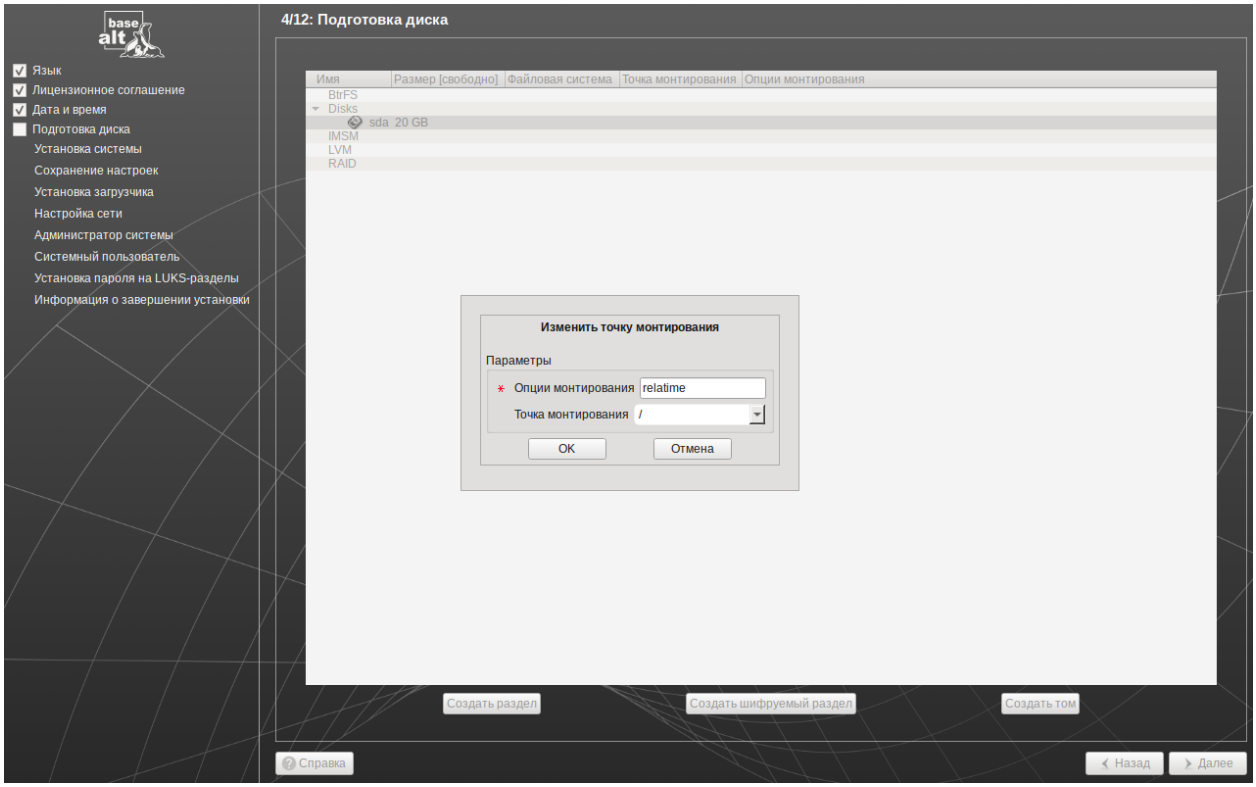

Рис. 1.21. Определение точек монтирования

Примечание 9. Некоторые существующие точки монтирования разделов.

/ (корень) — нужен для размещения системных файлов, программ и библиотек, необходимых для загрузки и работы операционной системы.

/home — нужен для хранения личных файлов пользователей (документы, видео, музыка) и их персональных настроек программ.

/var — нужен для хранения часто изменяющихся данных: системных логов, очередей задач, кэша пакетного менеджера.

/boot — нужен для хранения ядра Linux и файлов загрузчика (GRUB), используемых при старте системы.

/usr — нужен для хранения программ пользователя, библиотек, исходников и документации (обычно включен в корень).

/tmp — нужен для хранения временных файлов, создаваемых программами (часто очищается при перезагрузке).

swap — нужен как виртуальная память для выгрузки данных из ОЗУ при нехватке оперативной памяти или для режима гибернации.

Этап 11. Выбор диска для установки.

После проделывания вышеуказанных действий, вы получите готовый к установке операционной системы жесткий диск с необходимым количеством разделов. (рис.1.22, рис 1.23). Нажимаем кнопку «Далее».

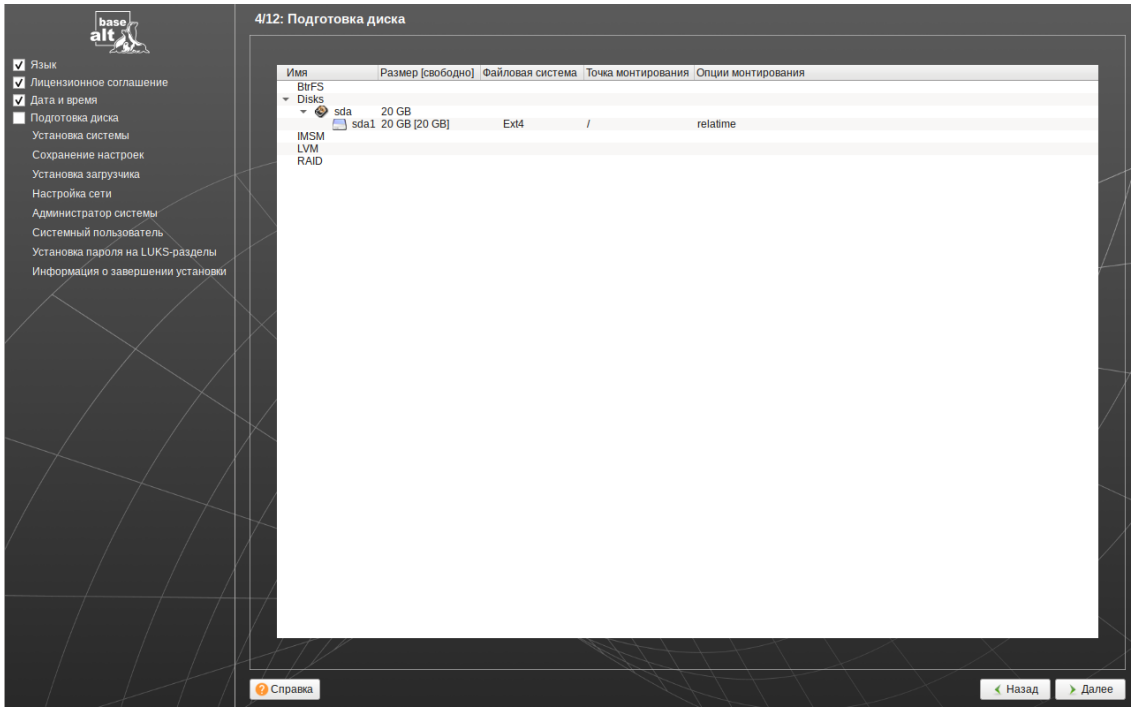

Рис. 1.22. Подготовка диска

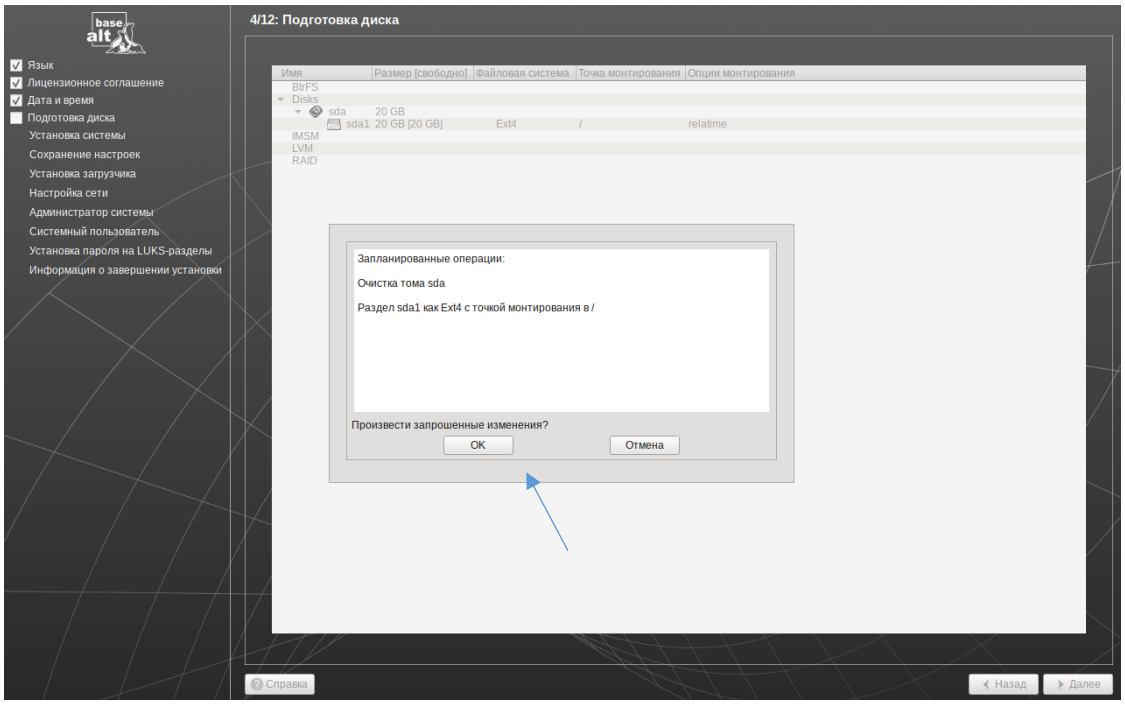

Рис. 1.23. Подтверждение форматирования разделов

Этап 12. Выбор компонентов для установки.

Следующим этапом появляется выбор того, что необходимо установить в довесок к чистой системе, в нашем случае выберем пункты: «поддержка графической подсистемы (Gnome)», «поддержка клиентской инфраструктуры SambaAD», «Поддержка управления через web-интерфейс». (рис. 1.24)

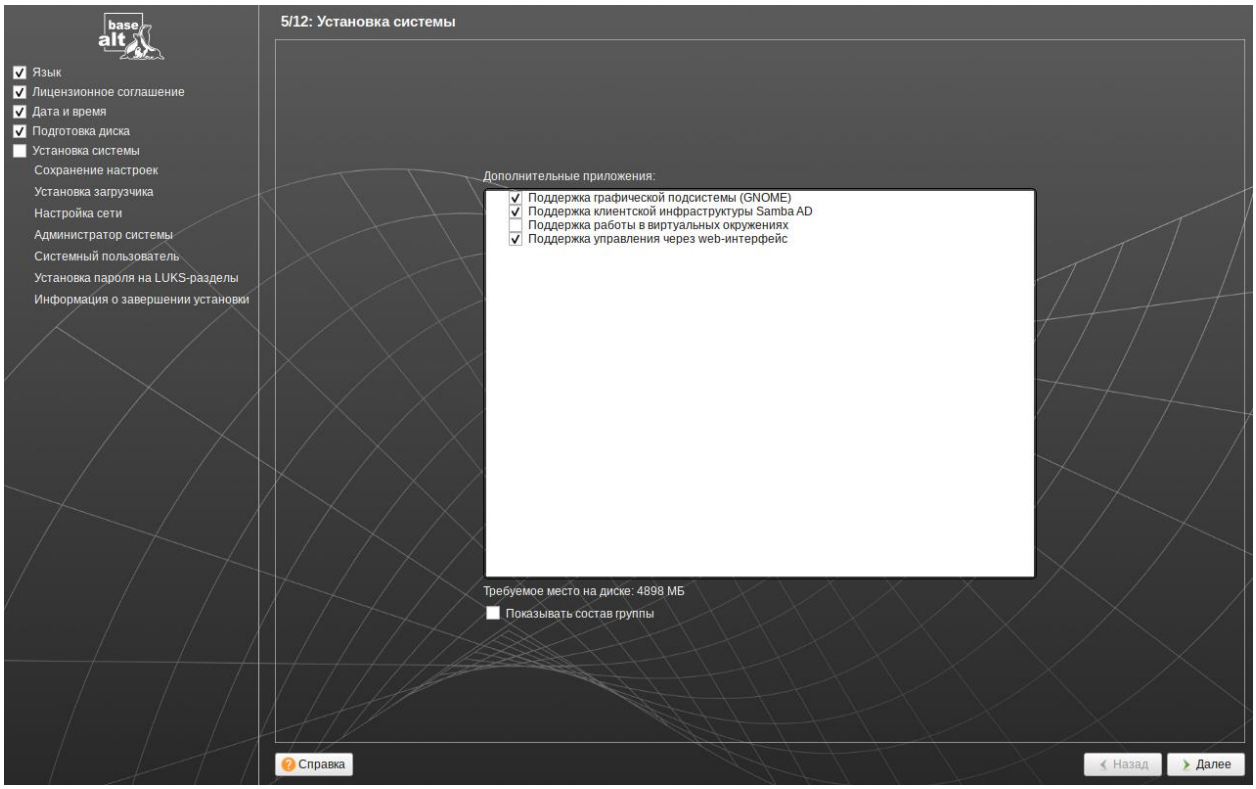

Рис. 1.24. Выбор компонентов для установки

Примечание 10.

SambaAD (Samba Active Directory) — это реализация контроллера домена Active Directory для Linux-систем на основе программного пакета Samba . Позволяет серверу Linux выполнять аутентификацию пользователей, управлять доступом к ресурсам и применять групповые политики так же, как это делает Windows Server.

Alterator — это фреймворк для создания графических интерфейсов настройки системы, используемый по умолчанию в дистрибутиве ALT Linux. Представляет собой набор модулей (виджетов) для настройки различных параметров: сетевых подключений, пользователей, служб, оборудования. Позволяет управлять системой через веб-интерфейс (удаленно) или локально.

GNOME — это свободная и популярная среда рабочего стола для Unix-подобных операционных систем. Отличается простотой, дружелюбным интерфейсом и строгим следованием стандартам юзабилити, что делает её

удобной для мигрантов с Windows. Включает набор базовых приложений: файловый менеджер (Nautilus), браузер, офисные.

После остается только нажать кнопку «Далее», начнется процесс установки базовой linux системы, который может занять от 1 до 5 минут (скорость установки зависит от мощности вашего компьютера). (рис. 1.25)

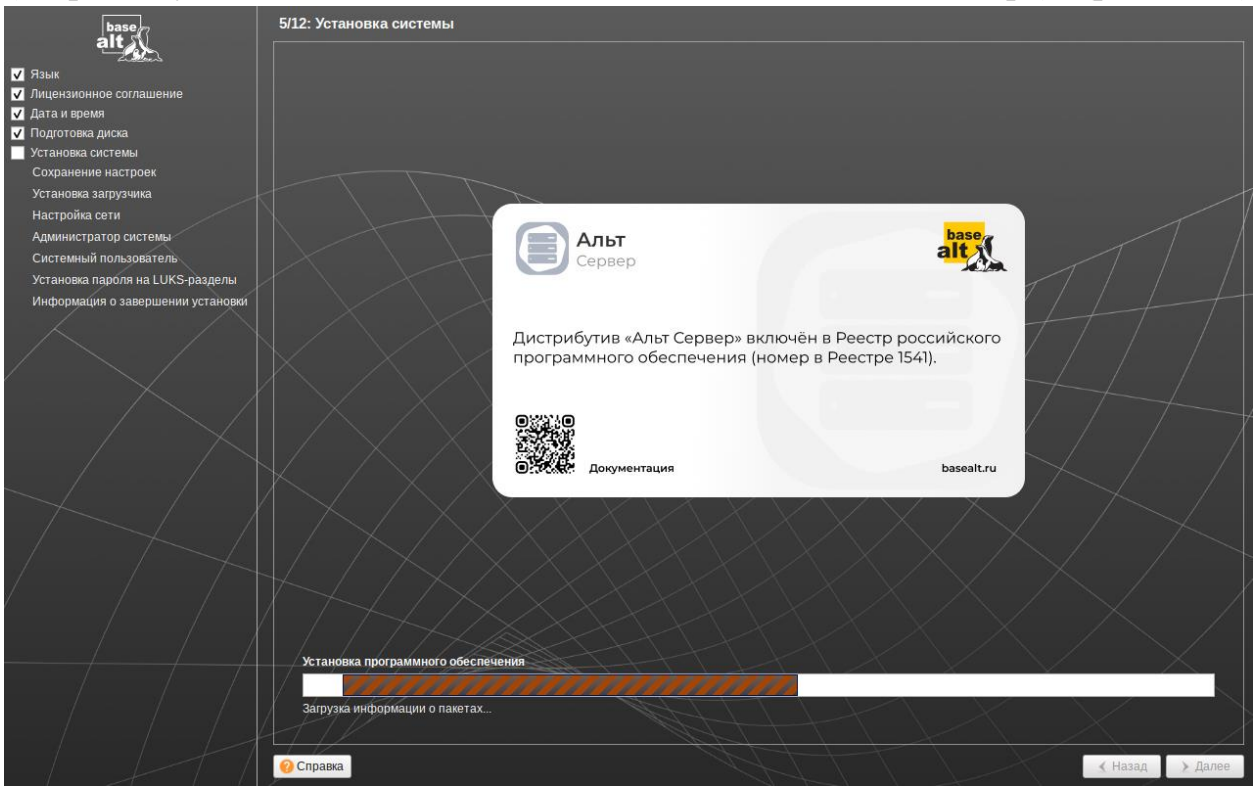

Рис. 1.25. Установка системы

Этап 13. Установка системного загрузчика.

После установки системы, программа установки предложит вам выбрать диск, на который будет установлен системный загрузчик grub (open source), вам следует выбрать ваш диск с системой, после чего продолжить установку. (рис.1.26)

Примечание 11:

GRUB (Grand Unified Bootloader) — это программа-загрузчик, которая запускается сразу после включения компьютера и позволяет выбрать операционную систему или ядро Linux для загрузки.

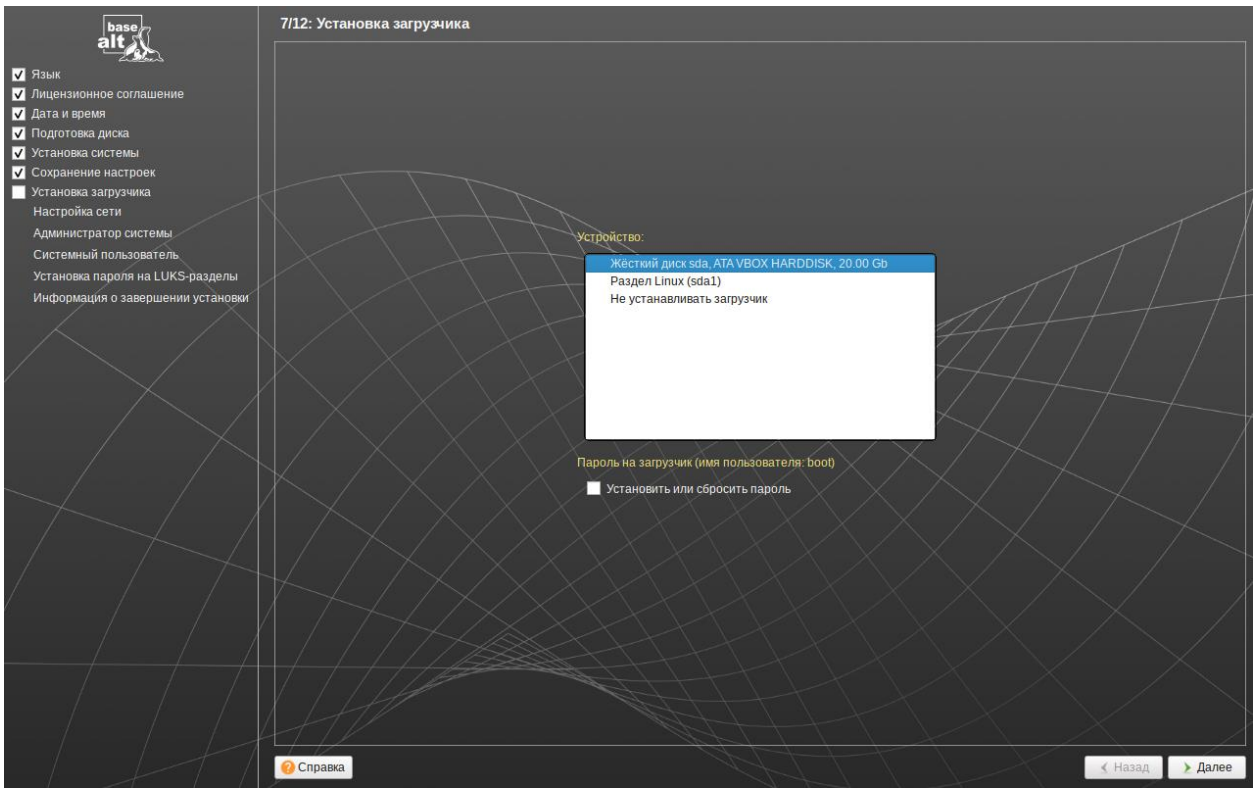

Рис. 1.26. Установка загрузчика системы

Этап 14. Смена имени компьютера и настройка сети.

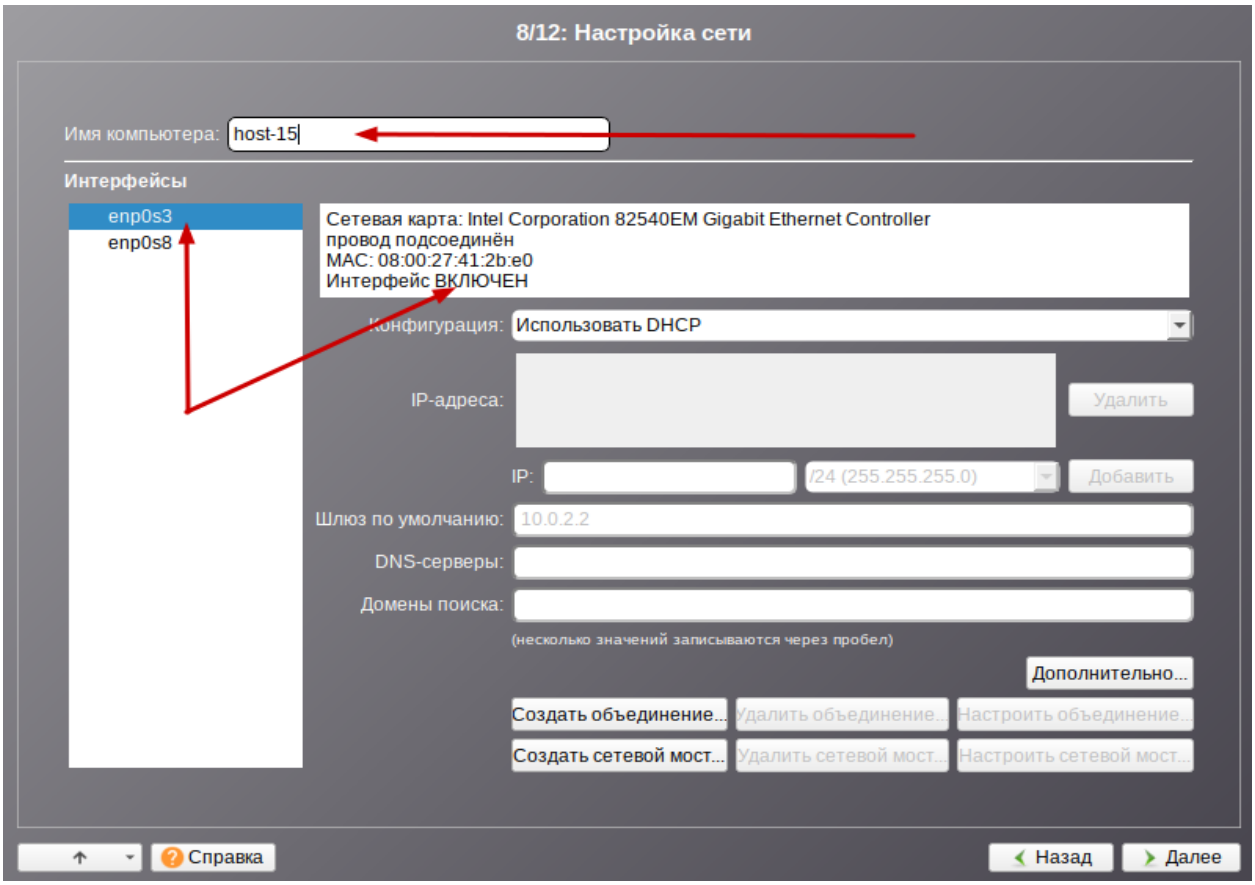

Рис. 1.27. Настройка имени хоста и сетевых настроек

Чтобы изменить имя вашего компьютера введите его в окне «Имя компьютера» вместо имени «host-15». Имя компьютера важно задать понятное для вас, помните, вам администрировать этот сервер и искать его в вашей локальной сети.

Следующим этапом становится настройка сети вашего сервера. Данную настройку лучше всего производить в уже установленной системе по средствам терминальных команд или специального программного интерфейса «alterator», поэтому: убеждаемся, что статус интерфейса enp0s3 ВКЛЮЧЕН, а статус интерфейса enp0s8 ВЫКЛЮЧЕН (рис.1.27).

Примечание 12: имена интерфейсов enp0s3 и enp0s8 могут отличаться в вашей установке, будьте с этим внимательнее!

Этап 15. Системный администратор и пользователи.

На данном этапе вам предстоит задать пароль суперпользователя системы он же пользователь с именем «root», а также имя и пароль вашего пользователя, задайте эти параметры. (рис.1.28, рис.1.29)

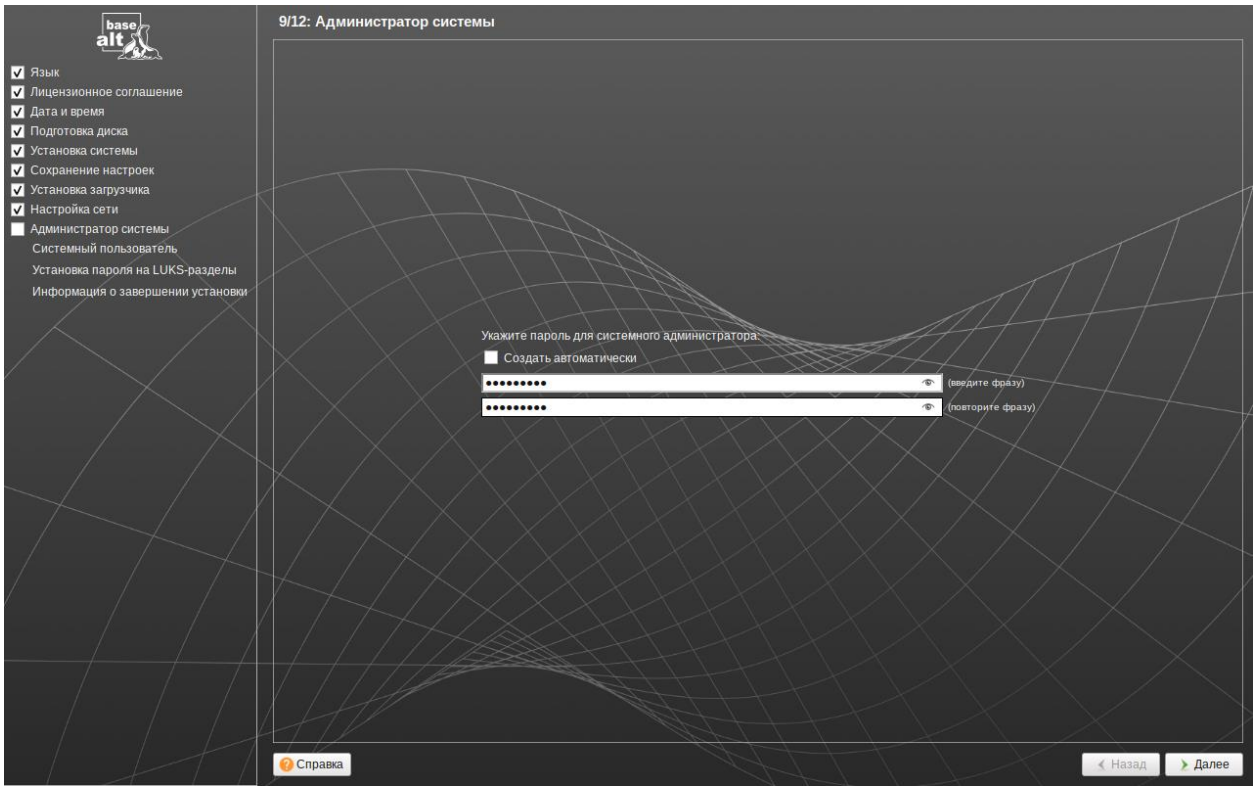

Рис. 1.28. Пароль суперпользователя

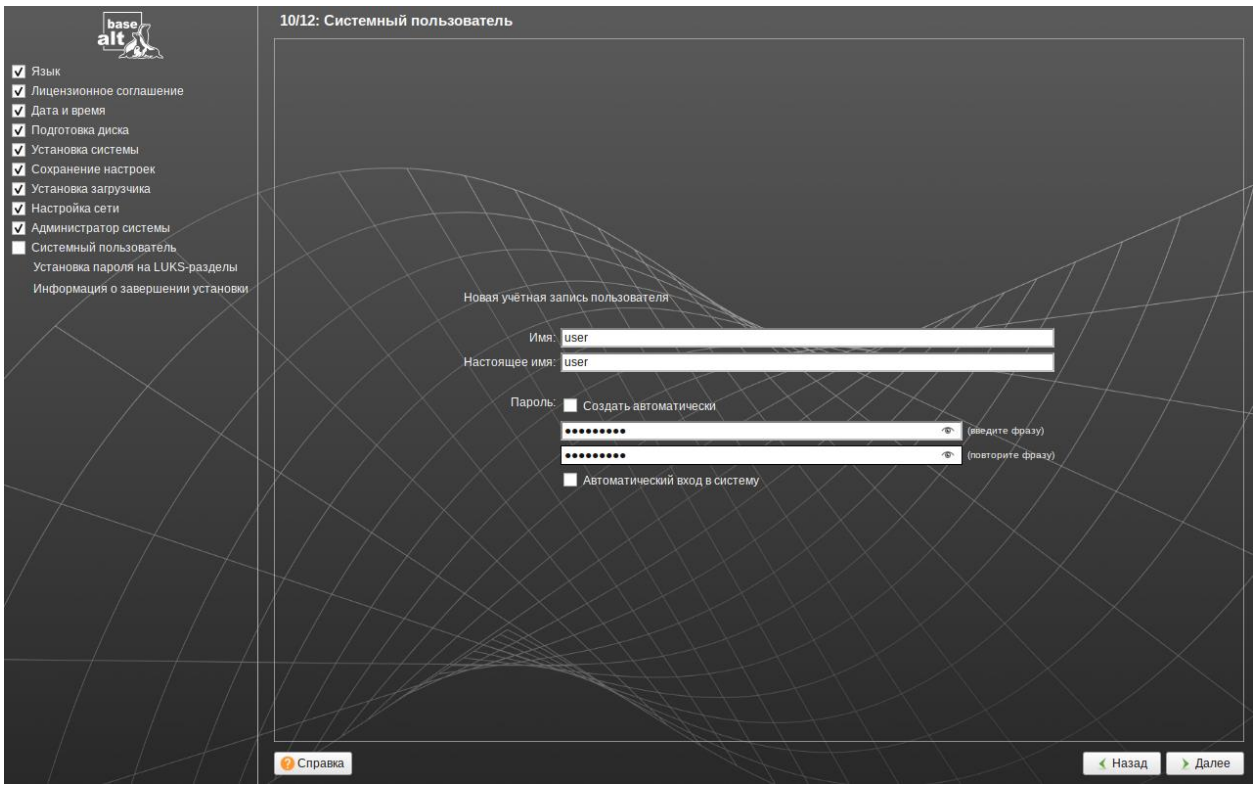

Рис. 1.29. Создание нового пользователя

Примечание 13.

root *— суперпользователь с неограниченными правами (UID 0);* ***обычный пользователь*** *— создается для повседневной работы, имеет ограниченные права и свою домашнюю папку; системные пользователи — создаются программами и службами для выполнения своих задач, не имеют пароля и домашней папки (UID обычно от 1 до 999).*

Этап 16. Завершение установки.

На этом установка системы будет завершена. После проделанных вами манипуляций система будет установлена, о чем сообщит соответствующее окно (рис.1.30), после нажатия на кнопку «Завершить» система будет перезагружена автоматически.

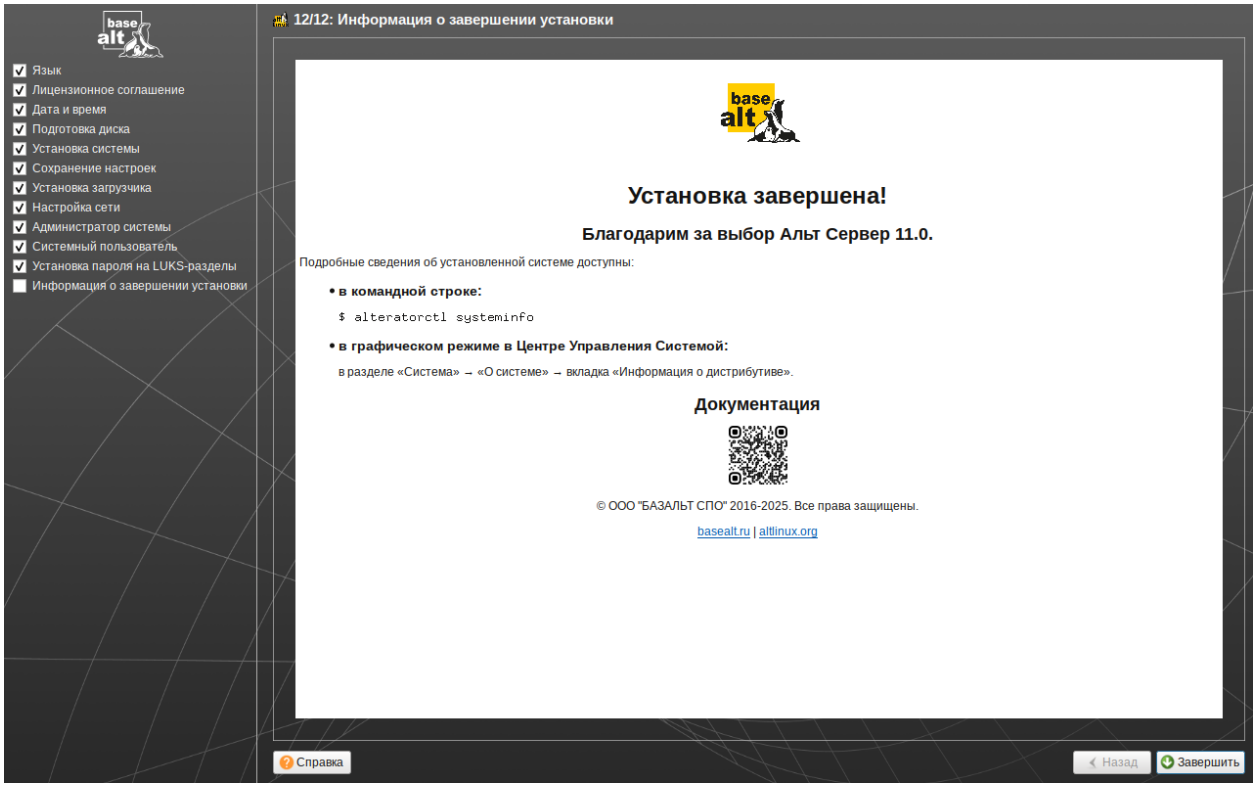

Рис. 1.30. Завершение установки

Некоторые выводы из Раздела 1. «Установка сервера»

Выбор и подготовка серверной платформы: В качестве серверной операционной системы был выбран дистрибутив Alt Linux 11 (серверный профиль), ориентированный на стабильную работу и обеспечение корпоративных сервисов. Для развертывания использована среда виртуализации VirtualBox, что позволило создать изолированную тестовую инфраструктуру без необходимости выделения физического оборудования.

1.1 Создание виртуальной машины: В VirtualBox выполнено создание новой виртуальной машины с оптимальными параметрами для серверной конфигурации: выделено достаточное количество оперативной памяти, создан динамический виртуальный диск, настроен сетевой адаптер в режиме "Сетевой мост" для обеспечения доступа виртуального сервера к локальной сети.

1.2 Предварительная настройка виртуальной машины: Второй сетевой адаптер виртуальной машины настроен для работы во внутренней сети intnet. Данный интерфейс будет использоваться для связи сервера с клиентскими машинами в изолированной среде, в то время как первый адаптер обеспечивает выход в локальную сеть (через NAT) для доступа в интернет и управления сервером.

1.3 Установка операционной системы: Произведена установка Alt Linux 11 с серверным профилем. Выбраны минимальные наборы пакетов, необходимые для дальнейшего развертывания сетевых служб, что позволило получить чистую и оптимизированную систему без лишних компонентов.

Раздел 2. Администрирование сервера.

Данный раздел посвящен практическим аспектам настройки и управления сетевыми службами в операционной системе ALT Linux. В нем рассматриваются базовые и продвинутые методы конфигурации серверных компонентов, необходимых для построения корпоративной инфраструктуры.

Раздел охватывает полный цикл создания сетевой среды: от базовой настройки сетевых интерфейсов до развертывания служб каталогов, файлового обмена и контроля доступа к интернет-ресурсам. Каждый пункт представляет собой отдельную задачу системного администратора с описанием принципов работы соответствующего сервиса, его места в инфраструктуре и практической реализации на Linux-серверах.

Материал построен по принципу "от простого к сложному": начиная с обеспечения сетевой связности (статическая адресация, DHCP) и заканчивая централизованным управлением пользователями и ресурсами (контроллер домена, DNS, файловый сервер) и управлением интернет-трафиком (прокси-сервер).

В данном разделе рассмотрим следующие пункты:

1. Настройка сети (статическая адресация);
2. Настройка dhcp сервера (isc-dhcp-server);
3. Настройка контроллера домена (samba-dc);
4. Настройка ДНС сервера (samba-ns);
5. Настройка файлового сервера (samba);
6. Настройка прокси сервера (squid).

2.1. Настройка сети (статическая адресация)

Так как наша задача настроить сервер, а сервер – это нечто иное, как устройство, доступное по одному и тому же «статическому» ip адресу в любой момент времени. Отсюда вытекает задача настроить статический ip адрес на установленном сервере. Мы предлагаем вам использовать один из удобных вам вариантов:

Вариант 1. Использование программного комплекса «Alterator».

Если вы выбрали данный способ настройки, то старайтесь придерживаться инструкции ниже:

Для того, что попасть в центр управления системой, именуемый как «Alterator», нужно открыть его из меню «Пуск» или щелкнуть на иконку на панели быстрого доступа (рис. 2.1[1]) внизу экрана (рис. 2.1).

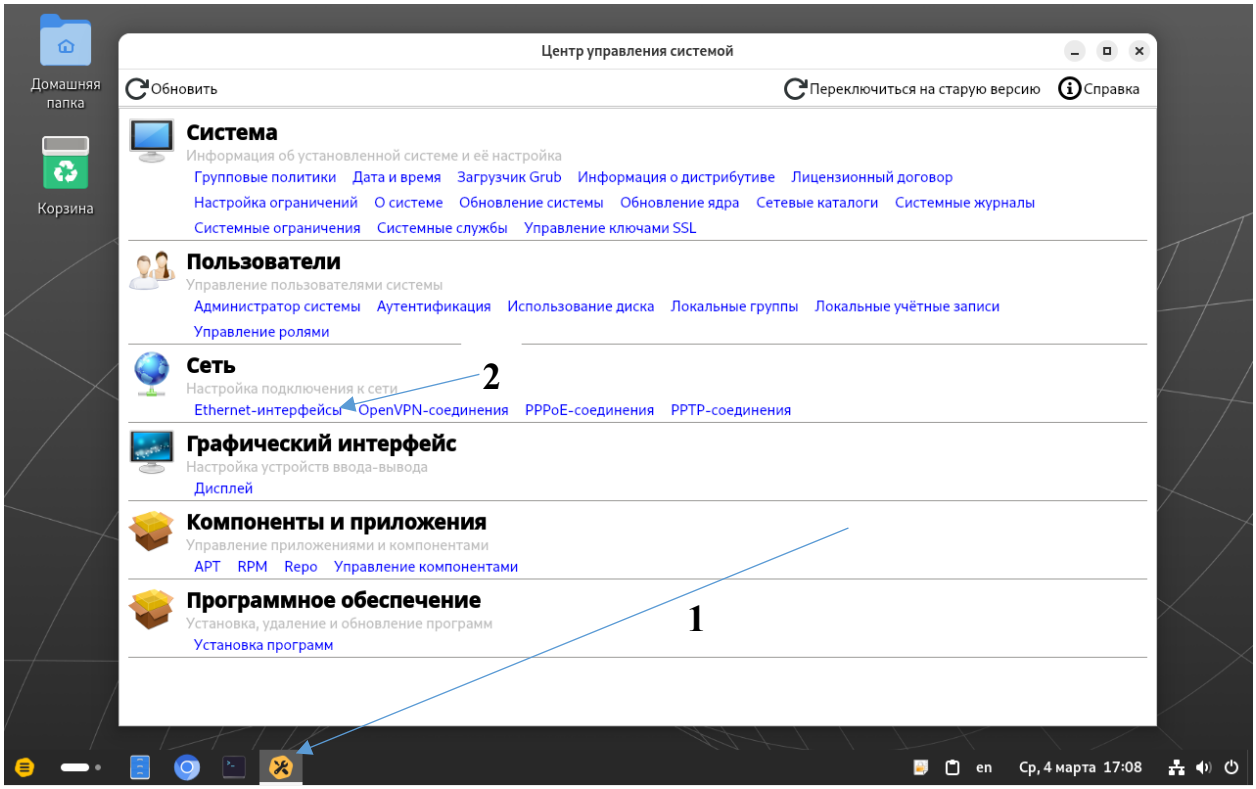

Рис. 2.1. Центр управления системой

Затем следует выбрать пункт «Ethernet-интерфейсы» (рис. 2.1[2]) и ввести запрошенный пароль администратора системы рис 2.2.

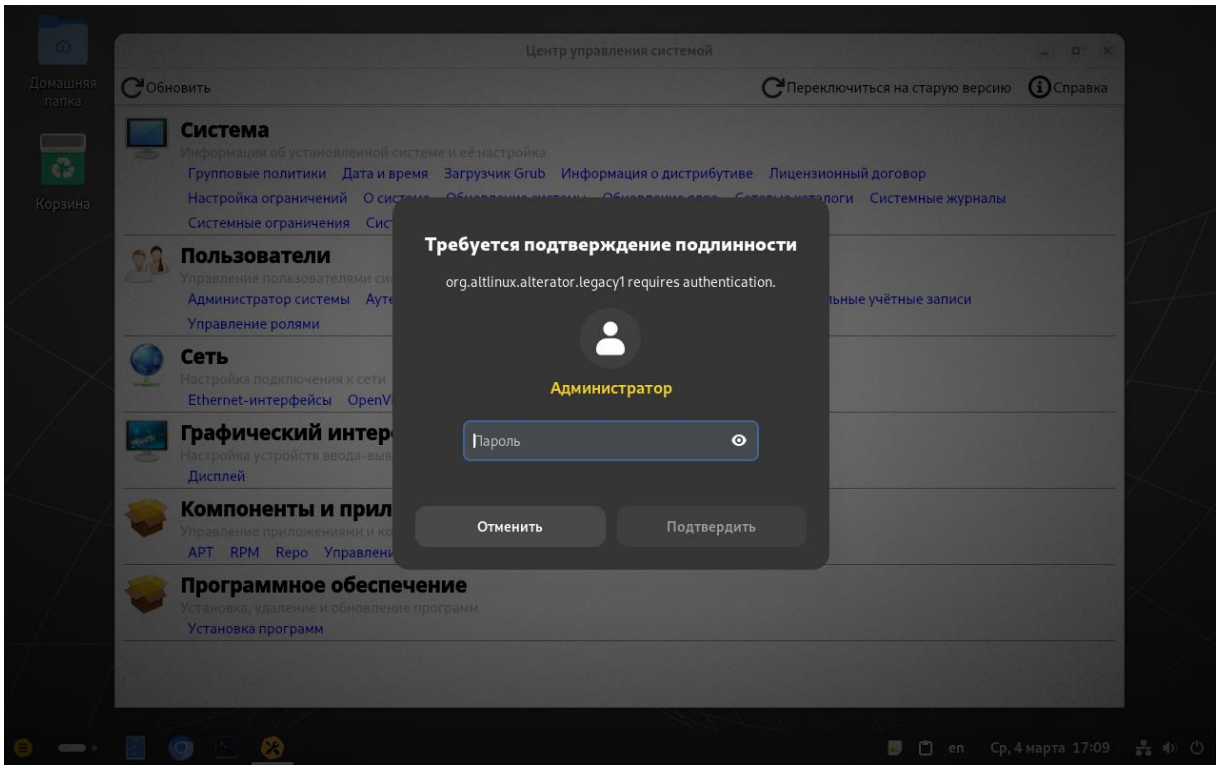

Рис. 2.2. Проверка подлинности

После подтверждения подлинности запроса перед вами откроется окно ЦУС *«Alterator»* в режиме «Ethernet-интерфейсы» рис. 2.3.

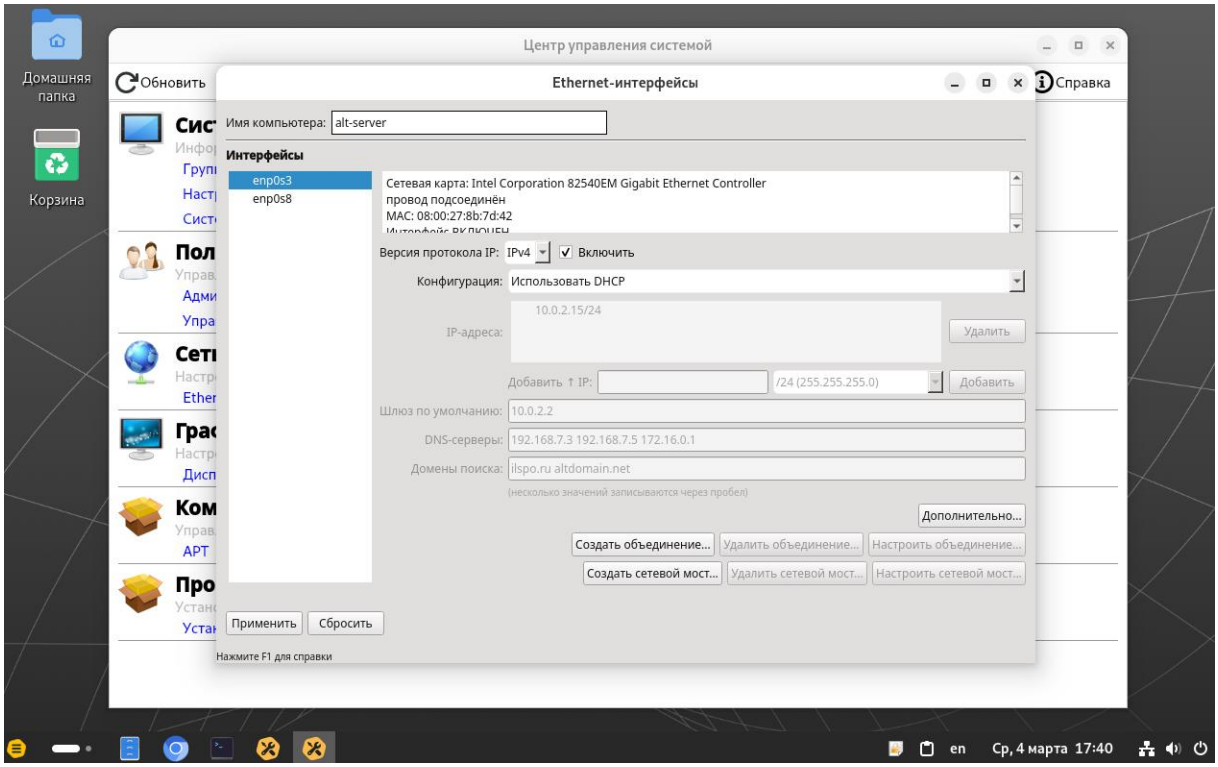

Рис. 2.3. Настройка сетевых интерфейсов

Переключаемся на интерфейс enp0s8 (это тот интерфейс, который в гипервизоре настроен в режиме «Внутренняя сеть»). Рис. 2.4 и нажимаем на кнопку «Дополнительно» (рис. 2.4[1]) для того, чтобы «перехватить» управление интерфейсом в ЦУС, после этого передаем его управление в подсистему «NetworkManager (etcnet)» (рис. 2.4[2]) и сохраняем действие нажав на копку ОК (рис. 2.4[3]).

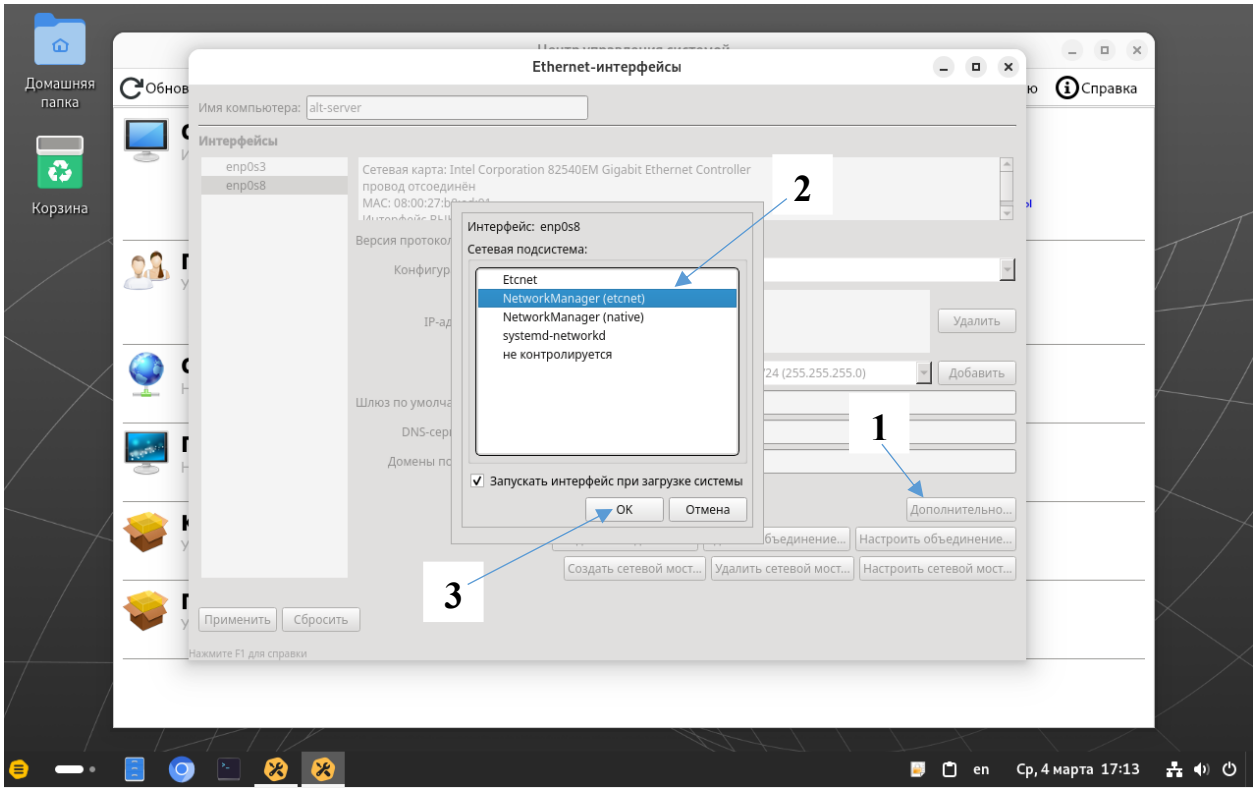

Рис. 2.4. Выбор типа подсистемы сетевого интерфейса

Примечание 14:

NetworkManager — это служба для автоматического управления сетевыми подключениями в Linux, которая упрощает переключение между разными сетями (Wi-Fi, Ethernet, VPN) и позволяет настраивать соединения через графический интерфейс, консольные команды (nmcli) или псевдографический интерфейс (nmtui).

После проделанных переключений у нас появится возможность управлять интересующим нас сетевым интерфейсом, для того чтобы присвоить ему статический ip адрес (рис. 2.5).

Примечание 15:

В нашем примере будет использоваться подсеть 172.16.0.0/27, в которой сервер ALT Linux будет выступать в роли маршрутизатора и займет адрес 172.16.0.1/27.

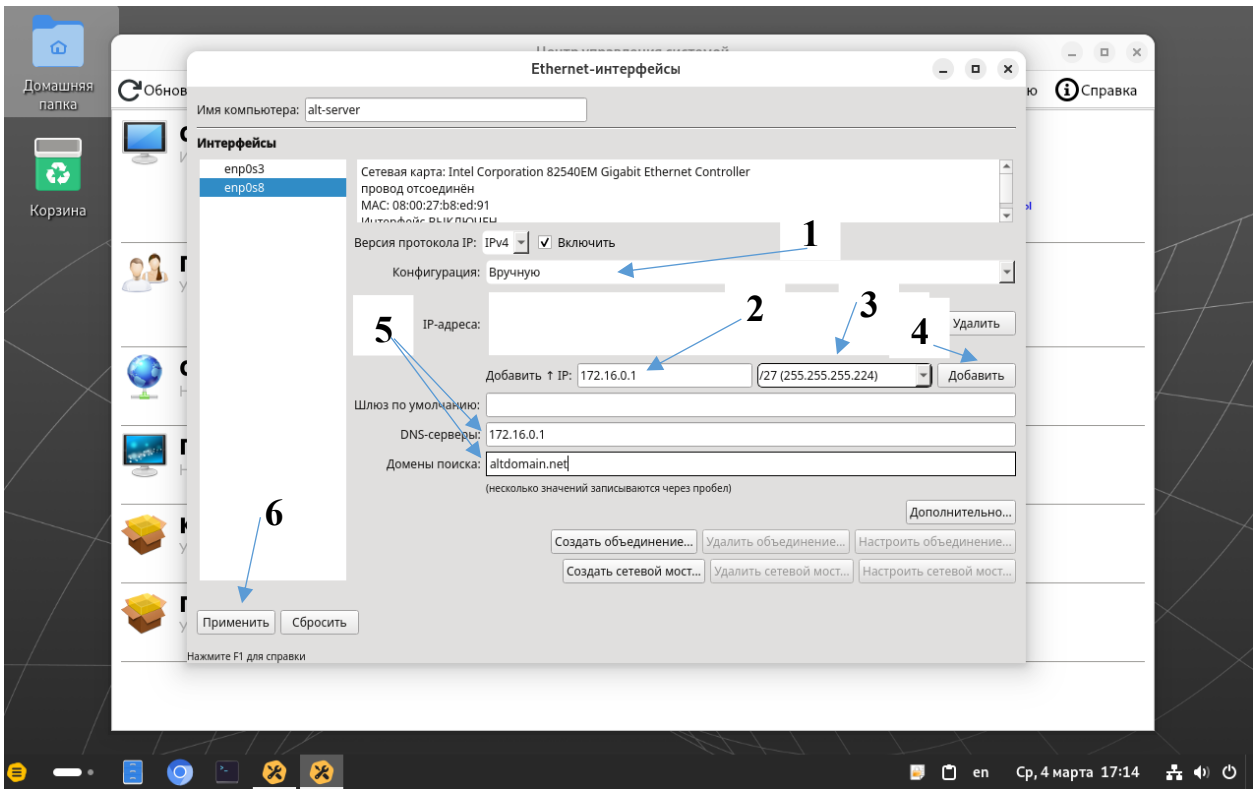

Рис. 2.5. Назначение ip адреса хосту

Рис. 2.5 [1] – Указываем метод присвоения ip адреса на интерфейс. В нашем случае – Вручную.

Рис. 2.5 [2] – Указываем новый статический сетевой адрес сервера.

Рис. 2.5 [3] – Указываем маску сети в которой будет располагаться сервер. *В нашем случае это 27-и битная маска сети, способная выдержать 32 адреса.*

Рис. 2.5 [4] – Нажимаем клавишу «Добавить» чтобы зафиксировать ip адрес (рис. 2.6 в разделе «IP Адреса»).

Рис. 2.5 [5] – Указываем ДНС сервера (можно один или несколько через запятую) и домены поиска (мы укажем не существующий в нашей сети домен altdomain.net)

Рис. 2.5 [6] – После того, как все данные введены, можно применить настройки сети. То, как должна выглядеть конечная настройка интерфейса показано на рис. 2.6.

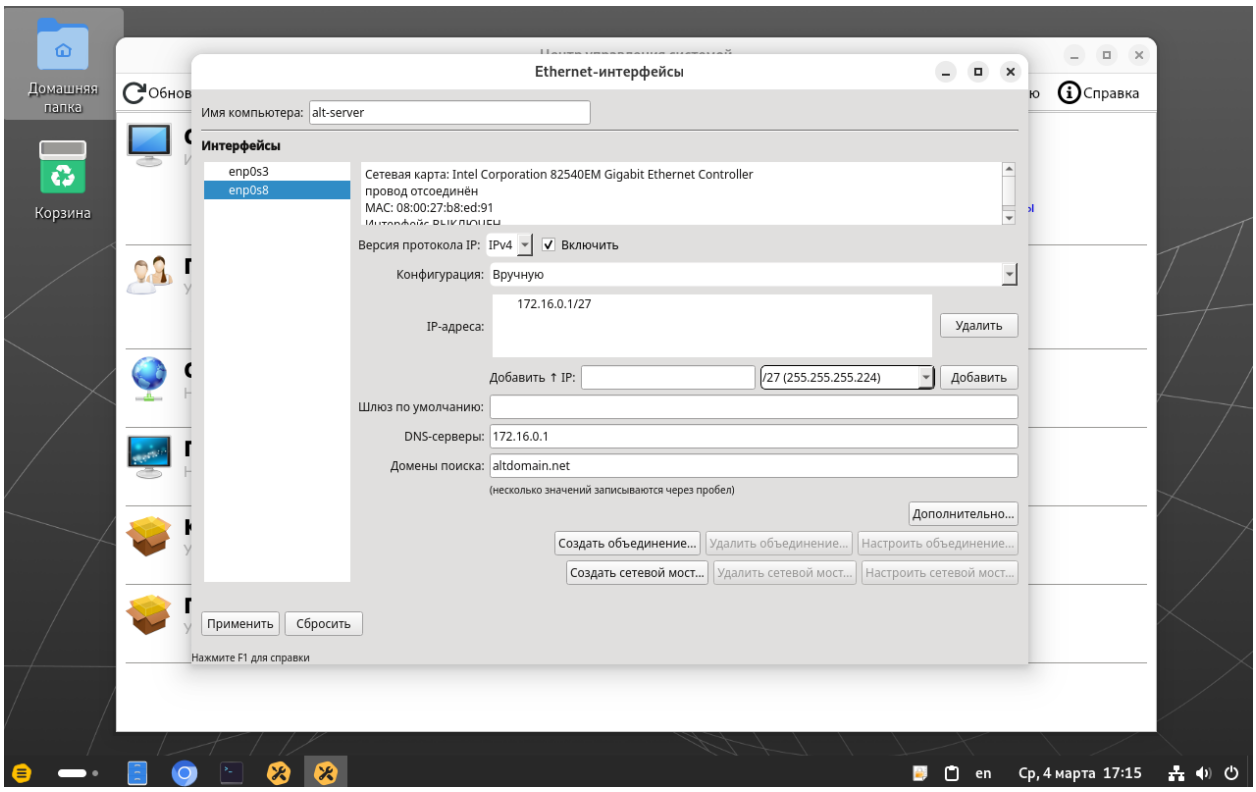

Рис. 2.6. Настроенный интерфейс внутренней сети

На данном этапе настройка сети по варианту 1 завершена, для того чтобы изменения вступили в силу необходимо перезагрузить систему, после чего настройка интерфейсов будут применены.

*Примечание 16. Система Linux является модульной и достаточно гибкой системой и при должном уровне знаний в области linux можно вспомнить метод перезагрузки отдельных модулей ядра или отдельных сервисов. Последний мы используем для ручной перезагрузки сети без необходимости выполнять перезагрузку все операционной системы. Вариант 2 исключает необходимость перезагрузки, т.к. настройка проходит напрямую через сервис NetworkManager и не нуждается в лишних действиях. Команда перезагрузки сервиса в ручном режиме (использовать от имени root или с помощью sudo)**: «systemctl restart NetworkManager».** (рис. 2.7)*

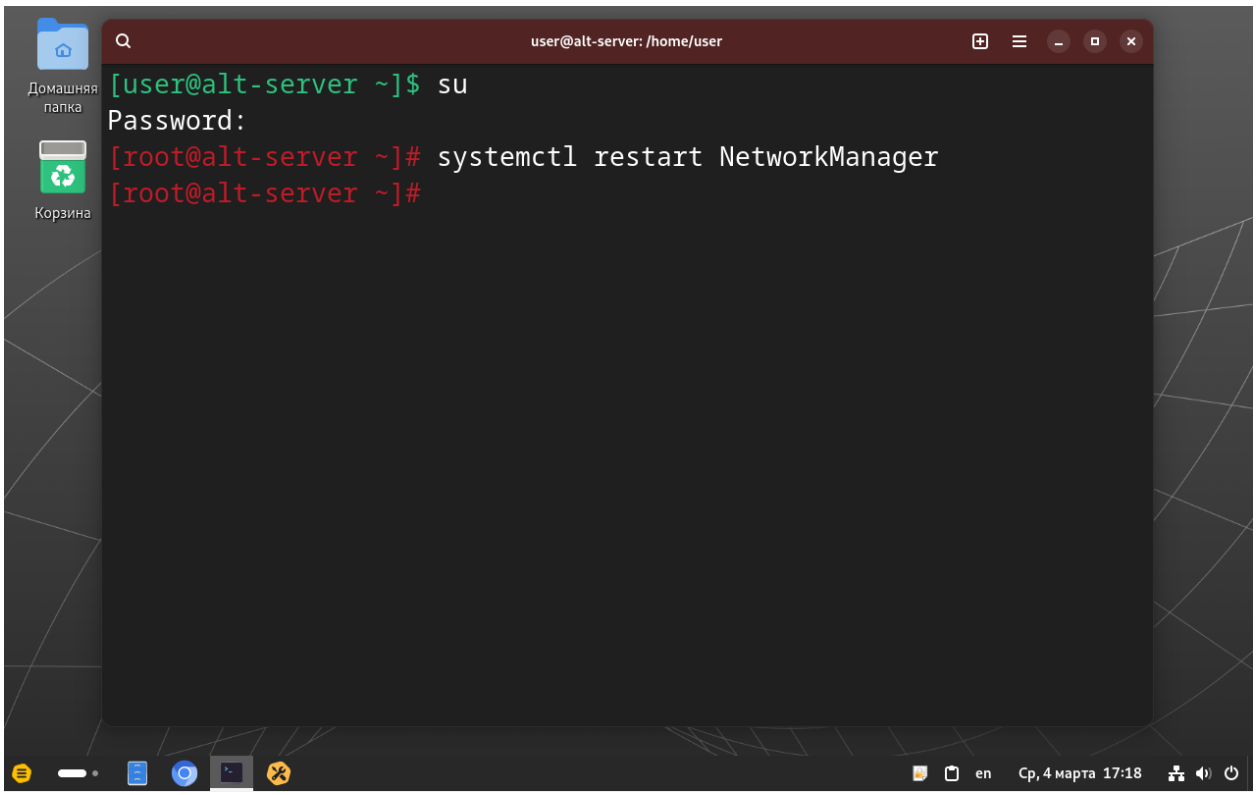

Рис. 2.7. Перезагрузка NetworkManager с использованием терминала

Проверить применились ли настройки можно из терминала с помощью команды «**ip a**», наличие прав суперпользователя не обязательно. (рис. 2.8)

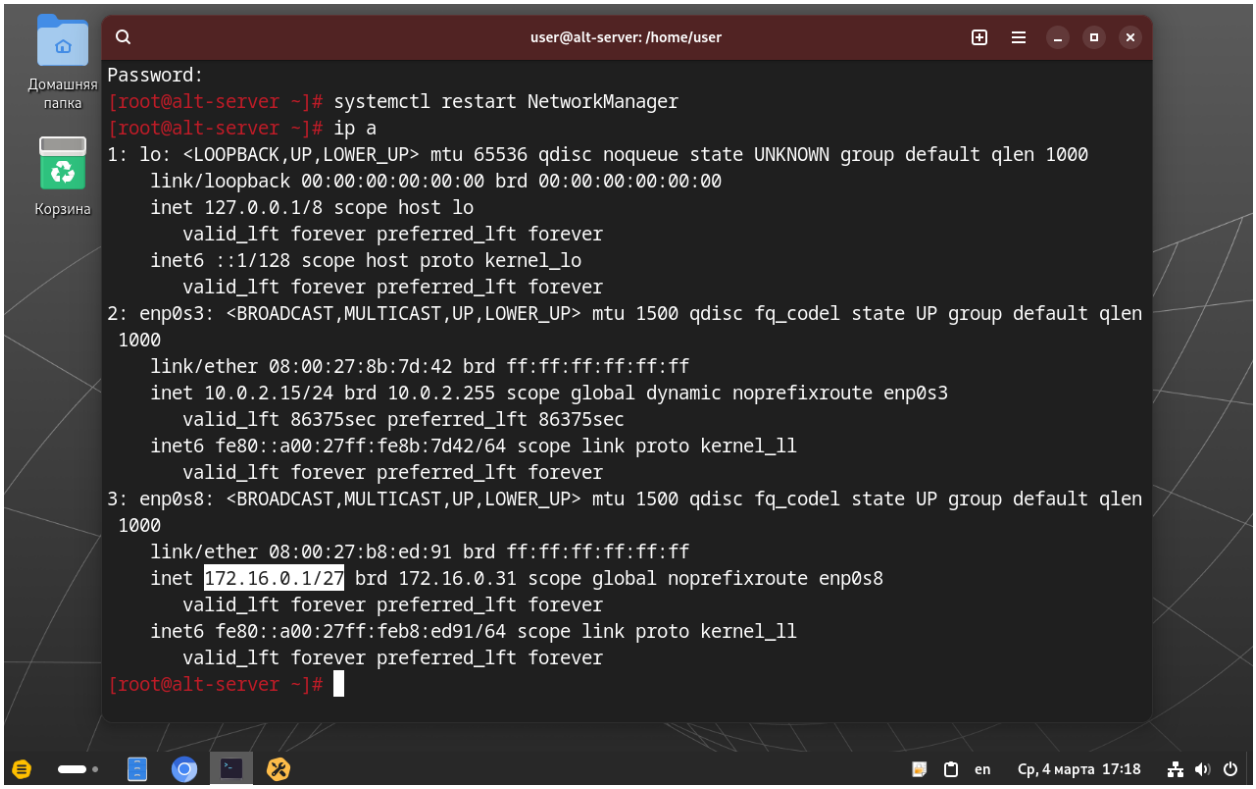

Рис 2.8. Проверка корректности настроек

Из рисунка 2.8 мы видим, что выполненные нами ранее настройки успешно применились и можно перейти к следующему этапу настройки 2.2.

Вариант 2. Использование командного интерфейса «nmcli».

Данные вариант настройки статических адресов системы linux будет напрямую взаимодействовать с терминальной оболочкой (tui) системы, этот способ позволяет применить настройки сети «на ходу», т.е. без необходимости перезапуска системы, все изменения будут применятся перезагрузкой сервиса NetworkManager.

Итак для начала откроем терминал, переключимся на суперпользователя командой **«su»**, и введем следующую команду: **«nano /etc/net/ifaces/enp0s8/optionos»**, где nano – бесплатный текстовый редактор для командной строки (рис. 2.9). О том как использовать данный текстовый редактор описано в *Примечании 16.*

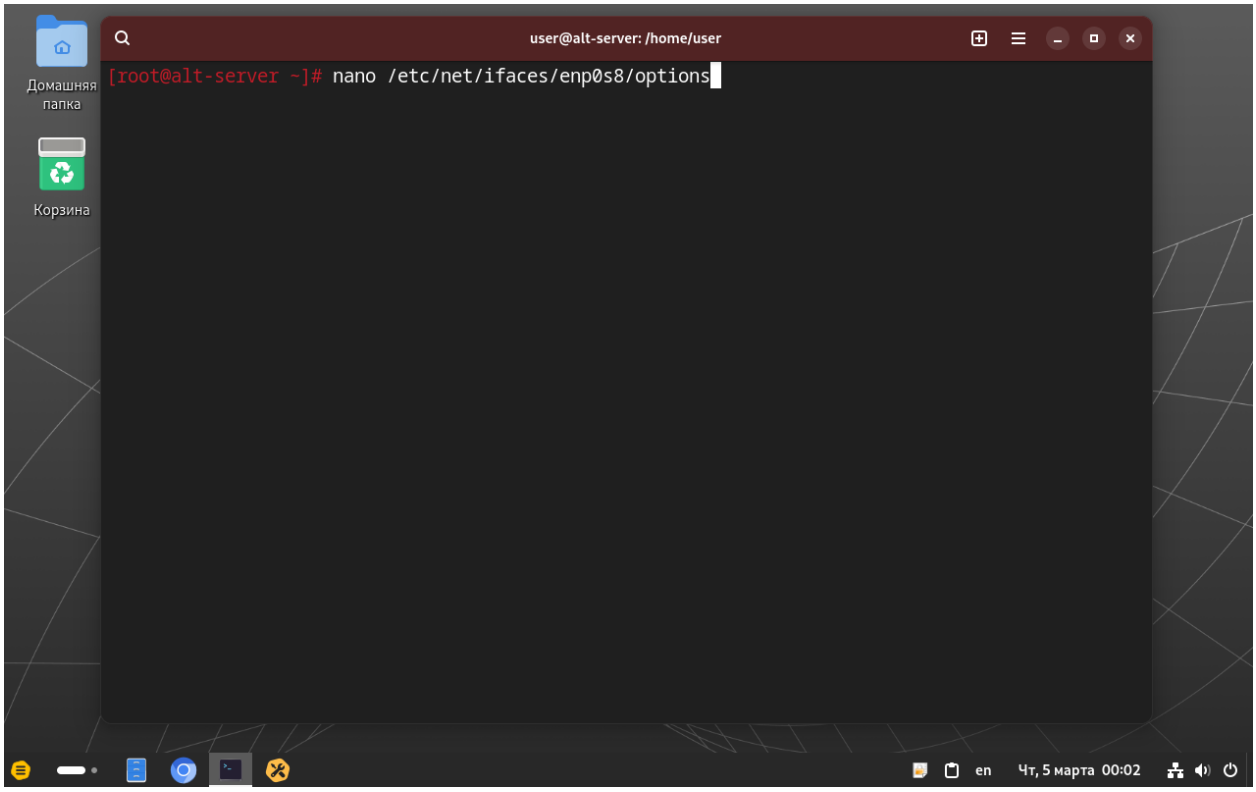

Рис. 2.9. Использование текстового редактора nano

После чего нажимаем на клавиатуре клавишу «Enter» и перед вами откроется окно текстового редактора с содержимым файла, который располагается по пути /etc/net/ifaces/enp0s8/optionos (рис. 2.10)

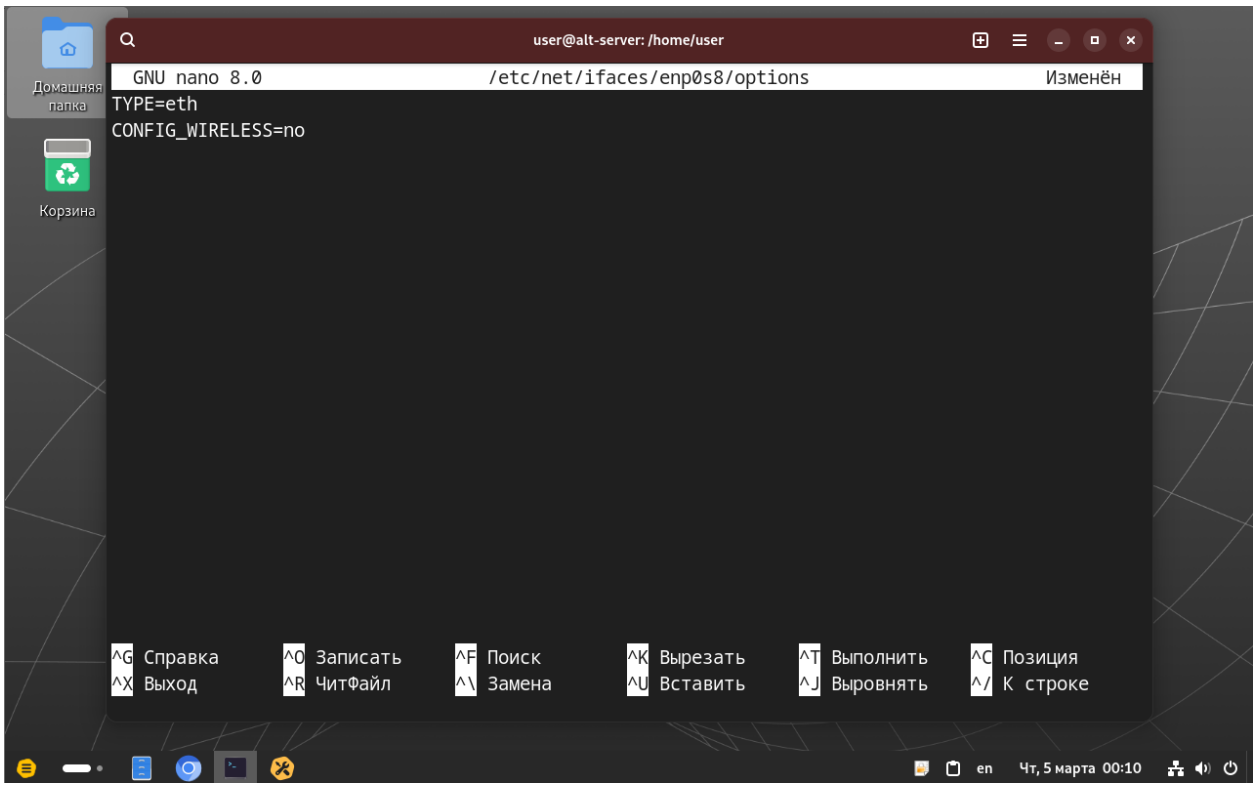

Рис. 2.10. Конфигурационный файл сетевого интерфейса до редактирования

Приведем данный файл к следующему виду рис. 2.11.

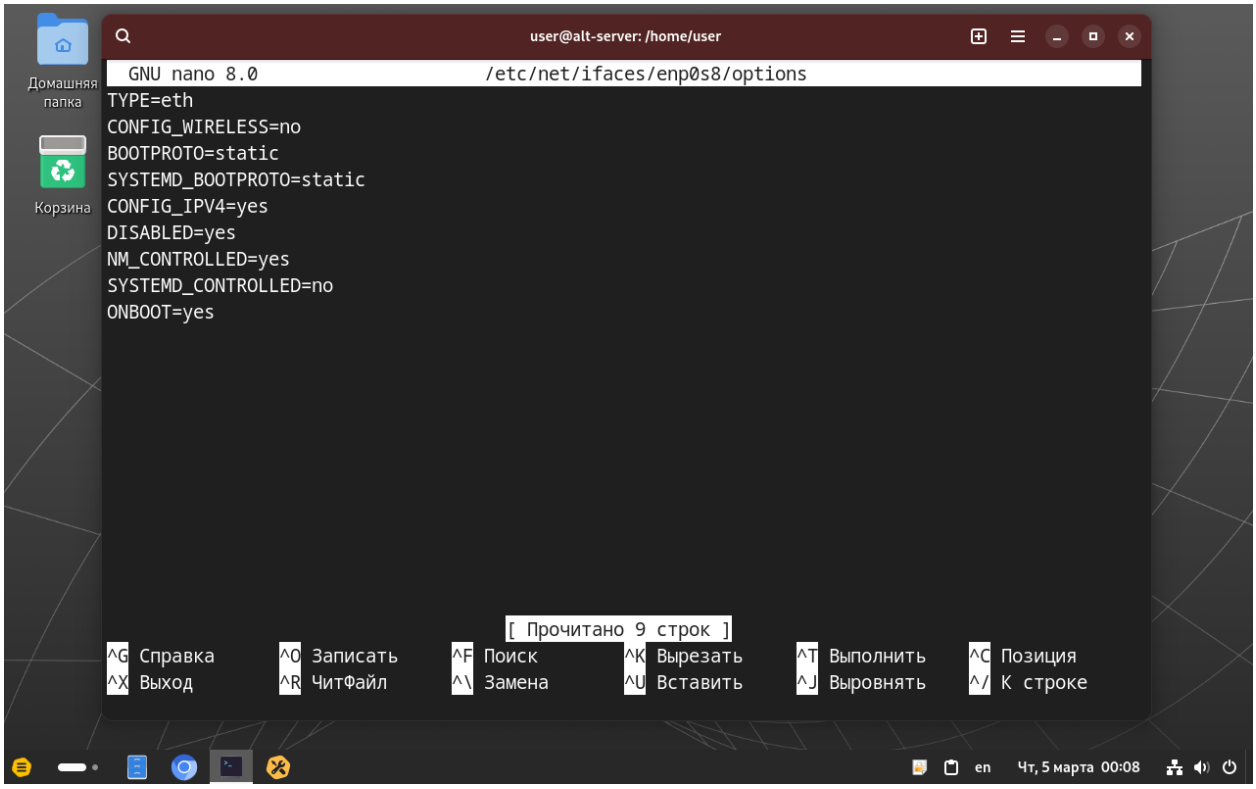

Рис. 2.11. Конфигурационный файл сетевого интерфейса после редактирования

Этот набор указателей задет протокол настройки сети на интерфейсе enp0s8 на статический, отключает Wi-Fi, т.к. его там и нет, отключает использование ipv6, поднимает настройки на интерфейс при включении системы, т.е. после перезагрузки сервера настройки не изменятся.

Примечание 17. Текстовый редактор nano имеет интуитивно понятный терминальный интерфейс и поддерживает большое количество различных «шорт-катов» (сочетаний клавиш для быстрых команд), так например для вырезки строки следует использовать сочетание клавиш Ctrl+K, а для вставки обратно Ctrl+U, для сохранения или применения изменений файла комбинация клавиш Ctrl+S или Ctrl+O, для действия «сохранить и выйти» Ctrl+X, для поиска Ctrl+W, для отмены случайного действия Ctrl+C.

После того, как мы передали управление интерфейсом в подсистему NetworkManager, можно приступить к присвоению статического ip адреса серверу. Для начала создадим профиль интерфейса enp0s8, назовем его «*native_enp0s8*» и зададим ему статический адрес: **«nmcli connection add con-name "native_enp0s8" type ethernet ifname enp0s8**», после чего система проинформирует вас: рис. 2.12.

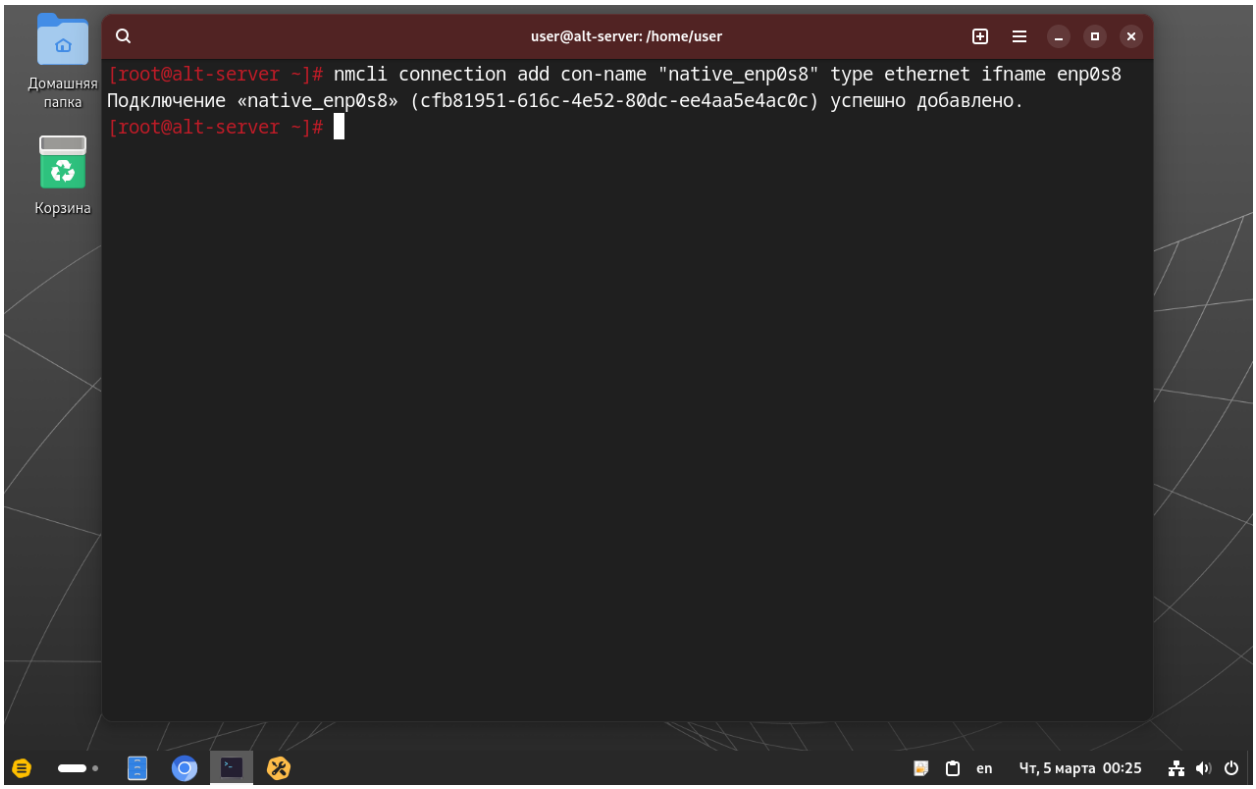

Рис. 2.12. Добавление профиля сетевого интерфейса

После чего зададим статику командой: «**nmcli connection modify native_enp0s8 connection.autoconnect yes ipv4.method manual ipv4.address 172.16.0.1/27**» и поднимем (запустим) наше подключение командой: «**nmcli connection up native_enp0s8**». В свою очередь, система проинформирует вас: (рис.2.13).

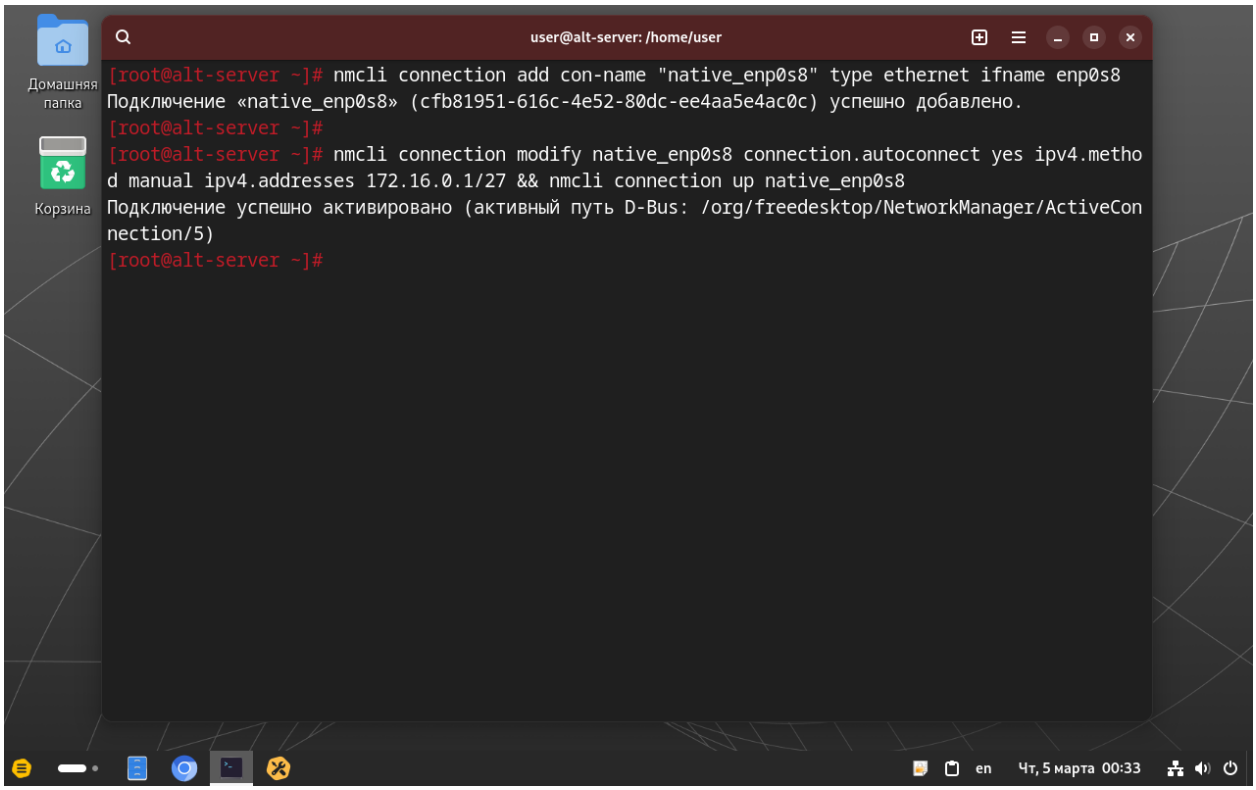

Рис. 2.13. Ручная настройка сетевого интерфейса

*Примечание 18. В данном случае (рис.2.13) вместо двух отдельных команд «**nmcli connection modify native_enp0s8 connection.autoconnect yes ipv4.method manual ipv4.address 172.16.0.1/27**» и «**nmcli connection up native_enp0s8**» выполнено соединение двух команд в одну при помощи оператора &&, который позволяет выполнять несколько подряд введенных команд отдельно без необходимости вводить их отдельно.*

Теперь проверить корректность проделанных настроек можно командой «**ip a**» (рис.2.14). На этом настройку статического адреса по варианту 2 можно считать завершенной.

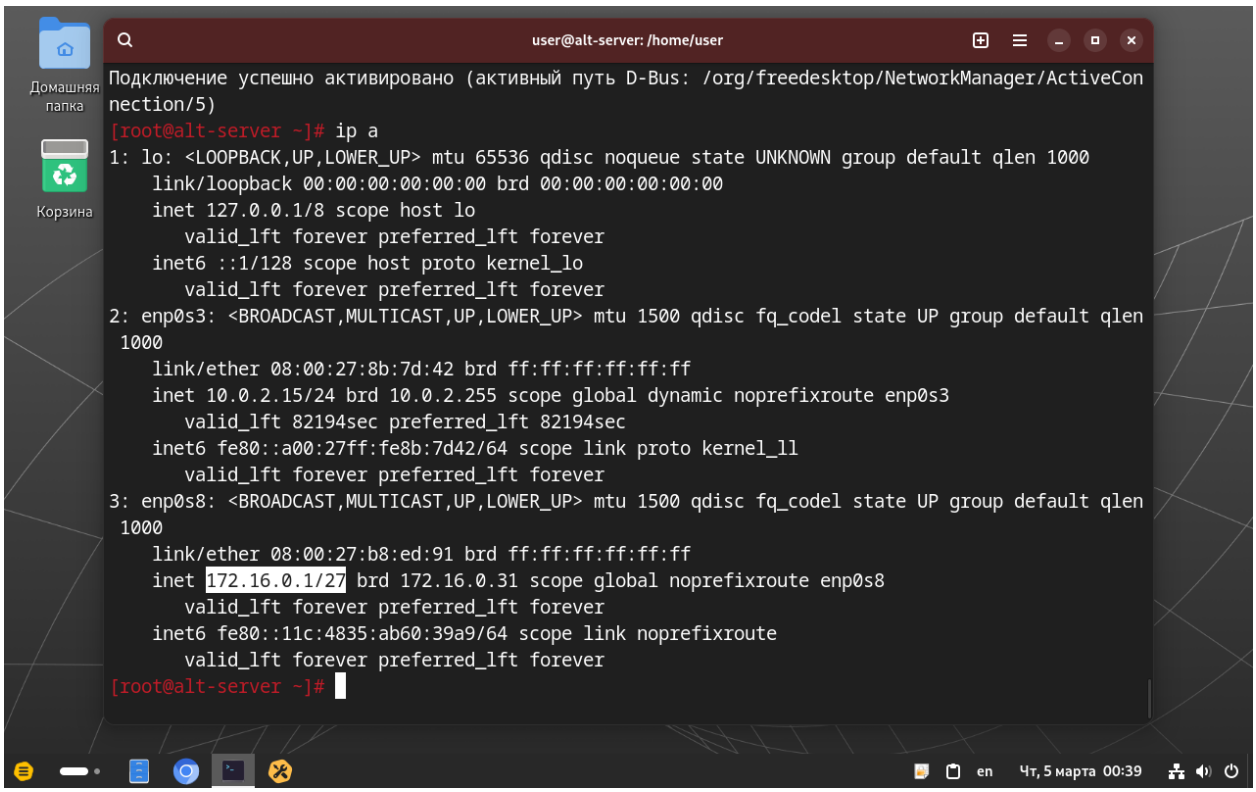

Рис. 2.14. Проверка текущих ip адресов системы

Теперь можно считать настройку статического адреса сервера завершенной, вы можете выбирать сами каким способом выполнять настройку: Графическим (вариант 1) или Терминальным (вариант 2); в обоих случаях настройки применятся и будут работать и после перезагрузки компьютера.

*Примечание 19. При использовании методики, описанной в варианте 2 и при дальнейших операциях в терминале, старайтесь создавать резервные копии редактируемых файлов во избежание их случайного искажения и в случае ошибки конфигурации вы всегда сможете вернуть исходную версию конфиг-файла быстро и без «головной боли». Сделать резервную копию файла network.conf, расположенному в директории /etc в домашнюю папку пользователя можно командой «**cp /etc/network.conf ~/network.conf**», где знаком ~ обозначена домашняя директория пользователя, этот знак используется как специальное обозначение пути и не нуждается правке.*

2.2. Настройка dhcp сервера (isc-dhcp-server)

Этап 1. Подготовка менеджера пакетов apt-get.

*Примечание 20. Важно учитывать, что после установки alt server ваш пользователь по умолчанию не будет иметь прав на внесение каких-либо изменений в системные файлы. Есть несколько способов исправления данной ситуации так, например можно внести необходимые изменения в файл по адресу: /etc/sudoers, либо использовать учетную запись суперпользователя «root», что мы, собственно, и будем проделывать ниже: открываем терминал и вводим команду «su», после чего система потребует от вас ввода пароля суперпользователя, который вы настраивали при установке системы. Если при вводе пароля у вас ничего не отображается (что-то вроде символов **** или ####), то это совершенно нормальное явление.*

Примечание 21. Стоит помнить, что, используя учетную запись суперпользователя (root), вы можете нанести вред вашей системе, поэтому следует быть предельно внимательным и аккуратным, а также делать резервные копии редактируемых файлов!

Прежде, чем начать установку самого сервера динамических адресов, сделаем обновление пакетов системы для того, чтобы обновить все устаревшие пакеты программного обеспечения системы.

Вводим в терминале команду: **apt-get update**, если система покажет необходимость обновления пакетов, то вводим команду на обновление найденных пакетов: **apt-get upgrade**. На этом процесс подготовки завершен (рис. 2.15).

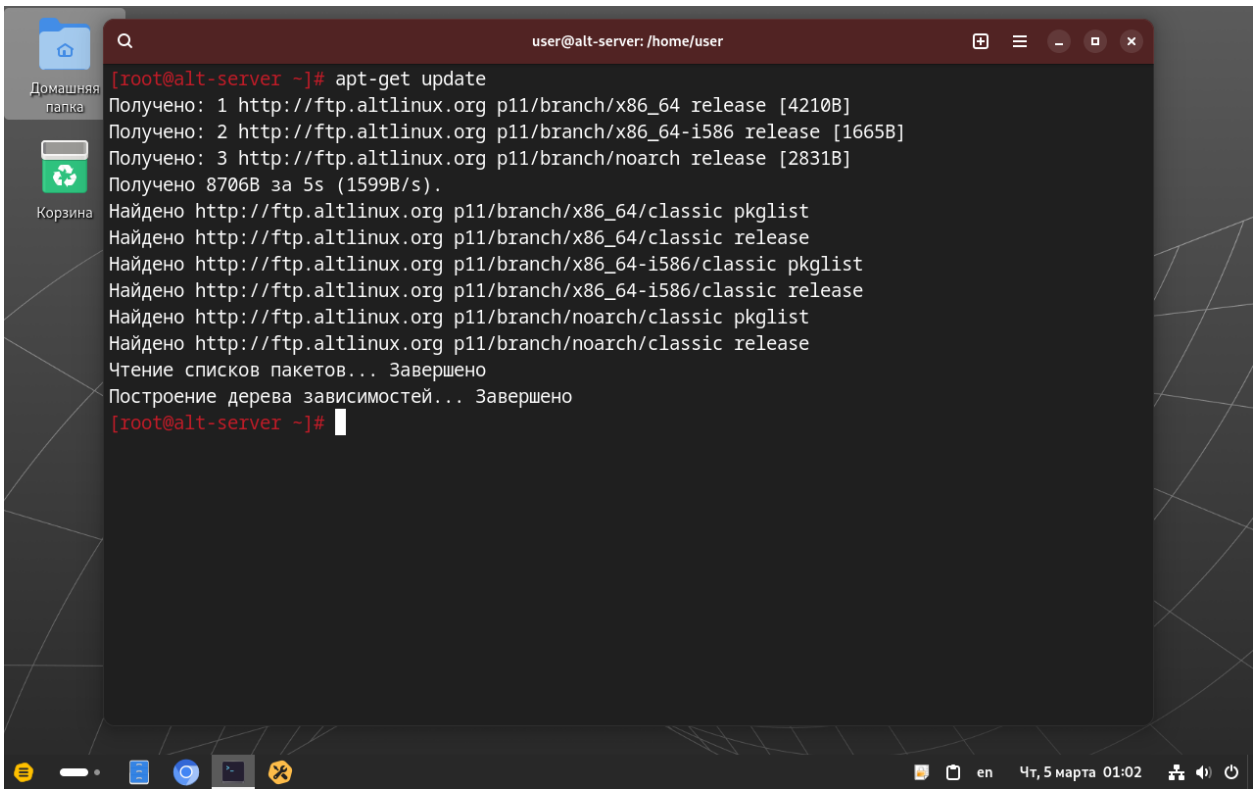

Рис. 2.15. Подготовка пакетного менеджера apt-get

Для установки сервера динамических адресов (dhcp) установим одноименный пакет при помощи пакетного менеджера apt-get. Сделать это можно командой «**apt-get install dhcp-server**». (рис. 2.16)

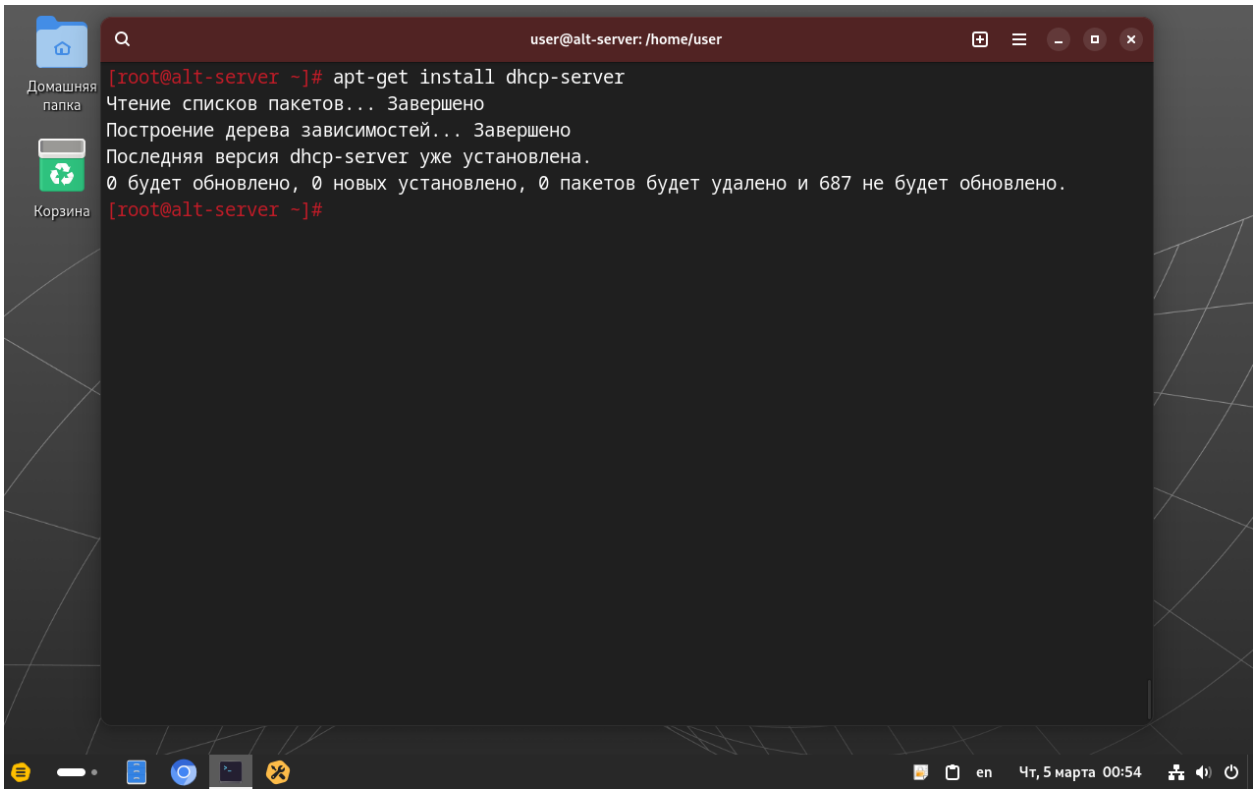

Рис. 2.16. Установка сервера динамических адресов

Начнется процесс установки, вводим в терминал команду: **apt-get install dhcp-server**, после обнаружения данного пакета в репозиториях, система предложит вам установить самую последнюю версию найденного пакета, с чем мы соглашаемся, вводя символ «Y» с клавиатуры, что означает «YES» или «ДА».

После того, как установка сервера выполнена, можно перейти к его настройке. Настройка будет выполняться в терминальном режиме. Каждую команду перед применением стоит тщательно перепроверять. Теперь необходимо убедится в том, что сервер dhcp выключен: **systemctl status dhcpd** данная команды покажет статус сервиса, после установки, по умолчанию сервер будет выключен (***inactive(dead)***) и его включение будет невозможным до тех пор, пока не будут внесены правки в конфигурационный файл сервера, что мы сейчас и сделаем. Прежде, чем вносить конфигурацию, нужно создать сам конфигурационный файл, обычно он называется *dhcpd.conf.example*, т.е. конфиг для примера, в нем есть много полезной информации, которую мы настоятельно рекомендуем внимательно изучить, а мы продолжаем.

Введем в терминал команду: **cp /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf**, данной командой мы скопируем файл примера и сделаем из него основной (рис. 2.17), тогда, при вводе команды **nano /etc/dhcp/dhcpd.conf** мы получим следующее: (Рис. 2.18)

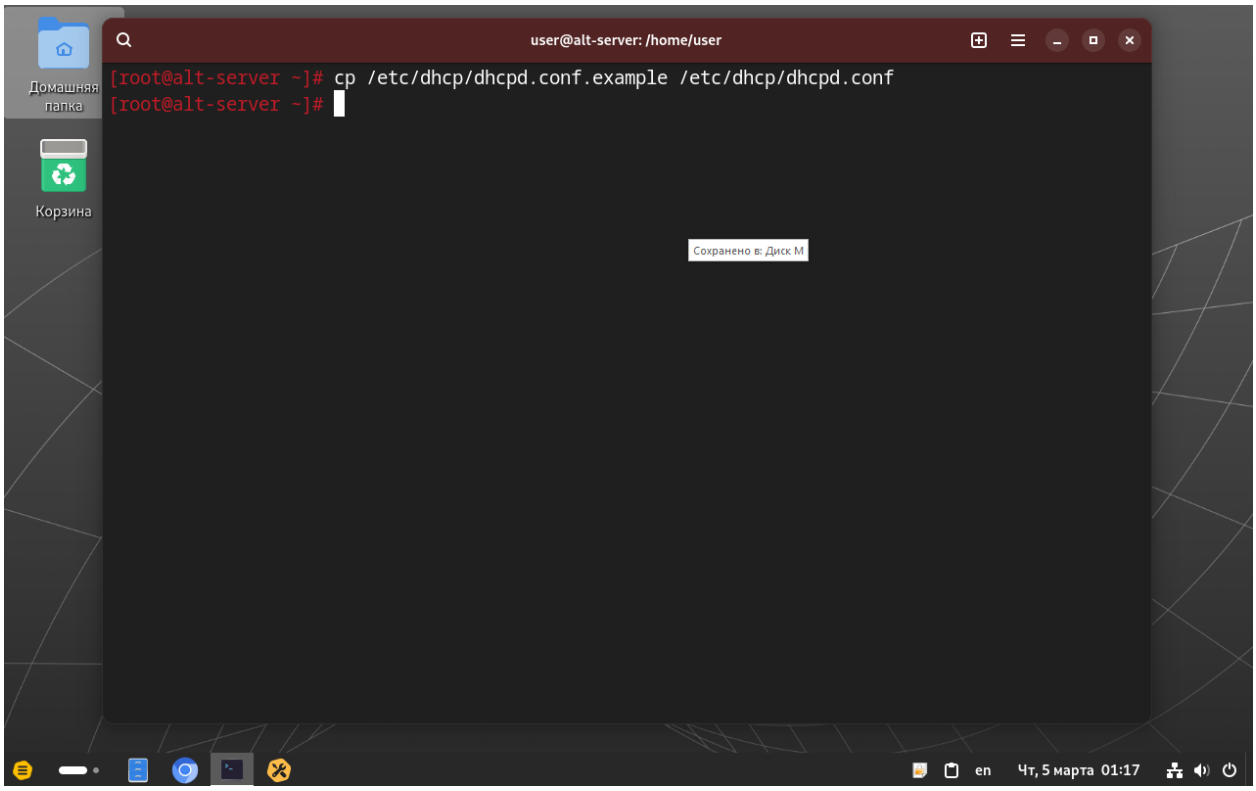

Рис. 2.17. Создание резервной копии файла

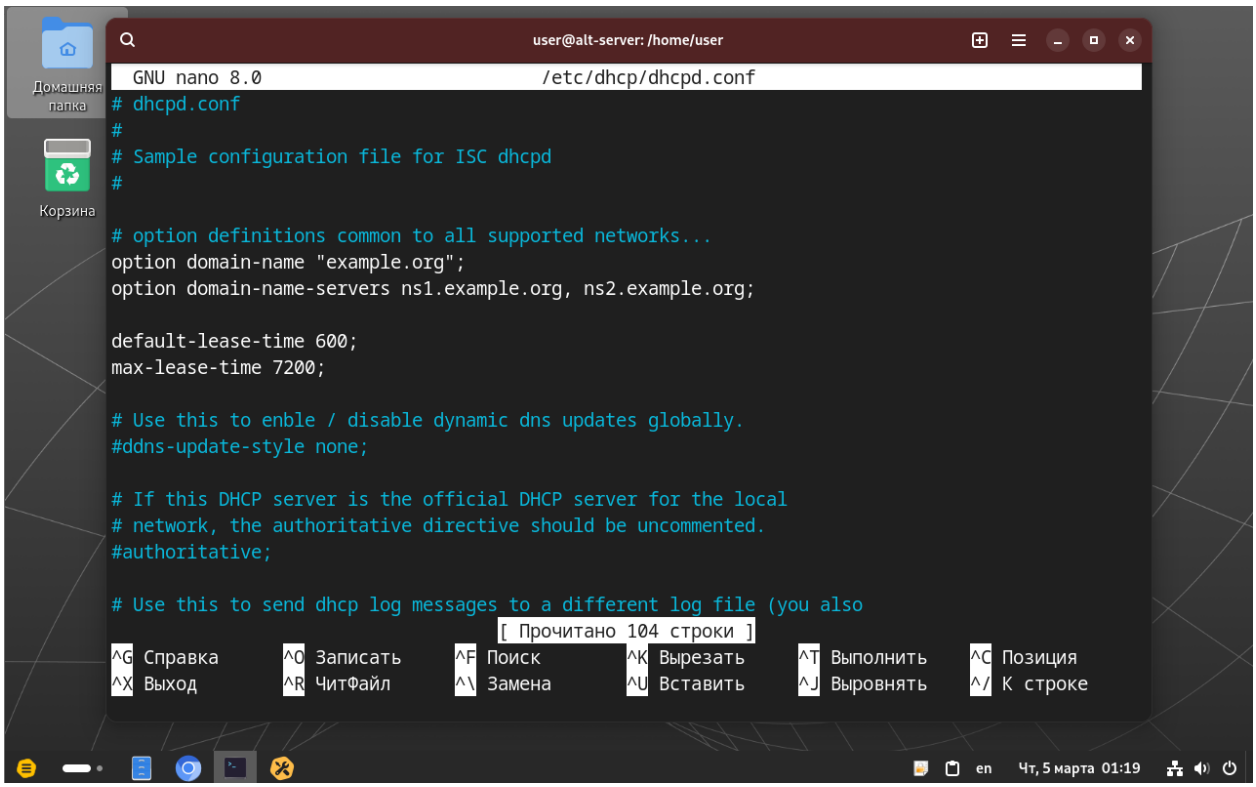

Рис. 2.18. Конфигурационный файл dhcp-сервера

Приведем файл конфигурации к следующему виду рис. 2.19.

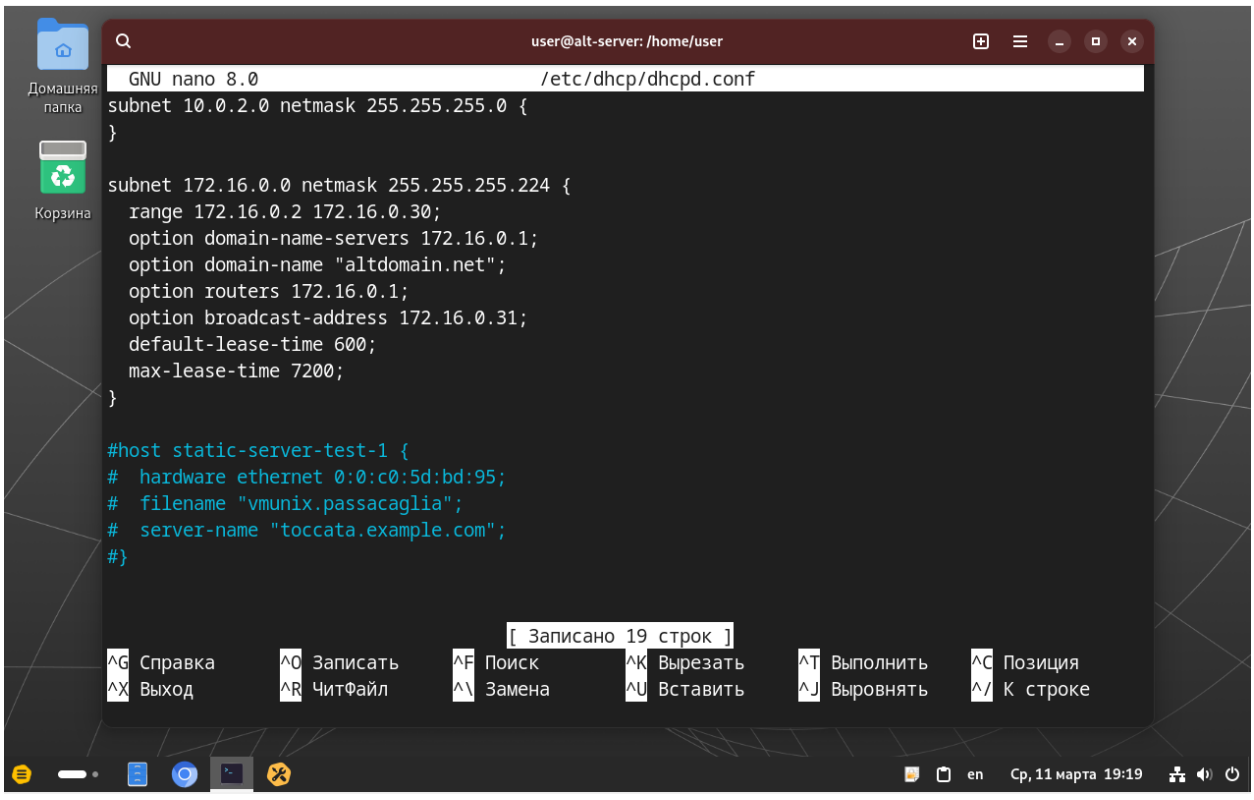

Рис. 2.19. Готовый файл конфигурации dhcp-сервера

Где:

1. **Subnet** – сама сеть, которая будет обслуживаться сервером;
2. **Netmask** – маска сети, которая будет обслуживаться сервером;
3. **Range** – пул ip адресов, которые будет выдавать сервер;
4. **Option domain-name-servers** – ip адрес или fqdn сервера доменных имен, который будет обрабатывать запросы от клиентов (dns сервера);
5. **Option domain-name** – имя домена, который будет присваиваться клиентам при аренде адреса;
6. **Option routers** – основной (сетевой) шлюз, через который осуществляется выход в сеть Интернет;
7. **Option broadcast-address** – широковещательный адрес сети;
8. **Default-lease-time** – время аренды адреса по умолчанию;
9. **Max-lease-time** – максимальное время аренды адреса.

Пример ***static-server-test-1*** на рис 2.19 позволяет задавать статические адреса некоторым клиентам сети при присвоении ip адреса по mac адресу устройства.

После внесенных изменений закрываем конфигурационный файл используя комбинацию клавиш Ctrl+O, затем Ctrl+X. Затем нам нужно настроить его запуск при включении системы (чтобы каждый раз не приходилось запускать сервис вручную), сделать это можно при помощи команды «**systemctl enable dhcpd**», а затем перезапустить сам dhcp сервер для применения настройки командой «**systemctl restart dhcpd**» рис. 2.20. Рис 2.20 – статус сервиса Active: active (running), подсвеченный зеленым цветом сообщает нам об успешном применении конфигурации и запуске dhcp сервера в режиме раздачи ip адресов клиентским машинам. Все тесты и проверки работоспособности и доступности сервера на клиентских машинах приведены в разделе 4.1.1 данного методического пособия.

На этом настройку dhcp сервера можно считать завершенной.

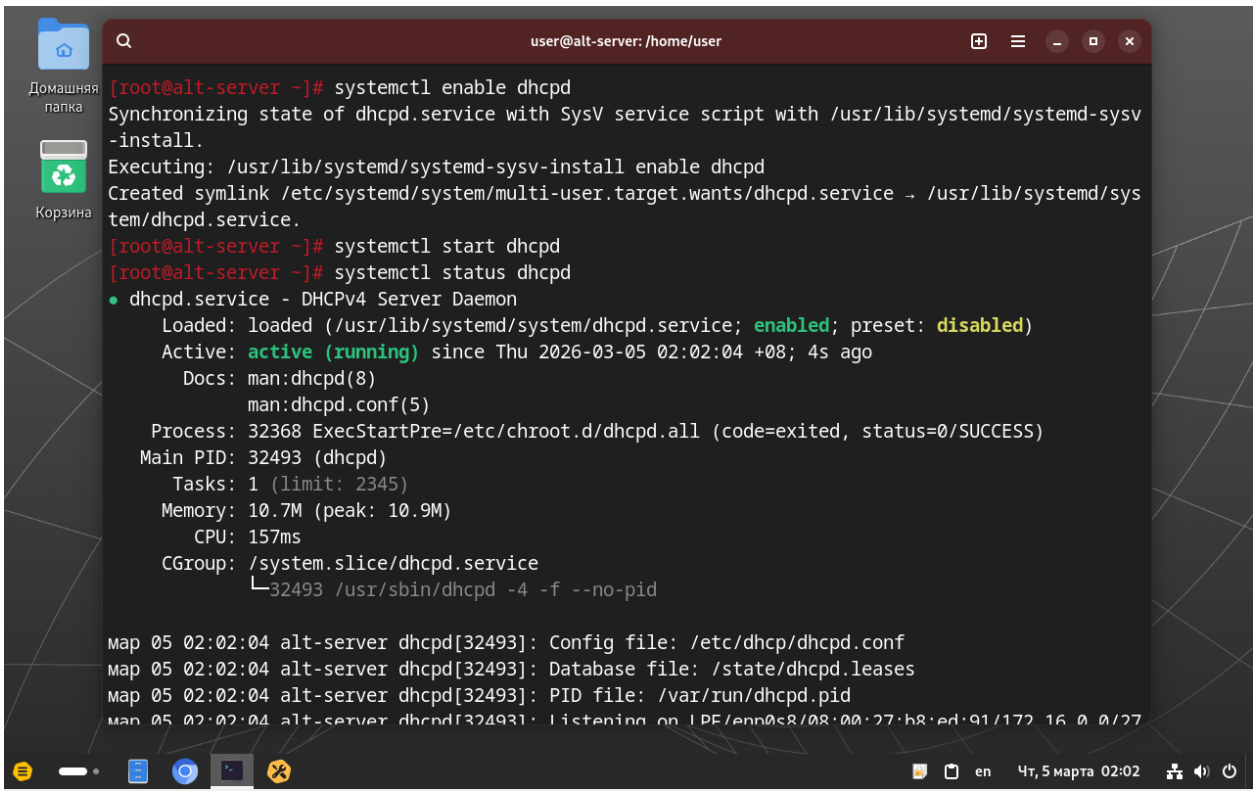

Рис. 2.20. Запуск и проверка статуса dhcp сервера

2.3. Настройка контроллера домена и сервера имен на базе SambaDC

В операционных системах семейства Linux присутствует возможность создания и управления контроллера домена, по своей архитектуре и настройкам близким к Microsoft Active Directory (службе сетевых каталогов от компании Microsoft на базе Windows Server) – samba active directory domain controller (samba-ad-dc).

Для развертывания контроллера домена на базе BaseALT Linux Server необходимо выполнить установку службы **task-samba-dc.** Сделать это нам позволяет команда **apt install task-samba-dc.** (рис. 2.21).

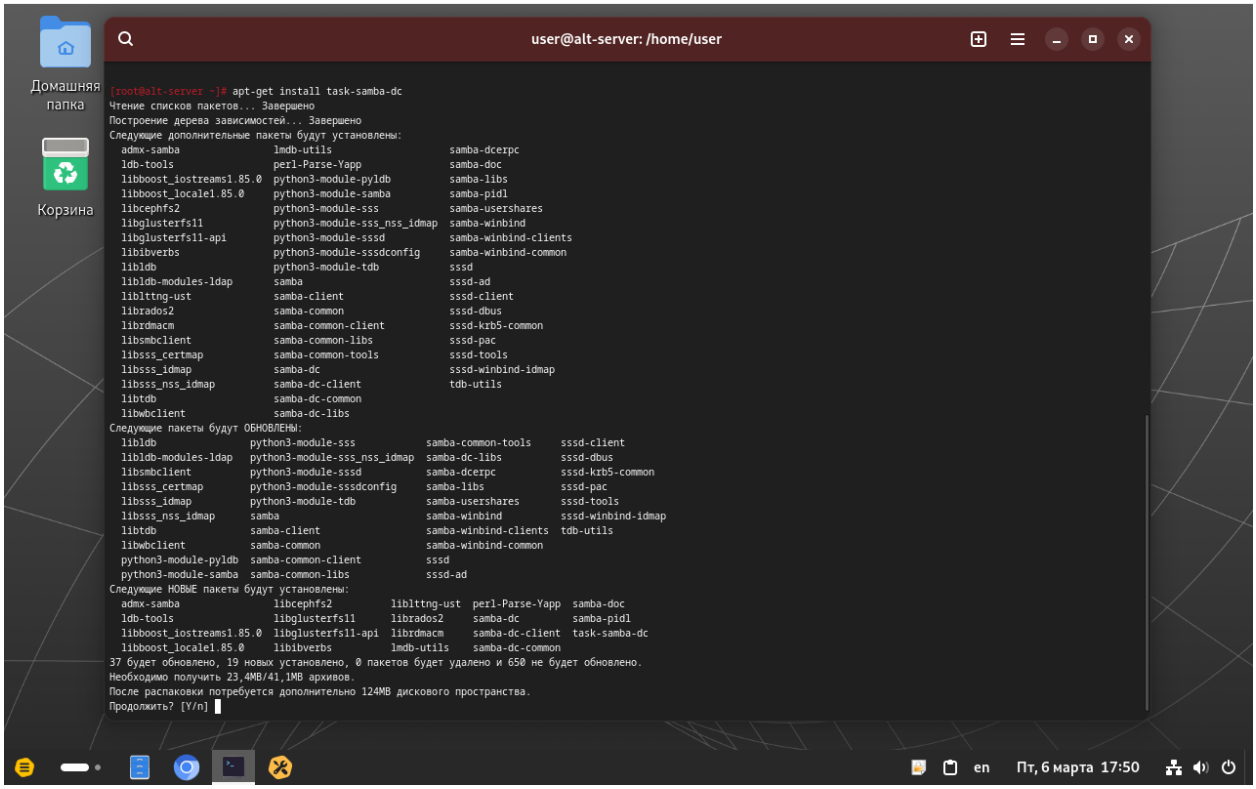

Рис. 2.21. Установка пакета SambaDC

В случае успешной установке перед вами выйдет примерно следующий вывод консоли (рис. 2.22), с сообщение «Завершено» или «Установка завершена»; в случае ошибки будет сообщение «Прервано» или «Не удалось разрешить конфликты».

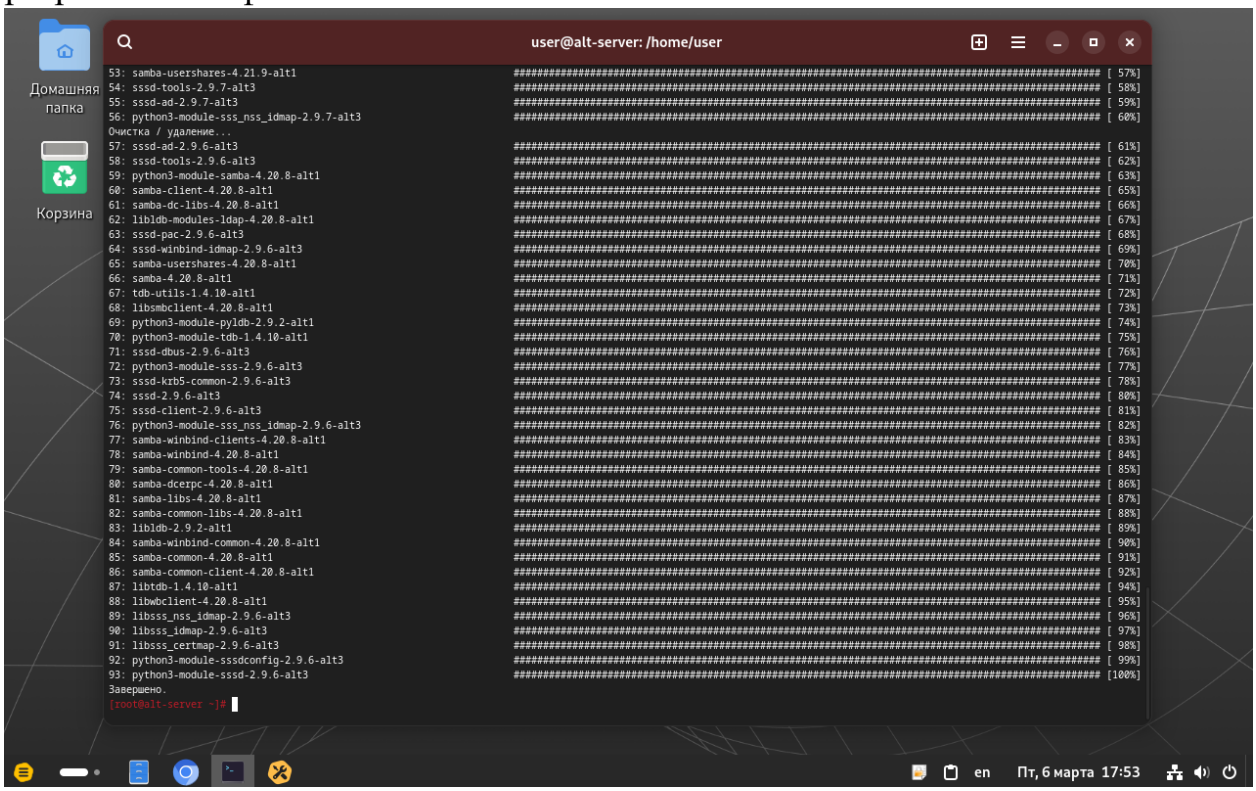

Рис. 2.22. Завершение установки пакета SambaDC

После установки пакета samba-dc нужно удалить все лишние файлы настройки, это делается для того, чтобы в процессе создания домена не возникало конфликтов с уже существующими файлами, т.к. при инициализации нового домена все файлы создаются автоматически. Используем команду: «**rm -f /etc/samba/smb.conf**», подтверждаем удаление клавишей «Enter» и идем далее.

Примечание 22. Стоит помнить, что Samba в режиме контроллера домена (Domain Controller, DC) использует свой сервер LDAP, свой центр распределения ключей KDC (сервер Kerberos) и свой сервер DNS (если не включен плагин BIND9_DLZ), поэтому, во избежание проблем совместимости и запуска, перед установкой остановите конфликтующие службы ***krb5kdc*** *и* ***slapd****, а также* ***bind*** *или его аналог* ***named****, если они были установлены вами ранее.*

Теперь все готово к созданию нового домена в среде samba-ad-dc. Перейдем к созданию домена в интерактивном режиме, используем команду «**samba-tool domain provision**», после запуска которой, система запросит от вас некоторые данные для вашего будущего домена (рис. 2.23).

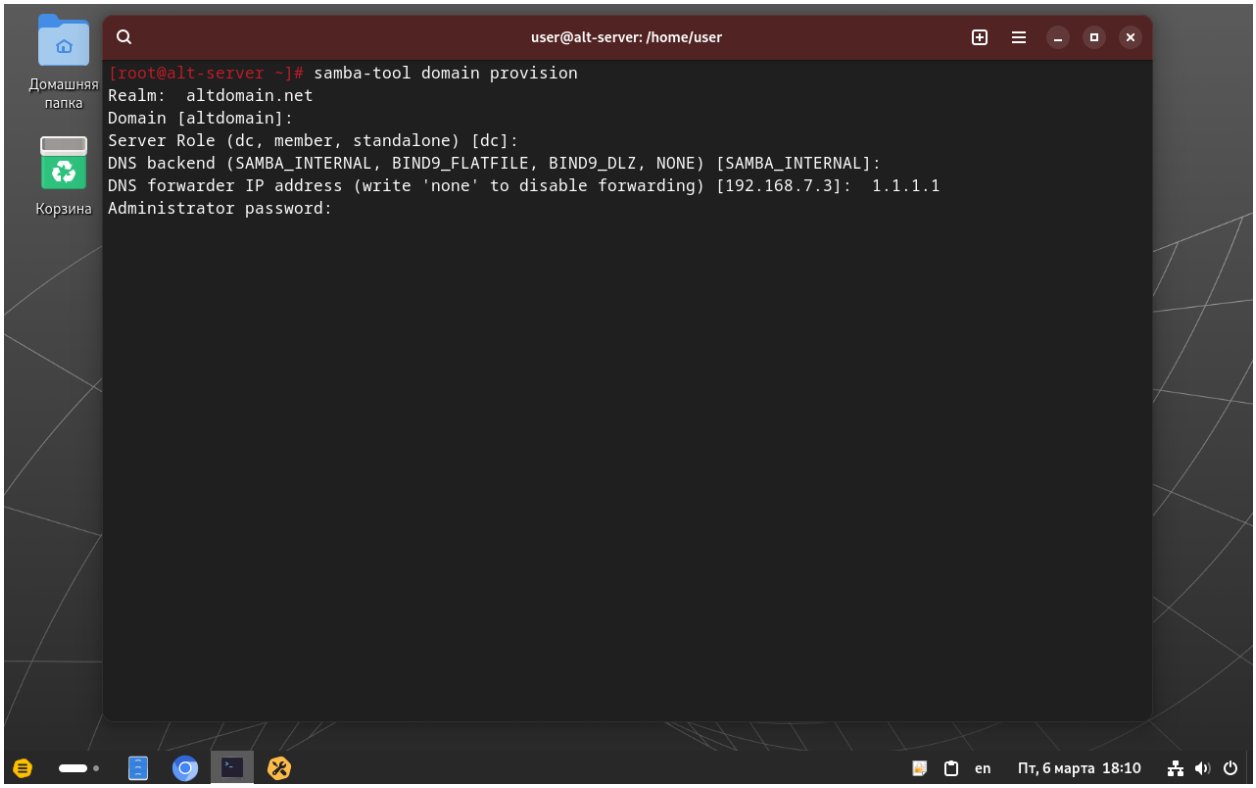

Рис. 2.23. Создание нового домена в интерактивном режиме

После того, как введете пароль учетной записи администратора домена, начнется процесс создания нового домена (рис. 2.24).

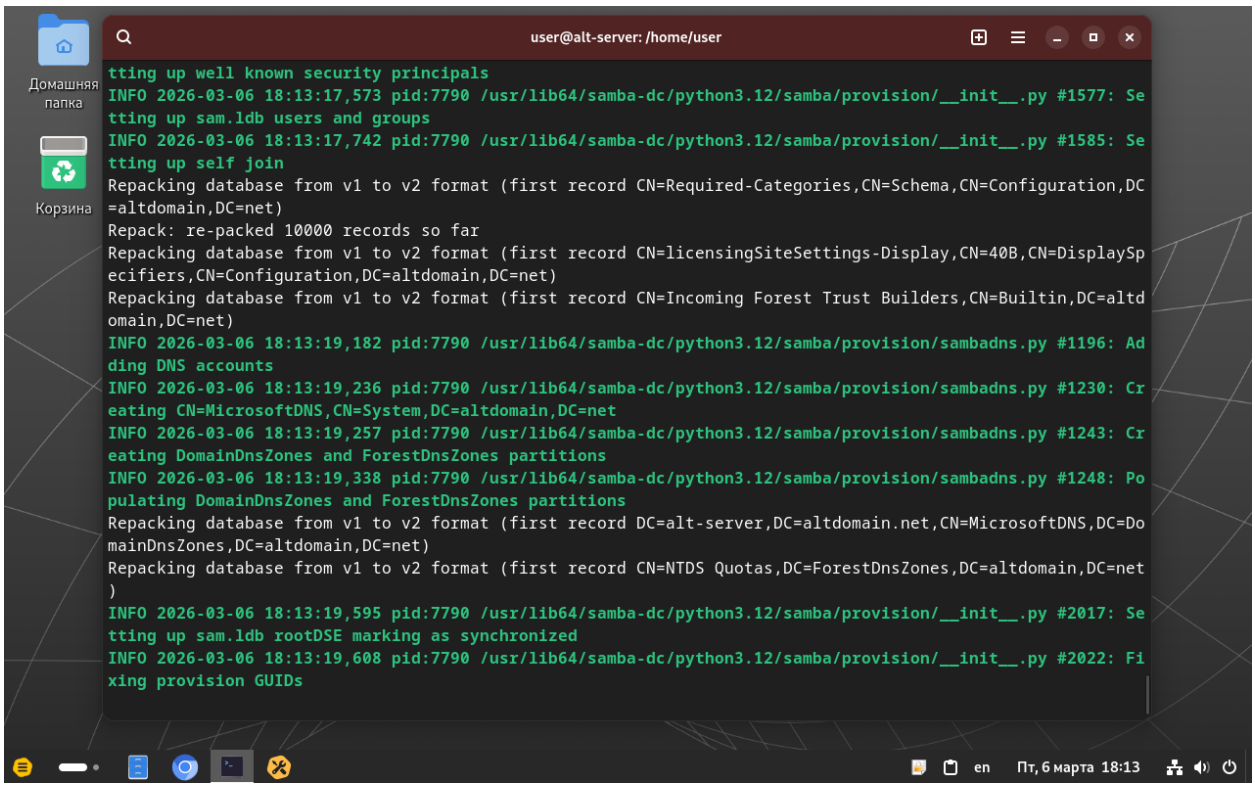

Рис. 2.24. Процесс создания нового домена samba-dc

В процессе создания нового домена у вас запросят некоторую информацию, а именно:

Realm – полное имя вашего домена со всему уровнями (1 .net, 2 altdomain, 3 и тд.)

Domain – имя домена без учета домена первого уровня (без .ru, .net и тд.)

Server Role – непосредственно роль самого сервера, в нашем случае DC.

DNS backend – среда, используемая в качестве сервер имен для домена.

DNS forwarder – адрес внешнего сервера имен, для запросов вне домена.

Administrator password – пароль одноименной служебной учетной записи домена «Administrator» (вводится при создании дважды для исключения появления различных ошибок).

После проделанных ранее манипуляций можно считать, что домен в службе каталогов Samba-DC успешно созданы, о чем нам говорит информация, представленная на рис. 2.25, и можно переходить к его дальнейшей настройки (тюнингу), также вместе с доменом при использовании «**DNS backend SAMBA INTERNAL**» у вас автоматически будет поднят сервер имен (dns сервер).

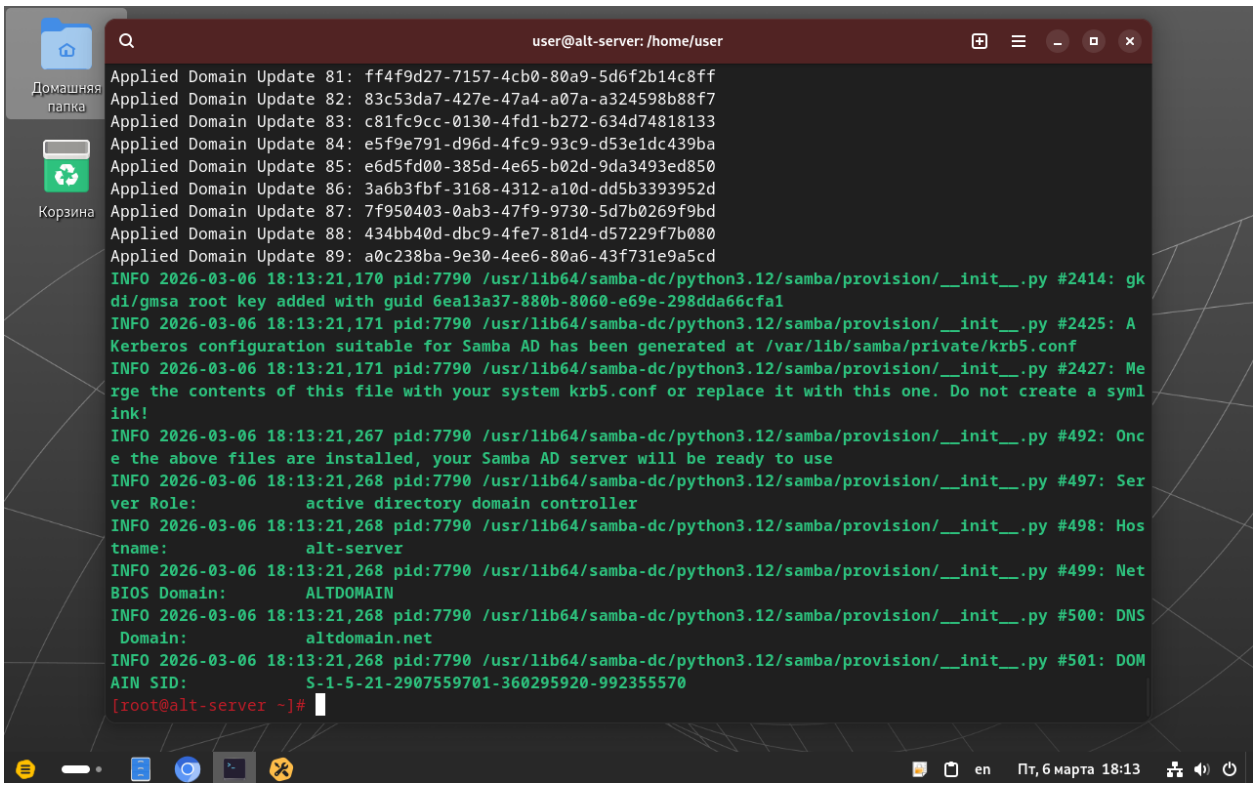

Рис. 2.25. Успешное завершение создания нового домена

Теперь можно убедиться в успешности создания домена и запуска служб samba-ad-dc, для этого следует ввести в терминале команду «**systemctl status samba**» рис. 2.26.

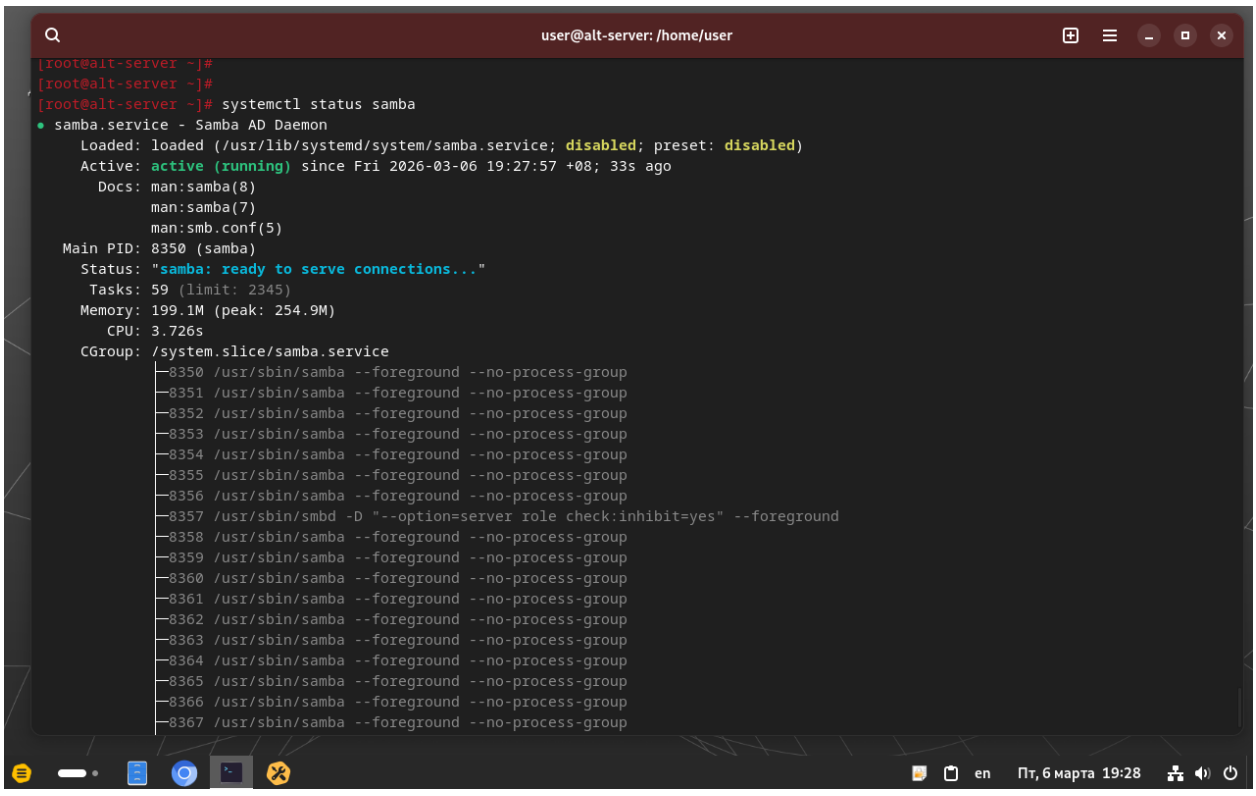

Рис. 2.26. Статус сервиса sambaDC

Если же у вас вместо статуса на рис. 2.26, выходит статус loaded или inactive (dead) рис. 2.27, то вам следует выполнить ручной перезапуск сервиса sambaDC путем ввода команды «**systemctl restart samba**».

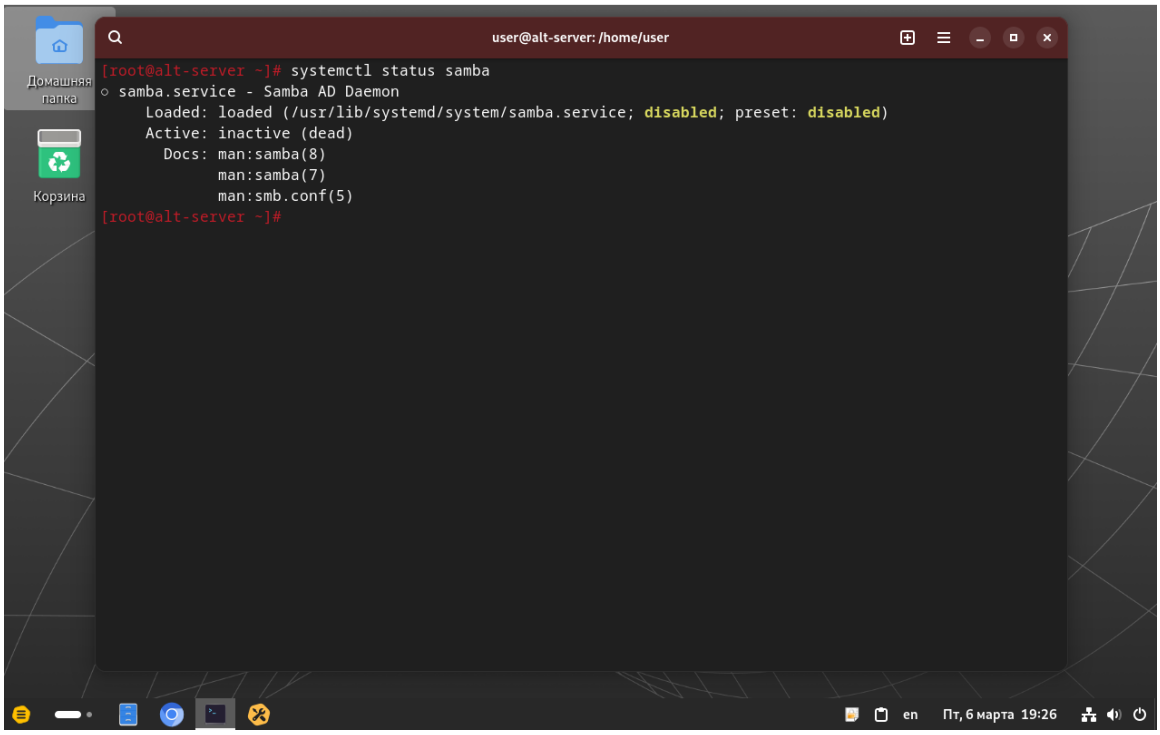

Рис. 2.27. Не запущенный сервис sambaDC

Если перезапуск прошел без ошибок, но статус сервиса горит красным рис. 2.28, то следует проверить порт 53 на наличие других сервисов, запущенных на данном порту рис. 2.29. Сделать это можно при помощи команду «**lsof -i :53**». После того, как вы выяснили, какой сервис прослушивает данный порт, то его можно остановить и отключить из автозагрузки рис.2.30 – это позволит вам при эксплуатации в дальнейшем избежать данной проблемы.

В нашем случае, на порту 53 был запущен сервис bind9 (также известный как named), в его функциях мы не нуждаемся, т.к. в роли сервера имен (dns) у нас выступает сервис samba-dc; его мы отключаем и исключаем из автозагрузки путем применения команды «**systemctl disable bind**».

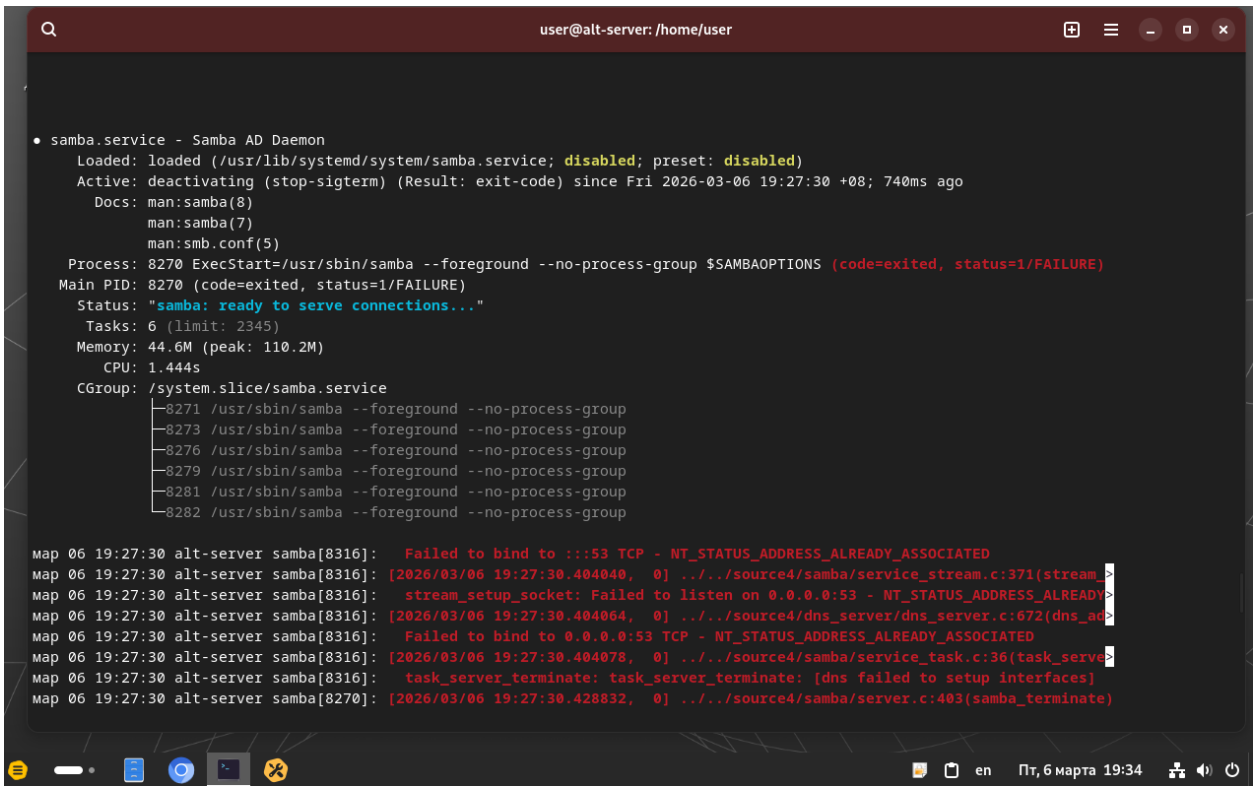

Рис. 2.28. Ошибки запуска сервиса samba-dc

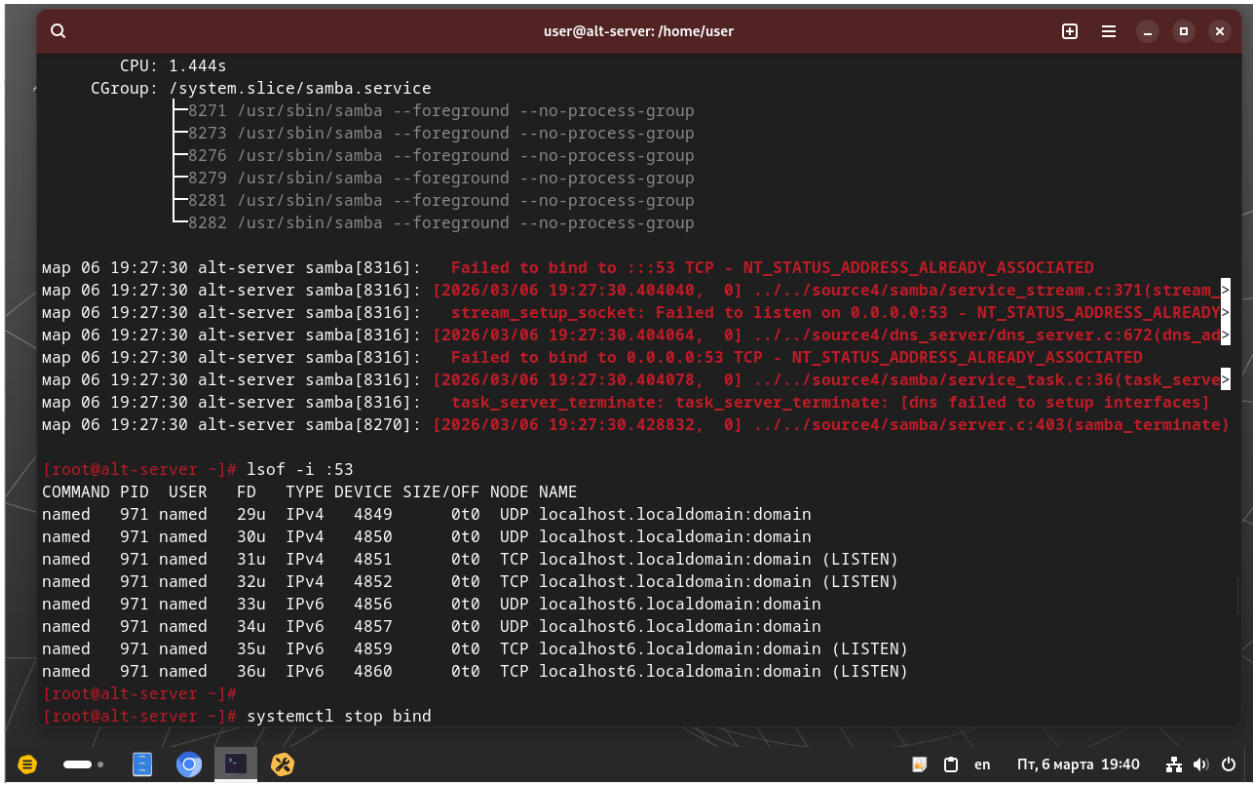

Рис. 2.29. Список сервисов на порту 53

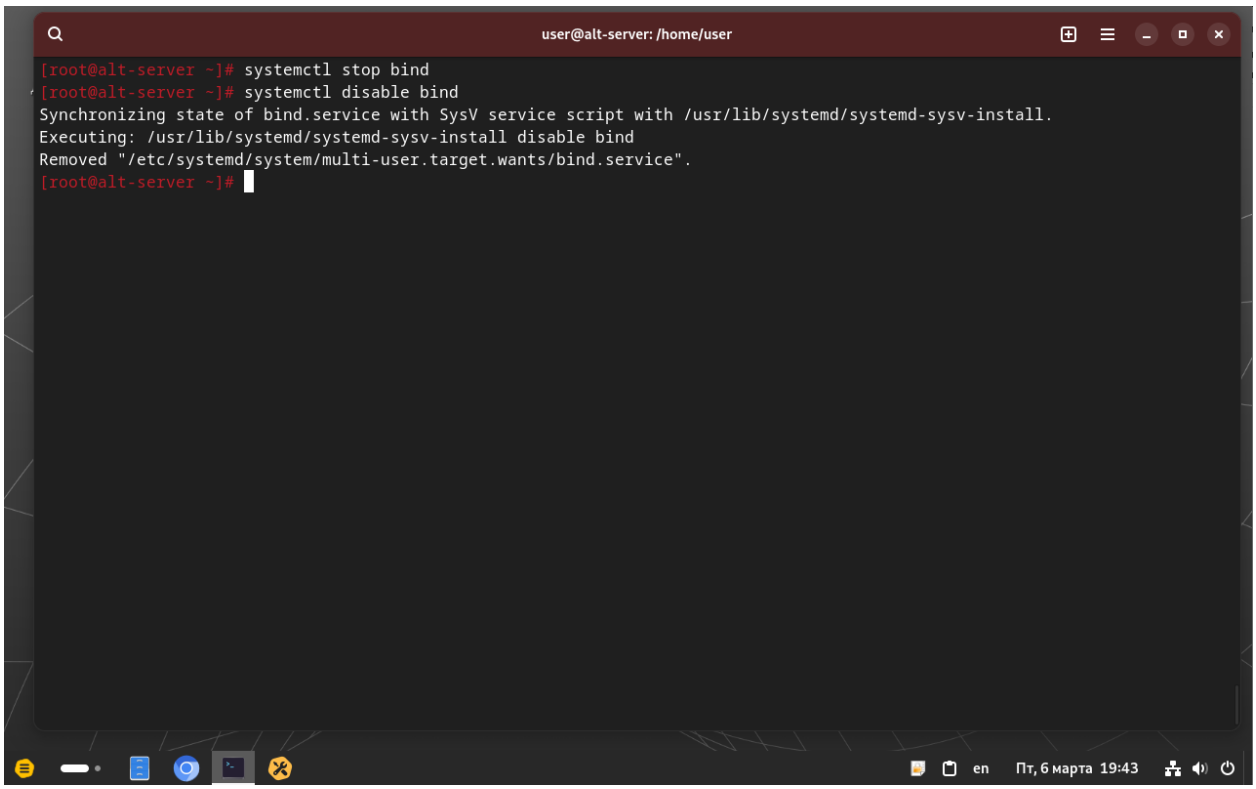

Рис. 2.30. Остановка и отключение сервиса bind

Теперь необходимо добавить наш контроллер домена в автозагрузку, делается это командой «**systemctl enable --now samba**». Проверить имя домена можно с помощью команды: «**samba-tool domain info 127.0.0.1**» рис. 2.31.

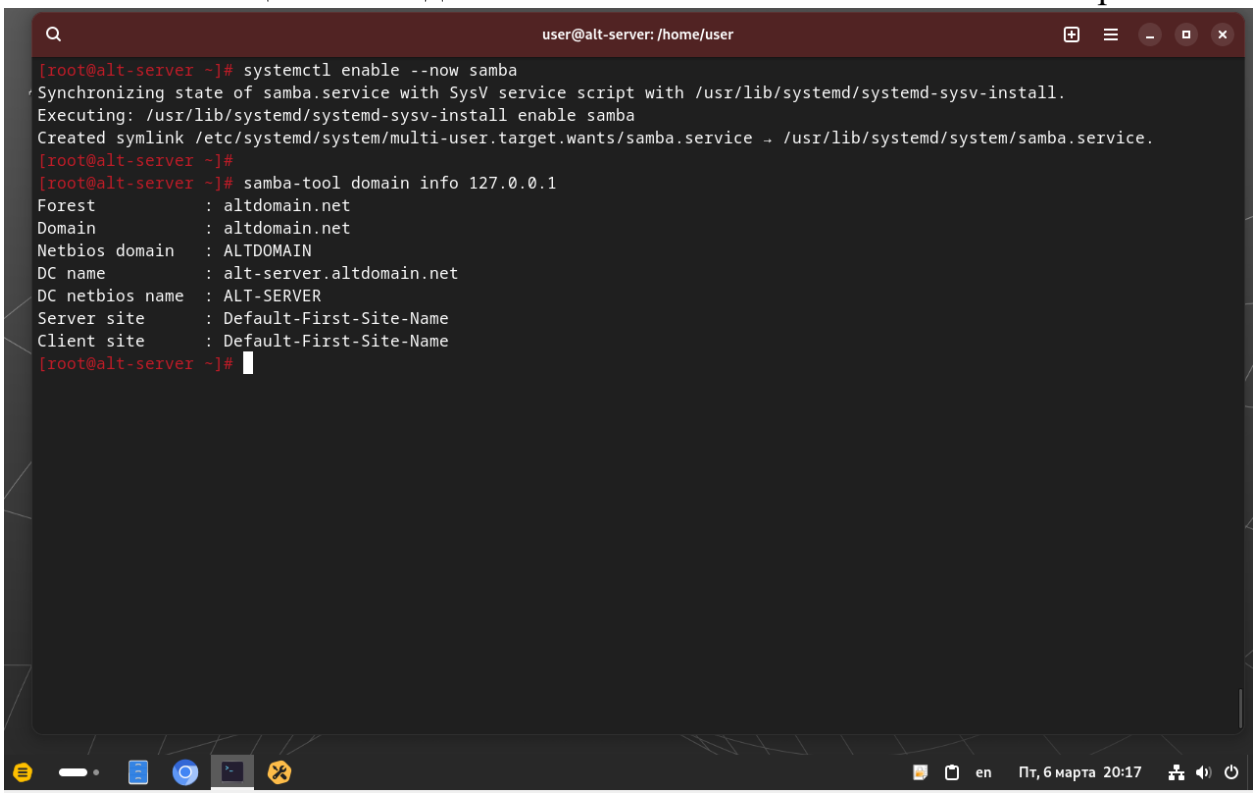

Рис. 2.31. Добавление сервиса в автозагрузку и просмотр статуса сервера DC

На этом можно считать настройку контроллера домена (samba-dc) и сервера имен (samba-dns) можно считать завершенной.

Все тесты и проверки работоспособности и доступности сервера на клиентских машинах приведены в разделе 4.1.2 данного методического пособия.

2.3.1. Управление пользователями в домене samba-dc

Теперь можно приступить к созданию пользователей, групп и прочих пользовательских структур. Для этого мы будем использовать терминал. Используя команды:

Создать пользователя с паролем: **samba-tool user create <имя пользователя>**;

Просмотреть доступных пользователей: **samba-tool user list**;

Удалить пользователя: **samba-tool user delete <имя пользователя>**;

Отключить пользователя: **samba-tool user disable <имя пользователя>**;

Включить пользователя: **samba-tool user enable <имя пользователя>**;

Изменить пароль пользователя: **samba-tool user setpassword <имя пользователя>**;

Управление группами производится в таком же режиме, но с использованием аргумента group вместо user.

Если у вас возникают трудности с управлением доменом в консольном режиме вы можете воспользоваться интерактивной инструкцией, вызвать которую можно использованием аргумента **help** в каждом разделе:

samba-tool --help

samba-tool user -- help

samba-tool group --help

и тд.

Для примера управления пользователями создадим пользователя «admin», который будет обладать правами администратора домена и позволит в дальнейшем вводить новые рабочие станции и сервера в домен samba.

Для этого воспользуемся комндами:

1. **samba-tool user add admin**
2. **samba-tool group addmembers «Domain Admins» admin**

Команда 1, после ввода запросит дополнительно создать пароля для пользователя; помните, доменные политики по умолчанию придерживаются требования к длине пароля не менее 7 символов – учитывайте это обстоятельство при создании новых паролей.

Процесс создания и добавления пользователя в группу приведен на рис.2.32

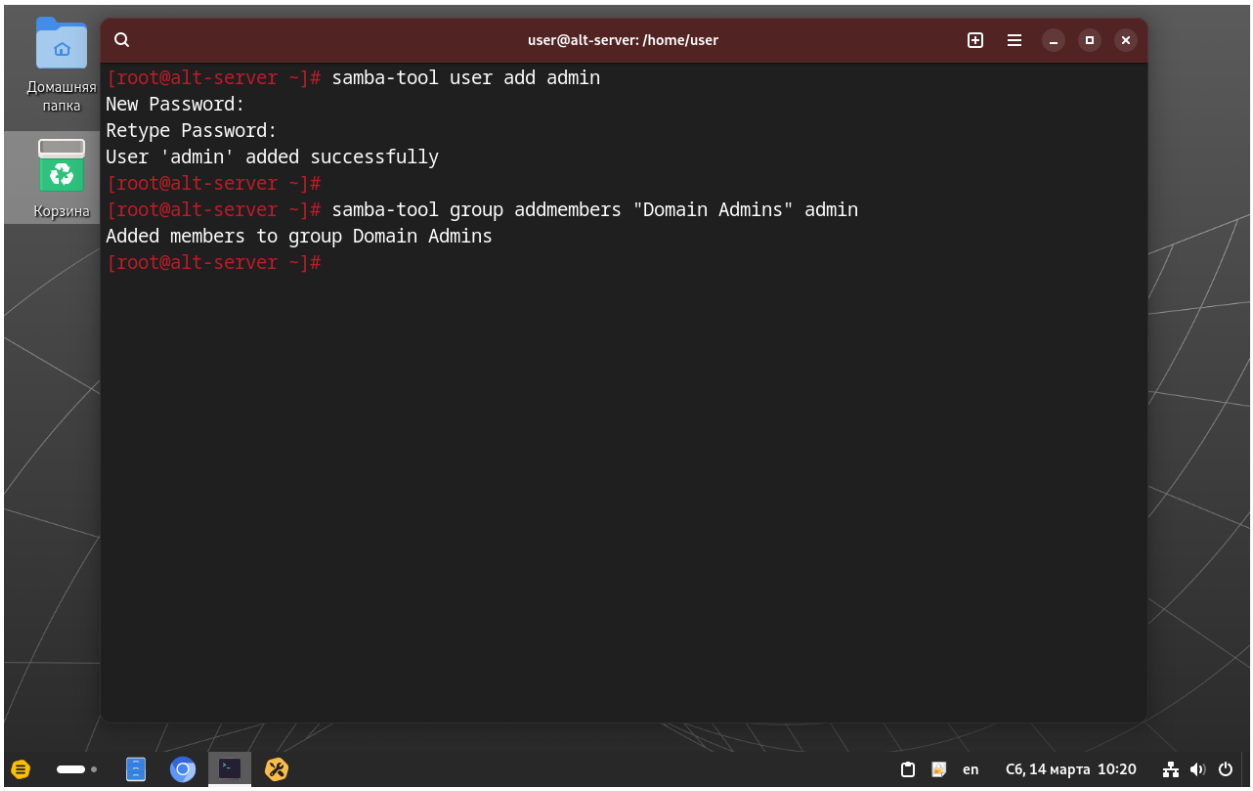

Рис. 2.32. Создание нового пользователя в домене с правами администратора

2.4. Настройка файлового сервера samba для общего доступа к ресурсам с авторизацией через контроллер домена на базе SambaDC.

После того, как была выполнена настройка контроллера домен, имеет смысл создать файловый сервер, который будет выполнять функцию сервера хранения пользовательских данных и документов, а также для служебной доменной информации.

Все настройки файлового сервера будут производиться в файле, расположенному по пути **/etc/samba/smb.conf**. Сделаем его резервную копию в домашний каталог текущего пользователя при помощи команды: «**cp /etc/samba/smb.conf ~/smb.conf**», затем перейдем к редактированию конфигурационного файла «**nano /etc/samba/smb.conf**». По умолчанию, после настройки контроллера домена данный файл должен выглядеть следующим образом рис.2.32.

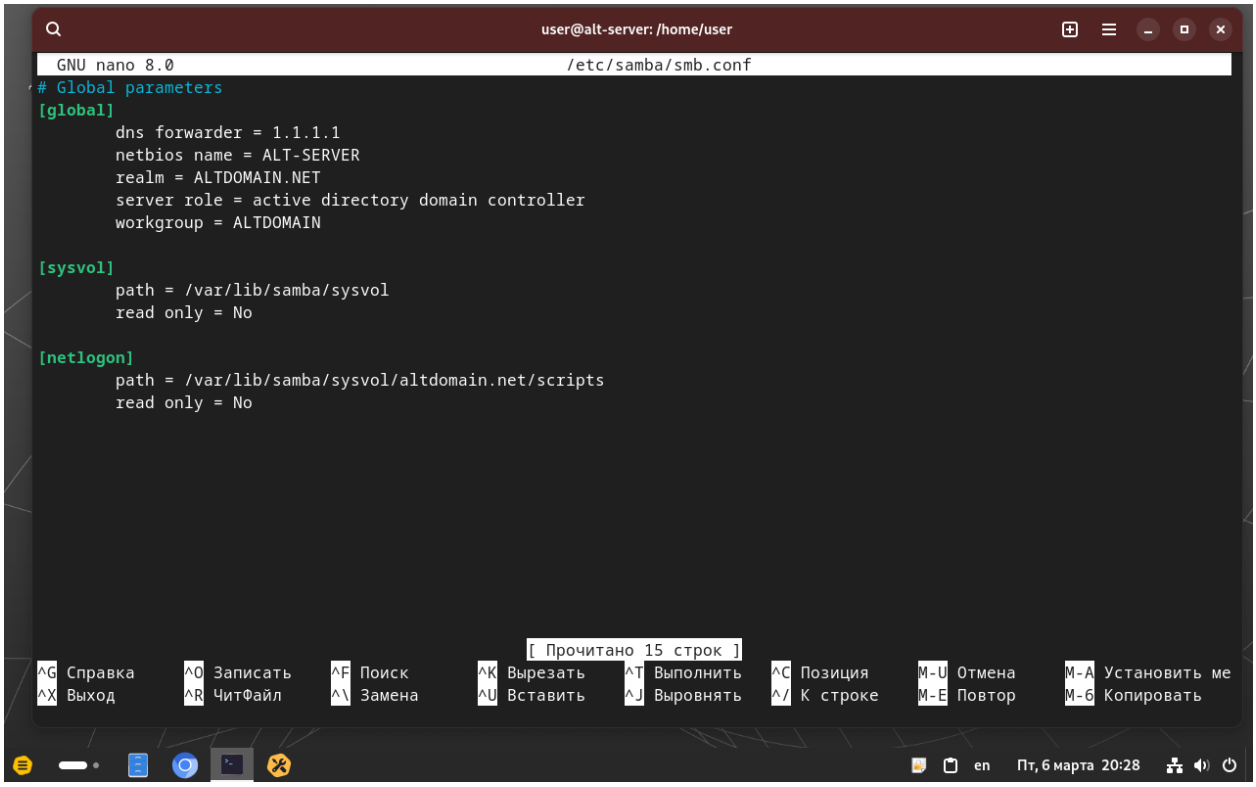

Рис. 2.33. Файл конфигурации сервиса Samba

В нем содержатся стандартные настройки контроллера домена, которые следует изменять с большой осторожностью, т.к. это может повлечь собой «падение» контроллера домена.

Когда вы сделали резервную копию файла, можно приступать к редактированию конфигурации. Простая настройка файлового сервера с 3 папками разного типа доступа приведена на рис. 2.33.

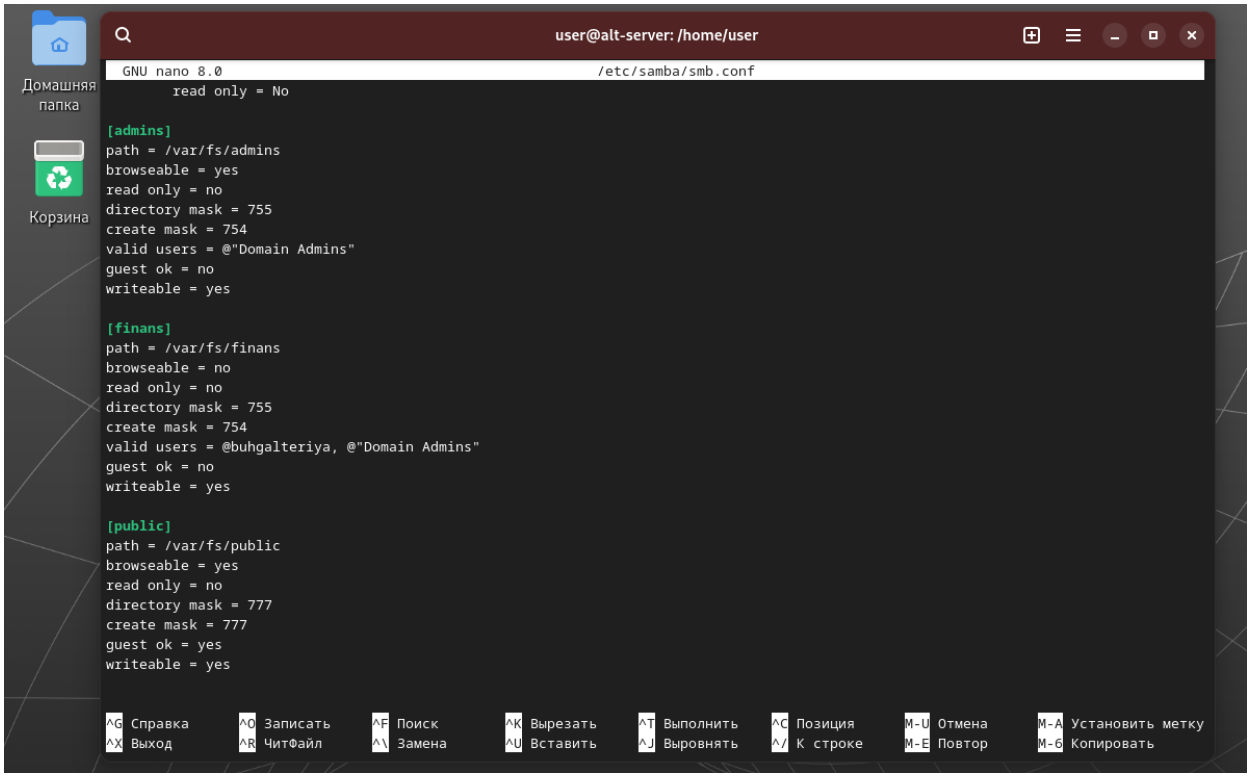

Рис. 2.34. Простая конфигурация файлового сервера

Выше приведена выдержка из файла smb.conf, который отвечает за настройку файлового сервера, предыдущие настройки и папки оставляем нетронутыми, они нужны для работы домена! Описание доступных параметров приведены ниже:

Path – параметр, указывающий на папку на самом сервере, где будет храниться данные

Browseable – отвечает за «видимость» папки при её перечислении в файловом менеджере клиентской системы, т.е. будет ли она видна при открытии сервера, если Yes, то видна, если No, то папка доступна только в том случае, если в файловом менеджере прописать полный путь до нее на сервере. (см. примечание 23)

Read only – параметр, позволяющий или запрещающий делать запись/сохранение файлов в каталог на сервере.

Directory mask - устанавливает права доступа (в восьмеричном формате, например 0755) для создаваемых внутри шары папок.

Create mask - задает права доступа для создаваемых внутри шары файлов (например 0644).

Valid users - определяет список пользователей или групп, которым разрешен доступ к ресурсу

writable — полный синоним параметра read only. Указывает, разрешена ли запись в шару (yes — запись разрешена, no — только чтение). Обычно используется вместо read only для большей понятности.

guest ok — разрешает гостевой (анонимный) доступ без ввода пароля (yes — гости могут подключаться, no — требуется аутентификация). Если включено, подключение происходит под пользователем, указанным в параметре guest account (обычно nobody).

*Примечание 23. При обращении к серверу по адресу **smb://file.server.net** для linux или **\\file.server.net** для windows у вас будет выведет список доступных сетевых ресурсов (шар/шары от слова share – делиться, раздавать). При присвоении файловой шаре значение **browseable = yes**, ресурс будет отображаться при таком запросе, если параметр **browseable** задан как **no**, то ресурс будет не виден при таком запросе и откроется только при обращении к нему напрямую, например: **smb://file.server.net/finans***

Теперь можно сохранить и закрыть файл конфигурации и перейти к созданию папок на самом сервере, сделать это можно с помощью команды «mkdir -p /var/fs/{admins,finans,public}» Во избежание проблем с правами доступа необходимо задать специальные разрешения на созданные ранее папки для сервиса samba, сделать это можно командой «**chmod 0775 -R /var/fs**» - данная команда предоставит достаточно «мягкие» права доступа к папкам. (рис. 2.34)

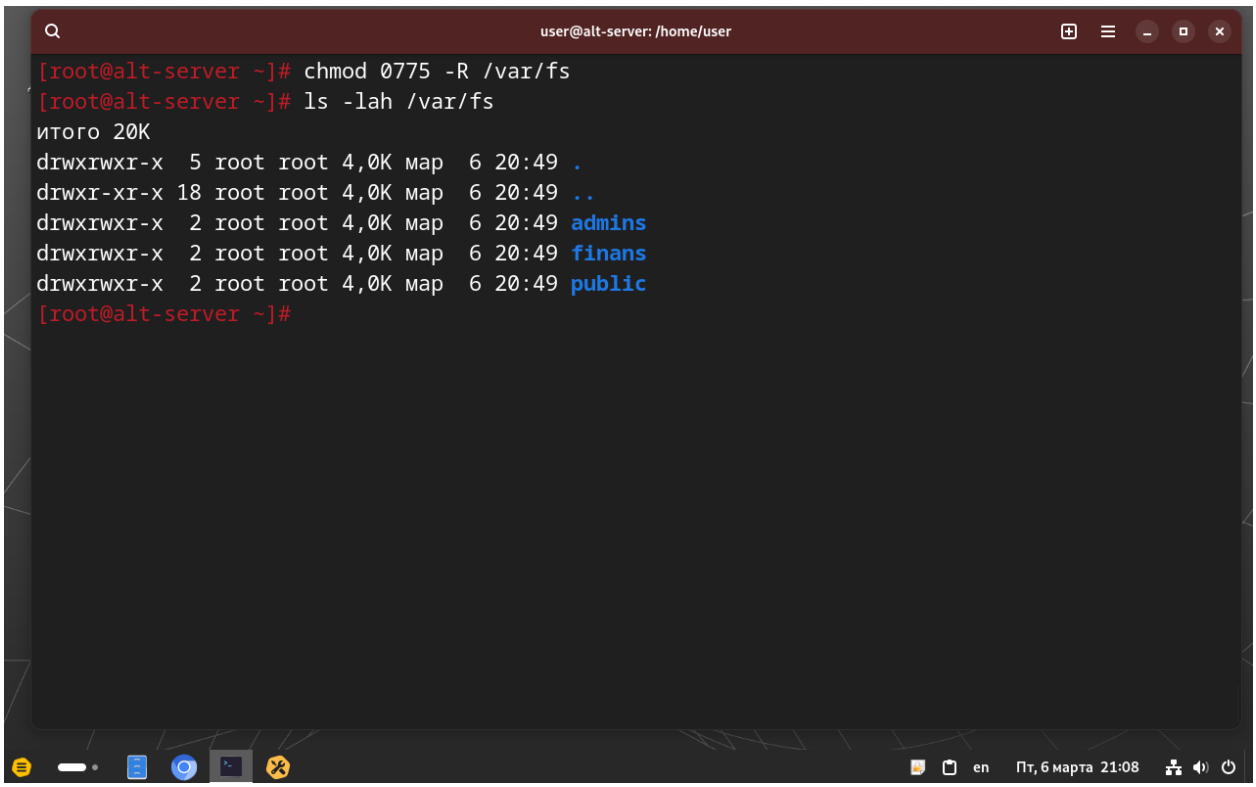

Рис. 2.35. Назначение и проверка прав доступа в системе Linux

Примечание 24. В нашем случае все 3 папки (admins, finans, public) имеют различные по мере доступа права: так например папку admin видят все, но доступ к ней имеет только группа пользователей «Администраторы домена» или «Domain Admin»; папка finans во первых скрыта от глаз, доступ к ней можно получить лишь при указании прямого пути до нее (а это еще и недо правильно угадать её название), во вторых доступ к ней имеет только группа «Бухгалтерия»; папка public доступна всем и без необходимости авторизации, это, конечно, не безопасно, но для общего знания и тестового стенда это стоит знать.

После проделанных в данном пункте манипуляций можно считать, что файловый сервер на базе samba успешно создан и уже может использовать в качестве файлового сервера доменной сети на базе samba-ad-dc.

Все тесты и проверки работоспособности и доступности сервера на клиентских машинах приведены в разделе 4.1.3 данного методического пособия.

2.5. Настройка программного прокси-сервера squid для управления пользовательским доступом в сеть Интернет

Программный прокси-сервер в нашем случае будет выполнять функцию контроллера доступа к сети Интернет, а также фильтровать допустимый контент. (Например отделу маркетинга запрещены соц.сети или бухгалтерии доступ разрешен только до сайта ФНС и других структур, занимающихся финансовым сектором)

Для начала запустим терминал, перейдем режим супер-пользователя и выполним установку пакета **squid** рис. 2.35.

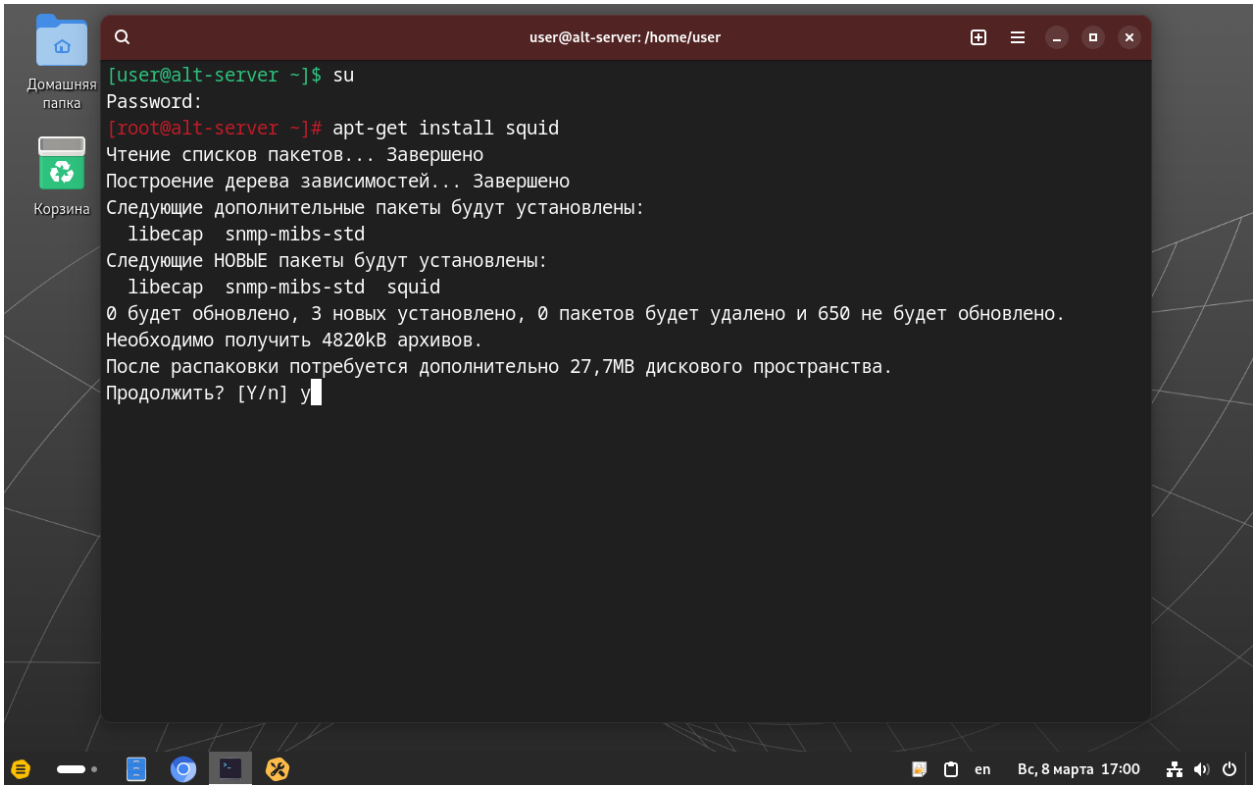

Рис. 2.36. Установка программного прокси-сервера Squid

После успешной установки пакета прокси-сервера выполним резервную копию файла конфигурации прокси-сервера squid, расположенного по пути /etc/squid/squid.conf рис. 2.36.: **«cp /etc/squid/squid.conf ~/»**. Затем откроем файл конфигурации для редактирования удобным для вас текстовом редактором, в нашем случае nano рис. 2.37.

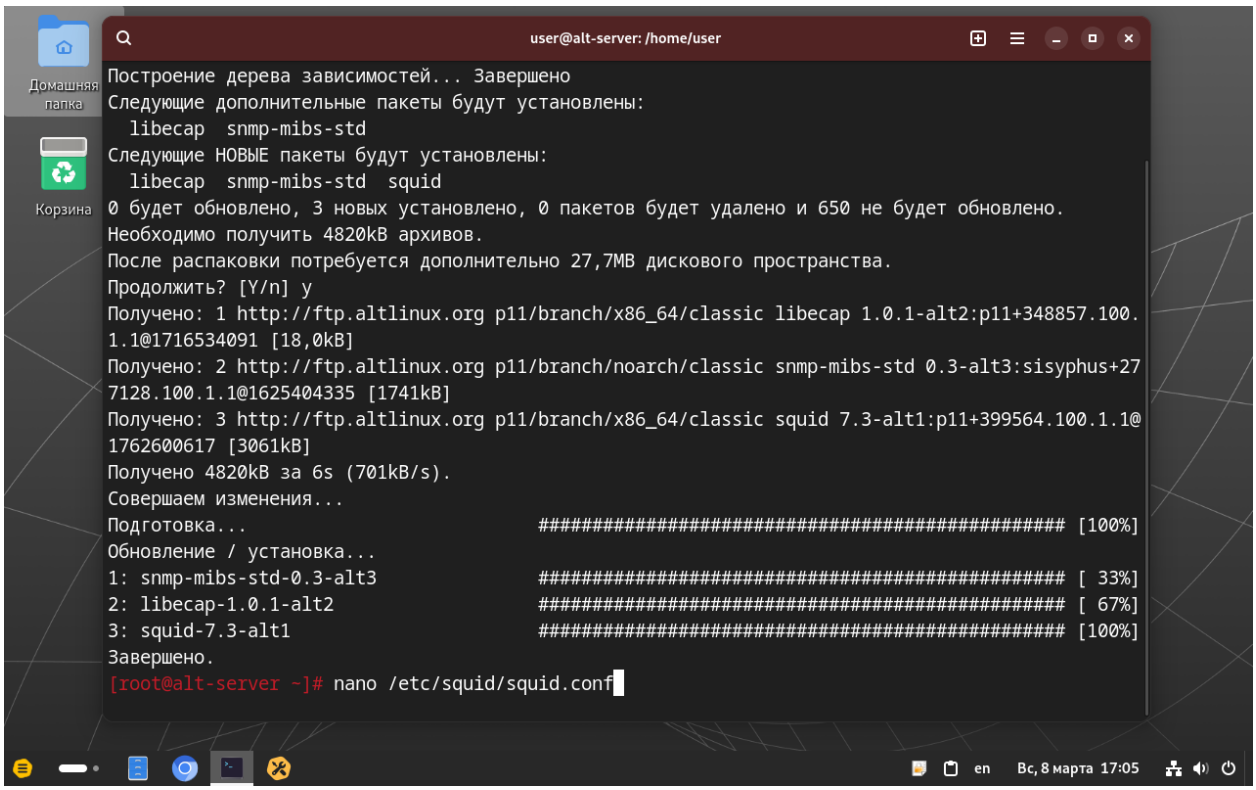

Рис. 2.37. Путь до файла конфигурации сервера squid.

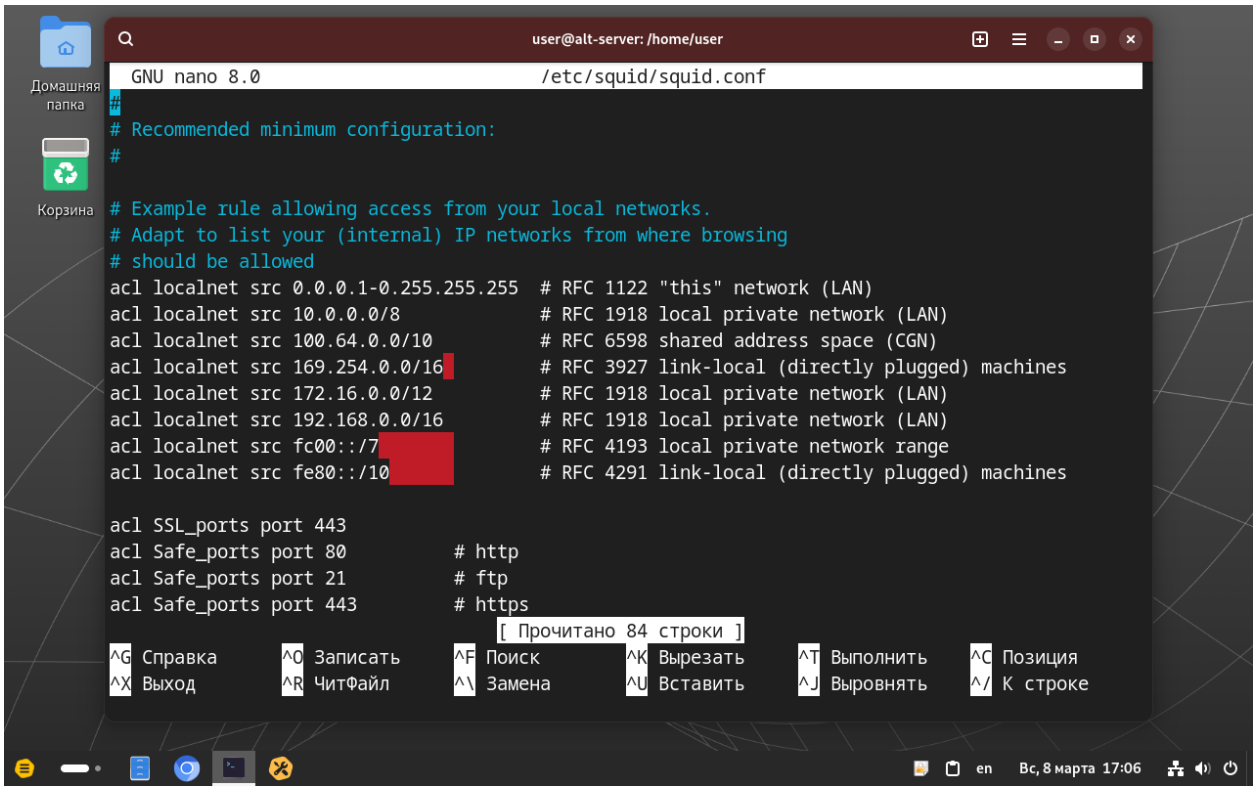

Рис. 2.38. Вид файла конфигурации прокси-сервера Squid по умолчанию

Файл настроек по умолчанию имеет множество различных механизмов, которые при должной настройке могут обеспечить достаточно гибкий контроль работы сервера и доменной сети в целом.

Перейдем к настройке самого сервера, минимальная рабочая конфигурация сервера squid приводится на рис. 2.38.

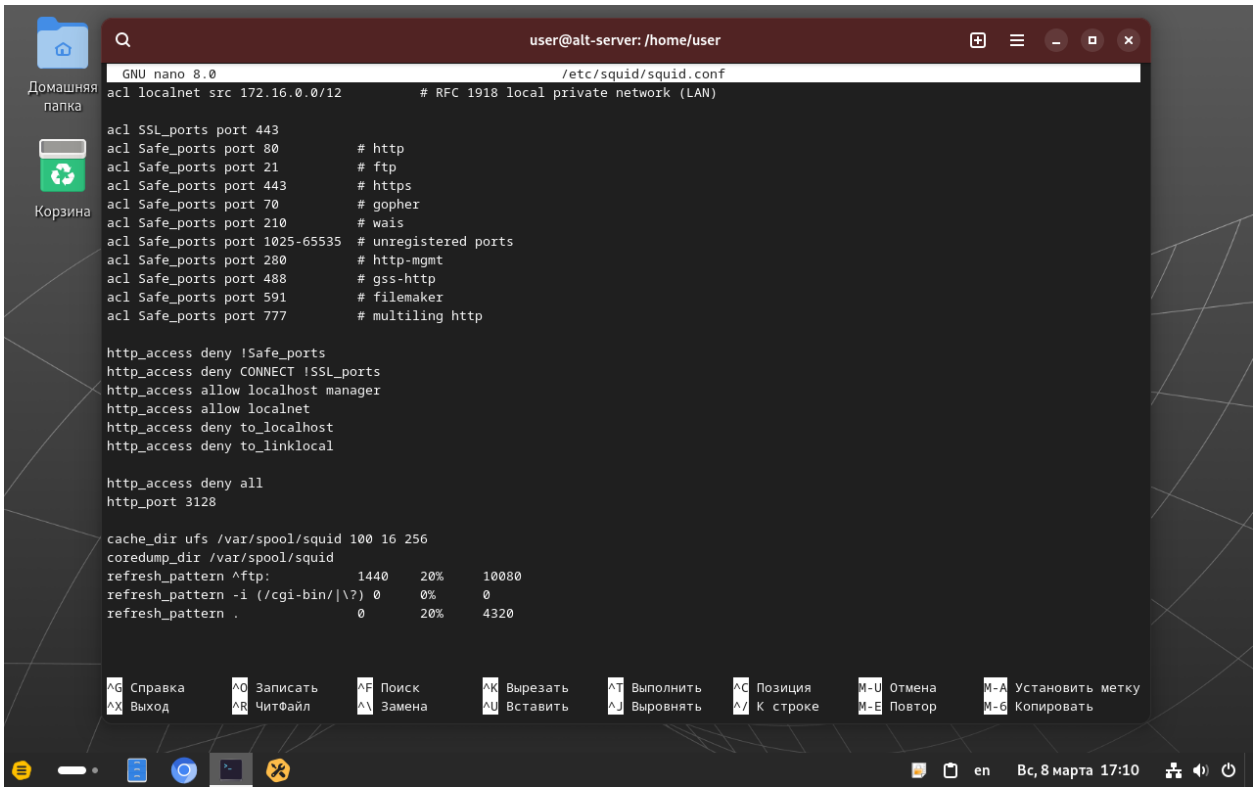

Рис. 2.39. Минимальная рабочая конфигурация прокси-сервера Squid.

Пояснение работы некоторых параметров настройки программного прокси-сервера squid:

acl localnet src 172.16.0.0/12 - Определяет частную сеть класса B согласно RFC 1918 для идентификации локальной сети;
acl SSL_ports port 443 - Создает список безопасных портов для SSL-туннелей, разрешая CONNECT только на порт 443;
acl Safe_ports port 80 - Добавляет порт HTTP в список разрешенных портов для веб-серфинга;
acl Safe_ports port 21 - Добавляет порт FTP в список разрешенных портов;
acl Safe_ports port 443 - Добавляет порт HTTPS в список разрешенных портов;
acl Safe_ports port 70 - Добавляет порт Gopher в список разрешенных портов;
acl Safe_ports port 210 - Добавляет порт WAIS в список разрешенных портов;
http_access deny !Safe_ports - Запрещает доступ к любым портам, не входящим в список Safe_ports;
http_access deny CONNECT !SSL_ports - Запрещает создание SSL-туннелей на любые порты, кроме указанных в SSL_ports;
http_access allow localhost manager - Разрешает локальному хосту доступ к статистике кэш-менеджера;

http_access deny manager - Запрещает удаленный доступ к статистике кэш-менеджера;
include /etc/squid/conf.d/*.conf - Подключает все конфигурационные файлы из указанной директории;
http_access allow localhost - Разрешает локальному хосту использовать прокси-сервер;
http_access deny all - Запрещает доступ всем остальным клиентам (правило по умолчанию);
http_port 3128 - Указывает порт 3128 для прослушивания входящих клиентских соединений;
coredump_dir /var/spool/squid - Задает директорию для сохранения дампа памяти при критическом сбое;
refresh_pattern ^ftp: 1440 20% 10080 - Устанавливает правила кэширования для FTP-объектов (мин 1440 мин, макс 10080 мин);
refresh_pattern ^gopher: 1440 0% 1440 - Устанавливает правила кэширования для Gopher-объектов;
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0 - Запрещает кэширование динамических страниц с CGI-скриптами или параметрами в URL;
refresh_pattern . 0 20% 4320 - Устанавливает правила кэширования по умолчанию для всех остальных объектов (макс 4320 мин).

После того, как произведена минимальная настройка прокси сервера следует выполнить создание директорий и файлов, в которые будет попадать кэш пользователей и их сеансов, но перед этим нужно полностью остановить сервис прокси-сервера squid, остановку можно сделать командой «**systemctl stop squid**», затем перейдем непосредственно к созданию папок: сделать это можно при помощи команды «**sudo squid -z**», sudo в данном случае вводится даже при использовании учетной записи супер-пользователя root, в противном случае система выдаст вам сообщение о том, что такой команды не существует.

Когда папки созданы, конфигурация завершена и сервис остановлен, можно записать squid в автозагрузку и сразу же выполнить запуск: «**systemctl enable --now squid**». Для убеждения в том, что сервис действительно готов к работе, можно проверить, заняты ли порты прокси-сервера нашей установкой squid, для этого выполним команду «**lsof -i :3128**», где 3128 – порт, настроенный ранее в файле конфигурации, по умолчанию это порт 3218. (рис. 2.39)

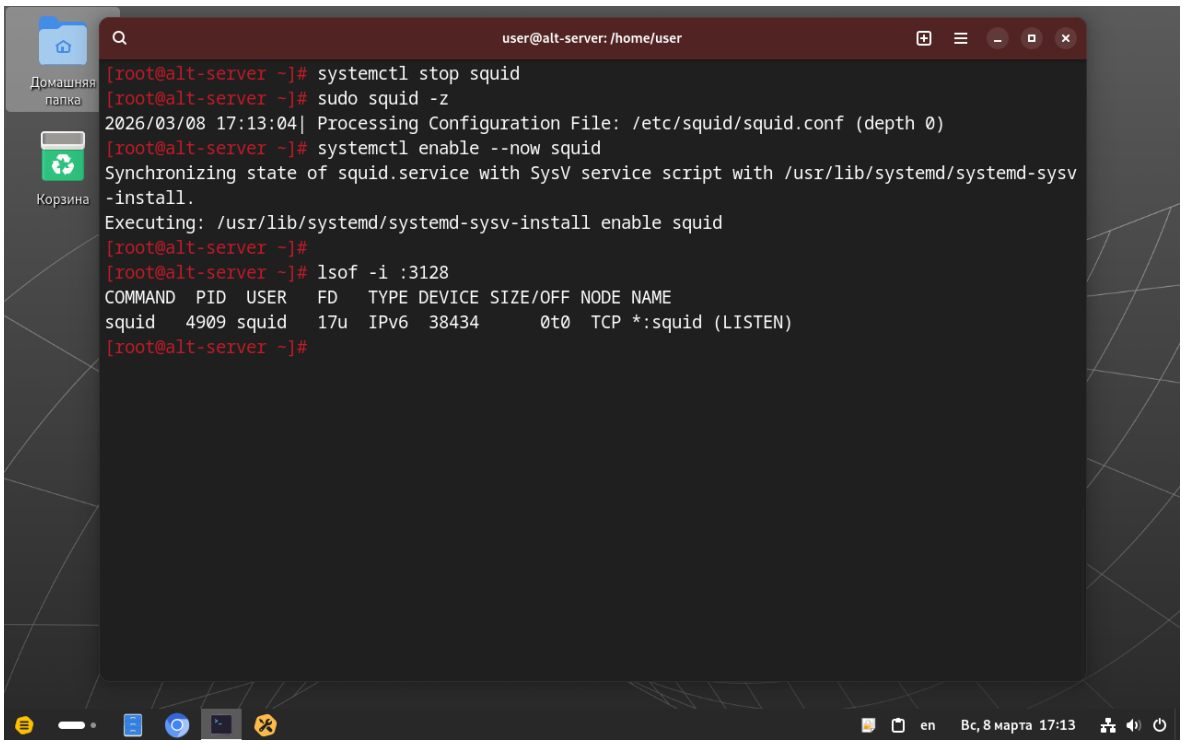

Рис. 2.40. Процесс запуска прокси сервера squid

После первоначальной настройки прокси-сервера Squid и его запуска, добавим в него, заявленную выше, авторизацию по логину и паролю. Для осуществления функционала вновь откроем файл конфигурации сервера squid. (напомним, что для этого используется команда «**nano /etc/squid/squid.conf**»)

Добавим некоторые параметры в файл: рис. 2.40:

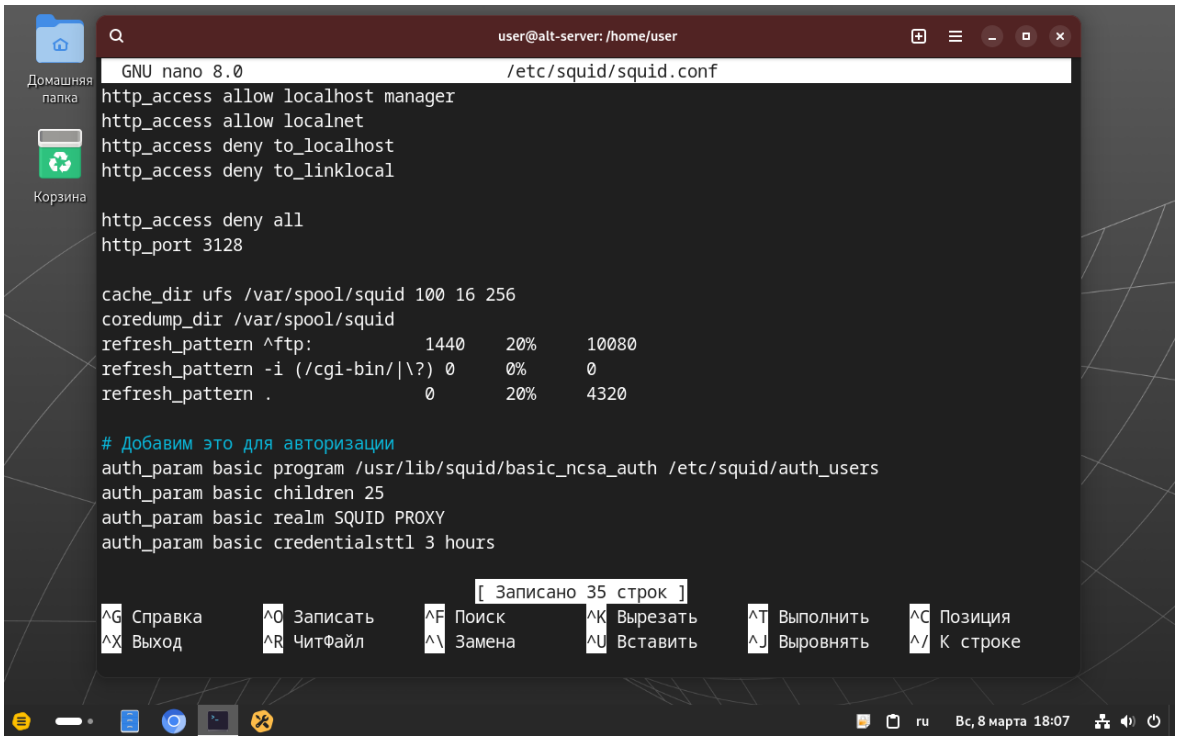

Рис. 2.41. Параметры проверки авторизации прокси-сервера squid

Где:

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/auth_users - Указывает путь к программе аутентификации Basic NCSA и файлу с паролями пользователей;

auth_param basic children 25 - Задает максимальное количество дочерних процессов-аутентификаторов (25) для обработки запросов авторизации;

auth_param basic realm SQUID PROXY - Определяет текст "SQUID PROXY", который будет отображаться в окне ввода логина/пароля браузера;

auth_param basic credentialsttl 3 hours - Устанавливает время жизни (3 часа) учетных данных в кэше после успешной аутентификации.

*Примечание 25. Пакет squid в репозиториях alt linux не содержит службы управления авторизацией, поэтому необходимо его установить отдельно: «**apt-get install squid-helpers**».*

Теперь мы можем сохранить конфигурацию и перезагрузить прокси-сервер. (напоминаем, что сделать это можно командой «**systemctl restart squid**»).

После сохранения настройки и перезапуска сервиса squid, можно перейти к созданию пользователей прокси: первого пользователя создаем командой: «**htpasswd -c /etc/squid/auth_users user1**», последующих пользователей стоит создавать командой «**htpasswd /etc/squid/auth_users user2**» - префикс «-c» в первой команде используется для генерации файла учета пользователей (рис. 2.41).

Примечание 26. Сам по себе прокси сервер squid не имеет встроенного веб-интерфейса для управления, поэтому зачастую администрируется прямо из терминала самого сервера, но сообщество пользователей создало большое количество своих (внешних) веб-интерфейсов для управления сервисом, одним из которых может выступать веб-панель для управления сервером Webmin, этот продукт ориентирован на администрирования различных ролей сервера от dhcp, dns, proxy до серверов печати (cups), почты (postfix), мониторинга (zabbix), контроллеров домена (samba-dc), программных RAID массивов (mdadm) и пр.

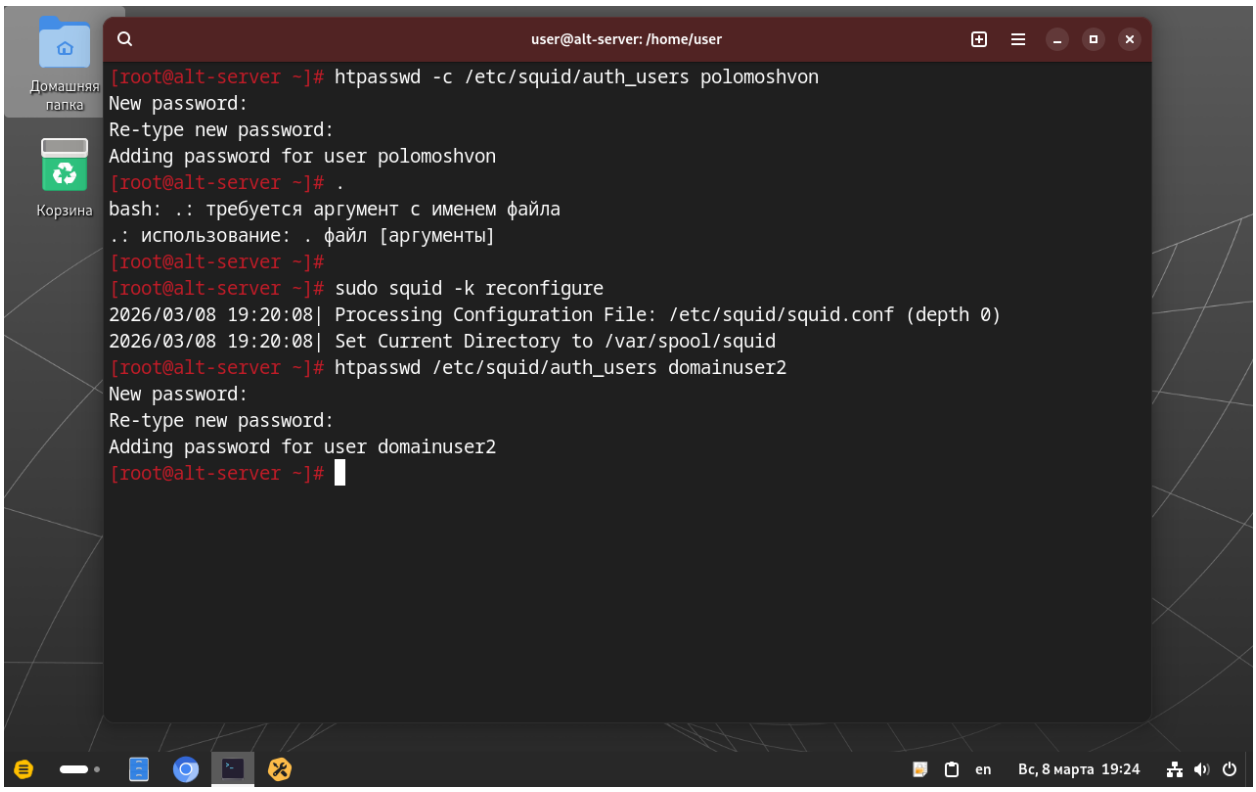

Рис. 2.42. Создание пользователей для прокси сервера

После добавления новых пользователей всегда обновляйте работу прокси сервера либо командой «**squid -k reconfigure**», либо «**systemctl restart squid**», заметим, что вторая команда может повлечь за собой прерывание всех уже поднятых (начатых) сессий (актуально для тех случаев, когда сервер уже настраивался ранее и используется реальными пользователями в настоящее время), вторая же просто обновляет записи без перезапуска самого сервиса squid.

Теперь можно считать, что настройка фильтрующе-кэширующего прокси-сервера squid с поддержкой идентификации пользователей завершен, проверка сервера показана в разделе 4.1.4 данного методического пособия.

Некоторые выводы из Раздела 2. «Администрирование сервера»

В разделе 2 нами была выполнена настройка сетевых служб в корпоративной среде, рассматривались следующие компоненты:

2.1 Базовая настройка сети: На первом этапе была выполнена настройка статической адресации на сервере. Это обеспечивает фиксированный IP-адрес, необходимый для корректной работы всех остальных служб и их доступности для клиентов.

2.2 Настройка DHCP-сервера (ISC DHCP Server): Развернут и настроен DHCP-сервер для автоматической выдачи клиентам сети IP-адресов и параметров конфигурации (шлюз, DNS-серверы). Это позволило централизованно управлять сетью и упростить подключение клиентских машин.

2.3 Развертывание контроллера домена (Samba DC): Установлен и настроен контроллер домена на базе Samba в режиме Active Directory. Это создало основу для централизованной аутентификации пользователей, управления политиками безопасности и организации единого доменного окружения.

2.3.1 Настройка DNS-сервера (Samba DNS): В процессе настройки контроллера домена был автоматически развернут встроенный DNS-сервер Samba. Он обеспечивает разрешение имен в домене, необходимое для работы Active Directory, и позволяет клиентам находить доменные службы.

2.4 Настройка файлового сервера (Samba): На базе Samba организован файловый сервер с сетевыми папками. Доступ к ресурсам разграничен на основе доменных групп пользователей, что обеспечивает централизованное хранение данных и совместную работу.

2.5 Настройка прокси-сервера (Squid): Установлен и настроен прокси-сервер Squid. Он обеспечивает контроль и фильтрацию web-трафика, кэширование данных для ускорения доступа в интернет, а также средства аутентификации для идентификации пользователей.

Раздел 3. Работа с клиентскими машинами

Данном разделе методического пособия будет разобран процесс установки операционных систем windows 10 и alt workstation 11 в качестве клиентских машин для последующей интеграции их с ранее развернутым сервером.

Разберем на примере:

3. Microsoft Windows 10 – данная операционная система была выбрана в виду того, что она и по сей день продолжает работать в подавляющем большинстве на пользовательских конечных машинах и хостах. Не ниже редакции «Про» (подходят: Про, Корпоративная и Корпоративная с долгосрочной поддержкой, а также для образовательный учреждений), редакция «Домашняя» не подойдет под наши задачи: как минимум она не поддерживает присоединение к домену Active Directory, аналогичная ситуация с windows 7 и windows 8;
4. BaseAlt Linux 11 – операционная система семейства BaseAlt СПО, которая входит в экосистему программного обеспечения «Базальт СПО». Входит в реестр отечественного программного обеспечения.

3.1. Работа с системой Windows

3.1.1. Создание виртуального окружения для windows 10

Для создания новой виртуальной машины под клиента на базе ОС Windows перейдем к созданию новой ВМ в virtual box (Рис. 3.1)

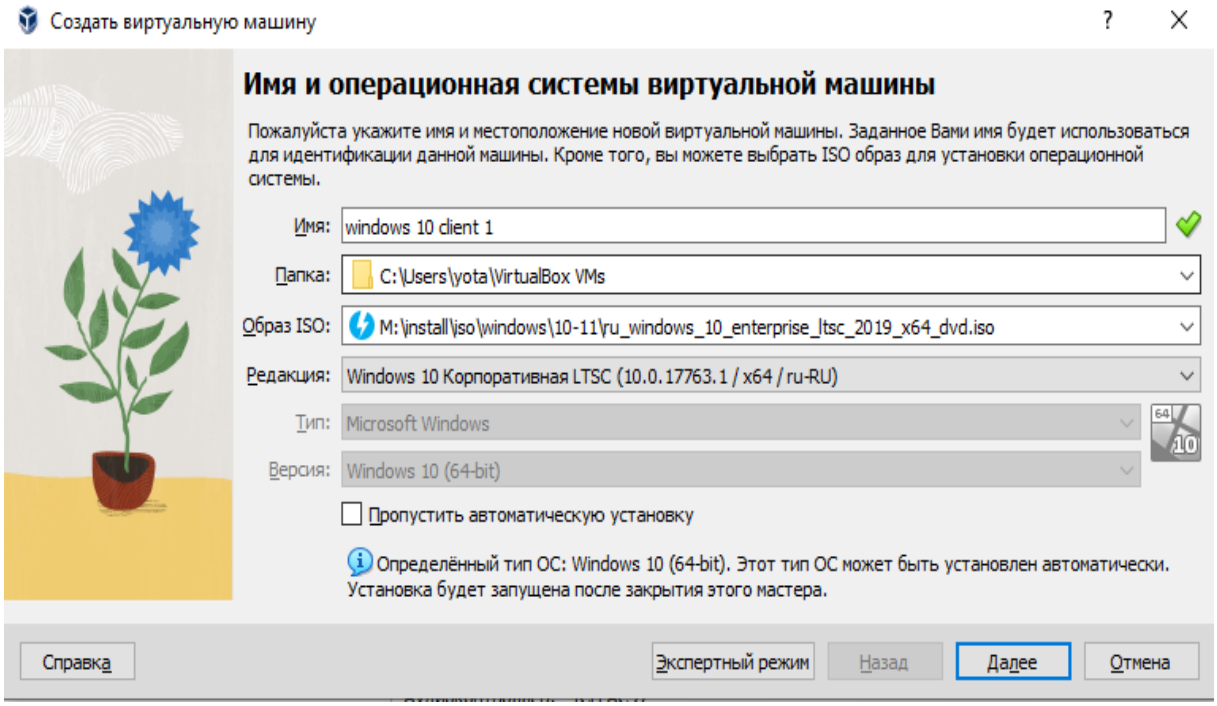

Рис. 3.1. Создание ВМ под клиентское окружение Windows

Затем поэтапно выполним все шаги создания, аналогично с разделом 1. Ниже приводится сами шаги (Рис. 3.2 – Рис 3.5)

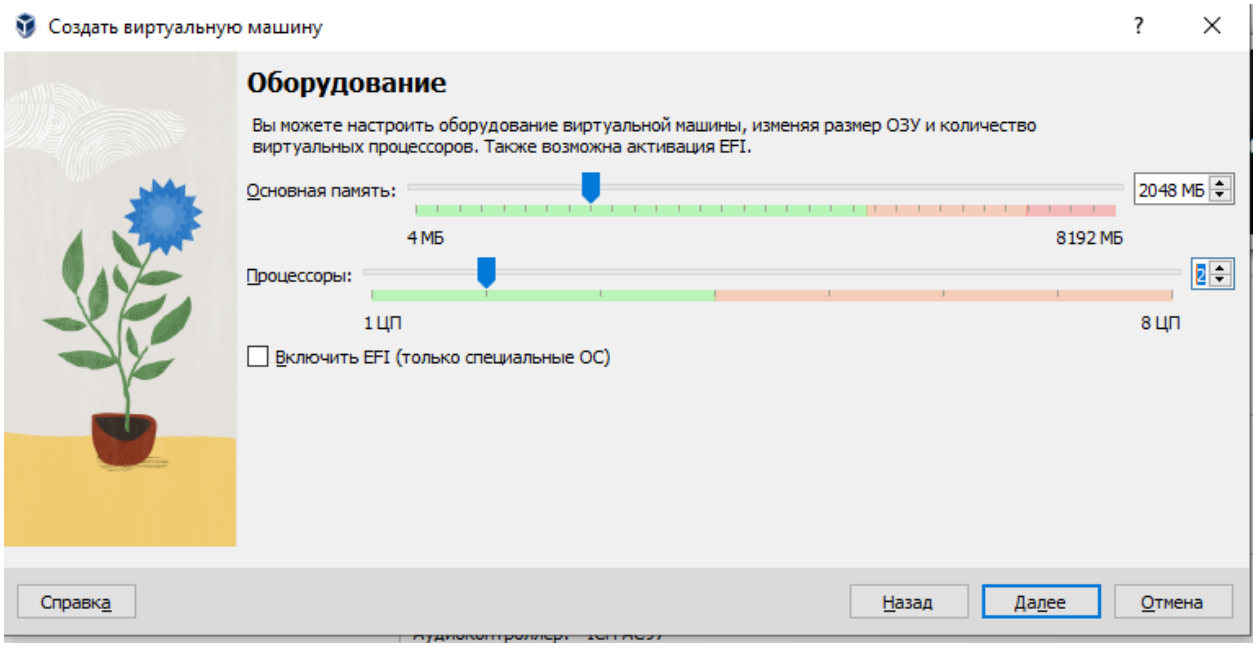

Рис. 3.2. Определение доступных ресурсов ОЗУ и ЦП

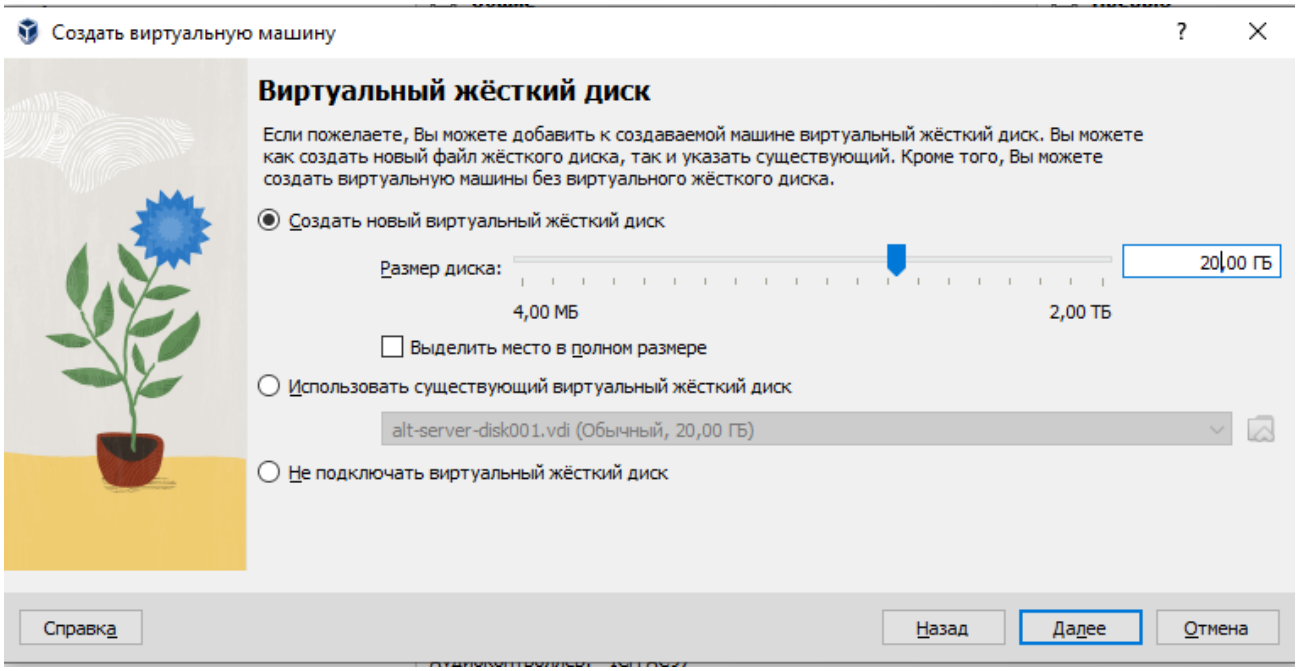

Рис. 3.2. Определение размера жесткого диска

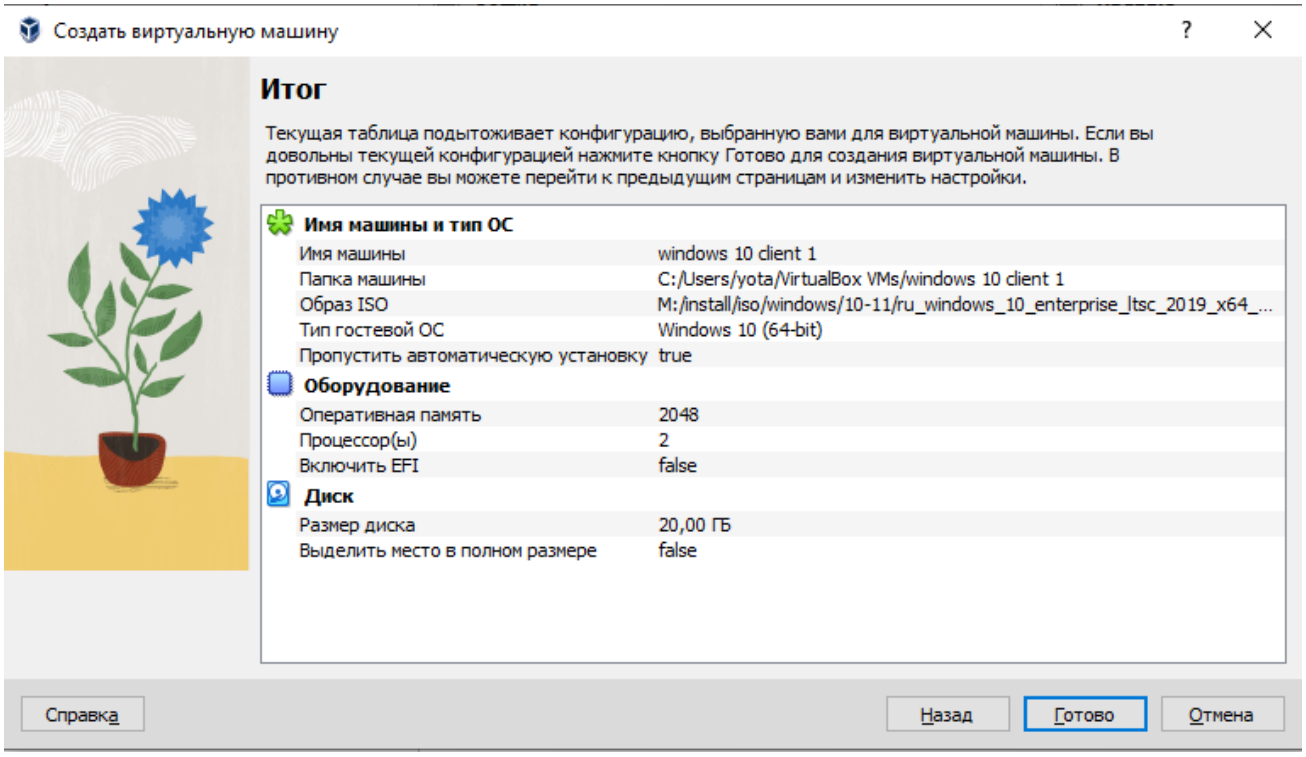

Рис. 3.4. Краткие сведения о создаваемой виртуальной машине

После того, как виртуальная машина создана, можно перейти к настройке её сетевых интерфейсов, а после непосредственно к запуску и установке самой ОС.

3.1.2. Предварительные настройки виртуальной машины

Для того, чтобы созданная ВМ и ранее развернутый сервер могли взаимодействовать друг с другом, необходимо настроить их сетевые интерфейсы, т.к. ранее уже был настроен сетевой интерфейс сервера, теперь настроим сетевой интерфейс клиента.

Перейдем в настройки ВМ в раздел «Сеть» рис. 3.5.

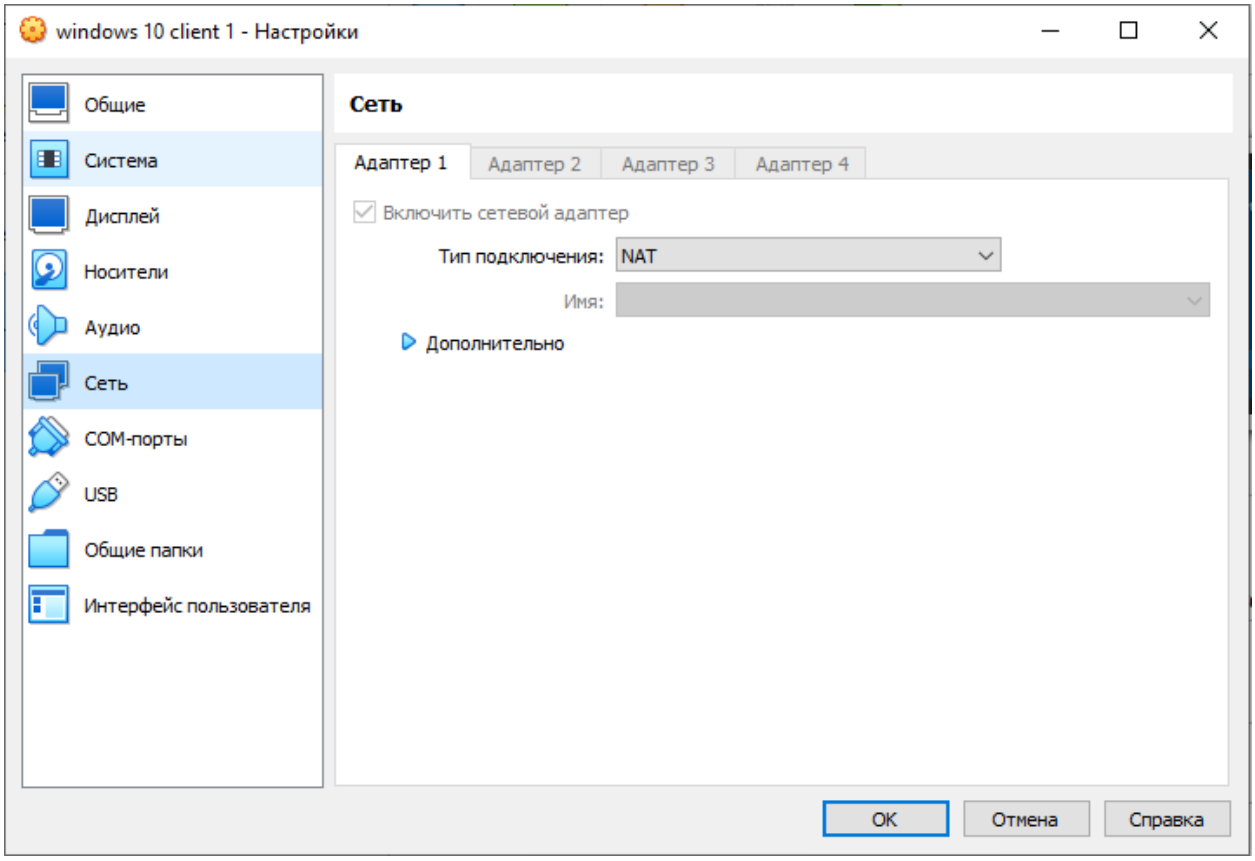

Рис. 3.5. Окно конфигурации сети виртуальной машины

Для обеспечения связности между сервером (в нашем случае BaseAlt 11) и клиентом (в нашем случае Windows 10) активируем сетевой протокол «Внутренняя сеть» вместо протокола «NAT». Рис. 3.6. После чего зафиксируем конфигурацию ВМ нажатием на кнопку «ОК».

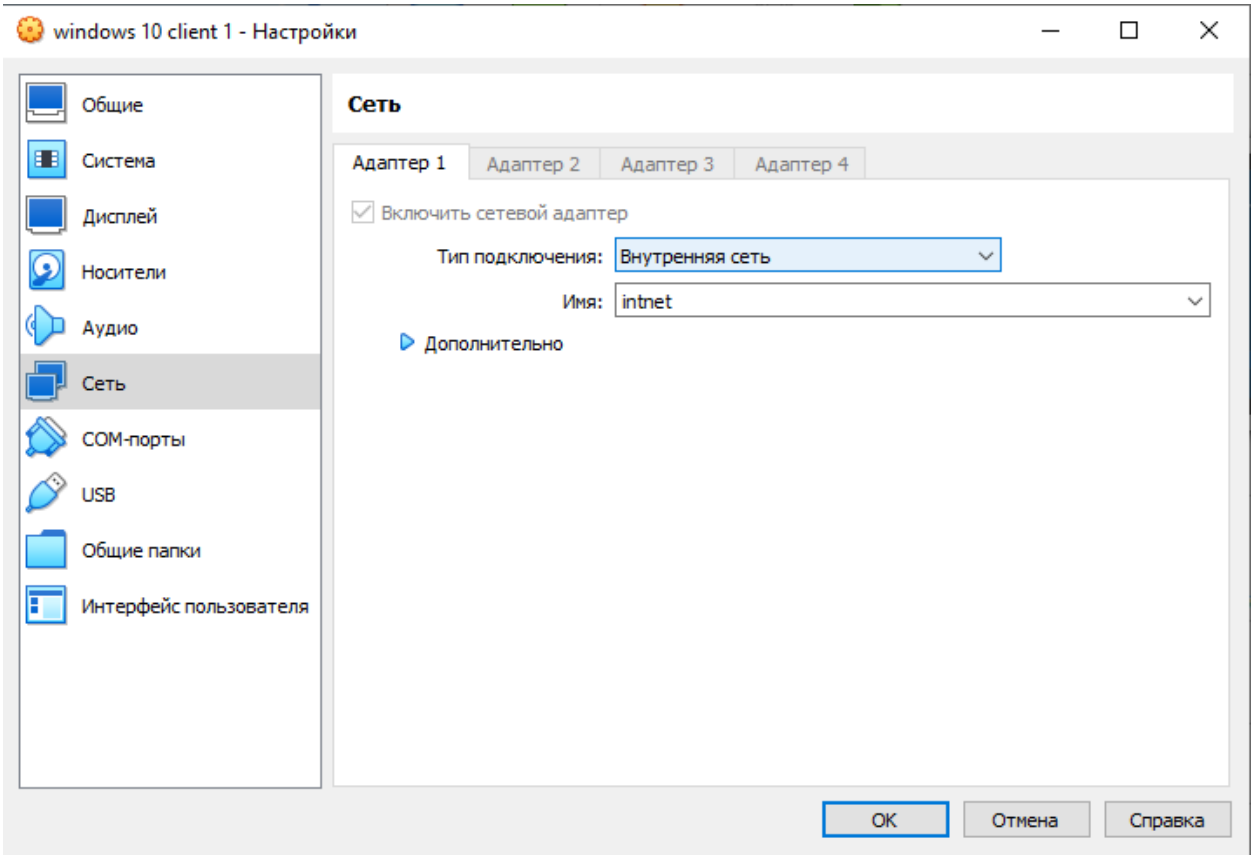

Рис. 3.6. Изменение настроек сетевого адаптера ВМ

После проделанных действий можно закрывать окно конфигурации виртуальной машины и переходить к этапу установки операционной системы на созданную и настроенную машину.

3.1.3. Установка операционной системы Microsoft Windows 10

Теперь, когда ВМ создана и сеть в ней настроена, можно перейти к установке операционной системы Microsoft windows 10, в нашем случае будет использовать редакция Windows 10 Enterprise 2019 LTSC, что означает долгосрочную поддержку (аж 10 лет), а также отсутствие лишних программ, т.е. достаточно чистая операционная система без лишних наворотов.

После запуска ВМ перед вами через некоторое время откроется окно установщика ОС Windows рис. 3.7., в котором мы выбираем нужные нам язык и регион и можно продолжать установку, нажав на кнопку «Далее».

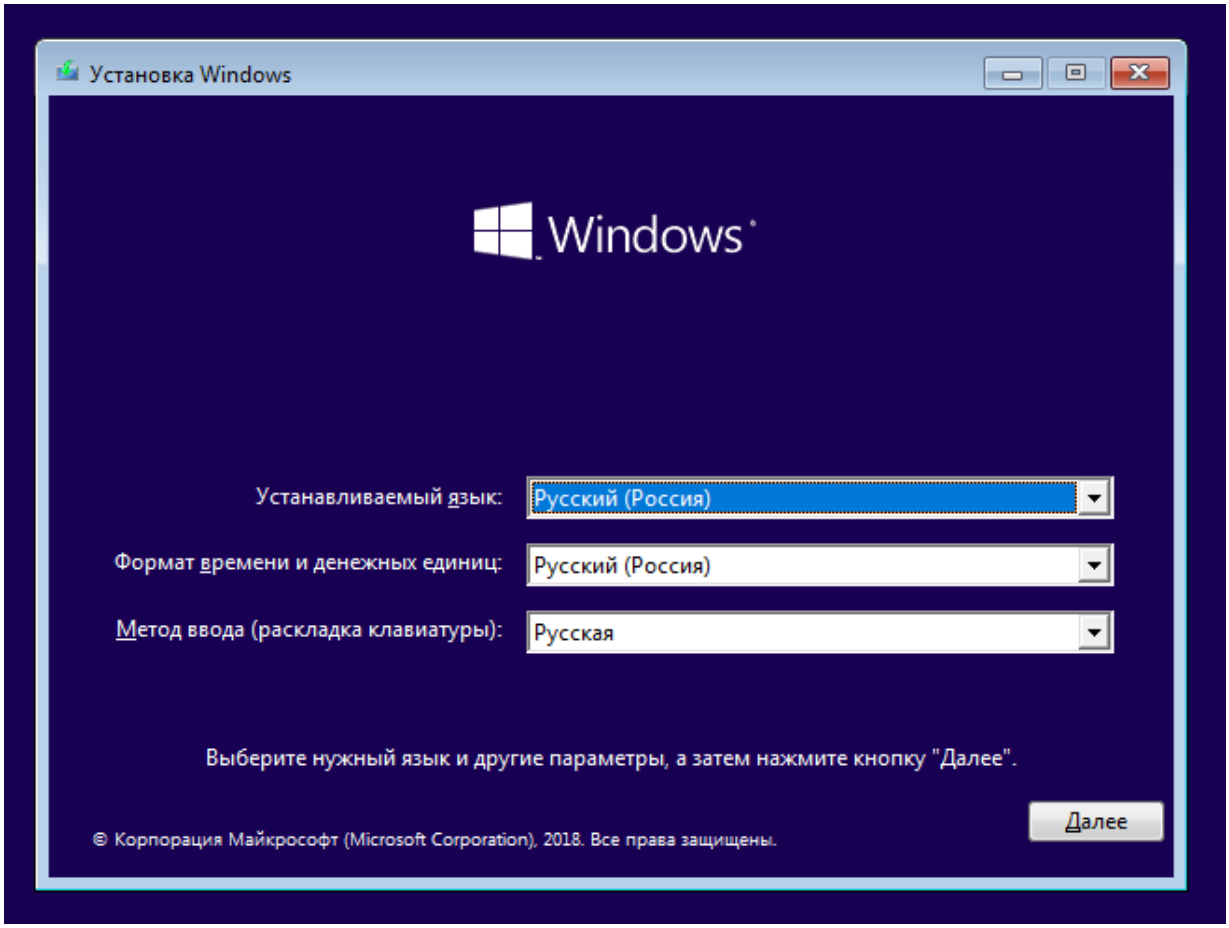

Рис. 3.7. Окно установщика ОС Windows

После перед вами откроется окно выбора действия: выполнить установку ОС (клавиша «Установить») или выполнить восстановление ранее установленной ОС (клавиша «Восстановление системы») рис. 3.8. – мы проводим установку ОС, поэтому нажимаем на «Установить» и движемся далее.

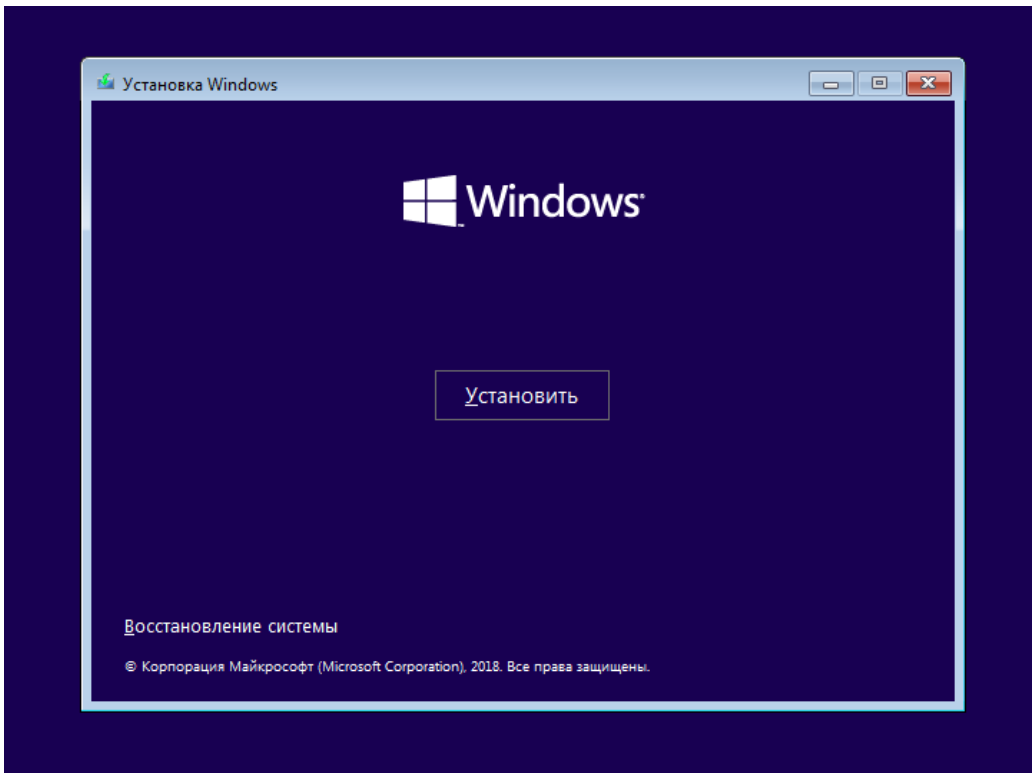

Рис. 3.8. Выбор действия установщика

После перед вами откроется окно лицензионного соглашения пользователя и компании Microsoft, ознакомившись с которым, можно продолжать, в случае согласия или прервать установку, в случае несогласия с соглашением. (рис. 3.9)

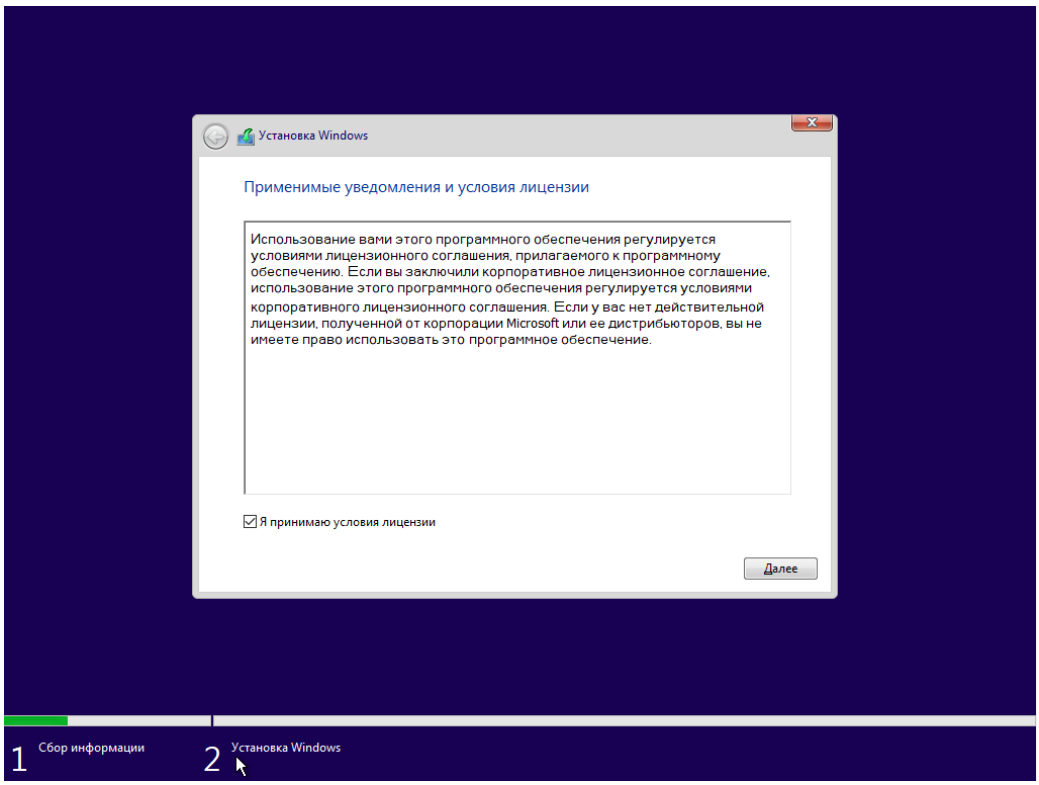

Рис. 3.9. Лицензионное соглашение

Затем откроется окно выбора режима установки: обновление уже имеющейся ОС до новой версии или чистая установка ОС, в нашем случае обновления никакого нет и мы выбираем пункт «Выборочная: только установка Windows (для опытных пользователей)» рис. 3.10.

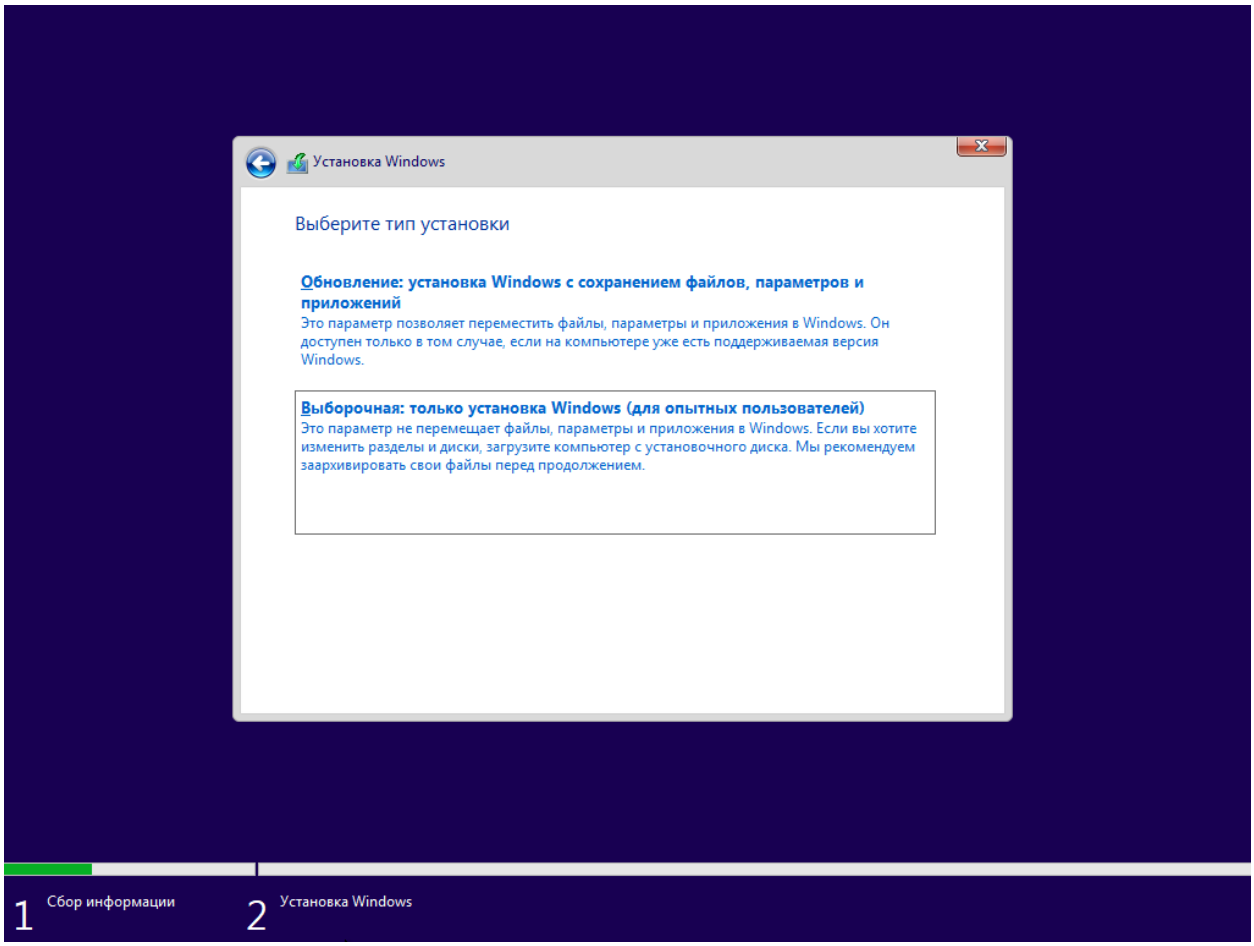

Рис. 3.10. Выбор режима установки ОС

Примечание 27: Режим установки «Обновление» подразумевает под собой наличие какой-либо старой версии windows, отличной от 10 версии, выпущенной до 2019 года, т.к. образ LTSC 2019, например windows 7, 8 или 8.1 до версии windows 10.

После того, как режим установки выбран, переходим к следующему этапу – выбор и разметка жесткого диска рис.3.11.

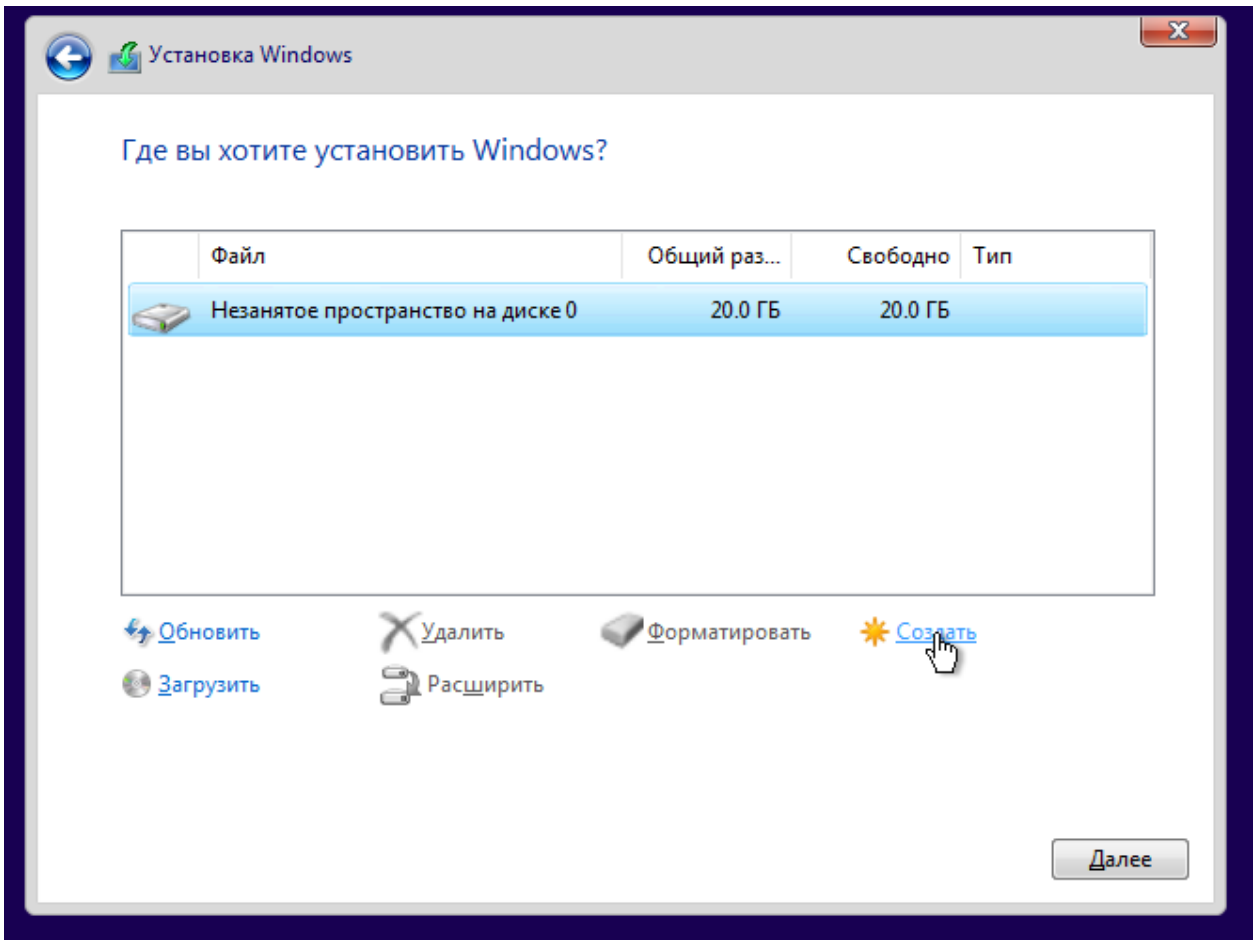

Рис. 3.11. Выбор и разметка жесткого диска hdd или ssd

После того, как выбор сделан в пользу диска 0 с отсутствующей таблицей разметки, можно создать нужные вам разделы с нужным объемом нажатием на клавишу «Создать» - она в автоматическом режиме создаст раздел на диске. Для дальнейшей установки подтвердим наш выбор ответом «ОК» на окно с предупреждением рис.3.12.

Примечание 28. При этом, если у вас ранее была установлена какая-либо ОС на данный жесткий диск, то при создании нового раздела, вся информация, которая содержалась в нем ранее будет безвозвратно удалена. В нашем случае диск уже был пустой, поэтому нам терять нечего.

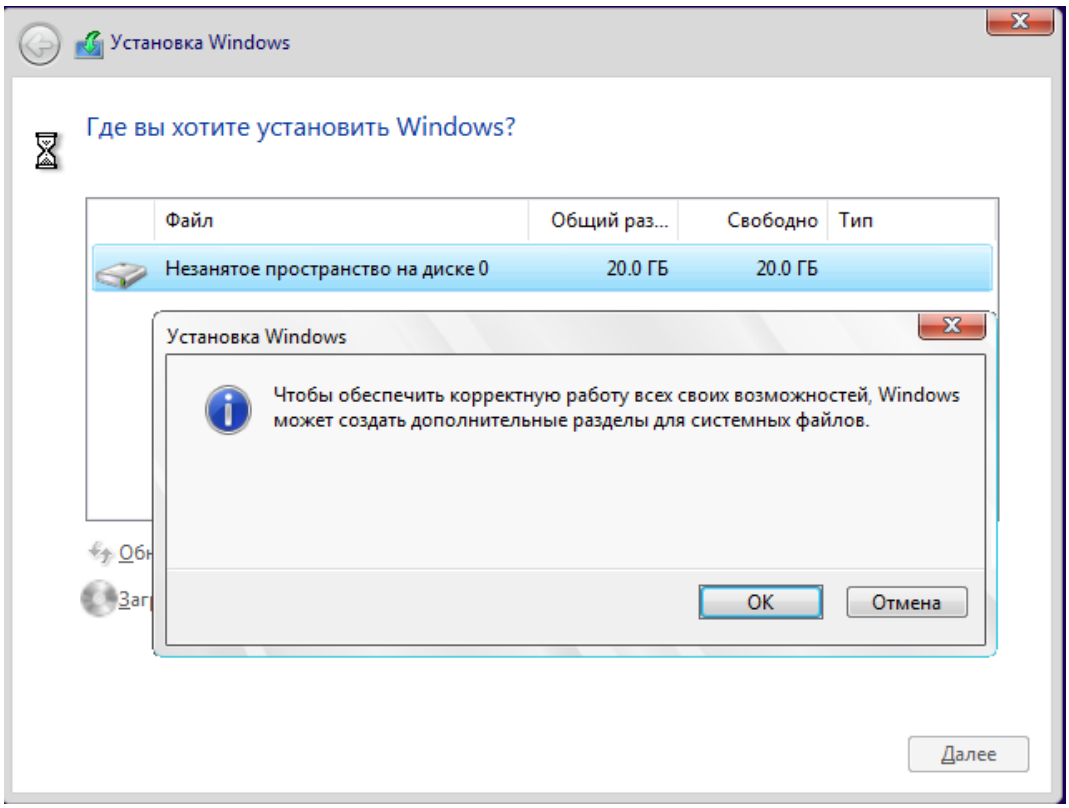

Рис. 3.12. Подтверждение создания раздела на диске

После этого начнется процесс установки операционной системы Windows, который может занять от 5 до 30 минут времени в зависимости от мощности вашего железа рис.3.13.

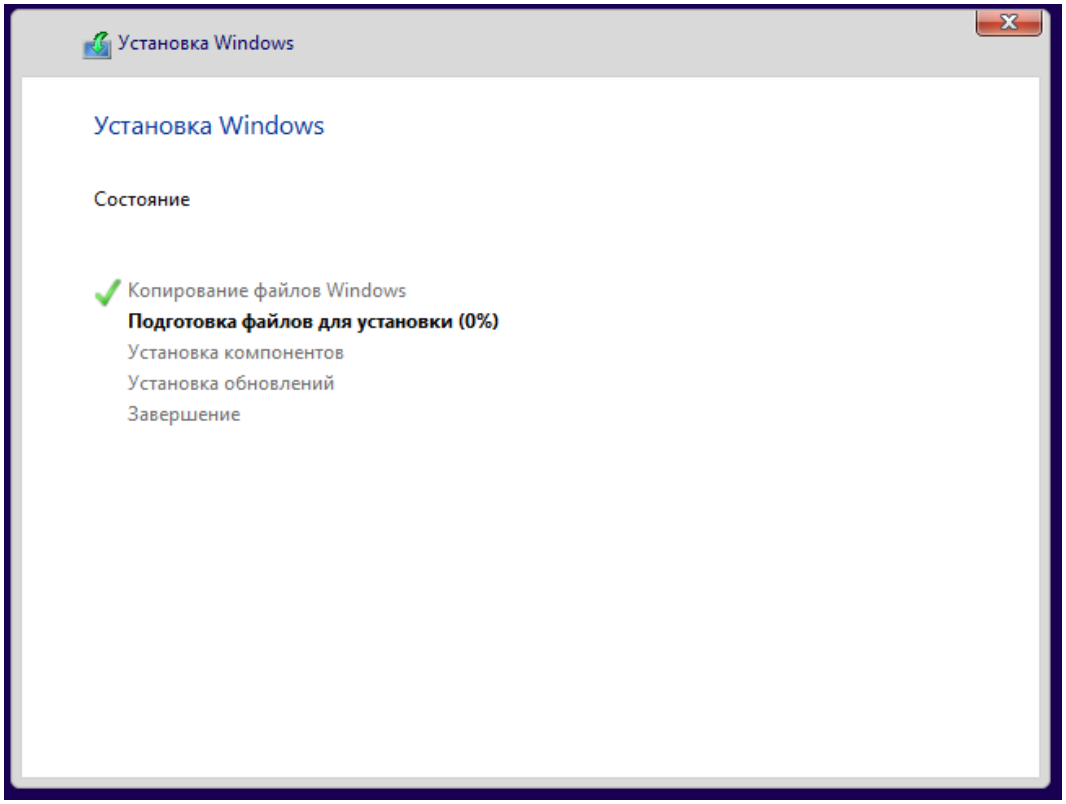

Рис. 3.13. Демонстрация процесса установки ОС Windows

В процессе установки ваш компьютер или виртуальная машина может несколько раз быть перезагружена – это нормальное явление при установке ОС, не паникуйте.

3.1.4. Настройка Windows 10 после установки.

После того, как установка операционной системы завершена (система перезагрузится и после её включения перед вами откроется окно выбора), необходимо настроить некоторые параметры ОС для ее дальнейшего функционирования: выбрать регион размещения (рис. 3.14); раскладка клавиатуры по умолчанию (рис. 3.15); дополнительные раскладки клавиатуры (рис. 3.16); указать параметры сети, если это необходимо (рис. 3.17); задать имя пользователя и пароль (рис. 3.18, рис. 3.19); настроить параметры журнала действий (рис. 3.20); указать параметры конфиденциальности (рис. 3.21); задать параметры обновления ОС (если таковые есть), дождаться создания пользователя (рис. 3.22).

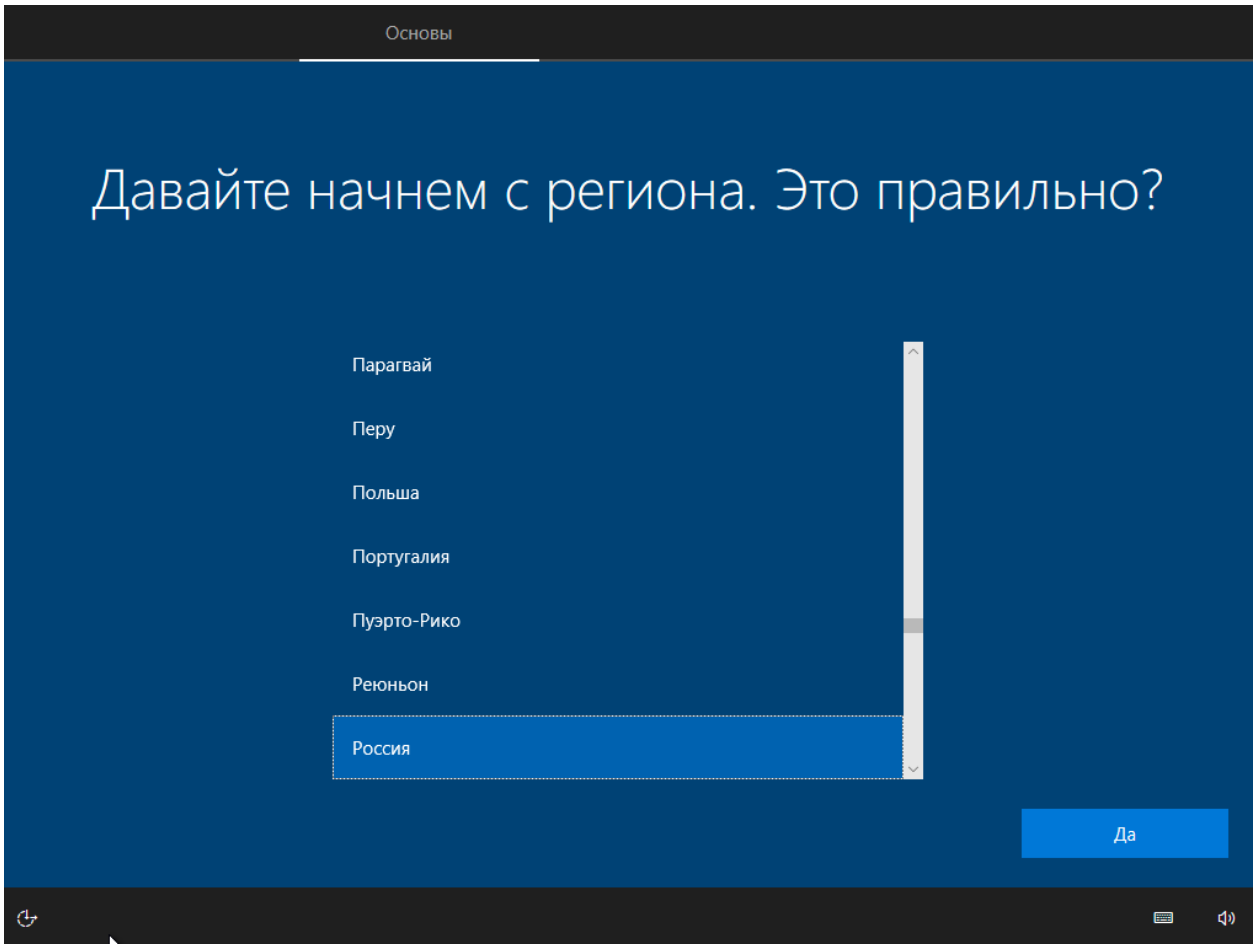

Рис. 3.14. Выбор региона размещения ОС

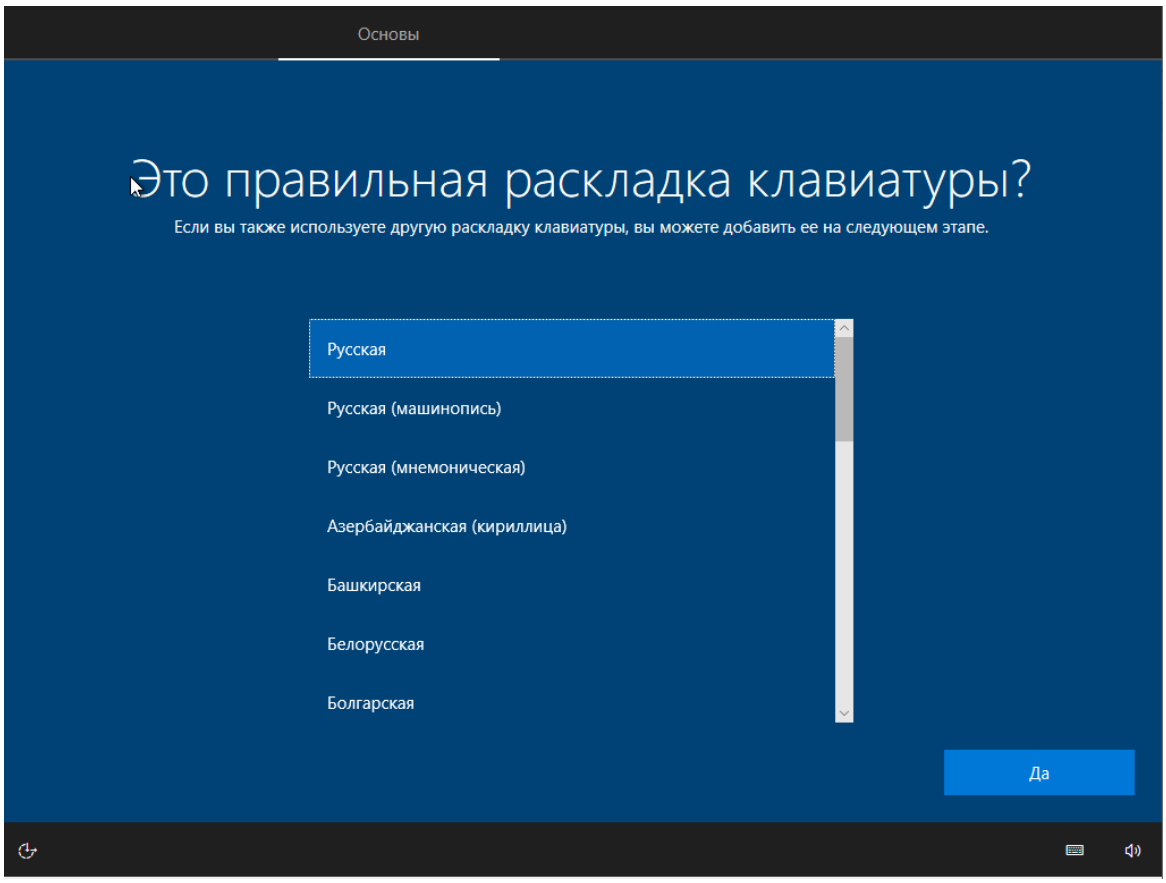

Рис. 3.15. Выбор раскладки клавиатуры по умолчанию

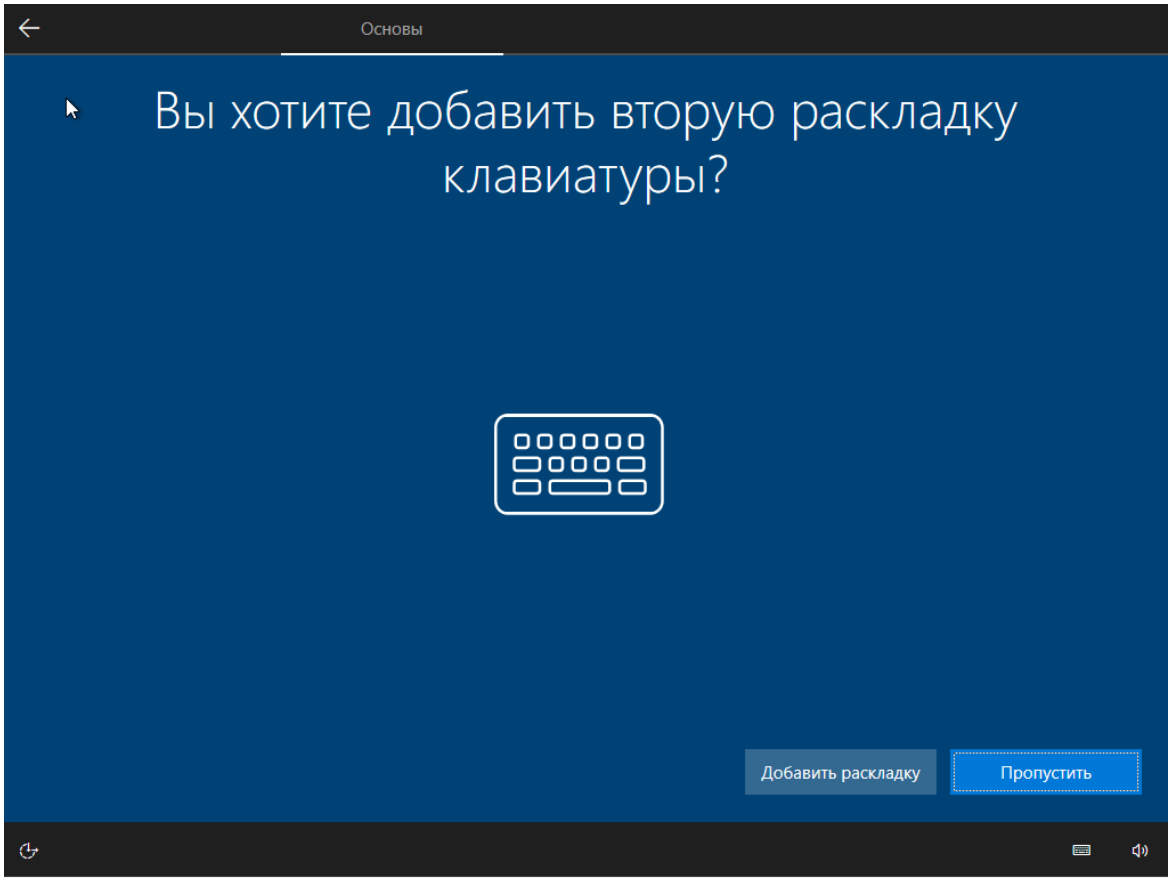

Рис. 3.16. Дополнительные раскладки клавиатуры

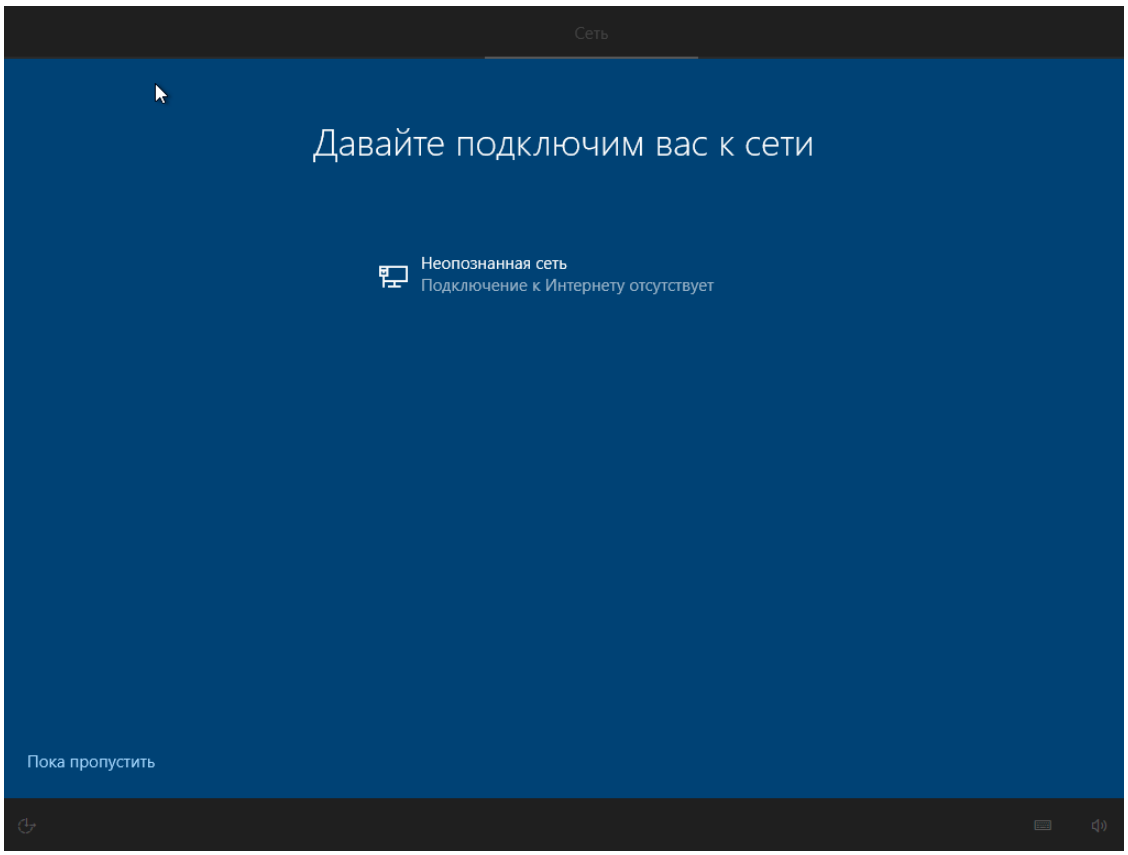

Рис. 3.17. Настройка параметров сети (при необходимости)

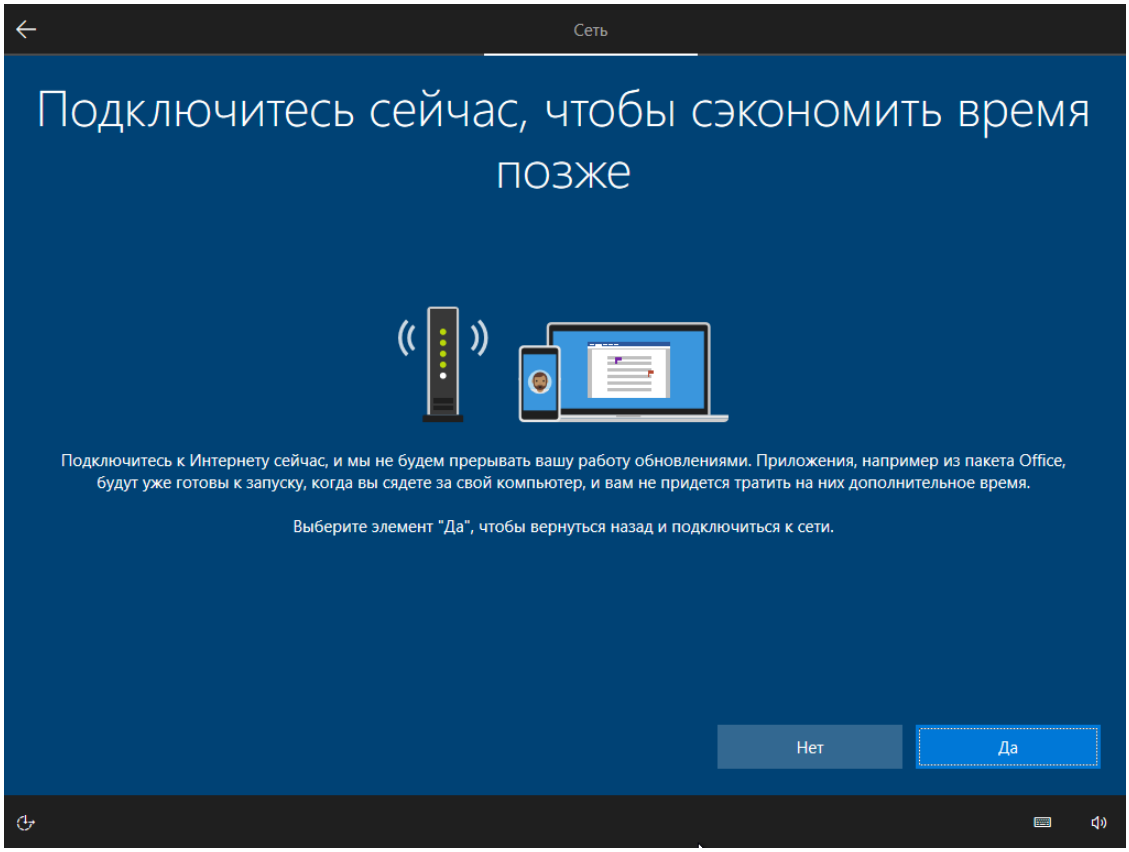

Рис. 3.17.1. Дополнительное подтверждение настройки сети (в случае отказа на рис 3.17)

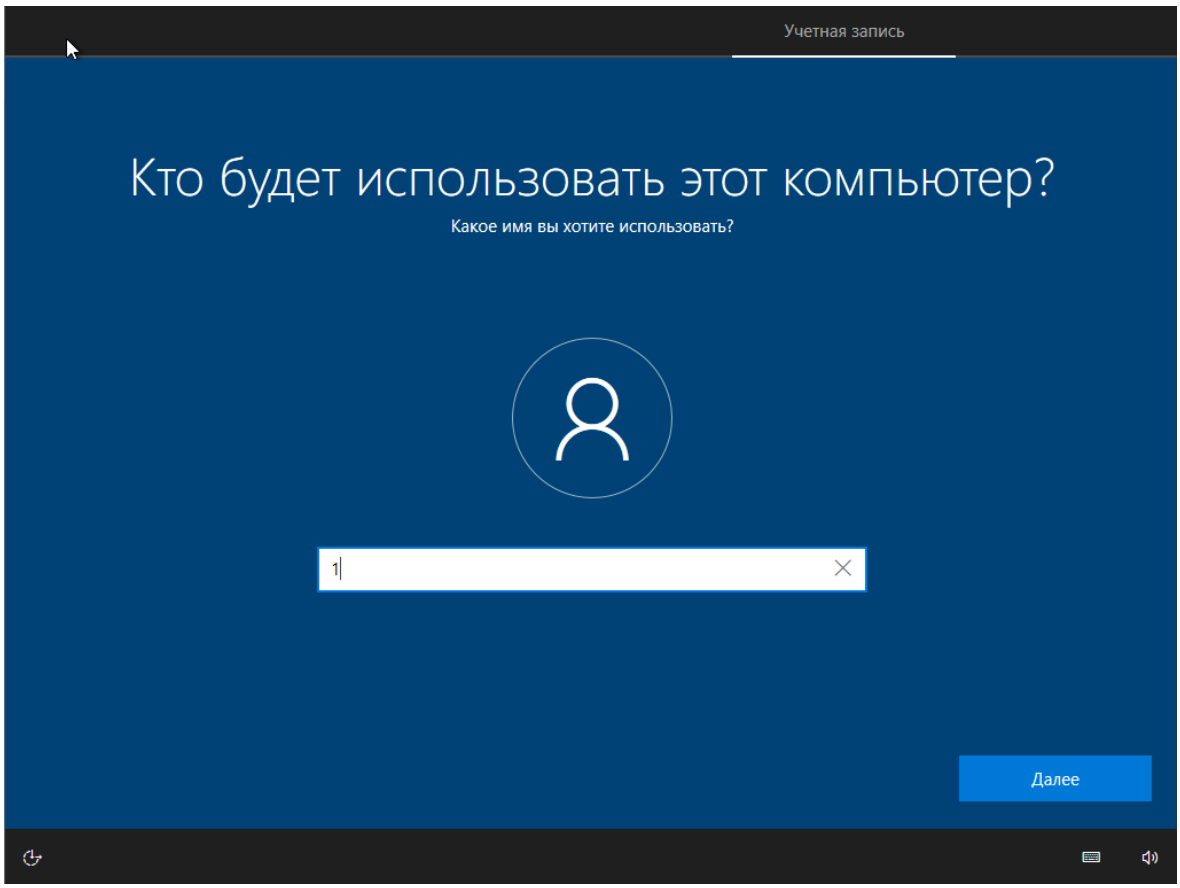

Рис. 3.18. Создание нового пользователя

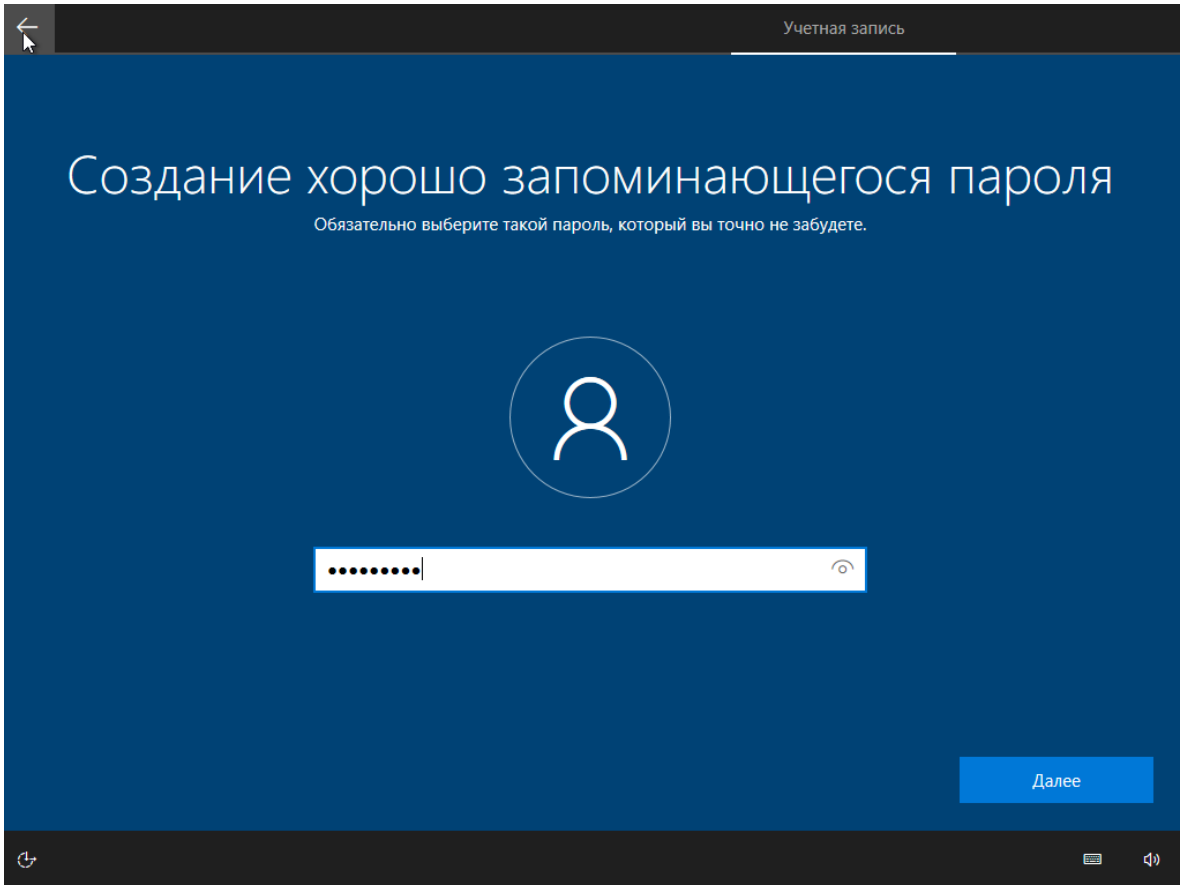

Рис. 3.19. Создание пароля новому пользователю

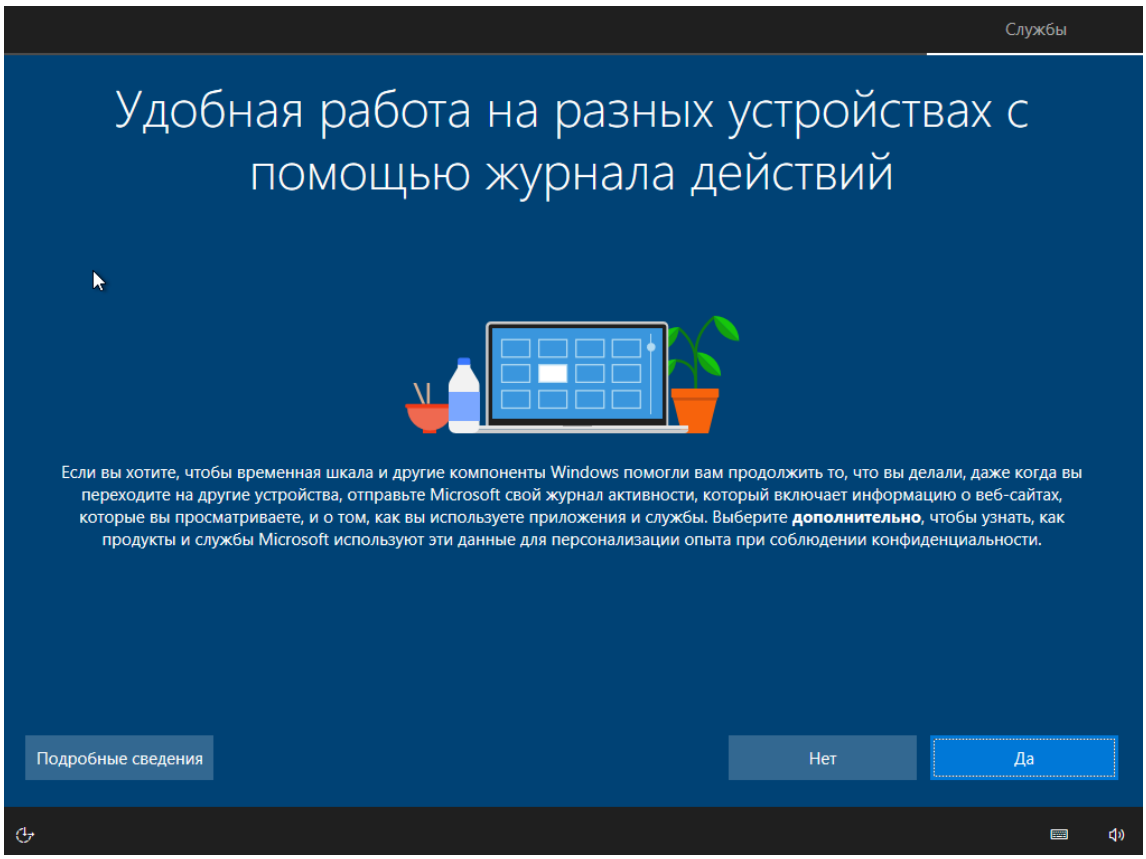

Рис. 3.20. Параметры журнала действий пользователя

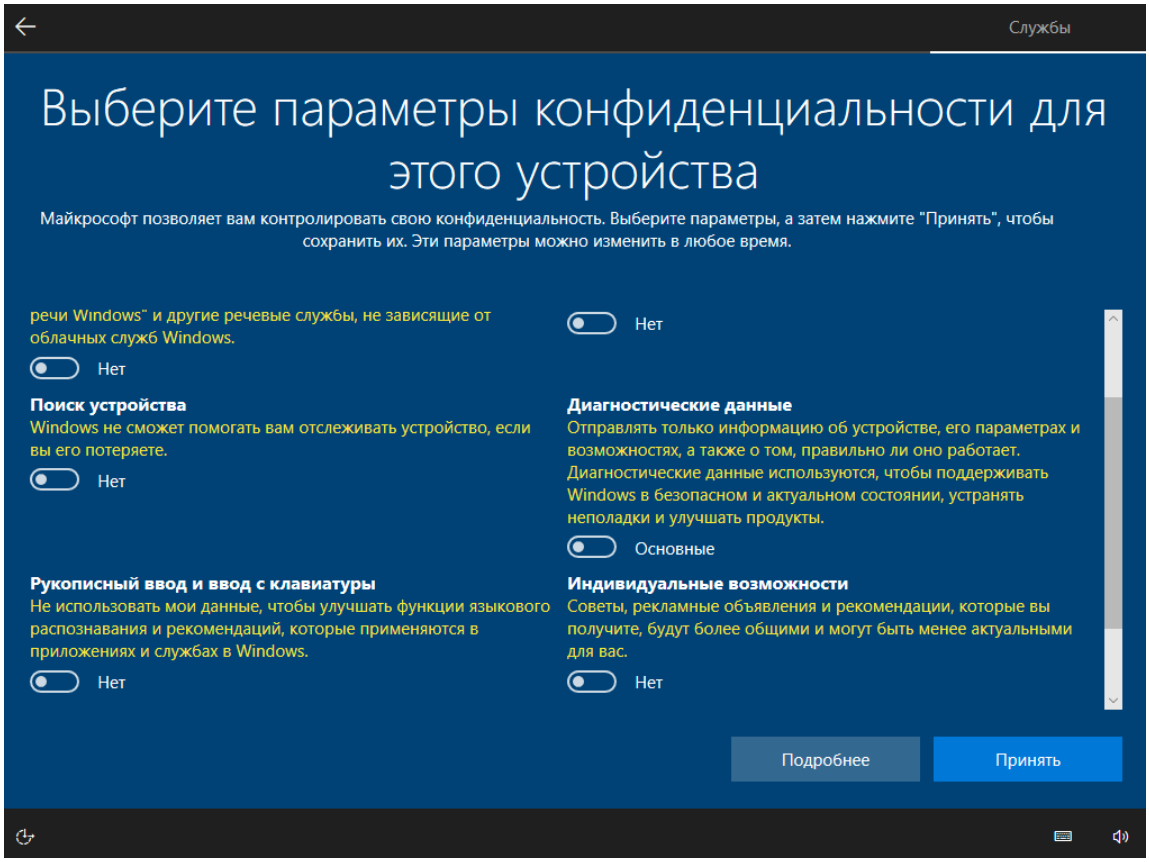

Рис. 3.21. Параметры конфиденциальности

Рис. 3.22. Процесс создания
пользователя и подготовки окружения рабочего стола

После 3-5 минут ожидания перед вами откроется рабочий стол установленной вами операционной системы рис. 3.23. На этом установка windows 10 в качестве клиентской ОС для дальнейшей настройки завершена.

Рис. 3.23. Рабочий стол операционной системы Windows

3.2. Работа с системой BaseAlt Linux 11

3.2.1. Создание виртуального окружения для BaseAlt linux 11

В очередной раз перейдем к созданию виртуальной машины для установки на неё BaseAlt Linux Workstation 11, набор ресурсов будет стандартным: 2 ядра ЦП, 2 ГБ ОЗУ, 20 ГБ жесткого диска. Сводная информация о создании машины приведена на рис.3.24.

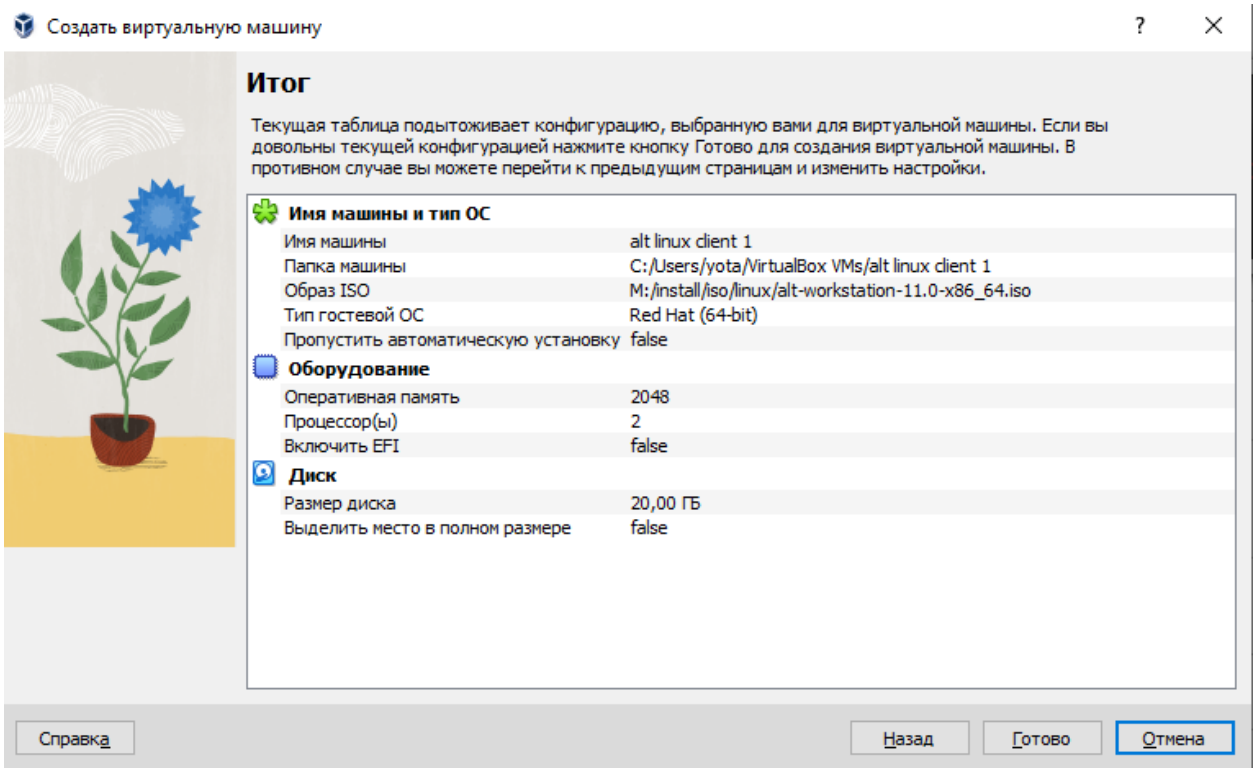

Рис. 3.24. Создание ВМ под клиента linux

Аналогичным разделу 3.1.2 «Предварительные настройки сети ВМ» для клиента на базе ОС BaseALT Linux Workstation 11 переключим сетевой адаптер из режима «NAT» в режим «Внутренняя сеть» для организации связности между основным сервером и клиентом linux, а также для взаимодействия клиентов windows и linux между собой.

3.2.2. Установка операционной системы BaseAlt Workstation 11

После создания ВМ переходим к установке самой ОС, запускаем машину и указываем путь к установочному образу если он не был выбран ранее, затем происходит загрузка с установочного диска рис. 3.25. Выбираем пункт «Установка ALT Workstation 11.0»

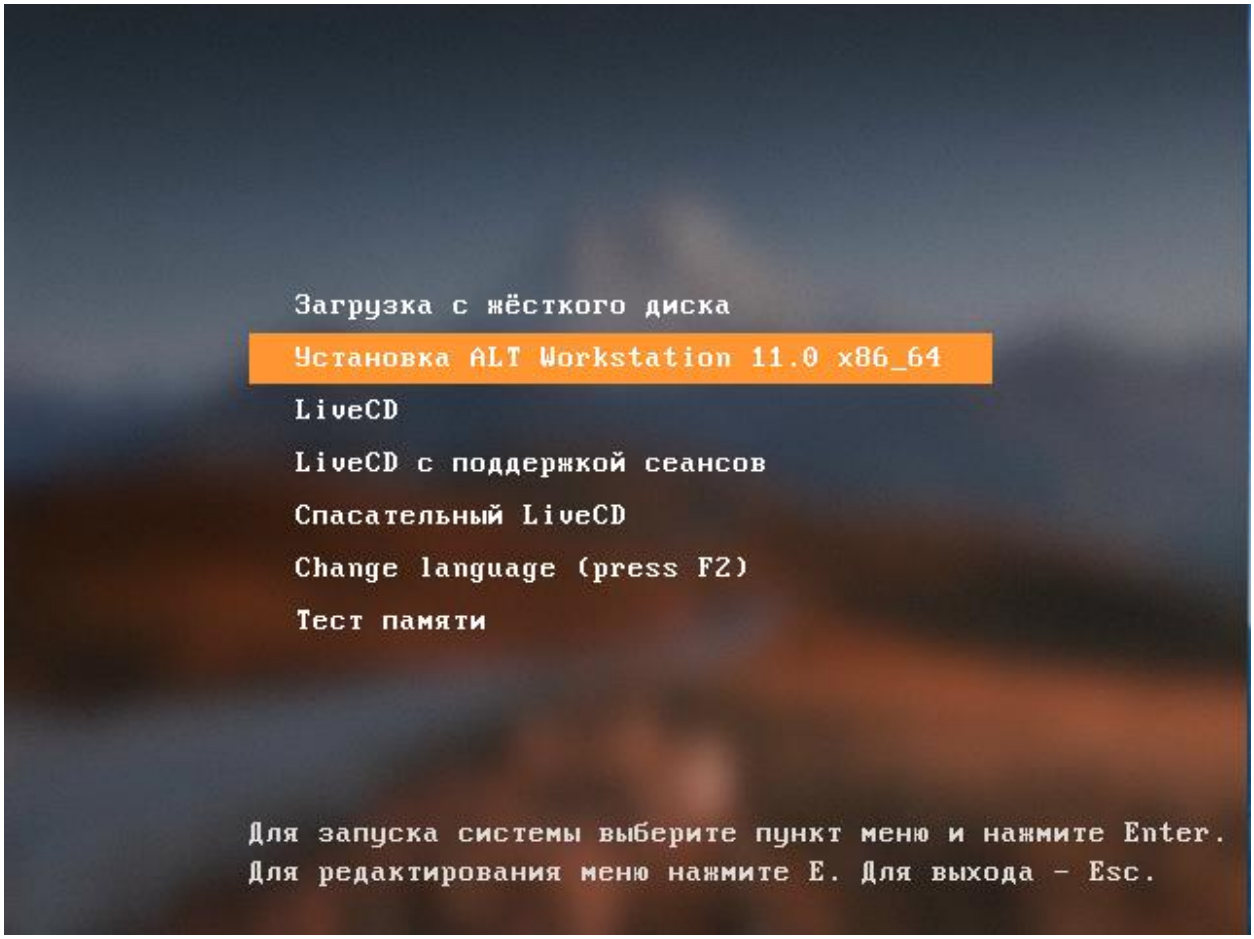

Рис. 3.25. Загрузчик установочного образа

Через некоторое время будет запущена графическая оболочка (в процессе загрузки перед вами может выйти окно загрузки рис 3.26), позволяющая провести установку в достаточно простом режиме рис. 3.27., где первым этапом будет выбор локали (языка) будущей установки.

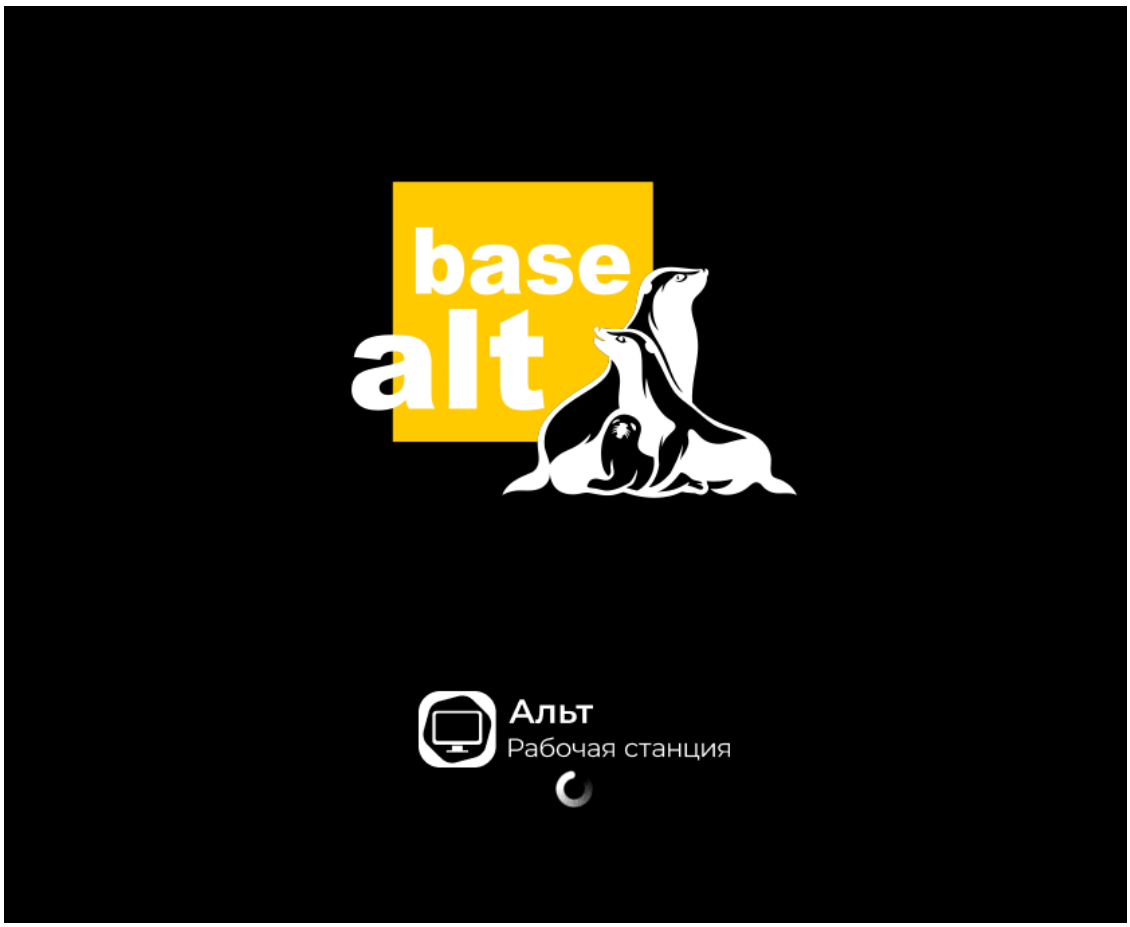

Рис. 3.26. Процесс загрузки установщика

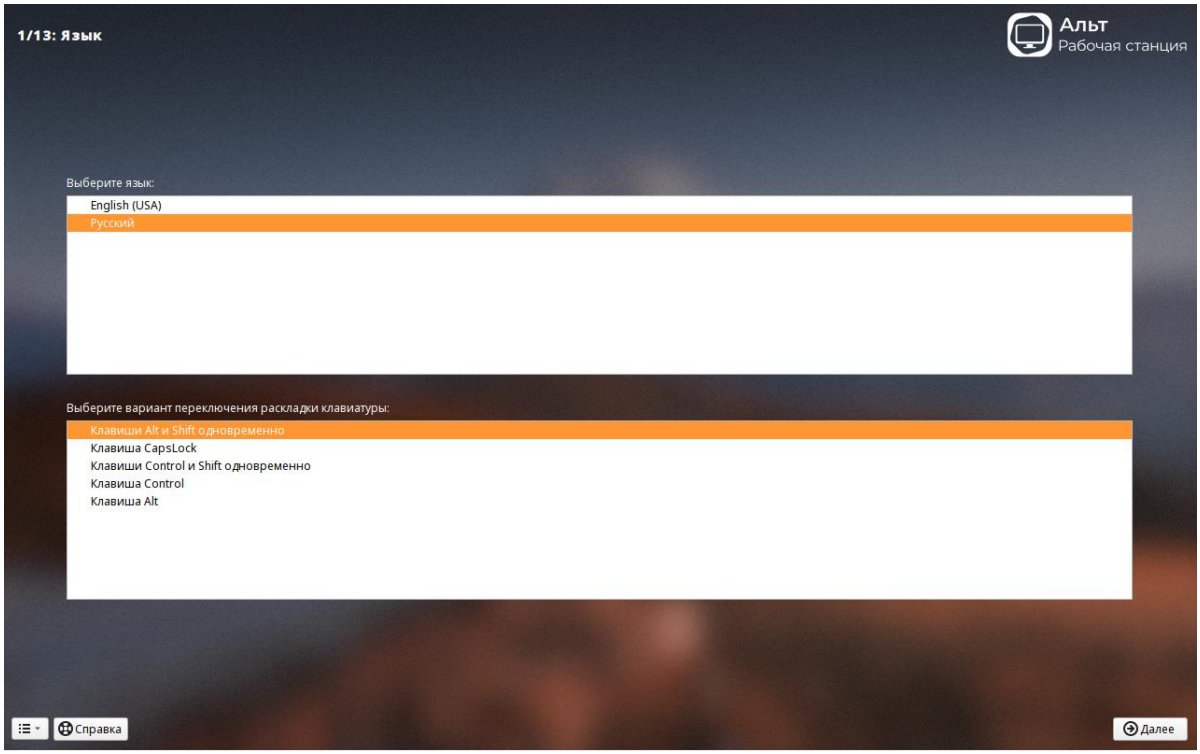

Рис. 3.27. Окно выбора языка операционной системы

Процесс установки рабочей станции alt linux 11 частично схож с установкой серверной редакции, за исключением меню выбора программ, которые будут установлены в ОС сразу во время инсталляции. Окна похожие на установку серверной редакции приведены на рис. 3.28 – рис. 3.39, основную разницу вы увидите в окне выбора ПО на рис.3.30.

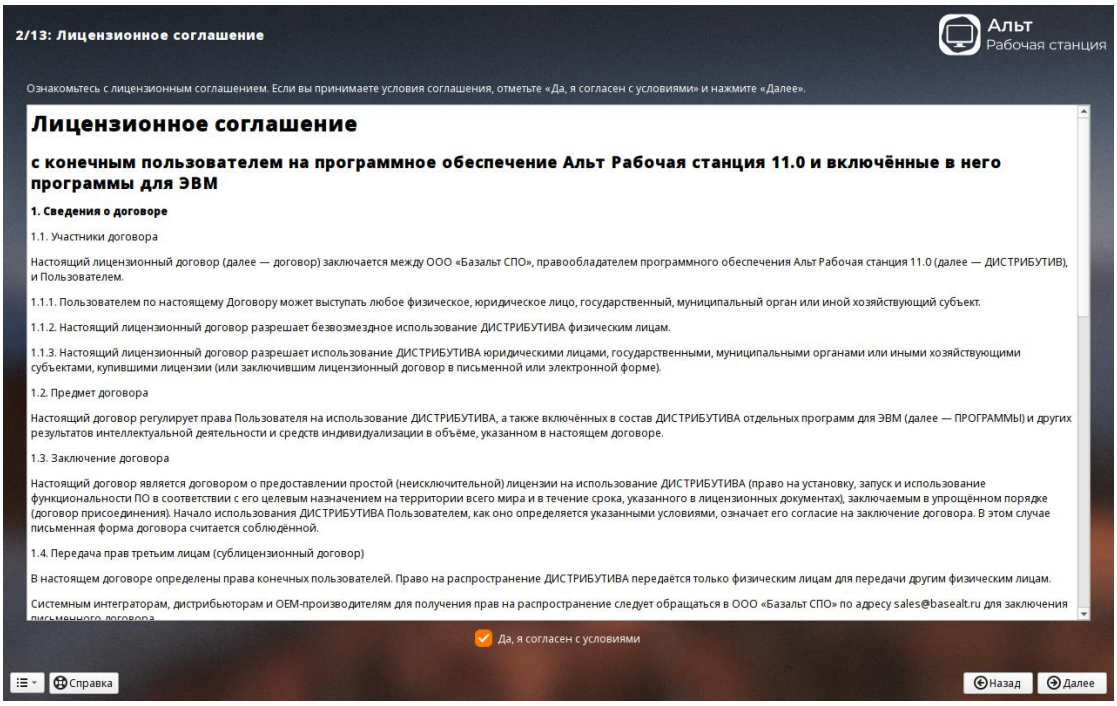

Рис. 3.28. Лицензионное соглашение

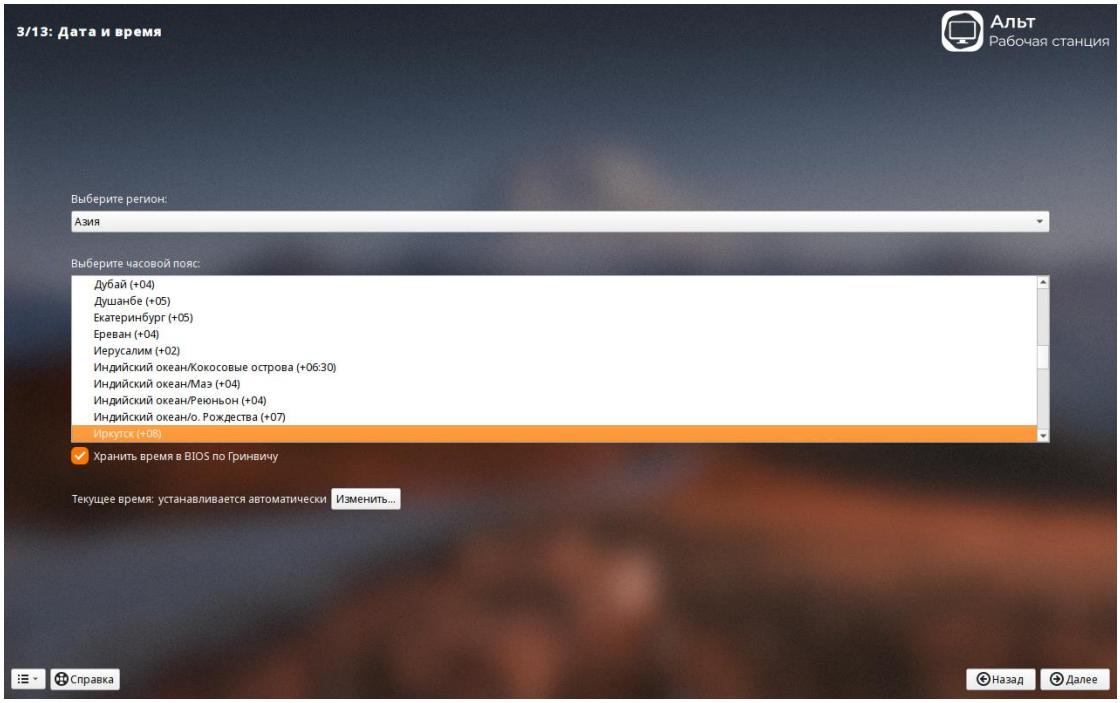

Рис. 3.29. Выбор часового пояса ОС

Следующим этапом предстоит выбрать компоненты, которые будут установлены в ОС сразу во время установки. Этот этап отличается от серверной тем, что в нем присутствует выбор дополнительного ПО для комфортной работы.

В нашем случае мы добавили следующие программы и компоненты: «Яндекс Браузер» - для тестирования подключения к сети Интернет и, при необходимости, загрузки дополнительных пакетов; «Групповые политики» - комплект ПО, позволяющий пользоваться групповыми политиками на уровне домена; «Альт Домен» - набор утилит для включения системы в домен; «Доступ к удаленным рабочим столам» - возможно пригодится для подключения к удаленному рабочему столу (в нашем примере он вряд ли понадобится, но для постоянной работы инструмент довольно удобный). Это позволит нам в дальнейшем сократить время установки дополнительных пакетов. Если вас интересует, что содержится в данных разделах, поставьте галочку напротив пункта «Показывать состав группы».

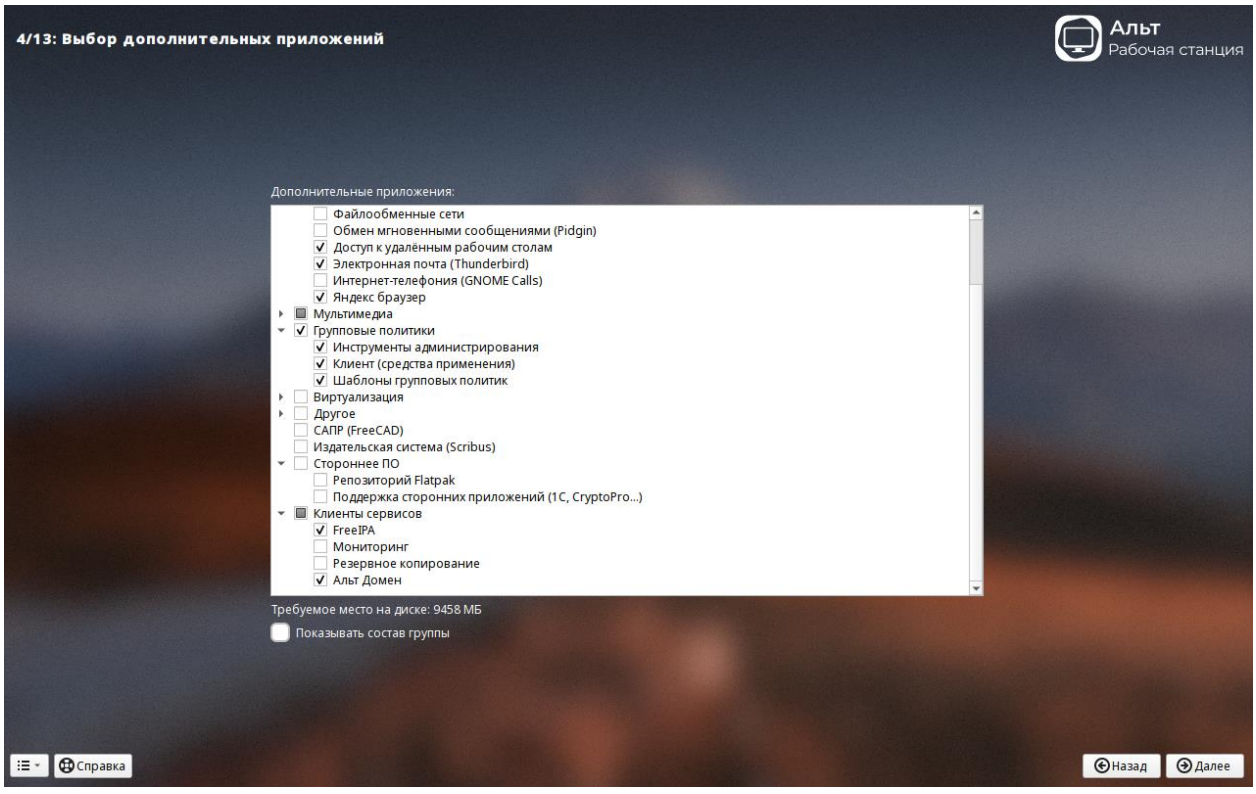

Рис. 3.30. Выбор программного обеспечения для установки

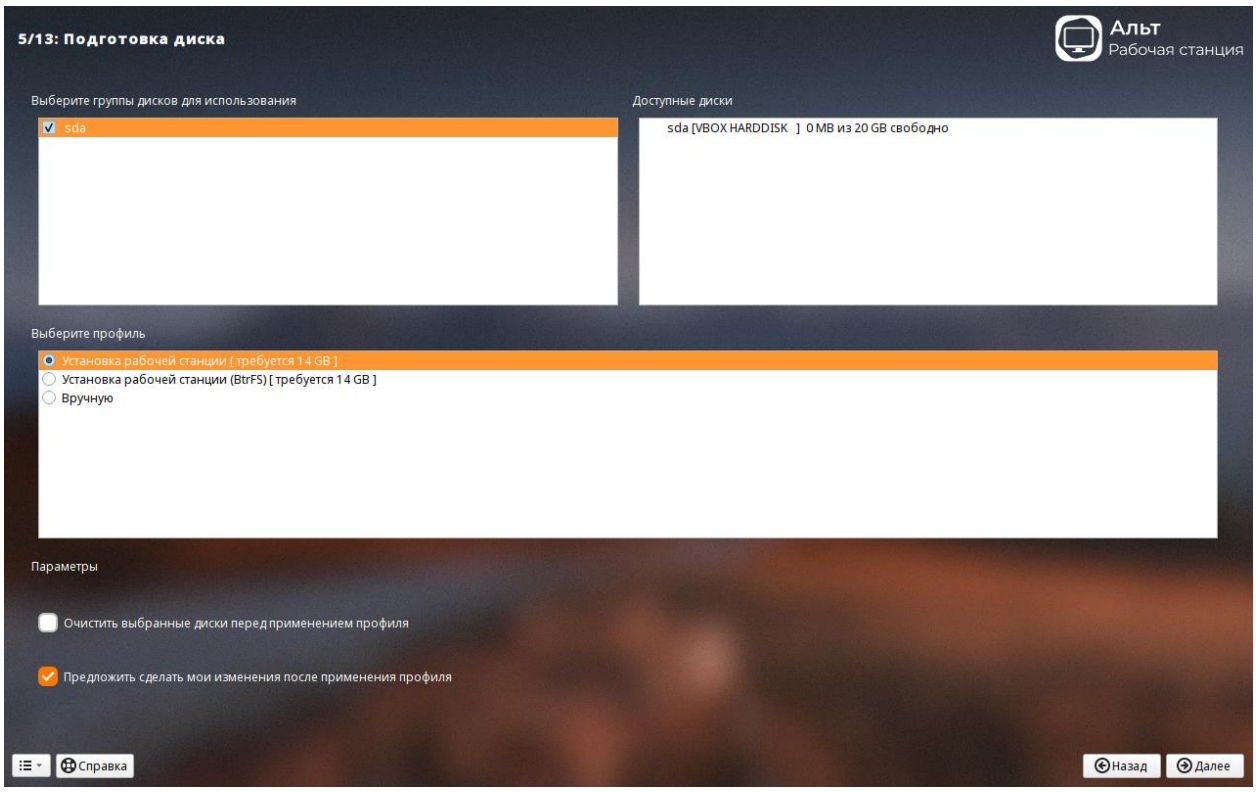

Рис. 3.31. Выбор диска для установки ОС

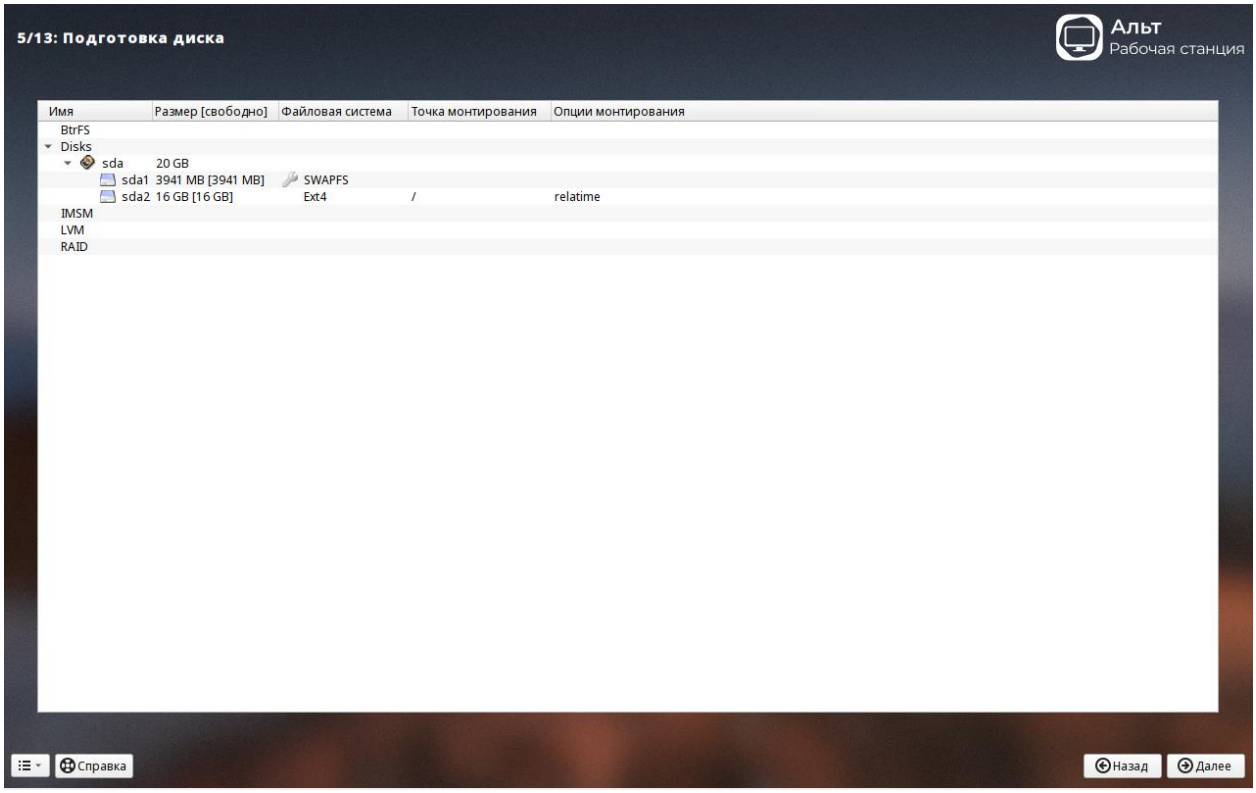

Рис. 3.32. Утилита редактирования разделов диска и настройки точек монтирования

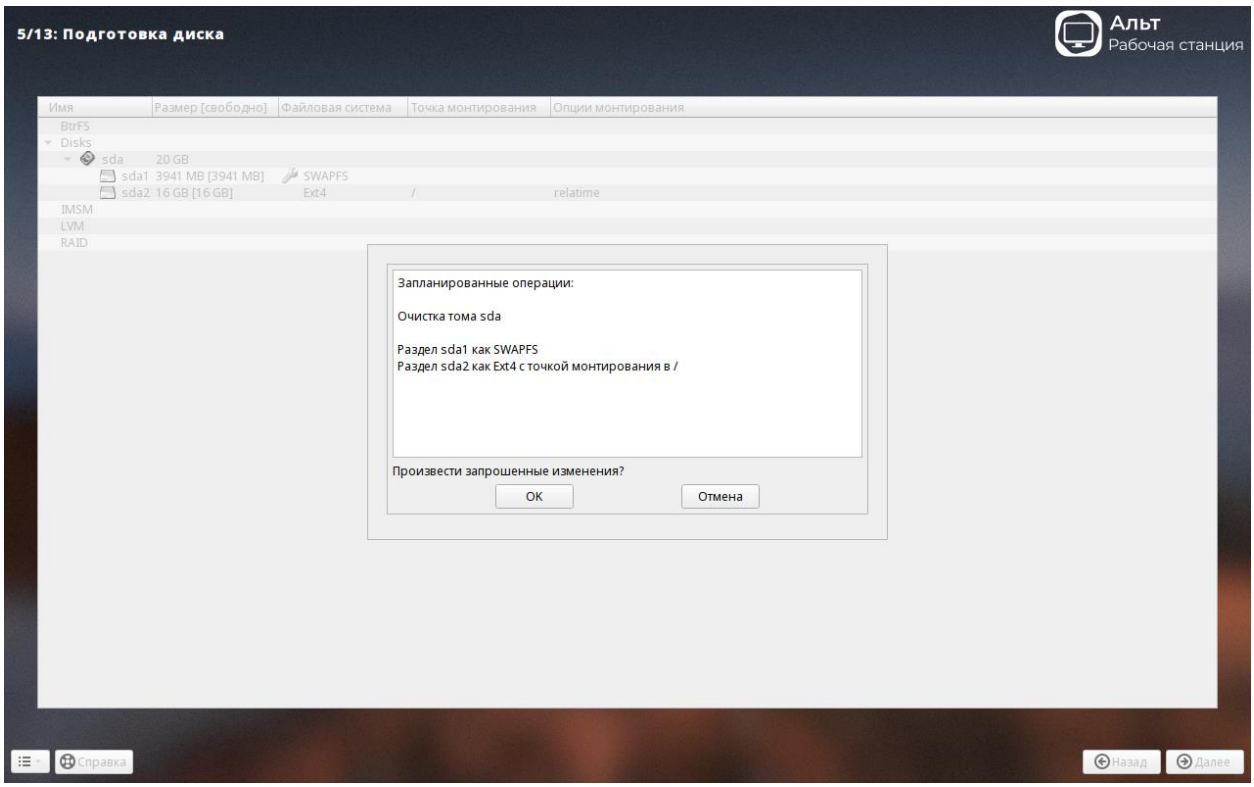

Рис. 3.33. Подтверждения операций с диском

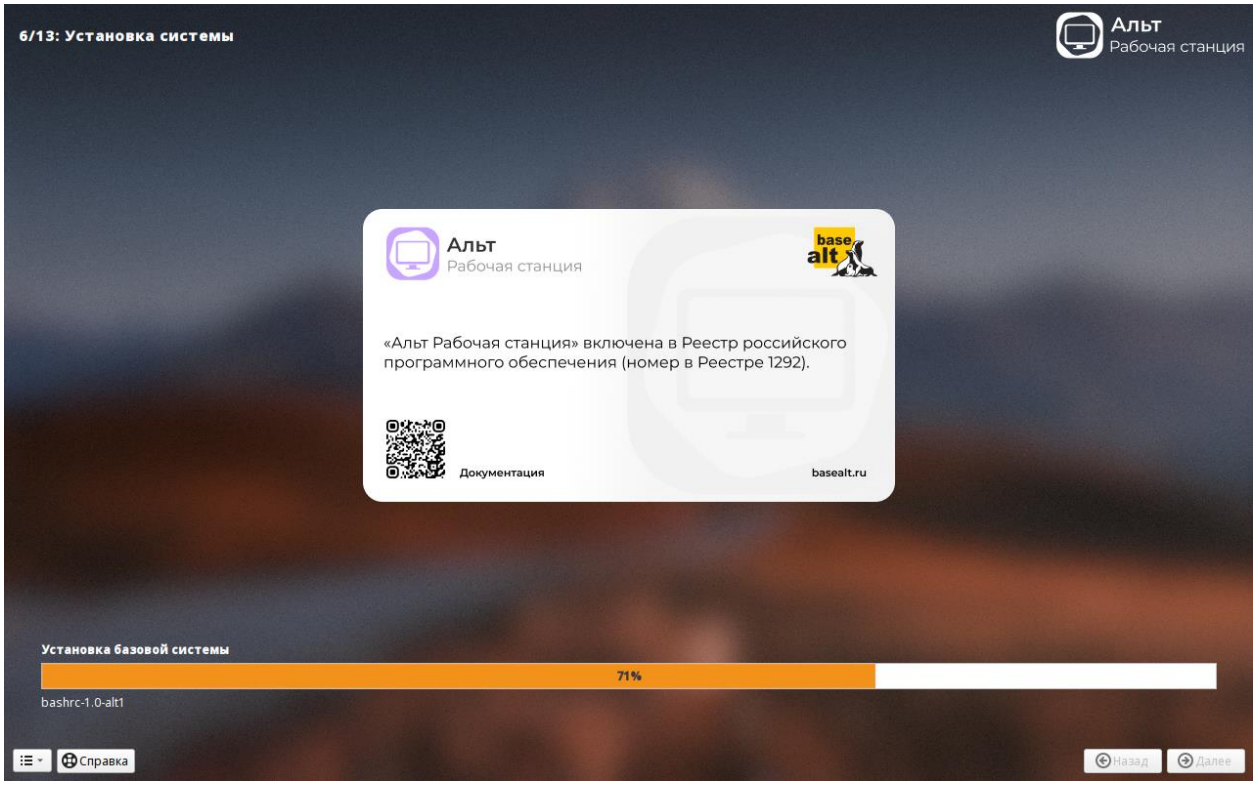

Рис. 3.34. Процесс установки базовой системы (ядро, системные утилиты)

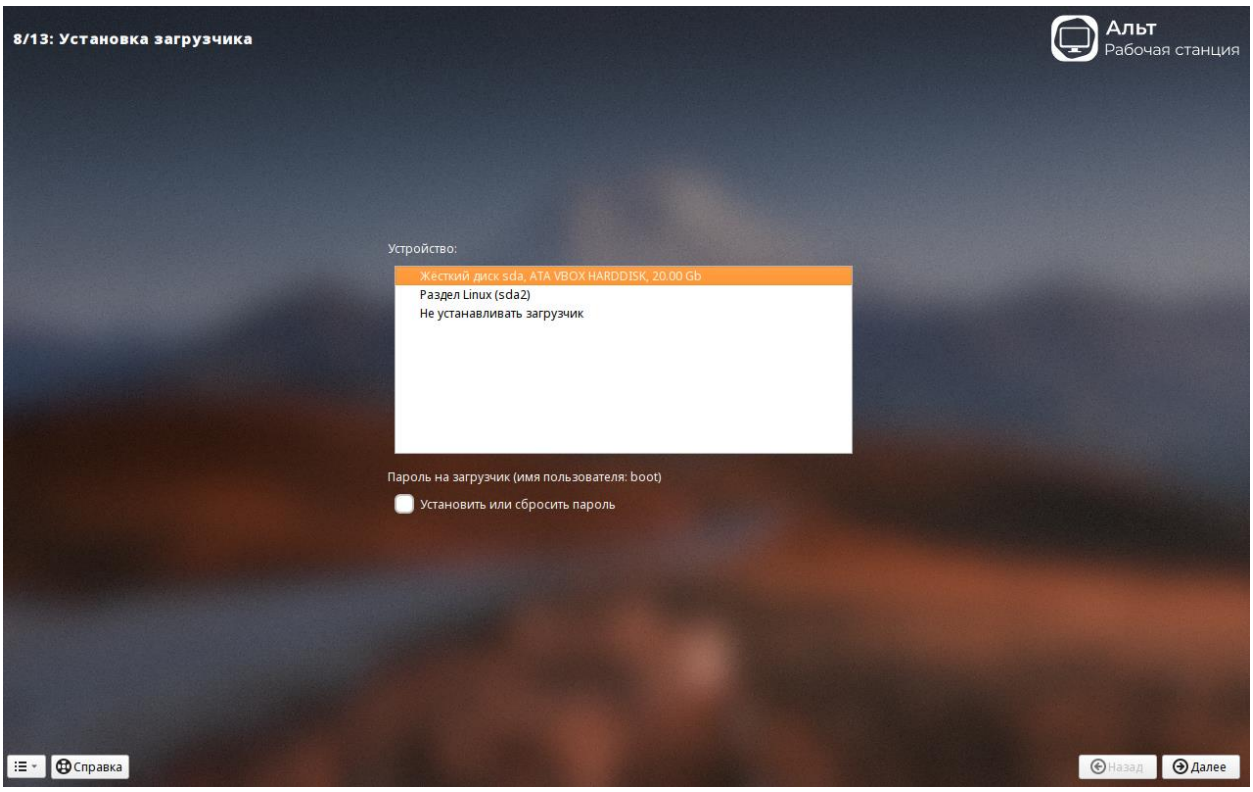

Рис. 3.35. Выбор места установки загрузчика ОС

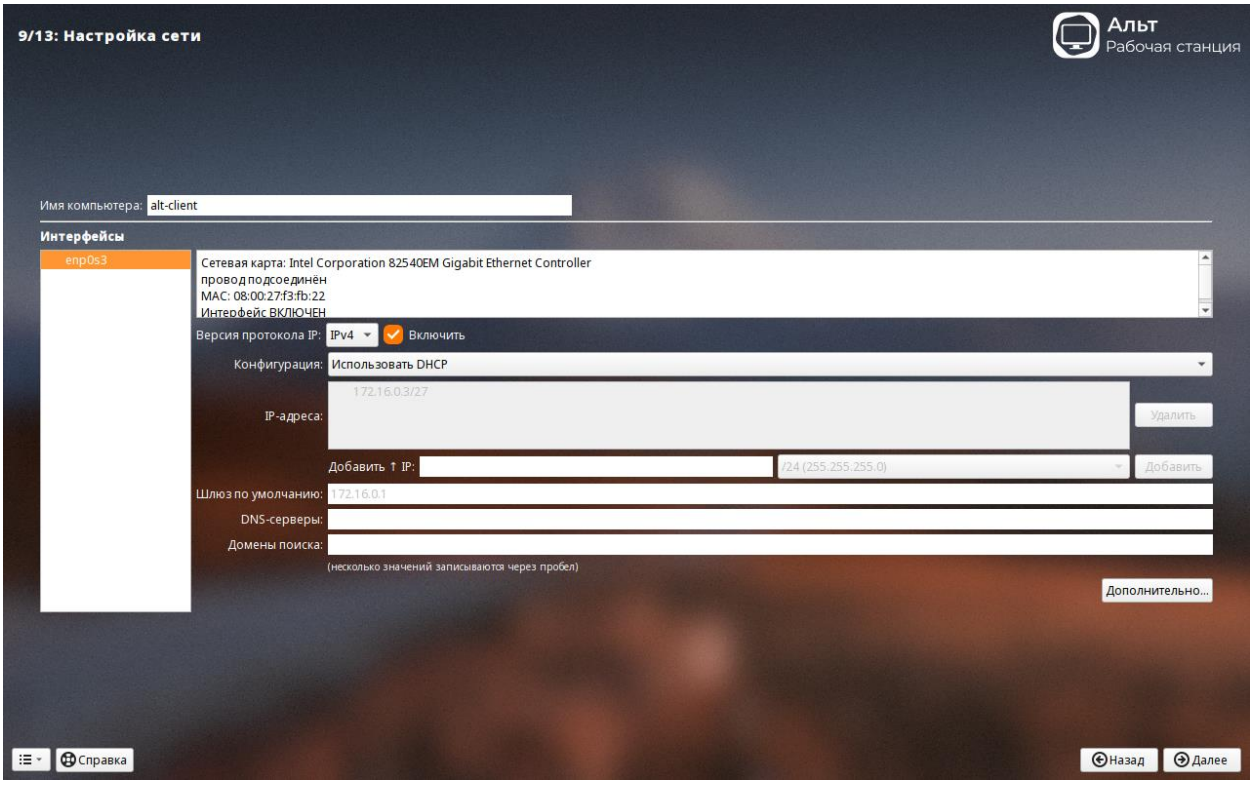

Рис. 3.36. Назначение сетевых параметров и имени хоста

В нашем случае изменено только имя хоста, настройки адреса получены автоматически с ранее настроенного dhcp сервера (ip 172.16.0.1).

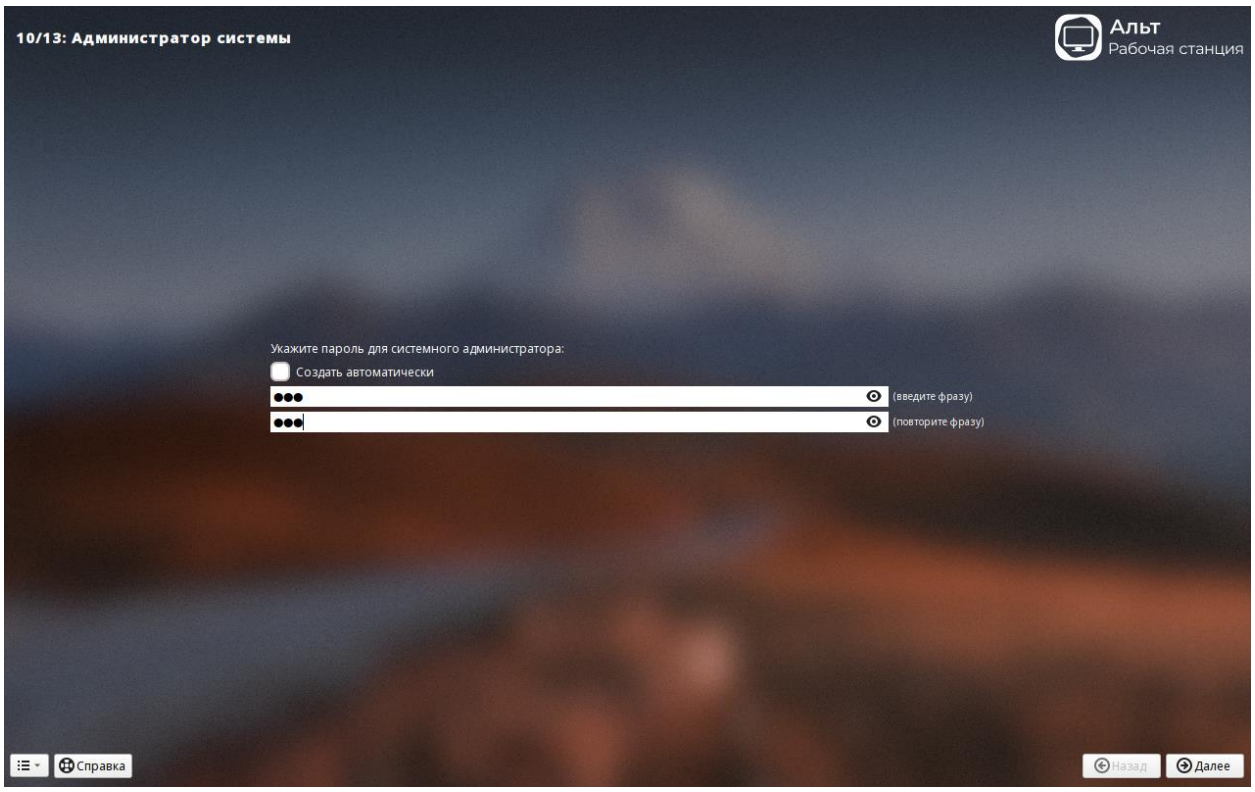

Рис. 3.37. Создание пароля суперпользователя (системного администратора)

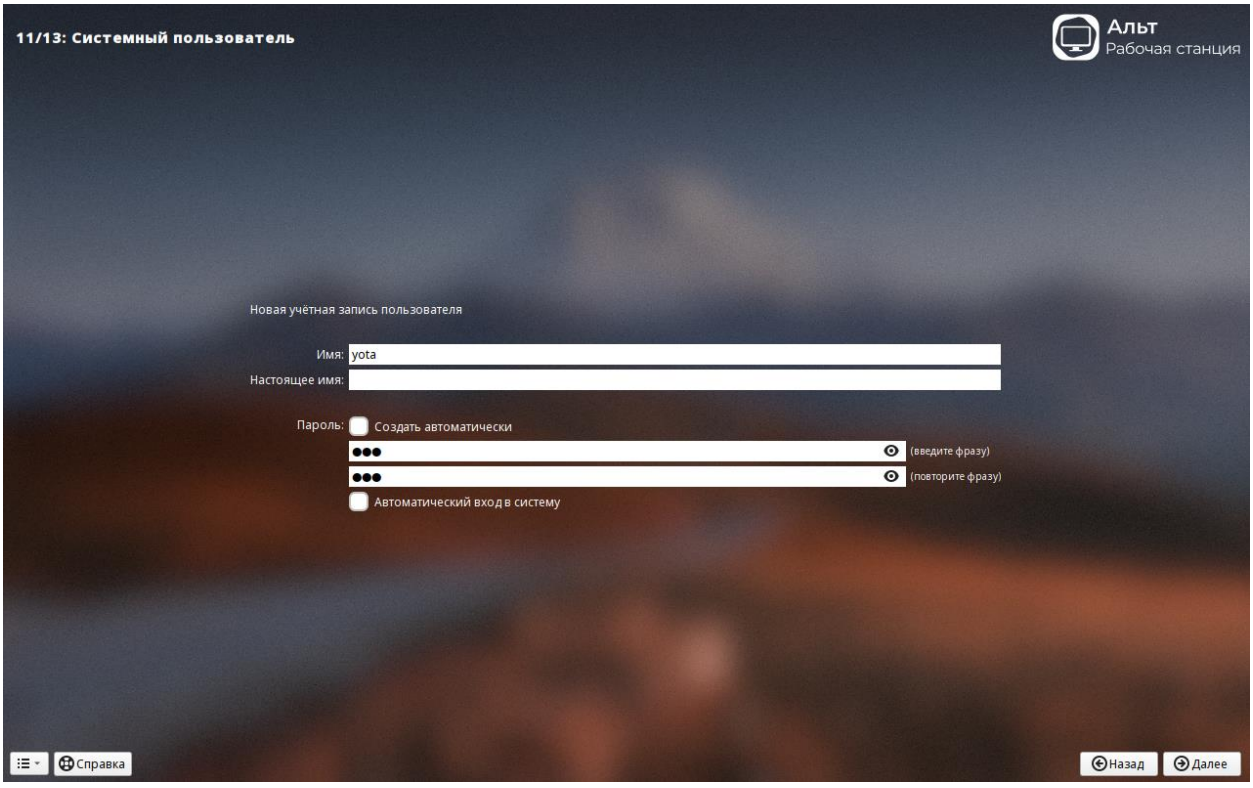

Рис. 3.38. Окно создание пользователя с обычными правами доступа и пароля к нему

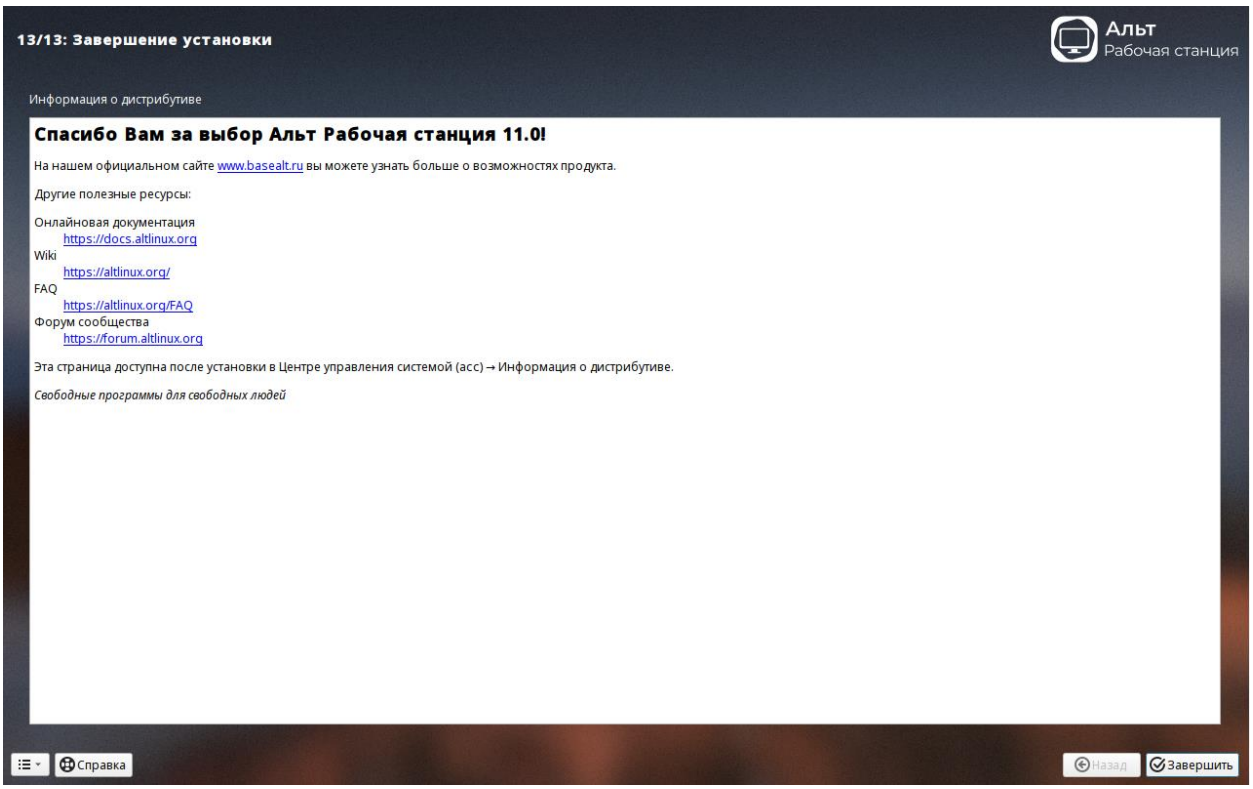

Рис. 3.39. Завершение установки ОС рабочей станции

На этом этапе перезагружаемся и входим в операционную систему, перед вами откроется интерфейс установленной операционной системы в качестве рабочей станции (рис. 3.40).

Рис. 3.40. Интерфейс установленной рабочей станции

Некоторые выводы из Раздела 3. «Работа с клиентскими машинами»

В данном разделе была произведена установка операционных систем для дальнейшего использования в качестве клиентских машин для сервера, созданного и настроенного в разделе 2 данного пособия. На практическом примере была произведена установка операционных систем 2 семейств: Microsoft Windows (версия 10) и Linux/UNIX (BaseALT Workstation 11).

Также рассмотрен процесс объединения всем ВМ (сервера, клиента linux, клиента windows) в единую сеть (сетевая связность) при помощи технологии «Внутренняя сеть» в гипервизоре Oracle VM VirtualBox. В данном случае «Внутренняя сеть» создает изолированный сегмент L2. Виртуальные машины видят друг друга, но полностью изолированы от внешней сети (хоста и интернета). Это идеальный полигон для отработки взаимодействия «сервер-клиент», так как мы исключаем влияние внешних факторов (DHCP-серверы офиса, атаки извне) и гарантируем чистоту эксперимента.

Раздел 4. Интеграция клиентских станций в серверную инфраструктуру на базе ранее развернутых служб

Предыдущие разделы настоящего пособия были посвящены созданию фундамента корпоративной информационной системы. В Разделе 2 был осуществлен выбор аппаратной абстракции (гипервизор) и произведено развертывание серверной операционной системы семейства Linux (на примере дистрибутива BaseAlt Linux Server 11) с последующей инсталляцией и первичной конфигурацией ключевых сетевых служб. К их числу были отнесены: служба каталогов (AD DC), обеспечивающая централизованное хранение учетных записей и политик; система динамической конфигурации узлов (DHCP), автоматизирующая назначение сетевых параметров; система доменных имен (DNS), критически важная для корректной разрешения имен в среде Windows-домена; служба файлового обмена (SMB), необходимая для организации совместного доступа к данным; а также прокси-сервер (Squid), призванный контролировать и оптимизировать доступ в глобальную сеть. В Разделе 3 была решена задача подготовки клиентского звена: созданы виртуальные машины, инсталлированы операционные системы двух различных семейств — Microsoft Windows 10 и Linux (BaseALT Workstation 11) — и обеспечена их базовая сетевая связанность на канальном уровне посредством технологии «Внутренняя сеть» гипервизора.

Таким образом, к началу данного, четвертого, раздела мы имеем в своем распоряжении все необходимые, но пока еще разрозненные компоненты будущей информационной системы. Существует подготовленный сервер, на котором работают службы, но они функционируют в изоляции от потребителей. Существуют клиентские машины, готовые к работе, но не имеющие доступа к сервисам, не знающие о существовании домена и не управляемые централизованно.

Целью данного раздела является преодоление этого разрыва и осуществление полномасштабной интеграции клиентских станций в созданную серверную инфраструктуру. Мы переходим от этапа «строительства» к этапу «пусконаладочных работ» и «ввода в эксплуатацию».

Для достижения поставленной цели необходимо решить следующий комплекс взаимосвязанных задач:

- **Обеспечение корректного функционирования DNS-инфраструктуры**. В контексте службы каталогов Active Directory (реализованной в Samba на Linux) протокол DNS приобретает критическое значение. Без возможности найти контроллер домена по имени ни один клиент не сможет пройти аутентификацию. Будет произведена проверка и, при необходимости, донастройка DNS-сервера для поддержки динамических обновлений и SRV-записей.
- **Активация и тонкая настройка DHCP-сервера**. Ранее созданный DHCP-сервер должен быть настроен не просто на выдачу IP-адресов, но и на трансляцию клиентам параметров, необходимых для вступления в домен: адреса DNS-сервера (которым является наш контроллер домена) и доменного суффикса.
- **Процедура ввода Windows-клиента в домен**. Будет продемонстрирован классический процесс присоединения рабочей станции под управлением ОС Windows к домену Active Directory. Рассматриваются вопросы аутентификации, создания компьютерной учетной записи в каталоге и применения начальных политик безопасности.
- **Интеграция Linux-клиента в домен Active Directory**. Особое внимание уделяется гетерогенности инфраструктуры. На примере рабочей станции BaseALT Workstation 11 будет показан процесс настройки подсистемы аутентификации (SSSD — System Security Services Daemon), позволяющей Linux-клиенту полноценно взаимодействовать с контроллером домена, обеспечивая вход пользователей с доменными учетными записями и разграничение прав доступа.
- **Верификация доступа к файловым ресурсам (SMB)**. После успешной интеграции в домен необходимо проверить работоспособность файлового сервера. Будут продемонстрированы примеры подключения сетевых дисков на Windows- и Linux-клиентах с использованием доменной аутентификации и разграничением прав доступа на основе групповой принадлежности пользователей.
- **Настройка авторизованного доступа через прокси-сервер (Squid)**. Завершающим этапом станет интеграция клиентских станций с прокси-сервером Squid. Будет показана настройка, при которой доступ в интернет разрешается только после успешной аутентификации пользователя в домене, что позволяет вести детальный учет трафика и применять политики фильтрации контента.

Ожидаемый результат выполнения практических действий, описанных в данном разделе, представляет собой логически завершенную, функциональную модель корпоративной сети малого или учебного предприятия. Все компоненты системы (сервер и разнородные клиенты) будут объединены не только на физико-канальном уровне (сетевая связность), но и на уровне прикладных сервисов и безопасности. Читатель получит целостное представление о том, как теоретические знания о сетевых протоколах и службах воплощаются в работающую инфраструктуру, управляемую из единого центра.

4.1. Интеграция станции Windows в доменную инфраструктуру

4.1.1. Автоматическое получение настроек с сервера (dhcp, dns)

Сразу после установки клиентской машины с ОС Windows, она должна в автоматическом режиме получить настройки с ранее настроенного сервера, а именно настройки ip адреса, для общения с другими устройствами по сети (корректность работы dhcp) и настройки dns для разрешения сетевых имен из доменных имен в ip адреса (корректность работы dns).

Для проверки настроек ip адреса в windows вызовем командную строку (для этого следуют нажать комбинацию клавиш «Win+R», затем в открывшимся окне ввести команду «cmd») рис.4.1.

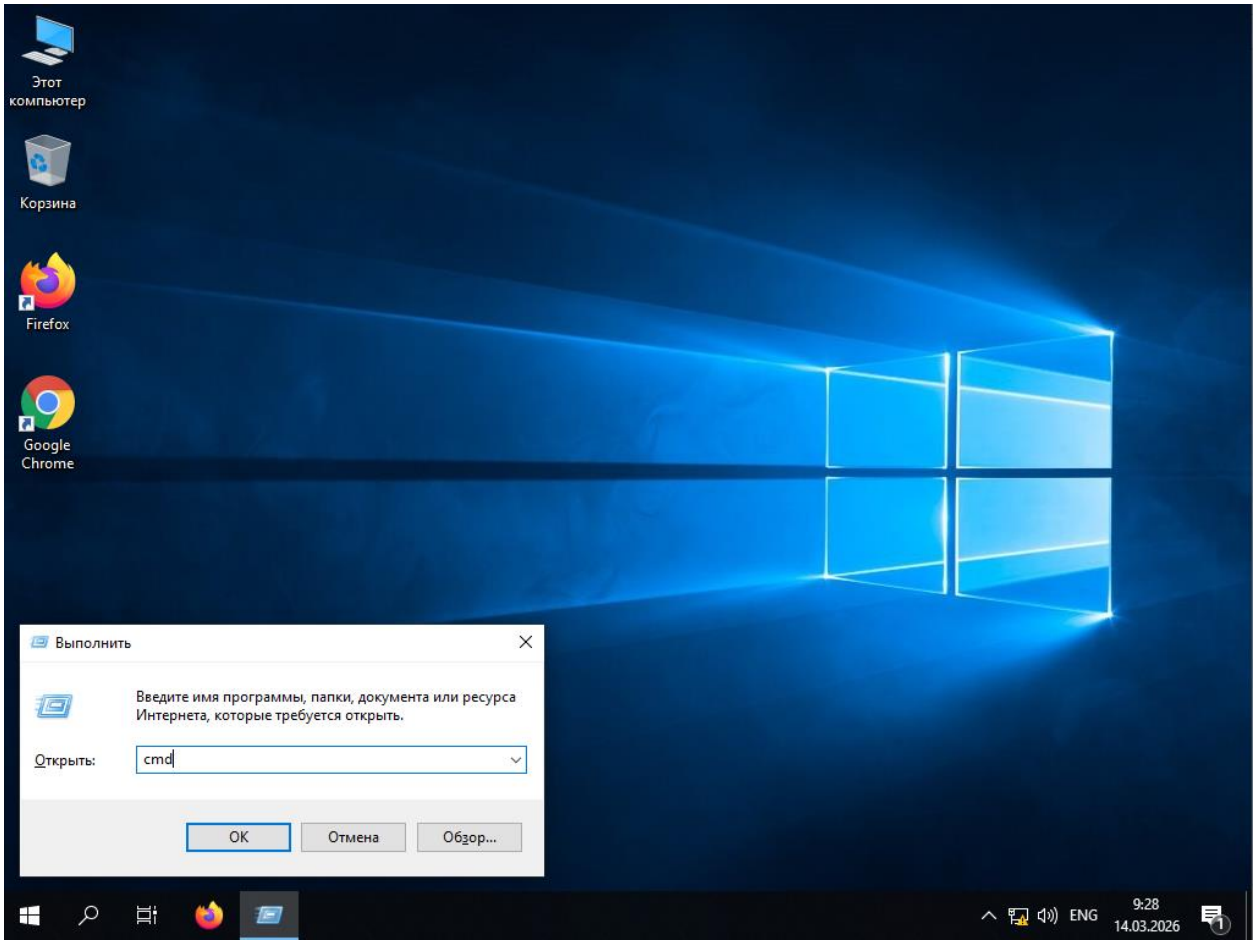

Рис. 4.1. Вызов окна «Выполнить» с последующим вызовом командной строки

После ввода команды нажмите «ОК» или клавишу «Enter» на клавиатуре для того, чтобы запустить процесс выполнения команды (рис.4.2.). Затем введем команду «**ipconfig**» в командной строке для просмотра свойств сетевого адаптера

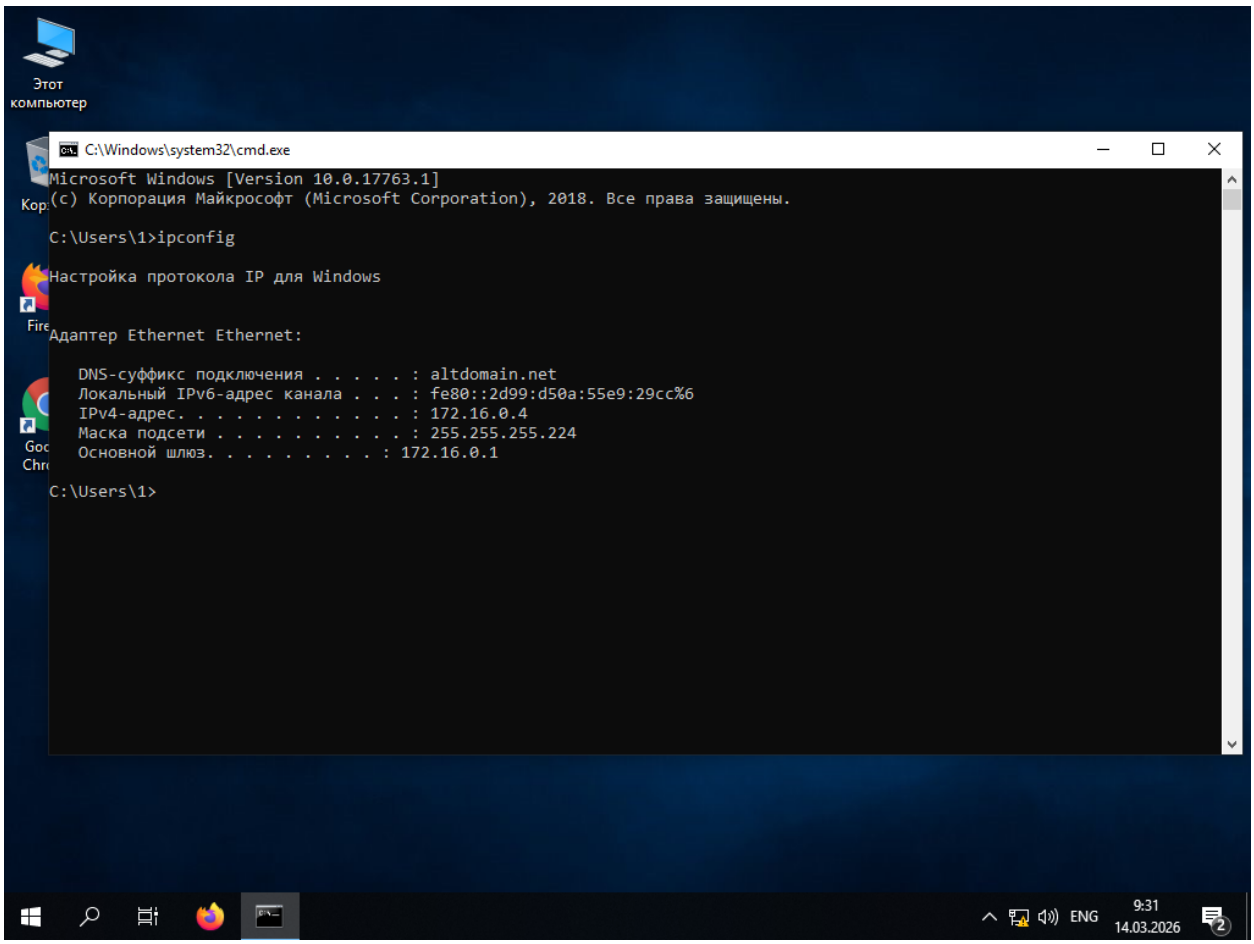

Рис. 4.2. Проверка настроек ip адреса в режиме командной строки

Также настройки ip адреса можно проверить через панель управления, используя следующий алгоритм действий: рис. 4.3 – рис. 4.6 - Данный способ подразумевает использование панели управления и параметров windows вместо командной строки.

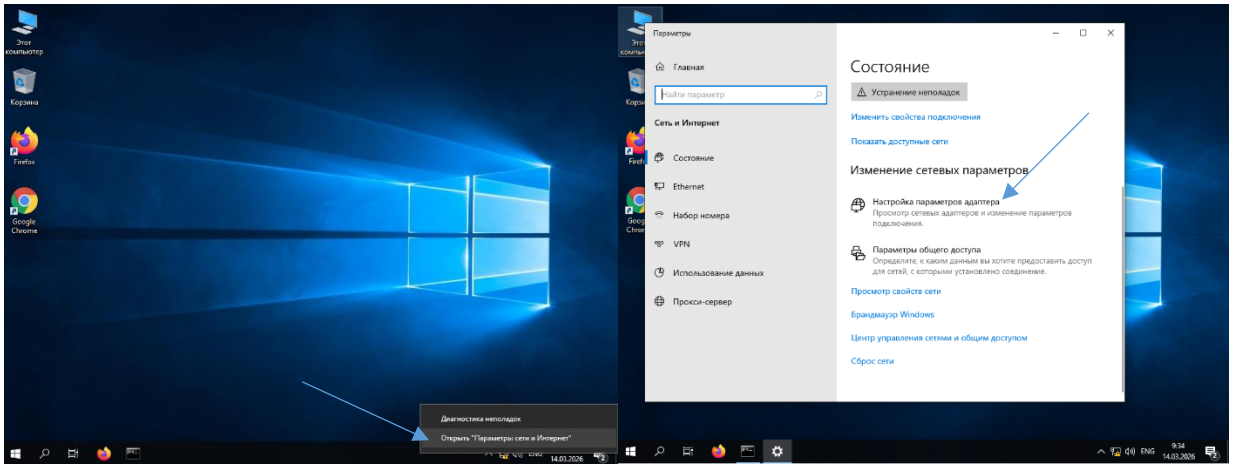

Рис. 4.3. Вызов параметров Сети

Рис.4.4. Переход к окну управления

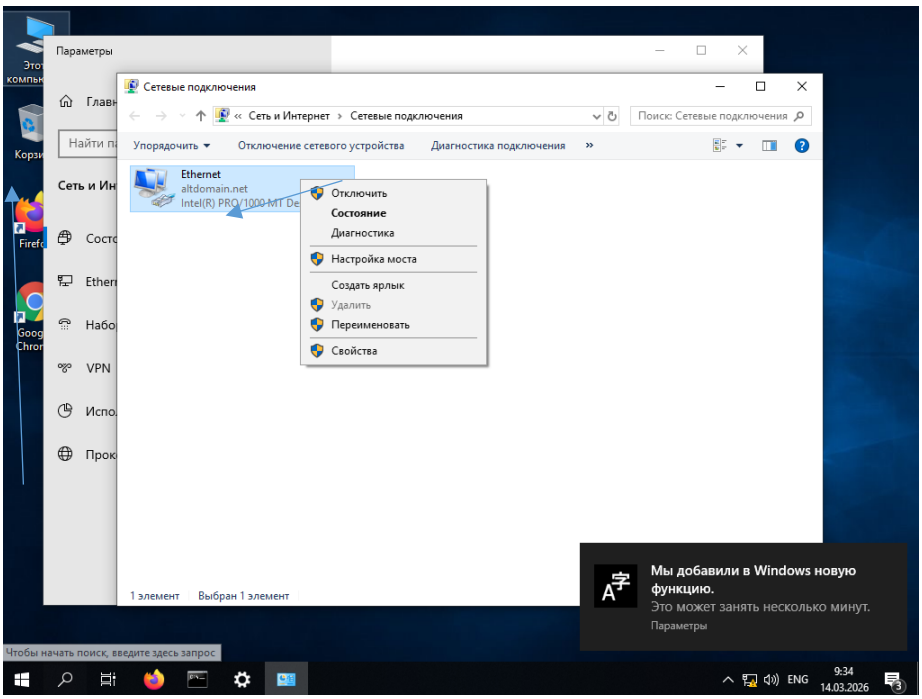

Рис. 4.5. Вызов окна свойств сетевого адаптера

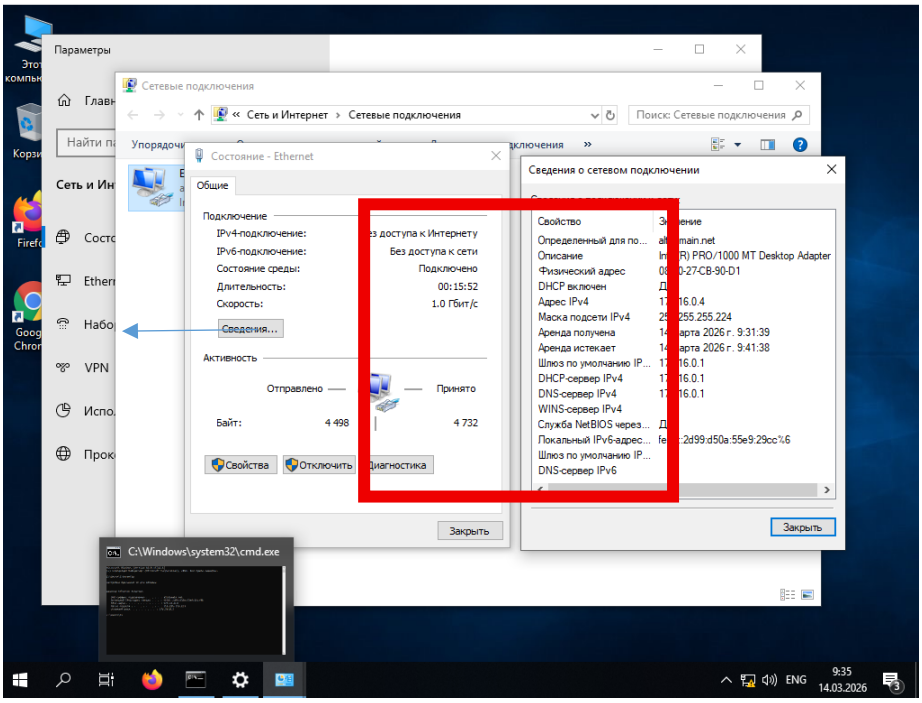

Рис. 4.6. Свойства сетевого адаптера

Как видно из рис. 4.6 (выделено красным) – параметры сетевого адаптера (настройки ip, dns, сетевого домена) полностью совпадают с рис. 4.2, что свидетельствует о корректной настройке dhcp сервера.

Далее проверим работу dns, путем написания некоторых запросов в командной строке: команда «**nslookup**» с указанием доменного имени какого-либо сервиса для проверки корректности работы «резольвирующего» (dns) сервера рис.4.7.

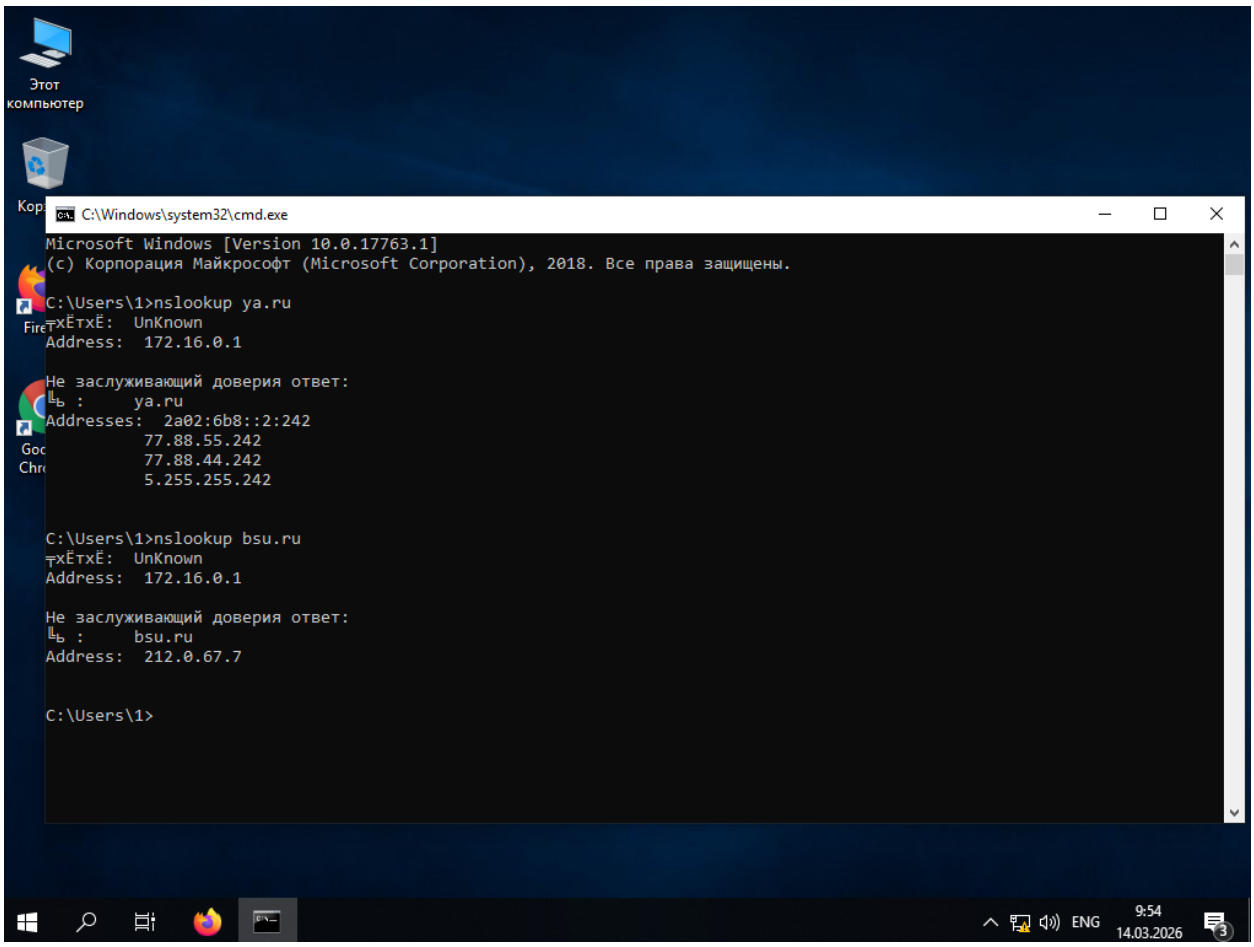

Рис. 4.7. Проверка работы dns сервера

Как видим из рис.4.7 – DNS сервер отлично справляется со своей работой: переводит доменные имена и ip адреса, что и было заявлено в разделе 2.

Вывод: роли DHCP и DNS сервера, показанные в разделе 2 настоящего методического пособия настроены верно, заявленные функции выполняются. Можно переходить к следующим этапам проверки/настройки.

4.1.2. Подключение Windows к контроллеру домена SambaDC

На данном этапе разберем процесс включения рабочей станции под управлением ОС Windows в домен, построенный на базе программного пакета SambaDC в ОС Linux.

Для этого откроем «Параметры ПК» на Windows 10 или «Панель управления» на Windows 8.1 и более ранних версиях ОС Windows. Рассмотрим процесс ввода машины в домен на примере Windows 10, для сокращения времени открытия и поиска нужных разделов, воспользуемся окном «Выполнить» (для вызова использовать сочетание клавиш «Win+R»), затем вызовем окно свойств системы, используя команду «**sysdm.cpl**» рис. 4.8., рис.4.9 (работает на ОС Windows с версии 7 и позднее).

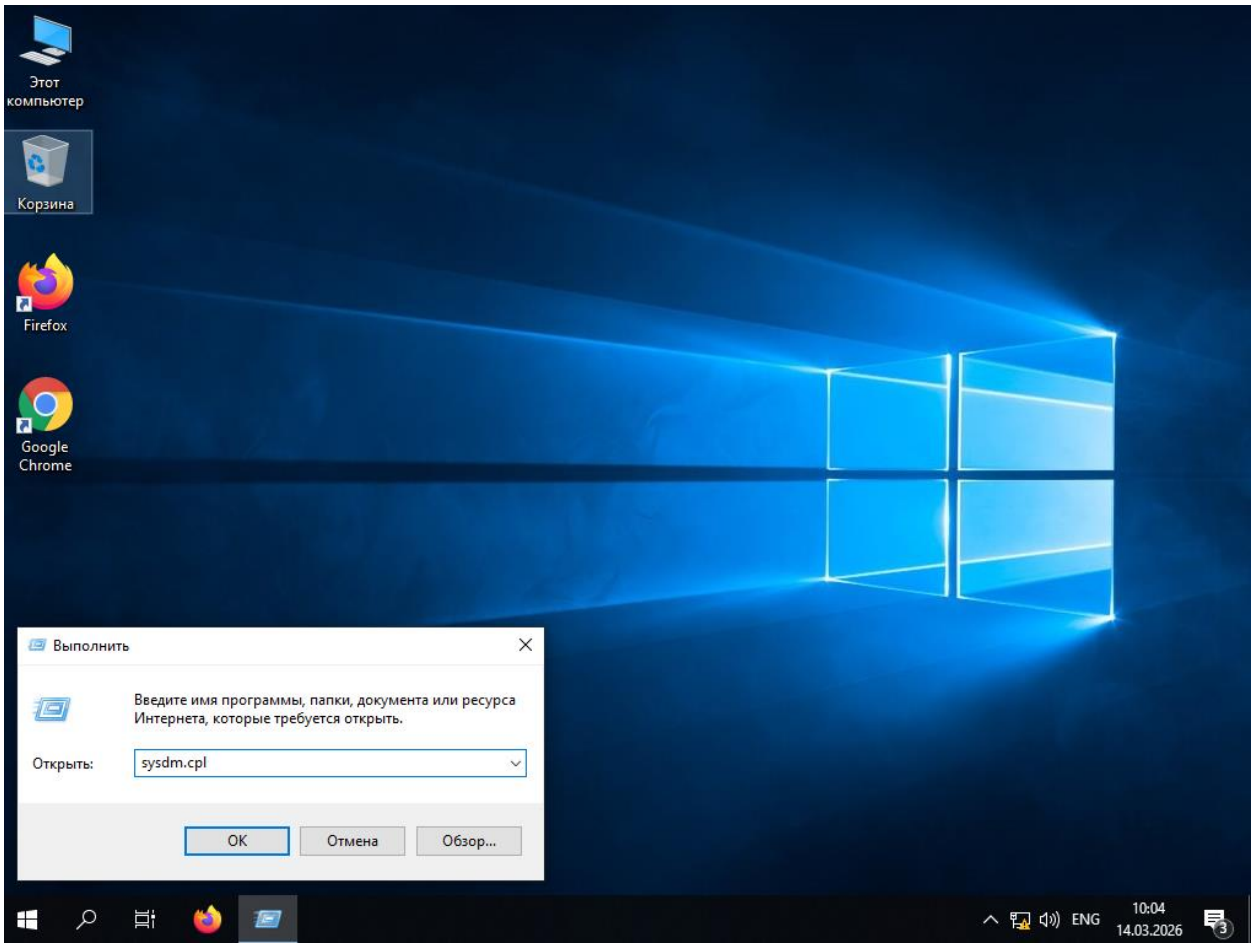

Рис. 4.8. Вызов окна свойств системы

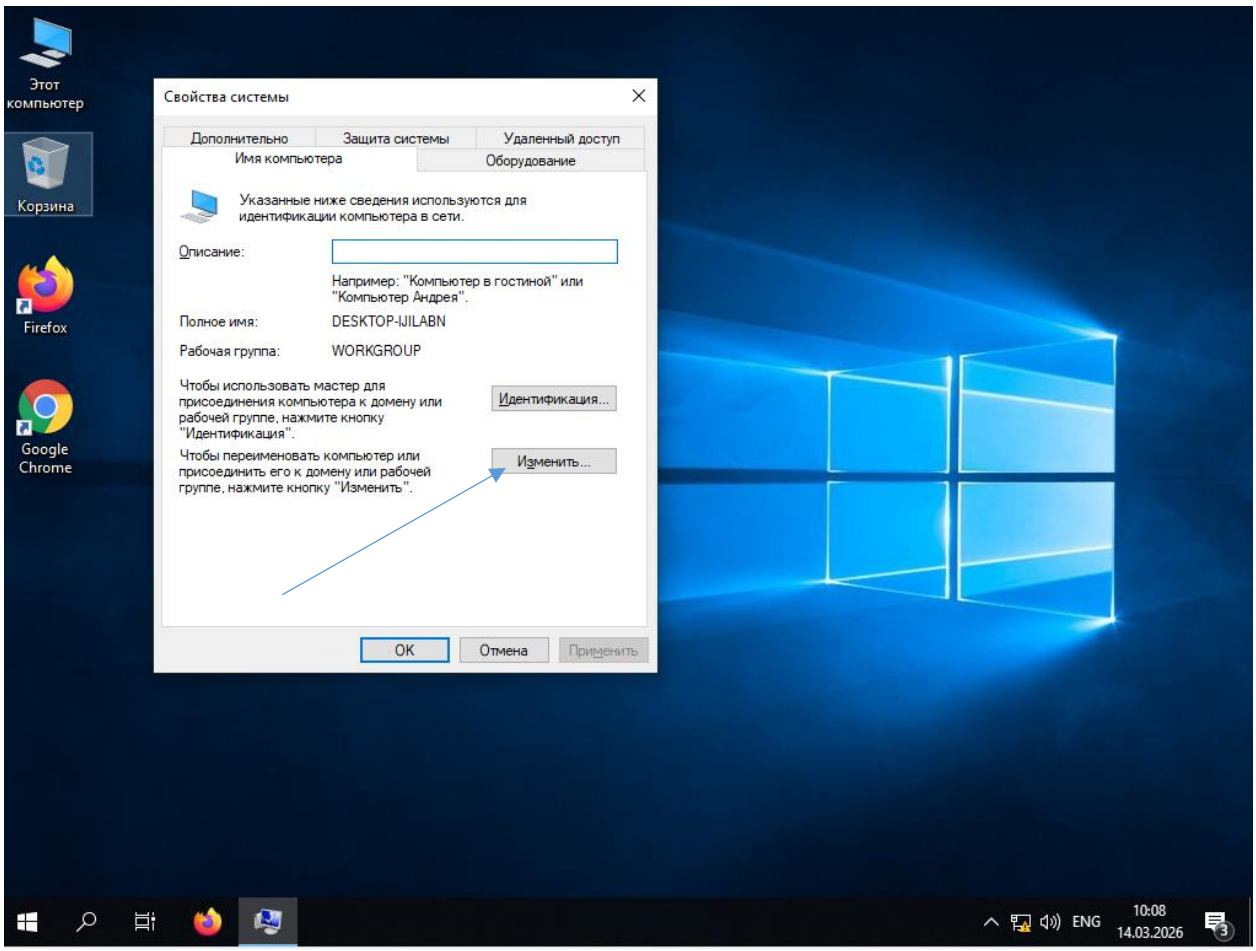

Рис. 4.9. Окно «Свойства системы»

На данном окне нас интересует параметр «Чтобы переименовать компьютер или присоединить его к домену или рабочей группе, нажмите кнопку «Изменить»» - нажимаем.

После чего перед нами откроется окно (рис. 4.10), в котором требуется указать осмысленное имя вашего клиента, чтобы в дальнейшем однозначно идентифицировать, что это за клиент такой и откуда он, а также в поле «Являюсь членом» указать на «Домена» и ввести соответствующее имя вашего домена. Когда все данные введены корректно, можно нажать кнопку «ОК», что запустит процесс переименования вашей рабочей станции и присоединение её к домену.

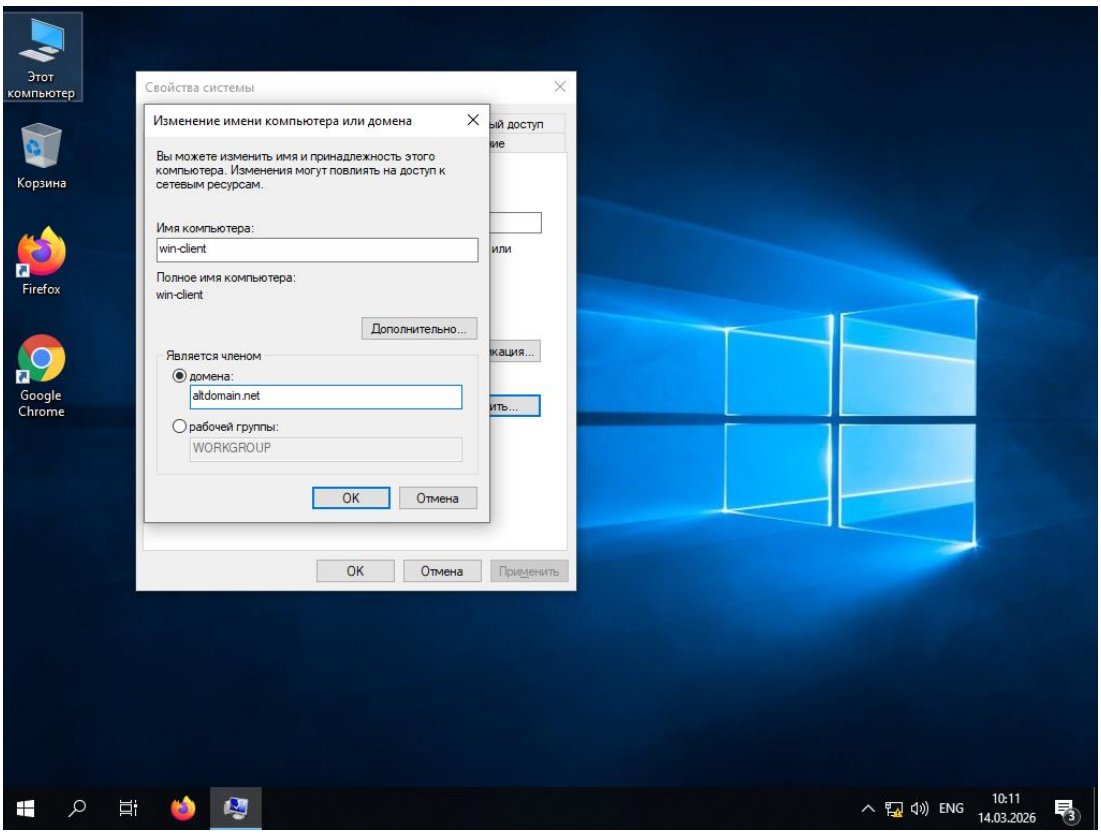

Рис. 4.10. Ввод имени устройства и имени домена на рабочей станции Windows

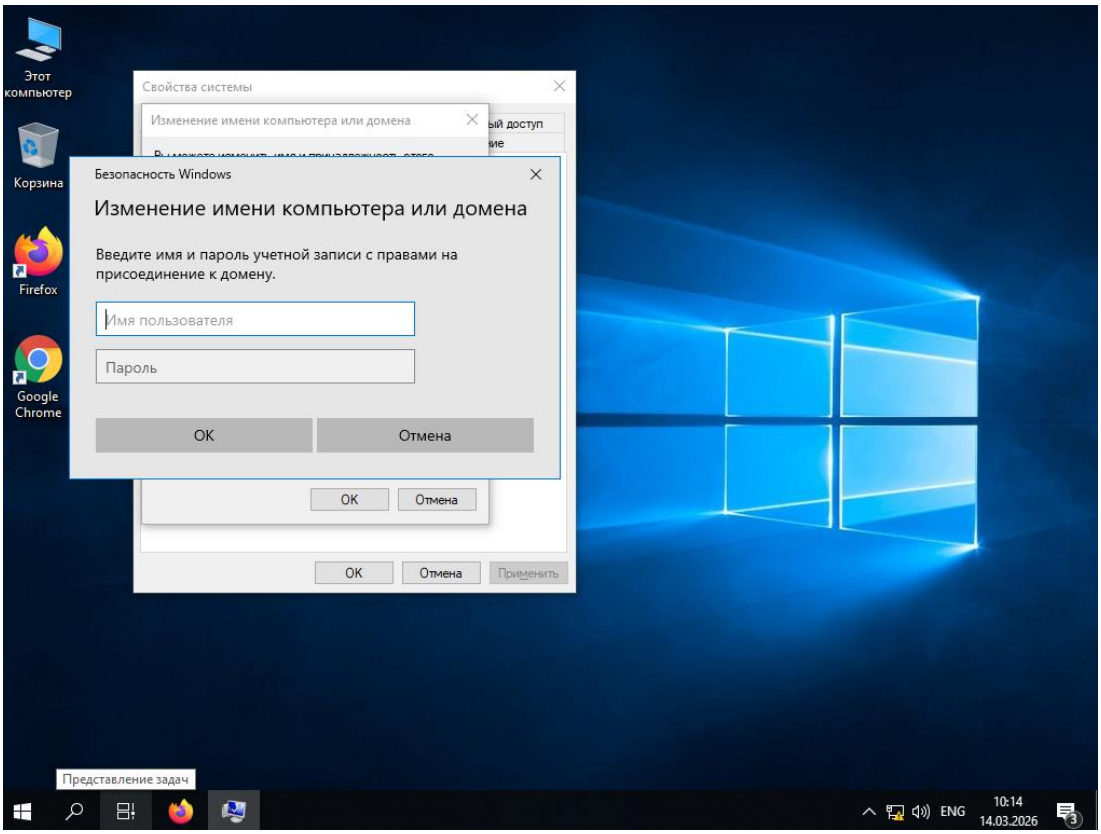

Рис. 4.11. Окно ввода имени пользователя и пароля для присоединения к домену

Если связь с контроллером домена была успешно установлена, то перед вами откроется окно ввода имени пользователя и пароля для присоединения к домену (рис. 4.11), обратите внимание, вводимый здесь пользователь должен обладать правами ввода рабочей станции в домен или правами администратора домена. Пример создания такого пользователя приведен в разделе 2.3.1, рис. 2.32.

Вводим имя и пароль администратора и нажимаем «ОК» рис. 4.12.

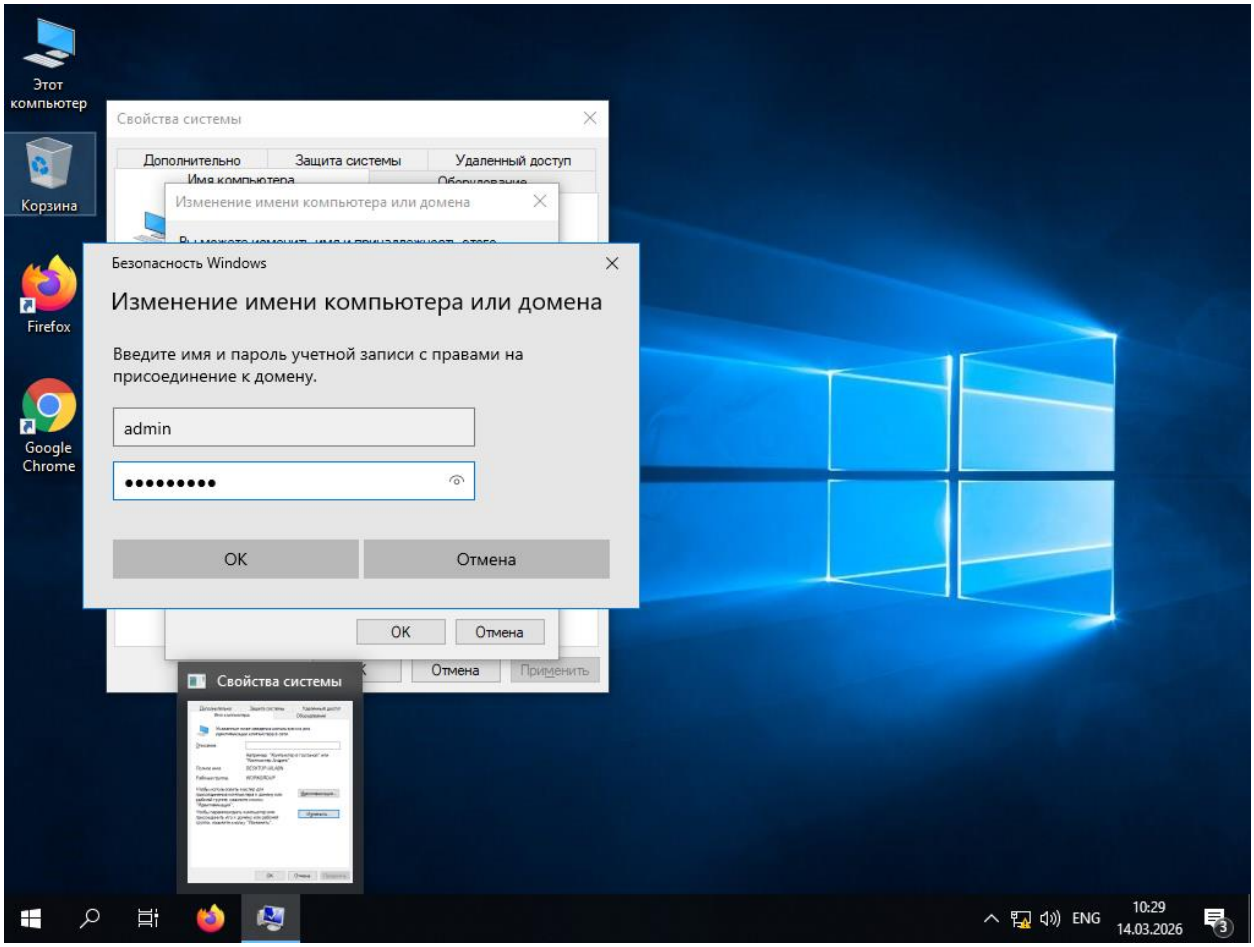

Рис. 4.12. Указание пользователя для подключения к домену

После того, как данные будут проверены, перед вами всплывет сообщение об успешности подключения к домену (рис. 4.13) или об ошибке подключения – в таком случае следует проверить актуальность вводимых данных пользователя (имя и пароль), а также статус службы SambaDC на сервере (команда проверки «**systemctl status samba**»).

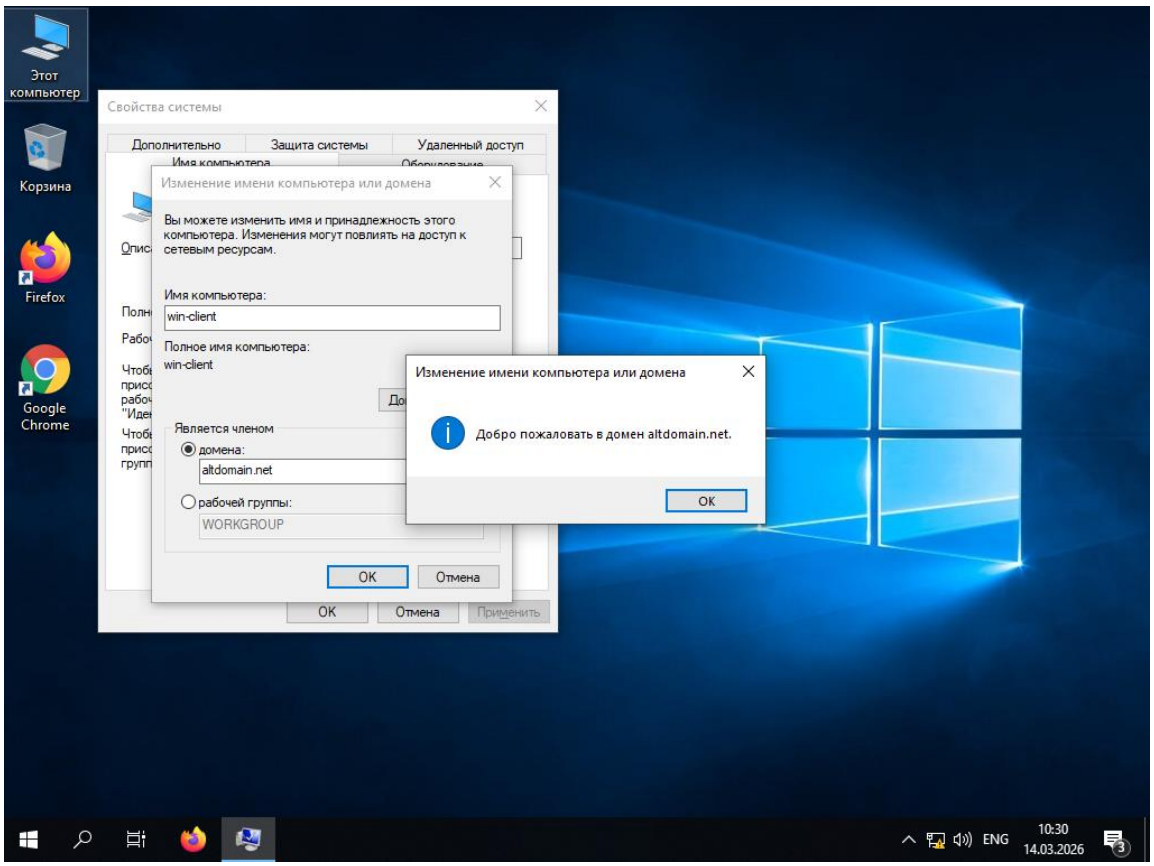

Рис. 4.13. Состояние ввода рабочей станции в домен

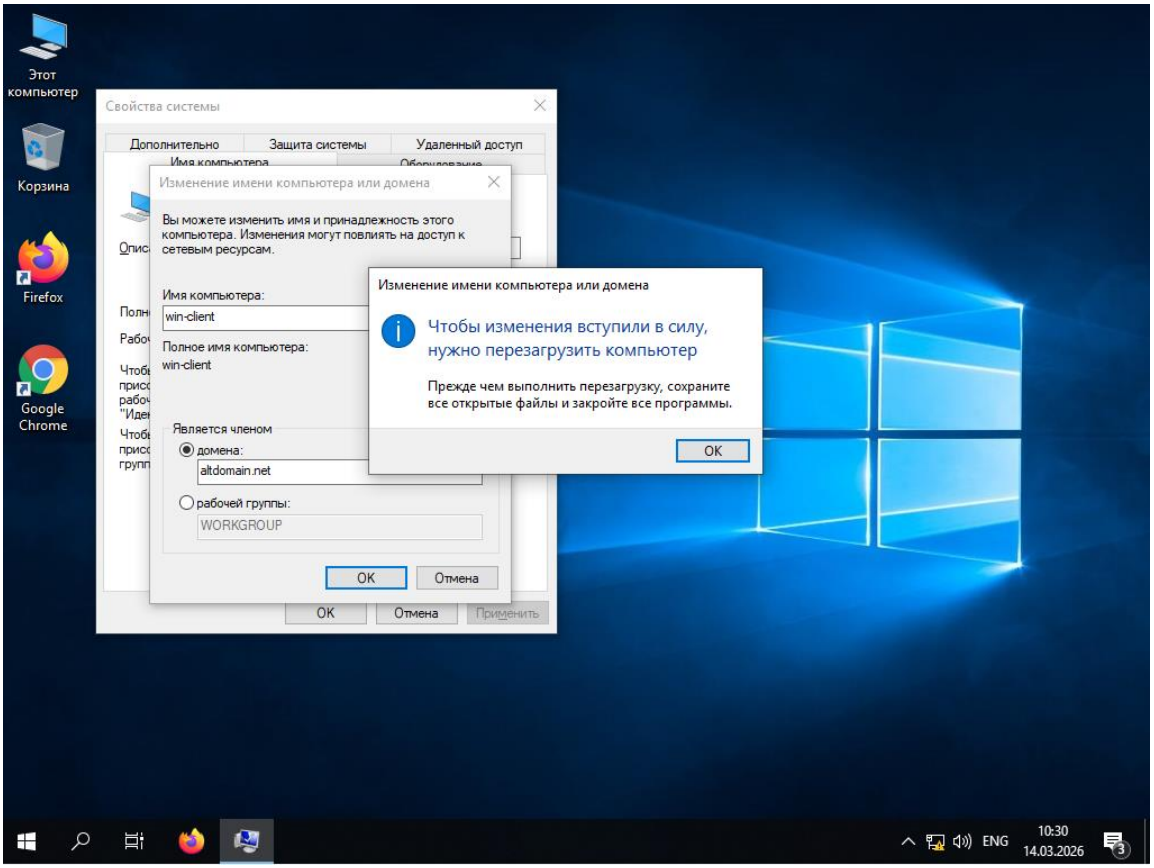

Рис. 4.14. Требование перезагрузки машины

Рис. 4.14 является следствием успешности подключения к домену, т.к. для работы доменной службы каталогов (в нашем случае samba-dc) требуется перезагрузка конечной операционной системы, после которой появится возможность входа в систему пользователям домена.

Выполняем перезагрузку Windows, затем наблюдаем возможность входа в систему от имени доменного пользователя (рис. 4.15)

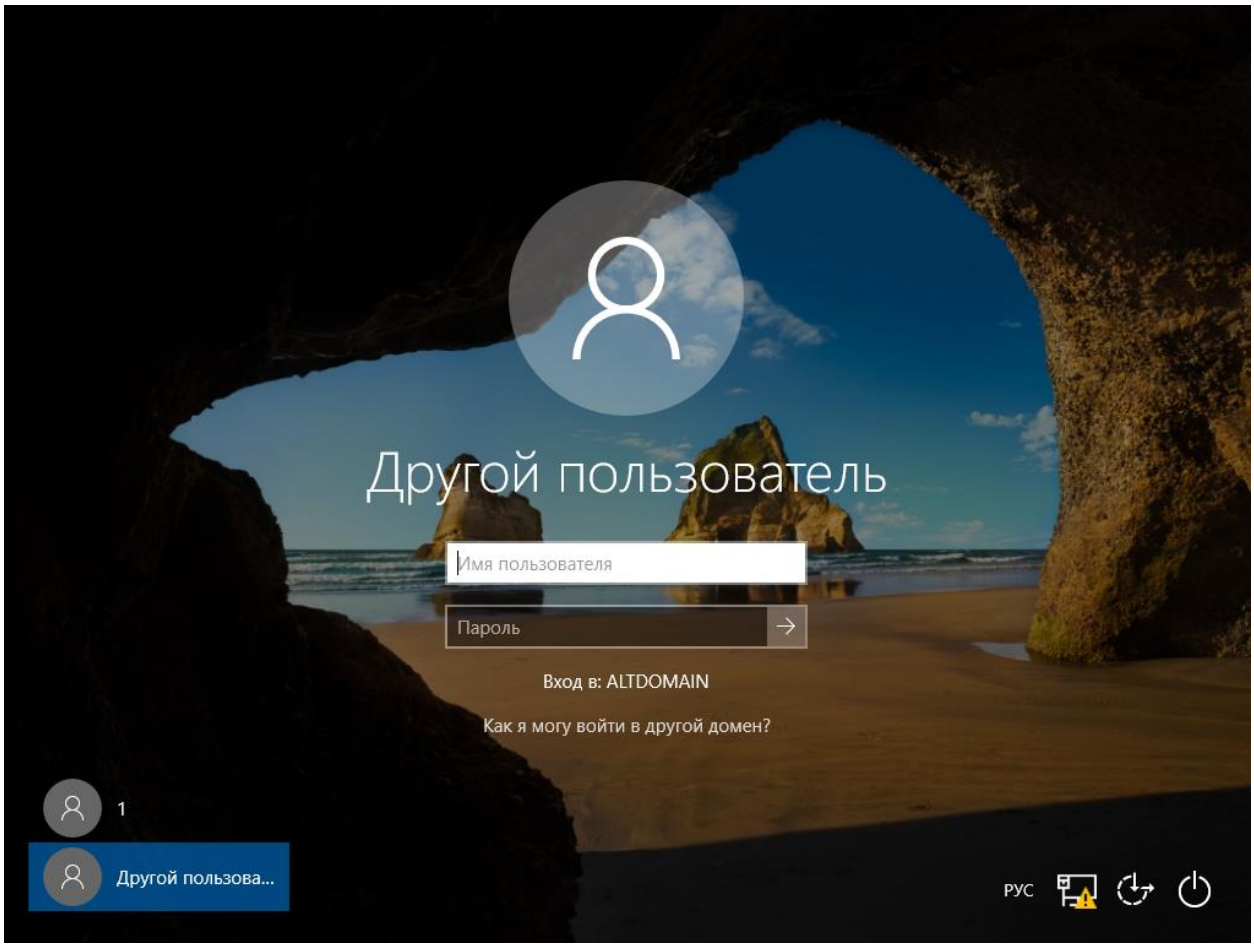

Рис. 4.15. Окно входа в систему доменного пользователя

Теперь, введя данные доменных пользователей (созданных в разделе 2.3.1), появилась возможность попадания в систему от имени домена.

После входа под доменным пользователем можно убедиться в этом при помощи команды «**whoami /all**» через командную строку windows (рис. 4.16).

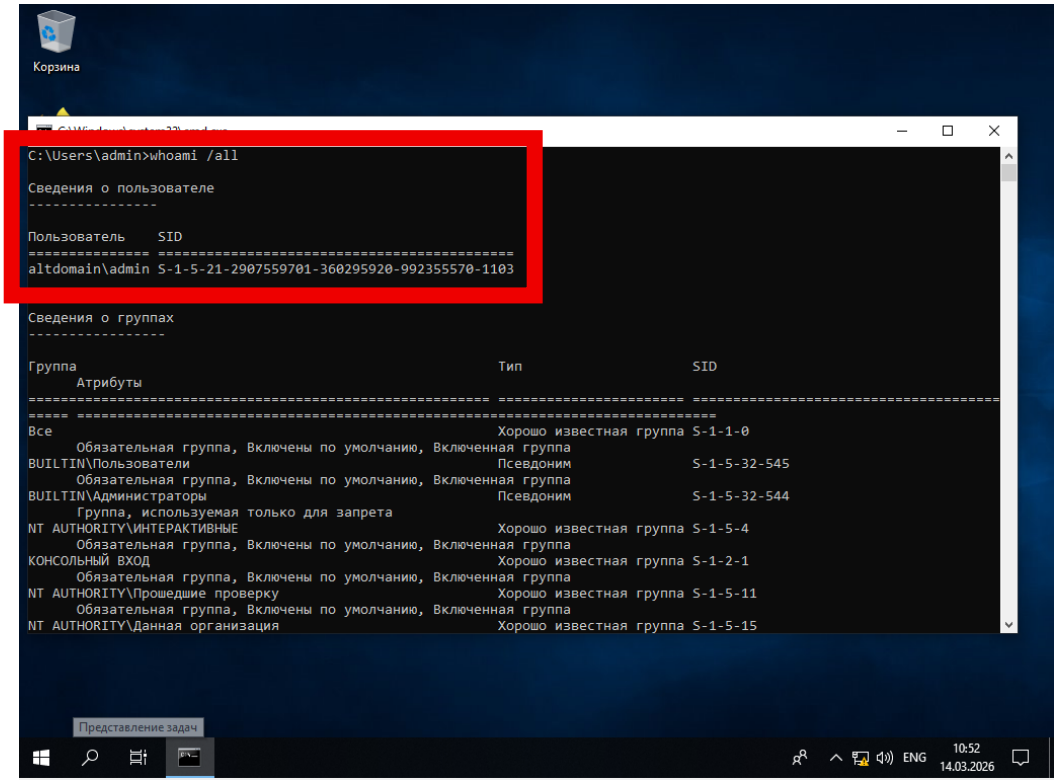

Рис. 4.16. Проверка данных пользователя

Как видно из рисунка 4.16, пользователь с именем «admin» является членом домена altdomain и видно его SID в системе (выделенно красным).

Теперь создадим пользователя с обычными правами и попробуем войти от его имени. Переключаемся на сервер и вводим команду «**samba-tool user add metoduser1**», пользователь, в нашем случае, будет иметь имя metoduser1 (рис. 4.17).

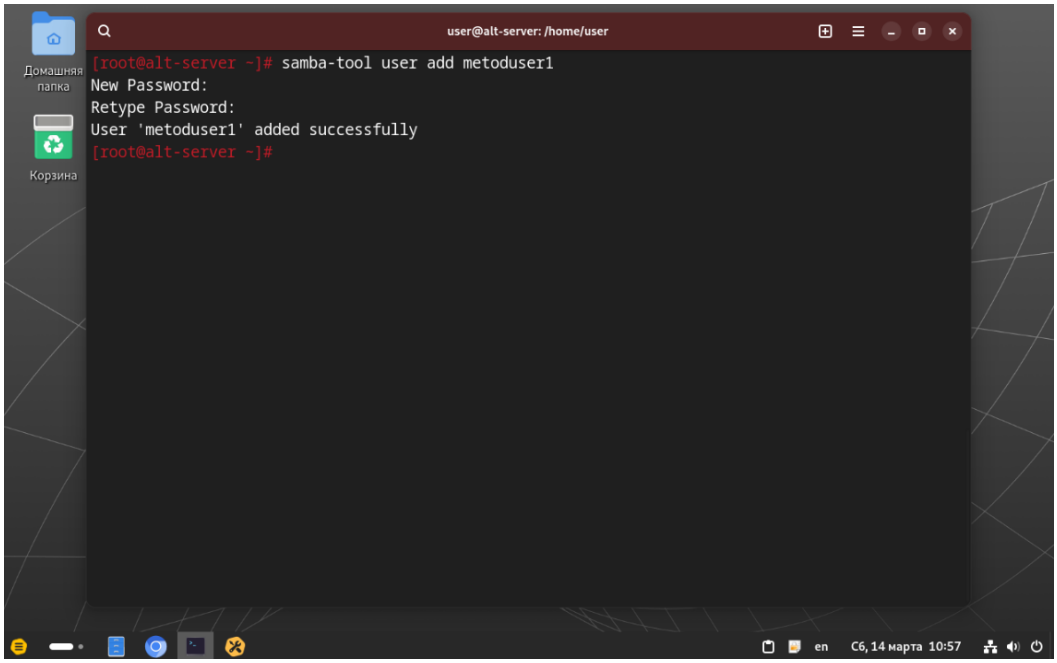

Рис. 4.17. Создание нового пользователя в домене

Теперь попробуем войти от имени пользователя metoduser1 в систему: рис 4.18. и проверим его данные через командную строку: рис. 4.19.

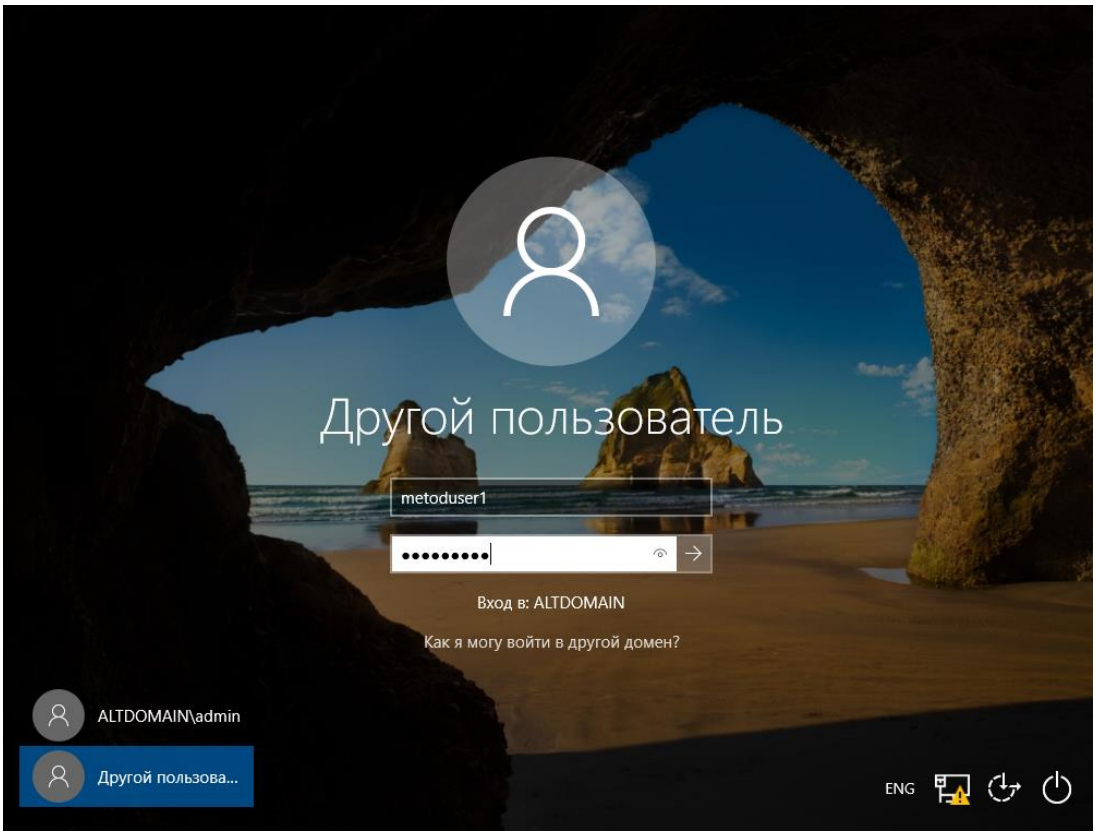

Рис. 4.18. Ввод данных пользователя при входе в систему

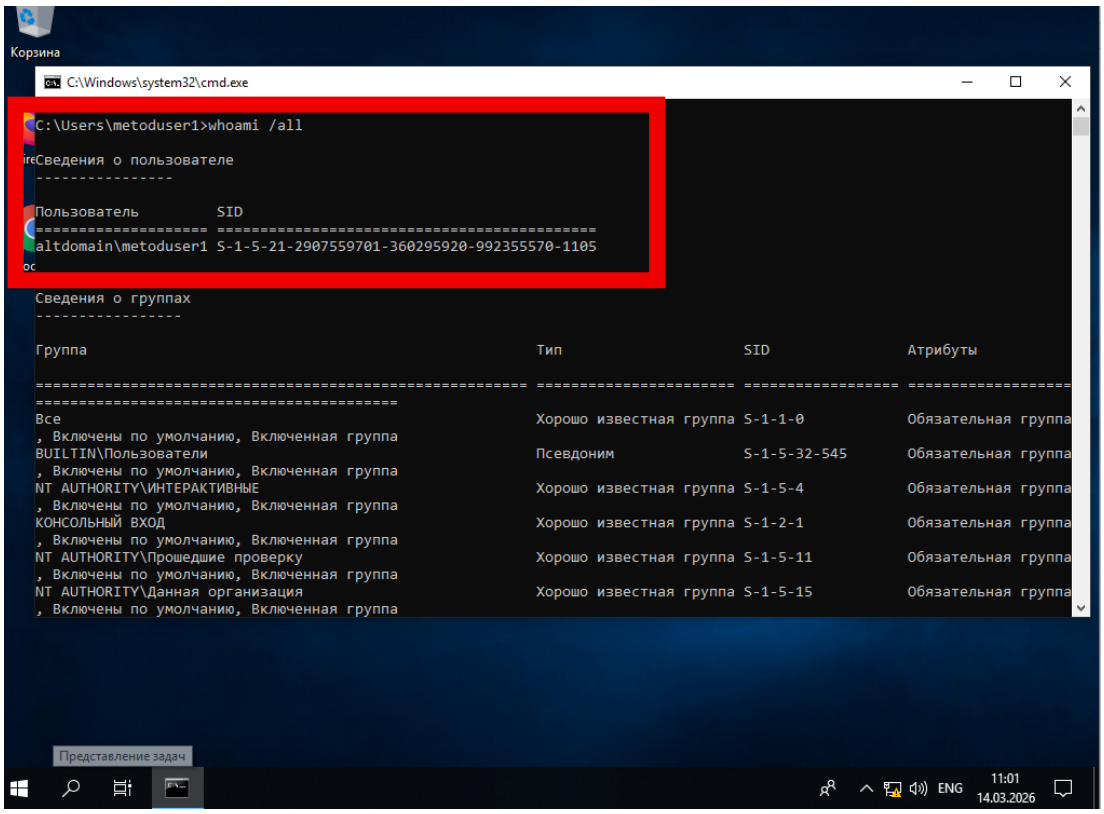

Рис. 4.19. Проверка данных пользователя через командную строку

Как видно на представленных рисунках (4.13, 4.15, 4.16, 4.18, 4.19) – доменная интеграция рабочей станции под управлением операционной системы windows 10 прошла успешно. Можно считать контроллер домена на базе sambaDC рабочим и готовым к дальнейшей работе в реальной серверной среде, некоторое управление которым приводится в разделе 2.3.1 настоящего методического пособия.

4.1.3. Использование файлового сервера в среде ОС Windows

Файловый сервер довольно удобный инструмент в компьютерной сети, в данном пункте рассмотрим процесс использования данной функции, развернутой в разделе 2.4 настоящего методического пособия.

Для подключения к файловому серверу по протоколу SMBv2, SMBv3 будем использовать Проводник Windows. Открываем проводник и в строке адреса пишем адрес вашего файлового сервера (в нашем случае \\alt-server) рис.4.20

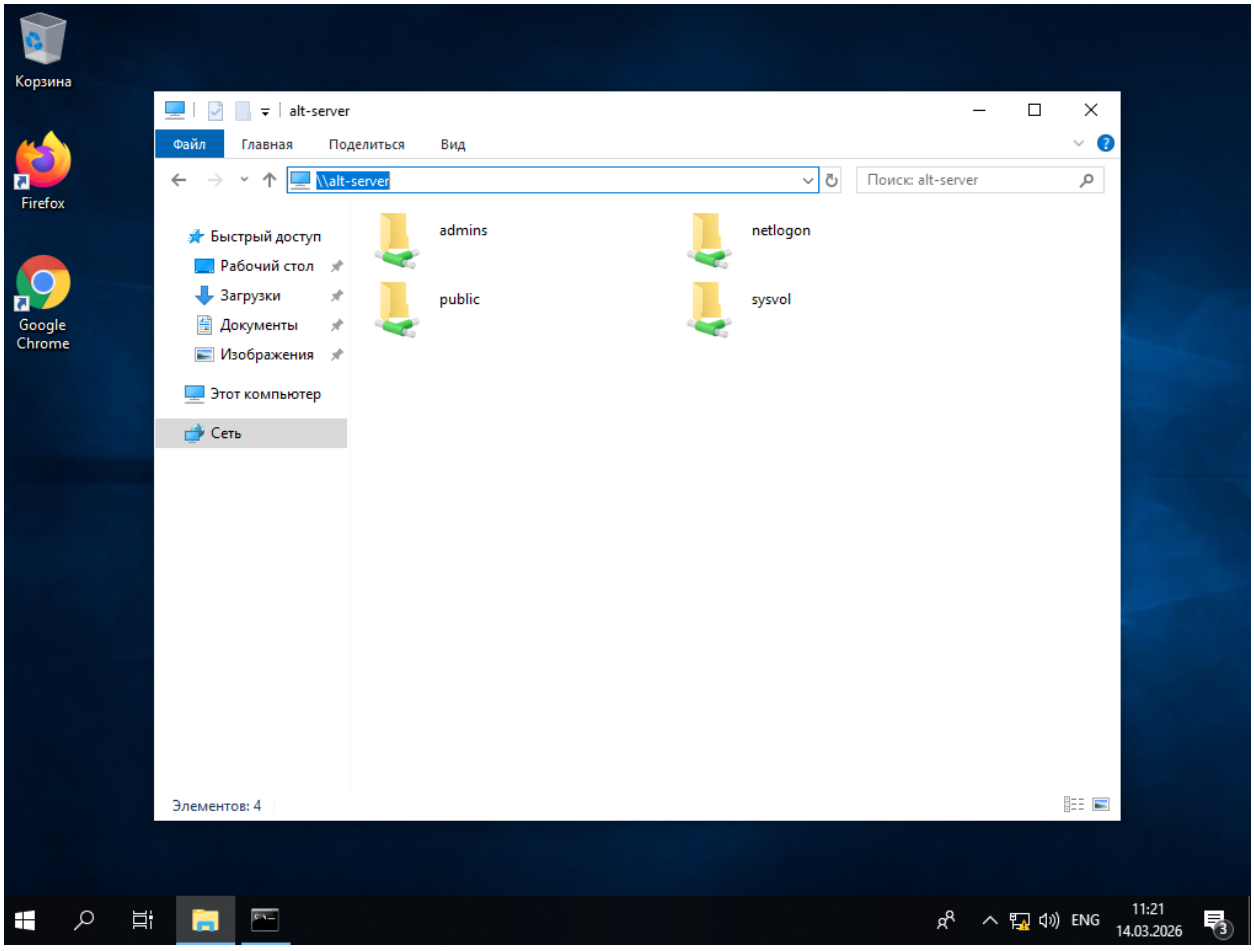

Рис. 4.20. Подключение к файловому серверу с использованием проводника

В нашем случае отображаются папки, настроенные на файловом сервере в разделе 2.4 настоящего методического пособия, среди них:

- Admins – папка, созданная для администраторов
- Public – папка, созданная для всех пользователей домена
- Netlogon – служебная папка, необходимая для сетевого входа в систему
- Sysvol – служебная папка, необходимая для репликации групповых политик
- Finans – папка, намеренно скрытая из списка, но доступная при прямом обращении \\alt-server\finans (пример попадания в неё показан на рис. 4.21)

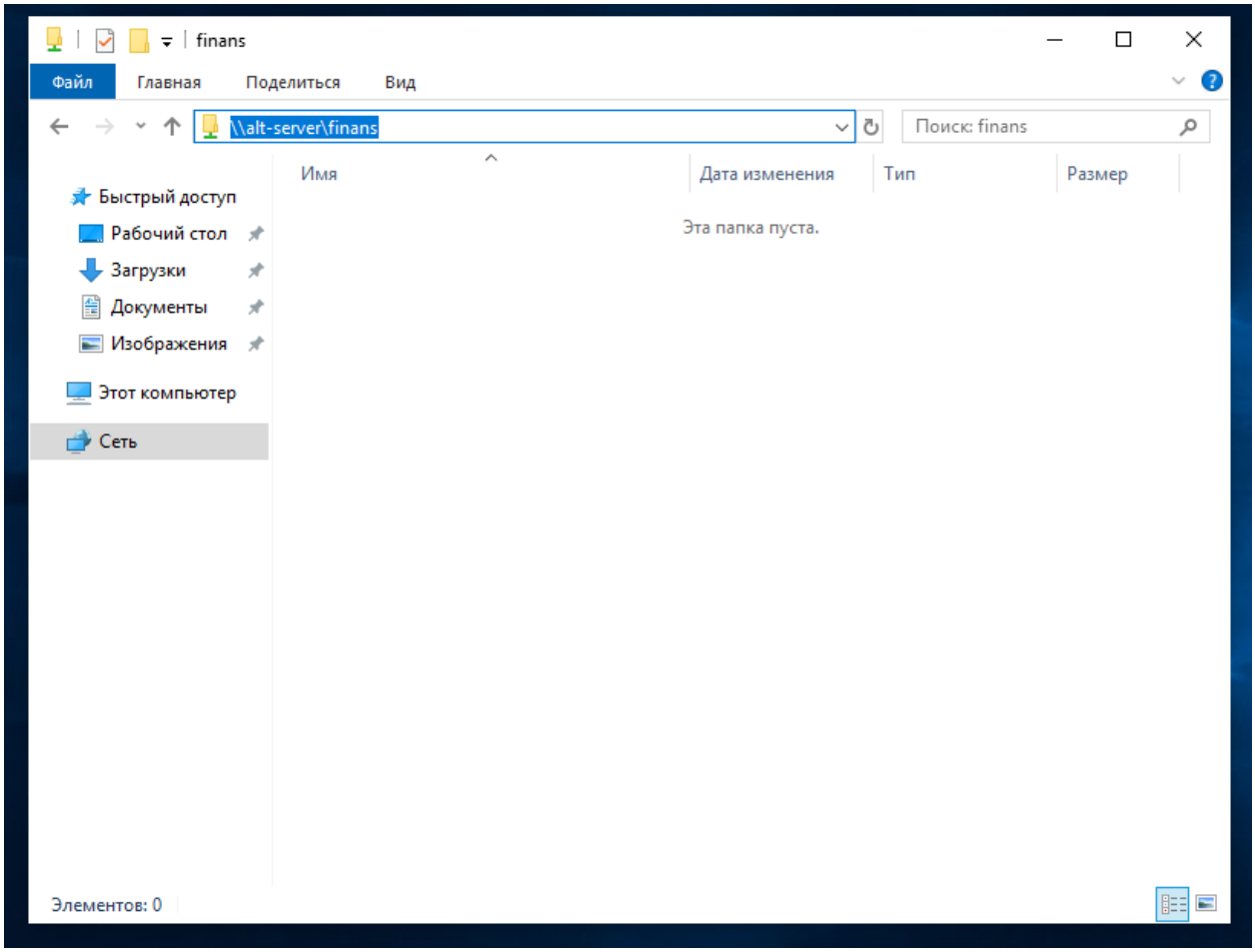

Рис. 4.21. Открытие скрытой папки на файловом сервере

Примечание 29. В целях безопасности, можно скрыть папки sysvol и netlogon путем присвоения им параметра ***browseable = no*** *в настройках файлового сервера рис. 4.22. Системные запросы идут напрямую к папкам, поэтому скрытие в данном случае не навредит, но скроет служебную информацию от пользователей рис. 4.23. На рисунках 4.24.1 и 4.24.2 приводится некоторое наполнение папок на файловом сервере.*

```
# Global parameters
[global]
        dns forwarder = 1.1.1.1
        netbios name = ALT-SERVER
        realm = ALTDOMAIN.NET
        server role = active directory domain controller
        workgroup = ALTDOMAIN

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No
        browseable = no

[netlogon]
        path = /var/lib/samba/sysvol/altdomain.net/scripts
        read only = No
        browseable = no

[admins]
path = /var/fs/admins
browseable = yes
read only = no
directory mask = 755
create mask = 754
valid users = @"Domain Admins"
guest ok = no
writeable = yes

[finans]
path = /var/fs/finans
browseable = no
```

Рис. 4.22. Скрытие служебных папок из файлового сервера

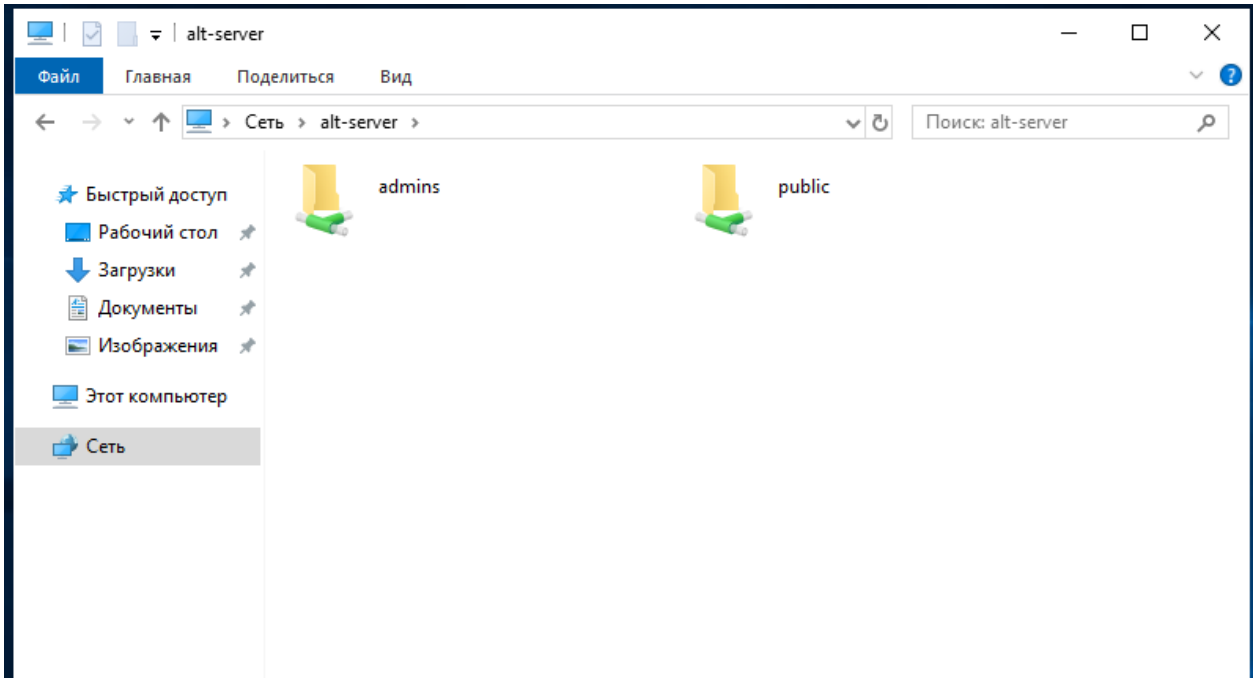

Рис. 4.23. Оставшиеся «видимые» папки

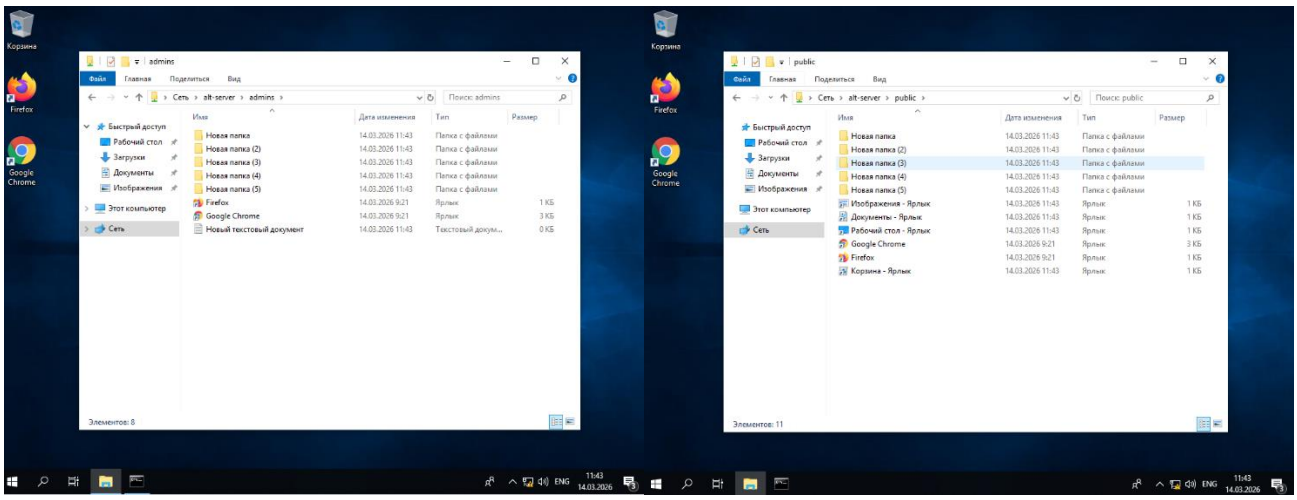

Рис. 4.24.1, 4.24.2. – некоторое наполнение папок файлового сервера из-под клиента с операционной системой Windows

После проделанных действий и проверок в разделе 4.1.3 можно считать, что файловый сервер, развернутый в разделе 2.4, успешно прошел проверку и готов к работе, ошибок в конфигурации и работе нет.

4.1.4. Проверка доступности сети Интернет в среде ОС Windows (тестирование программного прокси-сервера squid)

Для проверки доступности сети Интернет через прокси-сервер, развернутый в разделе 2.5 настоящего методического пособия воспользуемся любым интернет-браузером, доступным на вашем клиенте.

Без предварительной настройки сети на клиенте у вас будет либо бесконечная загрузка страницы (рис. 4.25) либо ошибка подключения/соединения (рис. 4.26) чтобы такого не возникало необходимо настроить клиентскую ОС на работу с программным прокси-сервером, развернутым ранее.

Примечание 30. Главное отличие настройки прокси-сервера в windows 7 и windows 10 заключается в уровне настройки: в Windows 7 параметры прокси задавались глобально, в основном через окно «Свойства браузера» (Панель управления), и они применялись ко всем приложениям, которые умели их считывать. В Windows 10 предусмотрено разделение контекстов. Настройки прокси вынесены в отдельный раздел параметров системы («Сеть и Интернет»), но самое важное — появилось четкое разграничение между использованием прокси для обычного веб-трафика (браузеры) и для приложений.

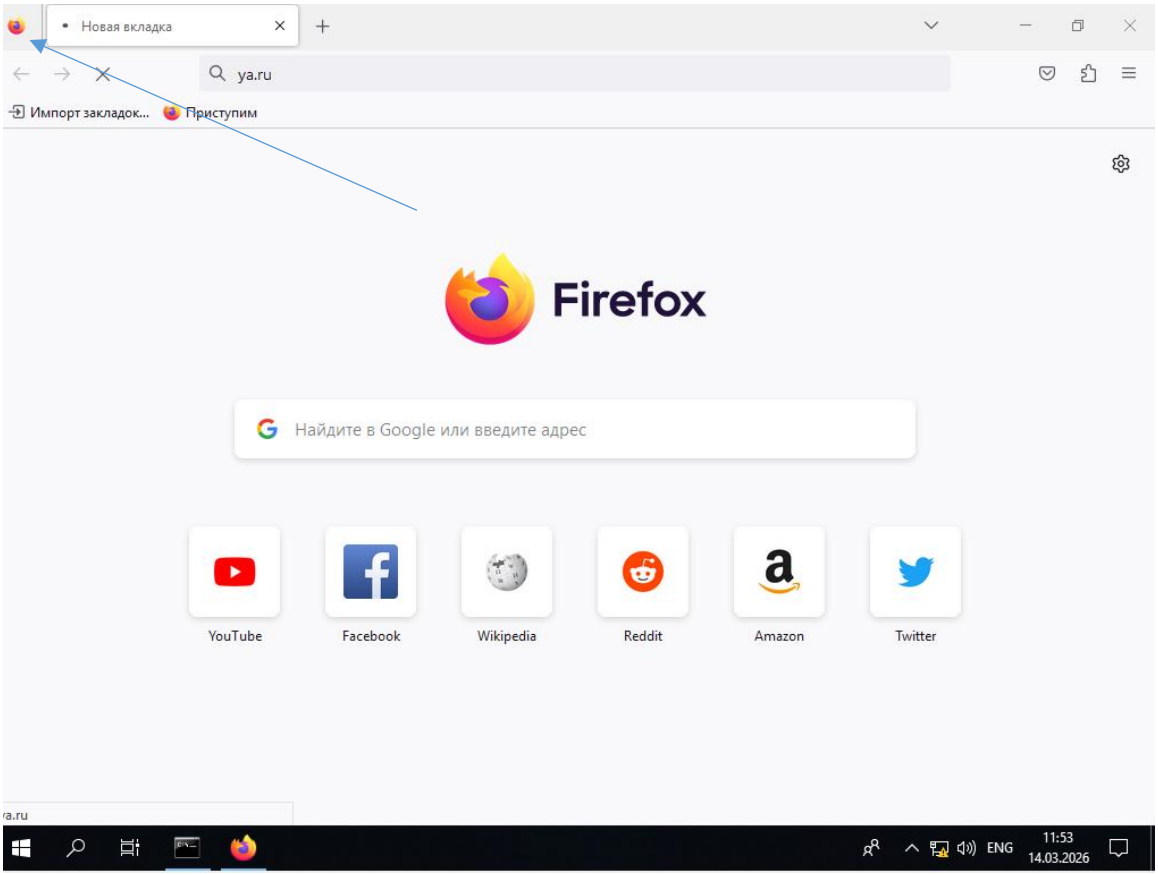

Рис. 4.25. Бесконечная загрузка страницы

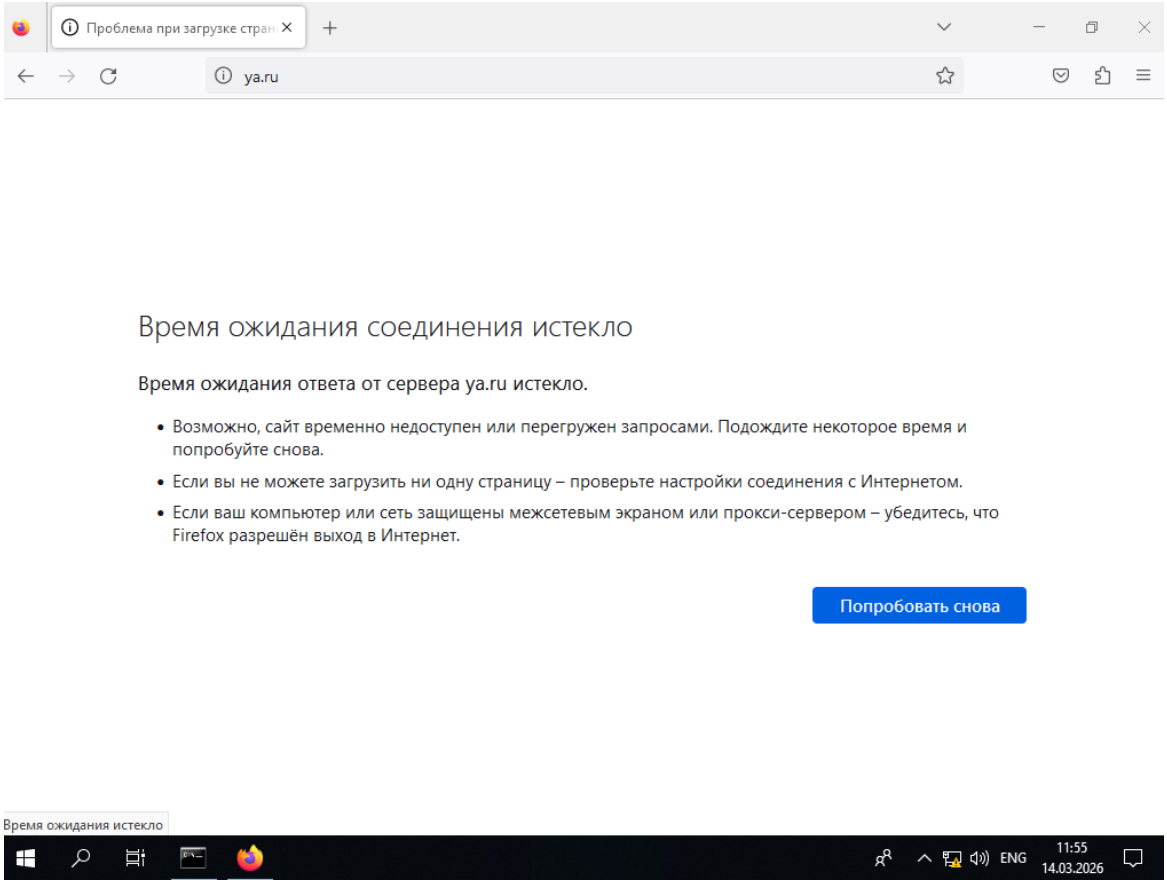

Рис. 4.26. Ошибка подключения

Для обеспечения работы сети Интернет на рабочей станции под управлением операционной системы Windows 10 перейдем в «Параметры ПК», раздел «Сеть и Интернет» рис. 4.27.

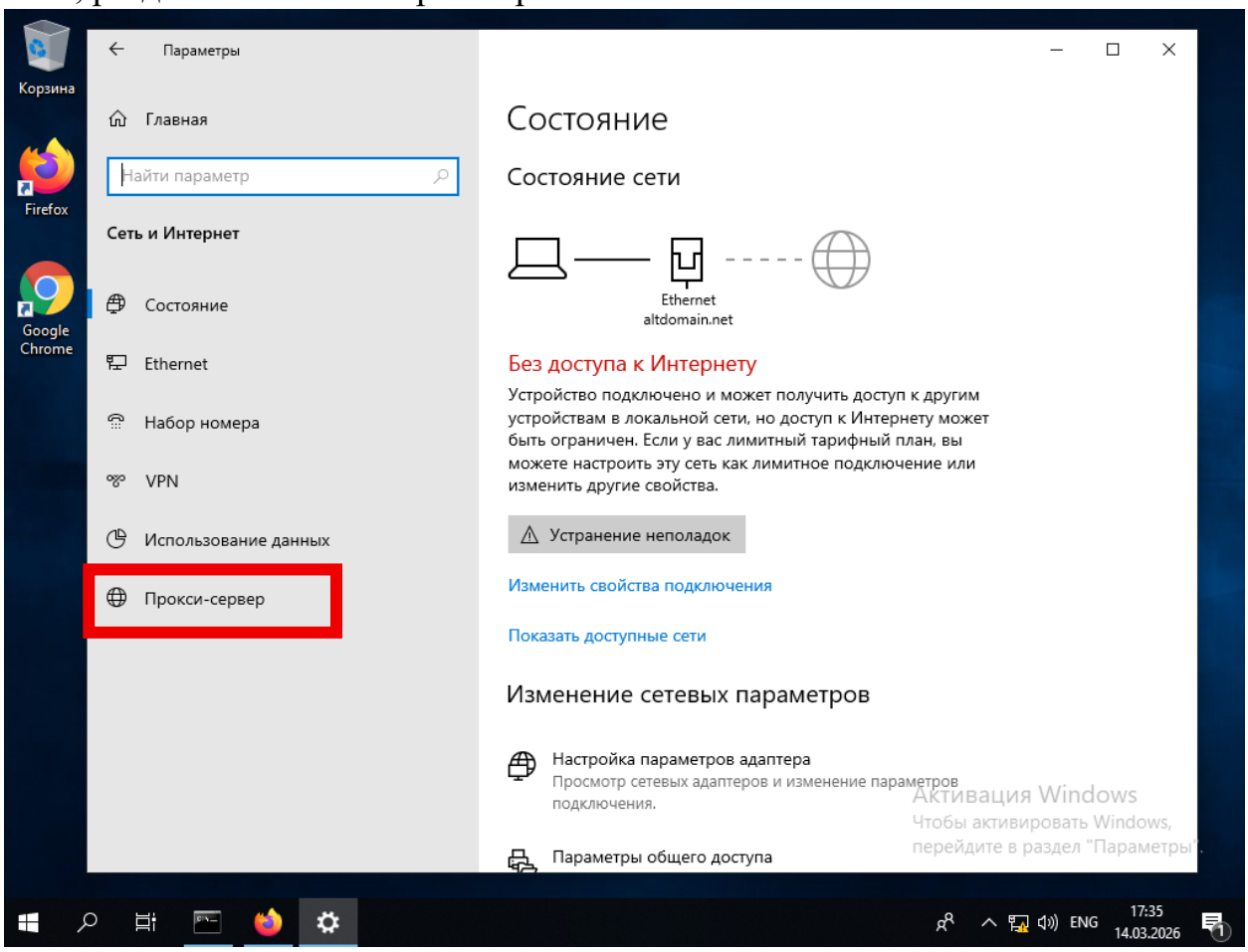

Рис. 4.27. Раздел «Сеть и Интернет» в приложении «Параметры ПК»

Перейдем в раздел «Прокси-сервер» - выделенно красным на рис. 4.27, где выполним настройку прокси-сервера для клиента. В данном разделе укажем адрес прокси-сервера и порт, на котором слушает прокси-сервер squid, настроенный в разделе 2.5 настоящего методического пособия, также переключим галочку на пункте «Не использовать прокси-сервер для локальных адресов» в положение включено, чтобы избежать проксирования запросов внутри локальной сети. Пример настройки прокси-сервера приведен на рисунке 4.28.

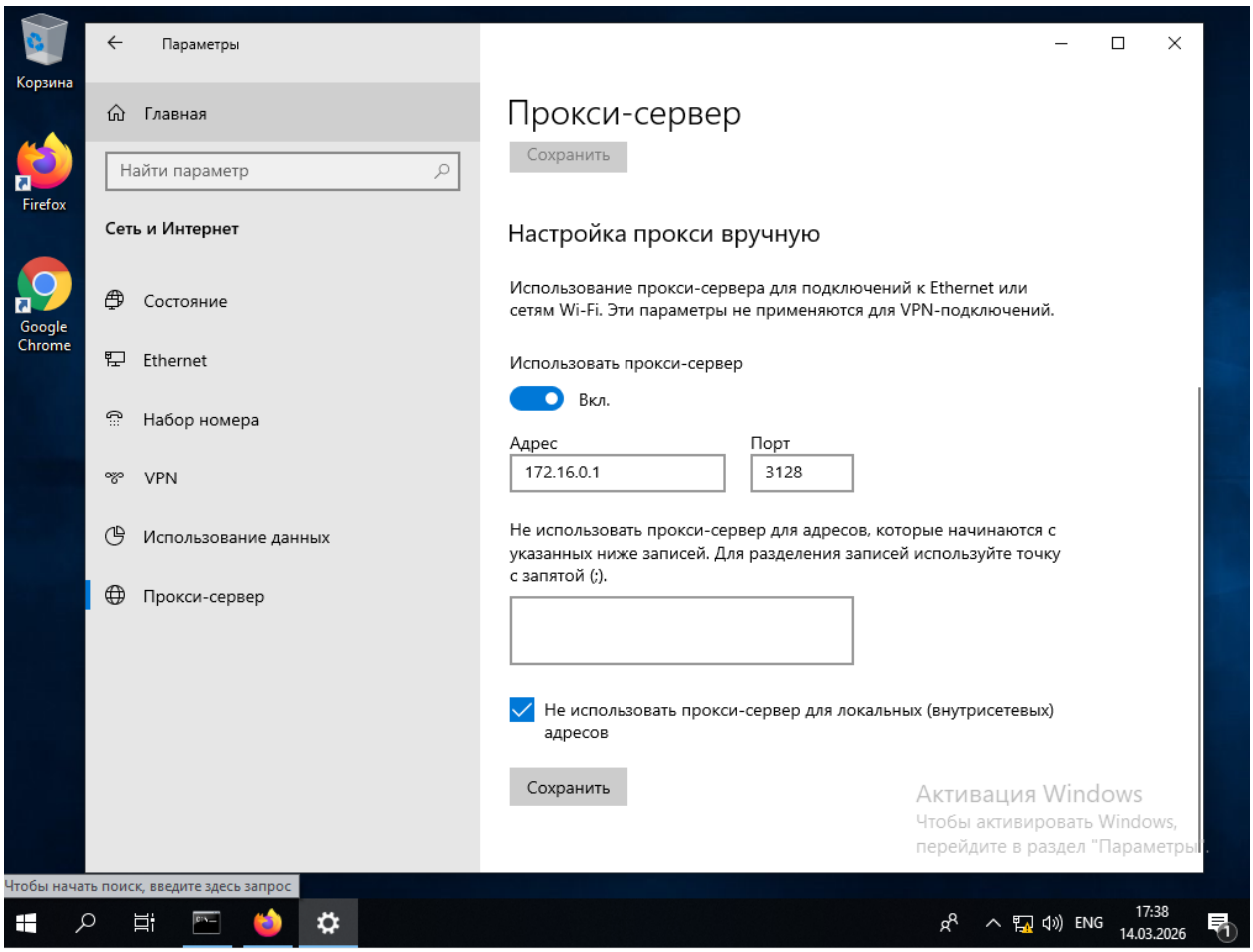

Рис. 4.28. Настройка прокси-сервера на клиенте

После чего сохраним указанные настройки и проверим доступность сети Интернет в браузере. При открытии браузера настройки прокси уже будут на него распространяться и настраивать браузер отдельно нет необходимости. Как видно из рисунков 4.29, 4.30, 4.31, 4.32 – прокси-сервер работает корректно и доступ в Интернет для клиентов обеспечен.

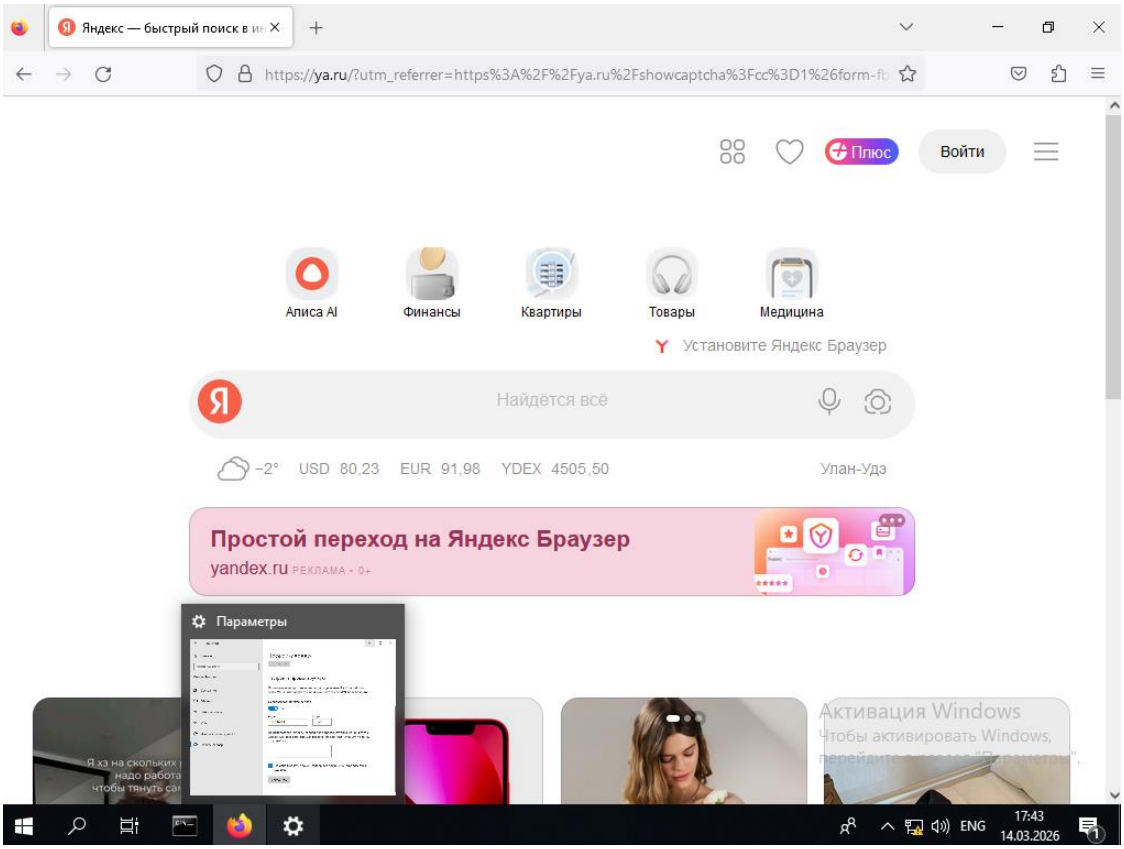

Рис. 4.29. Проверка доступности сети Интернет на примере поиска Yandex

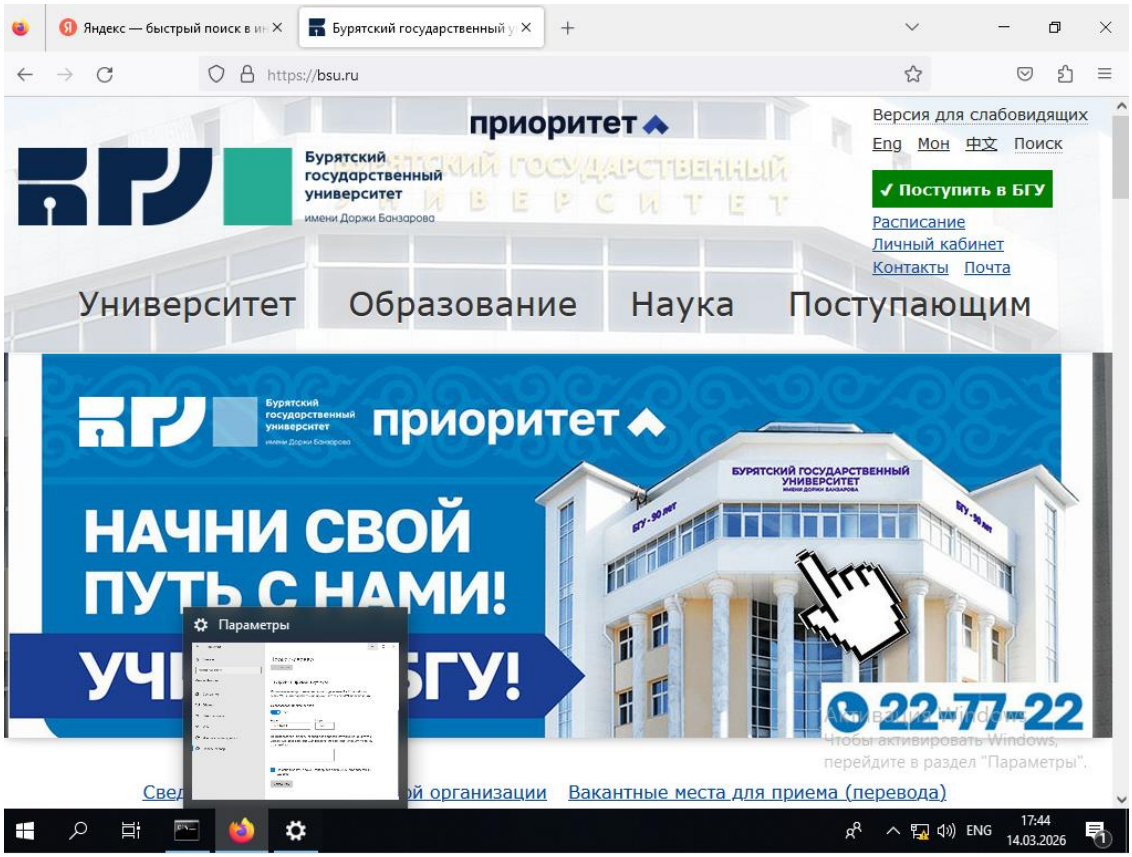

Рис. 4.30. Проверка доступности сети Интернет на примере сайта bsu.ru

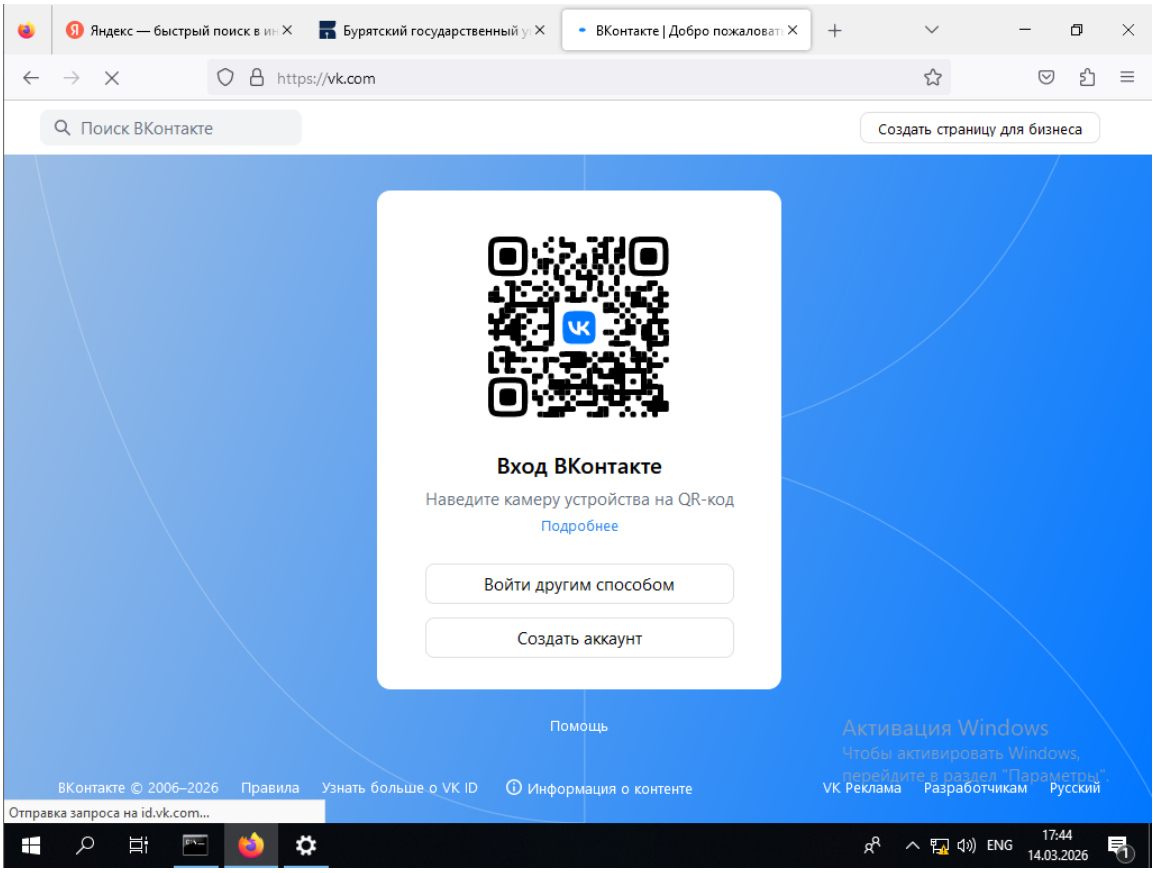

Рис. 4.31. Проверка доступности сети Интернет на примере сайта ВКонтакте

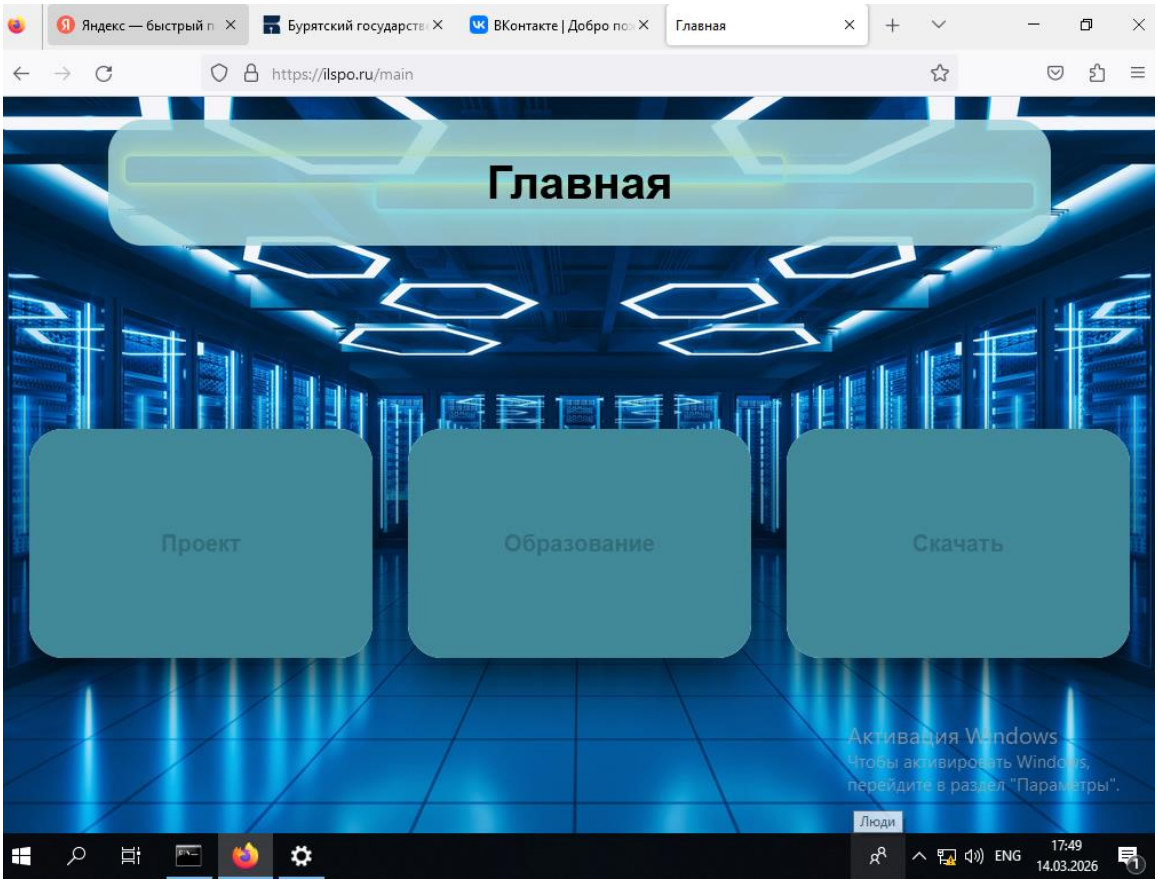

Рис. 4.32. Проверка доступности сети Интернет на примере сайта ilspo.ru

4.2. Интеграция станции BaseALT в доменную инфраструктуру

4.2.1. Автоматическое получение настроек с сервера (dhcp, dns)

Сразу после установки клиентской машины с ОС BaseALT Workstation Linux, она должна в автоматическом режиме получить настройки с ранее настроенного сервера, а именно настройки ip адреса, для общения с другими устройствами по сети (корректность работы dhcp) и настройки dns для разрешения сетевых имен из доменных имен в ip адреса (корректность работы dns).

Для проверки настроек ip адреса в linux вызовем утилиту «Терминал» или «Консоль», затем в открывшимся окне командной оболочки введем команду «ip a» для просмотра свойств сетевого адаптера рис.4.33 – в данном случае нас интересует сетевой адаптер с именем enp0s3, который настроен на работу во внутренней сети с сервером на базе BaseAlt linux server (белым выделен, полученный с сервера, ip адрес)

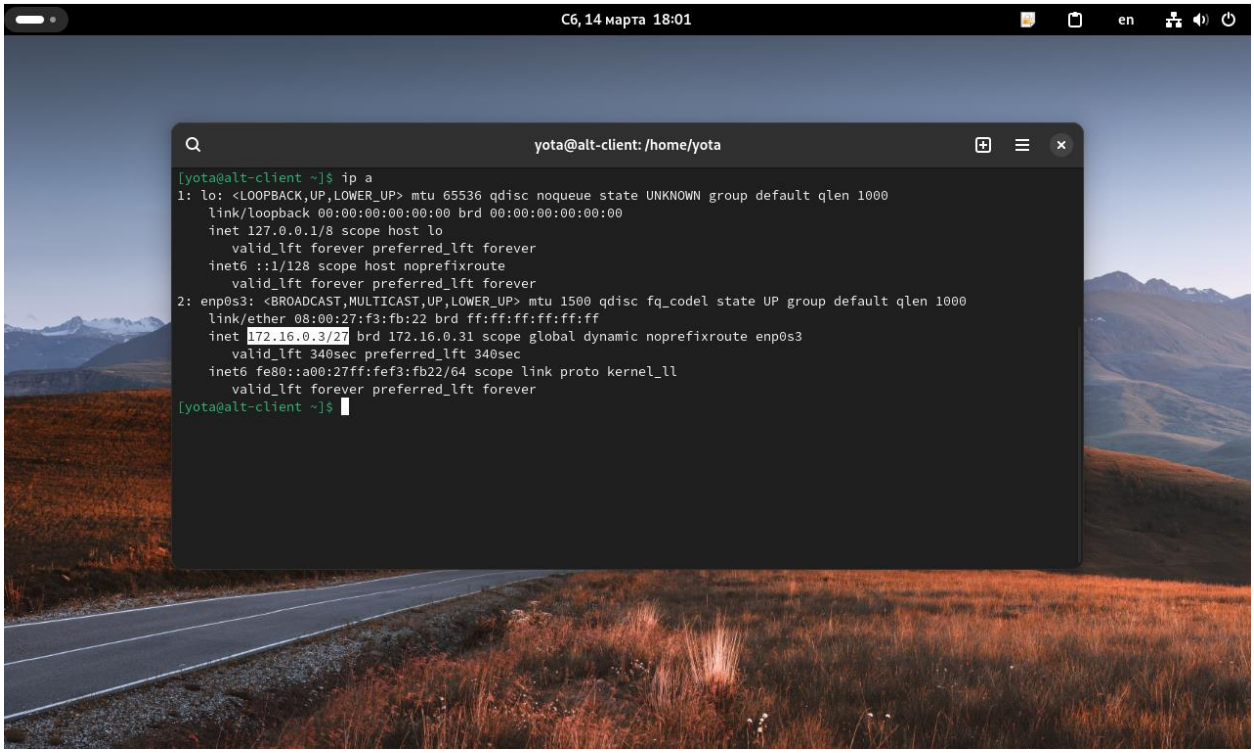

Рис. 4.33. Проверка свойств сетевого адаптера в linux

Затем можно проверить и убедиться в работоспособности dns сервера, развернутого в разделе 2.3 настоящего методического пособия, как в ОС windows, в данном случае нам поможет команда «nslookup» с указанием доменного имени ресурса, например «**nslookup ya.ru**» - проверим ip адреса Яндекса рисунок 4.34. – как видно из рисунка, настройки корректны и запросы от клиента отрабатываются.

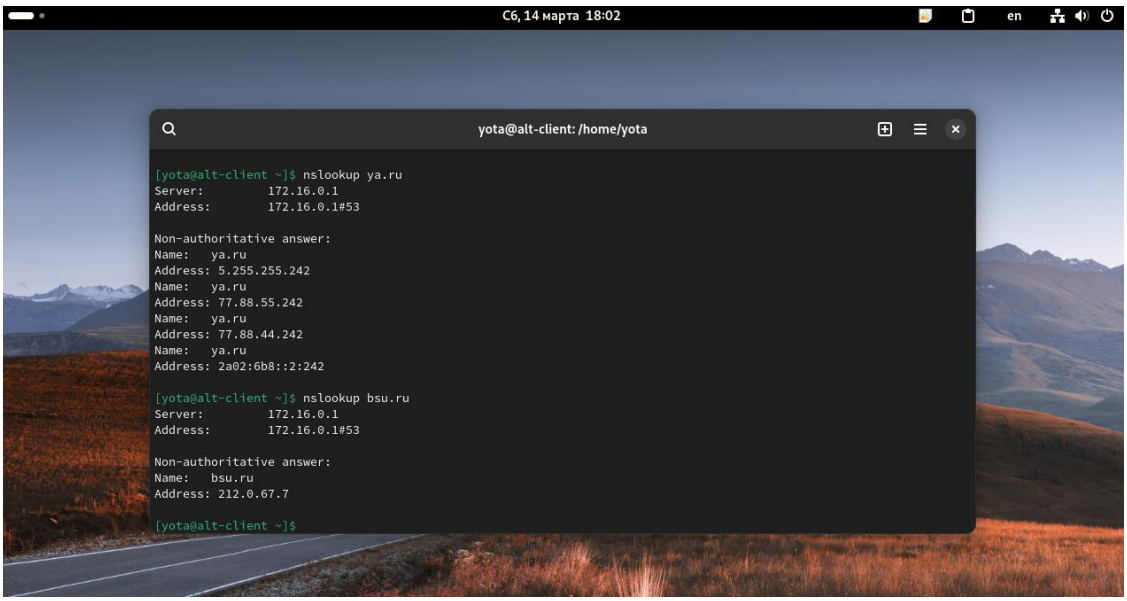

Рис. 4.34. Проверка dns сервера на базе ос linux

4.2.2. Подключение Linux к контроллеру домена SambaDC

Операционная система BaseAlt Workstation 11 поддерживает интеграцию с различными типами доменных инфраструктур: FreeIPA, ActiveDirectory, ALD Pro, ALT домен, SambaDC и тд.

Для интеграции системы с доменом откроем приложение «Центр управления системой» в разделе «Пользователи» выберем «Аутентификация» - рисунок 4.35, выделено красным.

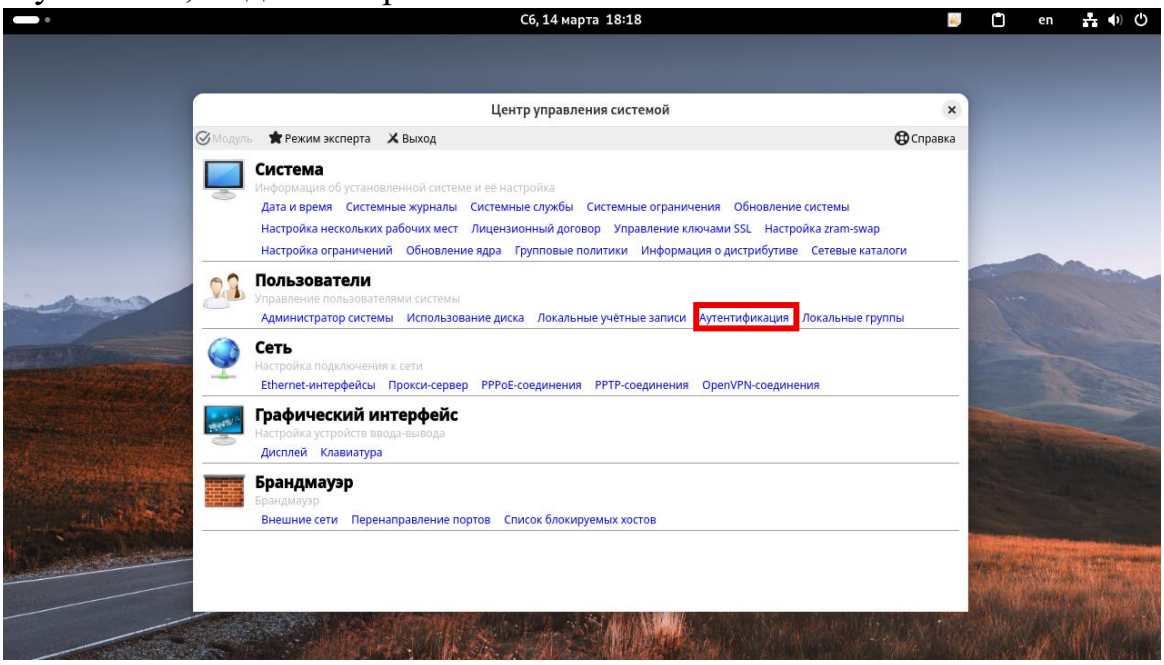

Рис. 4.35. Центр управления системой на клиенте

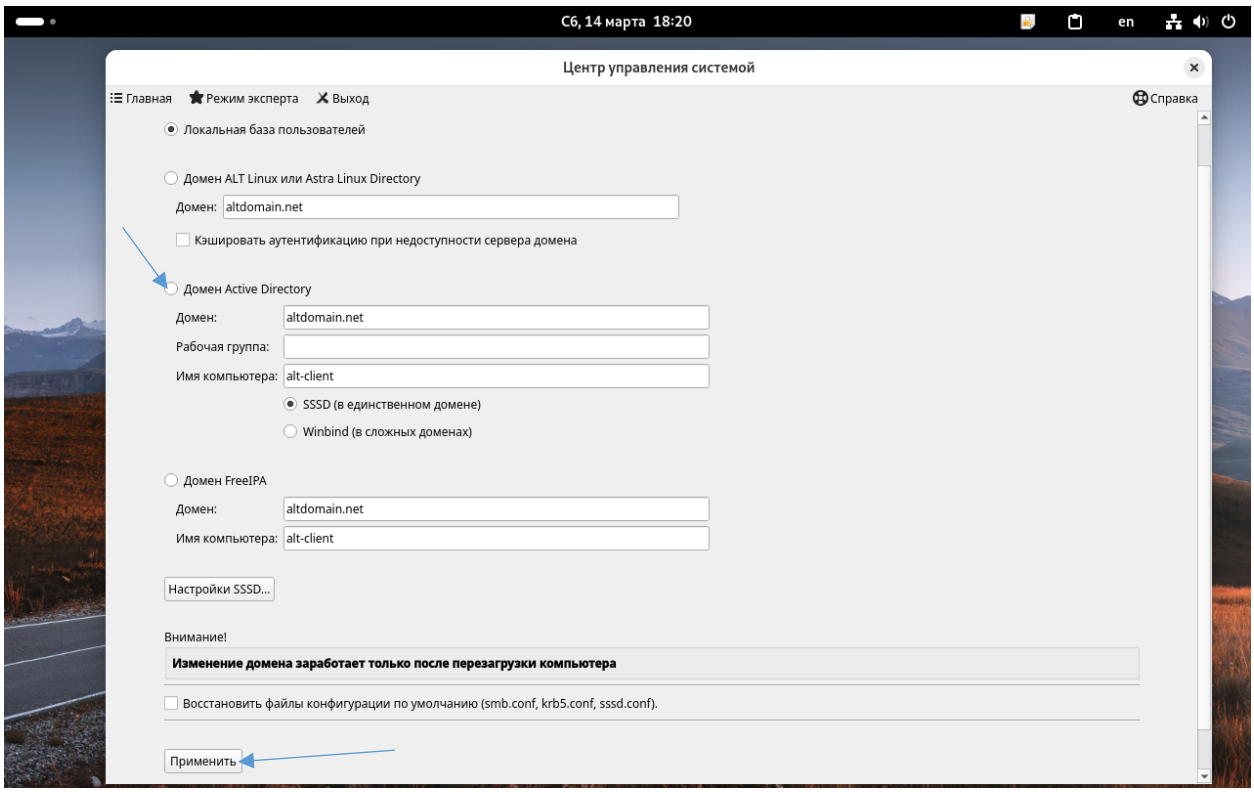

Рис. 4.36. Аутентификация станции в домене

В нашем случае домен SambaDC работает в режиме ActiveDirectory, поэтому имя домена и имя компьютера (хоста, клиентской машины) определились автоматически. Ставим галочку напротив пункта «Домен ActiveDirectory» и нажимаем клавишу применить.

После этого, как в случае с windows, система потребует данные пользователя для входа в домен, обладающего правами администратора домена или правами на ввод клиента в домен: укажем данные пользователя, созданного в разделе 2.3.1 настоящего методического пособия. Пример приведен на рисунке 4.37.1, 4.37.2.

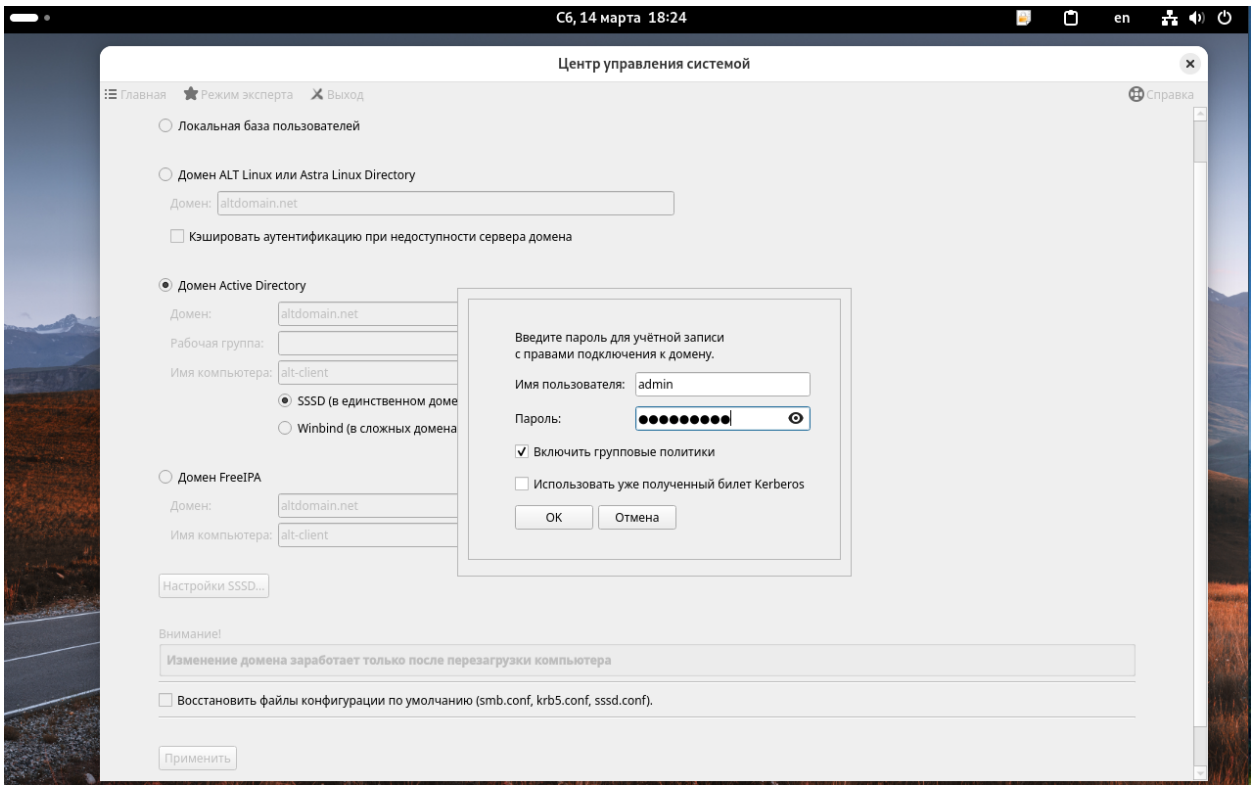

Рис. 4.37.1. Ввод данных пользователя

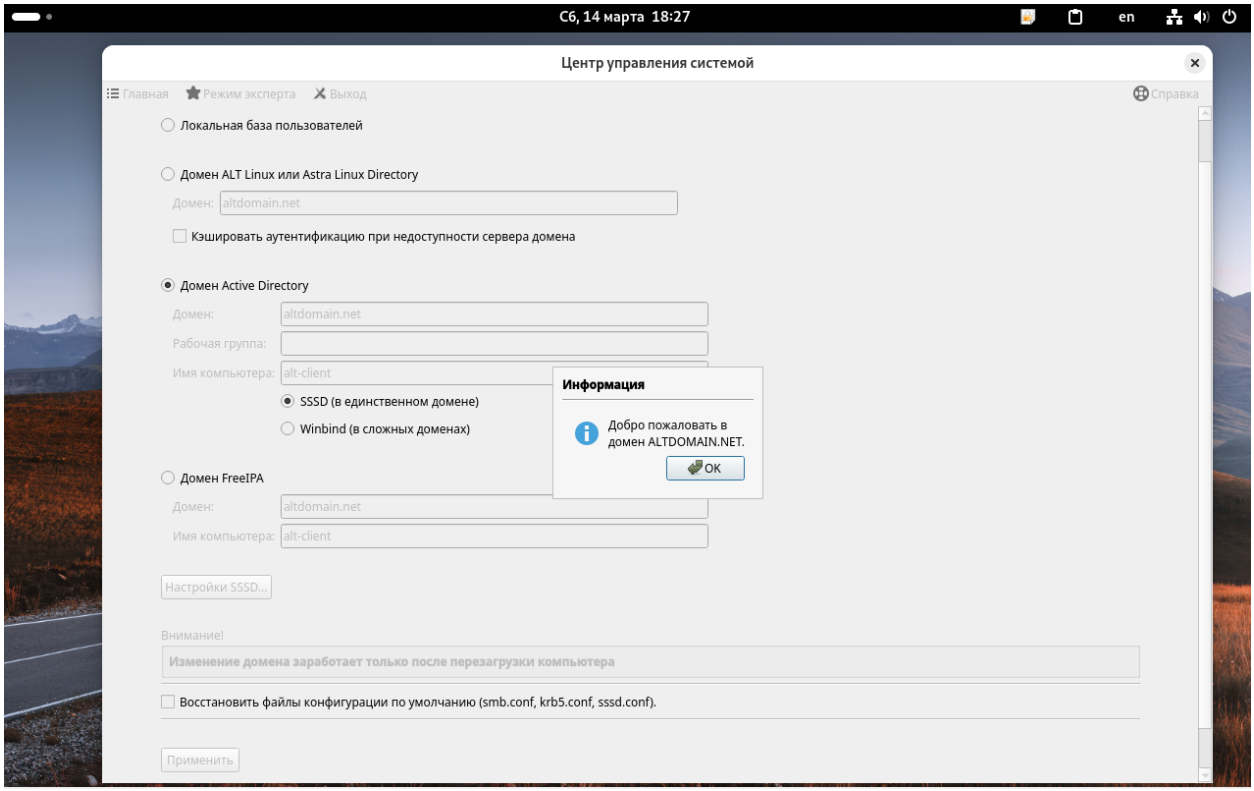

Рис. 4.37.2. Сообщение об успешности ввода машины в домен

После данного сообщения перезагрузим систему.

После перезагрузки перед вами откроется стандартное окно входа в систему без ощутимых изменений, но вход домен уже доступен, для этого нажмем на кнопку «Нет в списке?» рис. 4.38, обведено красным.

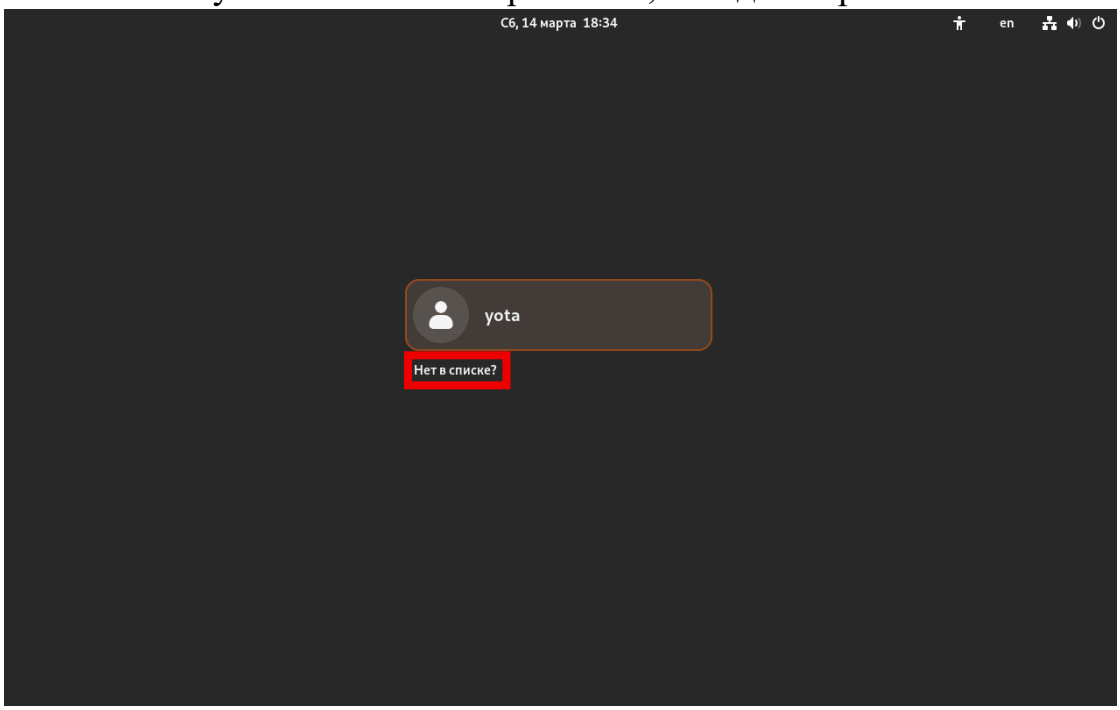

Рис. 4.38. Окно входа в систему

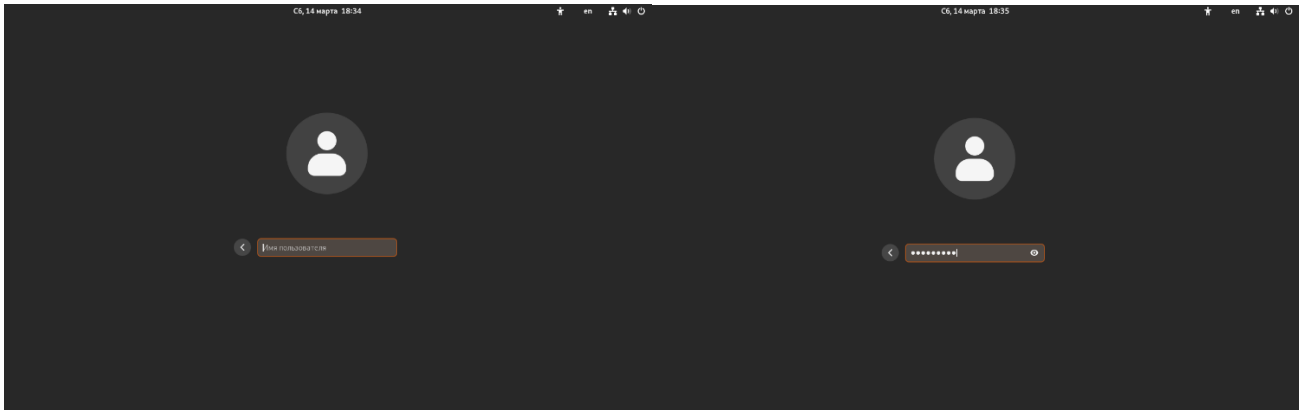

Рис. 4.39.1, 4.39.2 Окно ввода имени пользователя и пароля

Перед вами откроется окно ввода имени пользователя домена, после ввода которого следует нажать клавишу «Enter» на клавиатуре. После чего потребуется ввод пароля пользователя рис. 4.39.2. Через некоторое время вход через доменного пользователя будет выполнен, проверить учетную запись можно через консоль командой «**whoami**» обведено синим или в строке адреса командного интерпретатора (в качестве абсолютного пути до папки пользователя) обведено красным рис.4.40.

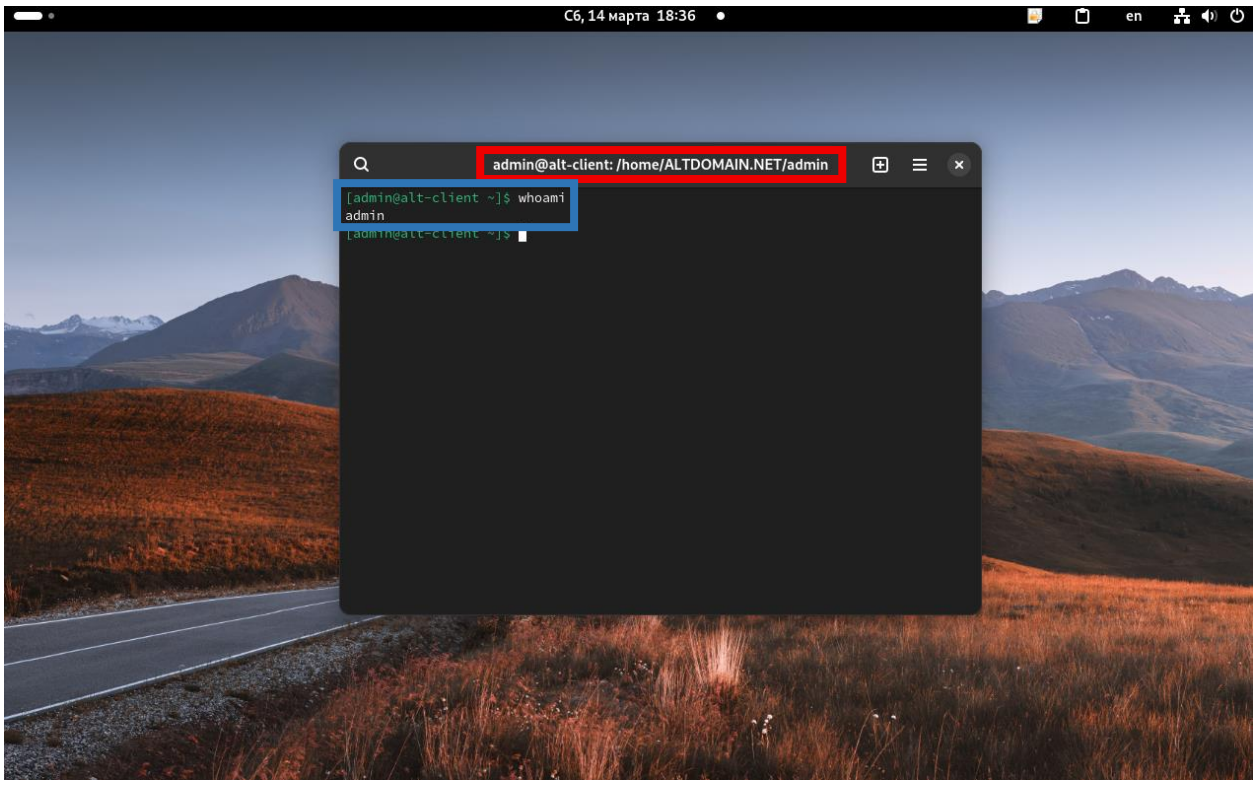

Рис. 4.40. Запуск консоли из-под доменного пользователя

После проделанных действий можно считать, что ввод клиентской рабочей станции под управлением операционной системы BaseAlt Workstation 11 выполнен успешно.

4.2.3. Использование файлового сервера в среде ОС Linux

Подключение файлового сервера в системе linux отличается от подключения к файловому серверу в windows необходимостью явного указания протокола подключения (т.к. linux в отличие windows поддерживает большее количество протоколов подключения к файловым хранилищам «из коробки» и без сторонних приложений).

Для подключения к файловому серверу в linux откроем приложение «Файлы» (иногда в роли него могут выступать приложения thunar, nemo, pcmanfm, nautilus, dolphin) и введем в адресной строке полный путь до сервера с явным указанием протокола: smb://alt-server.altdomain.net, пример приводится на рис.4.41.1, 4.41.2.

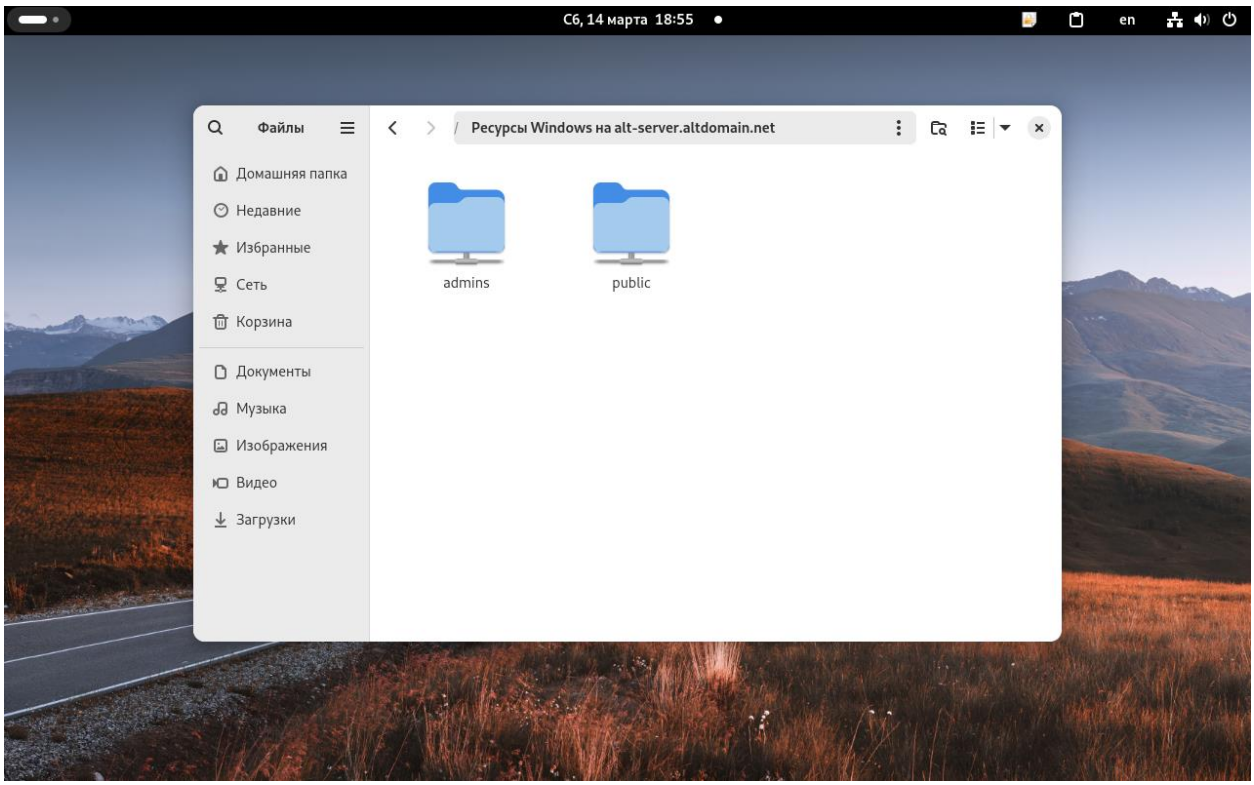

Рис. 4.41.1. Подключение к файловому серверу

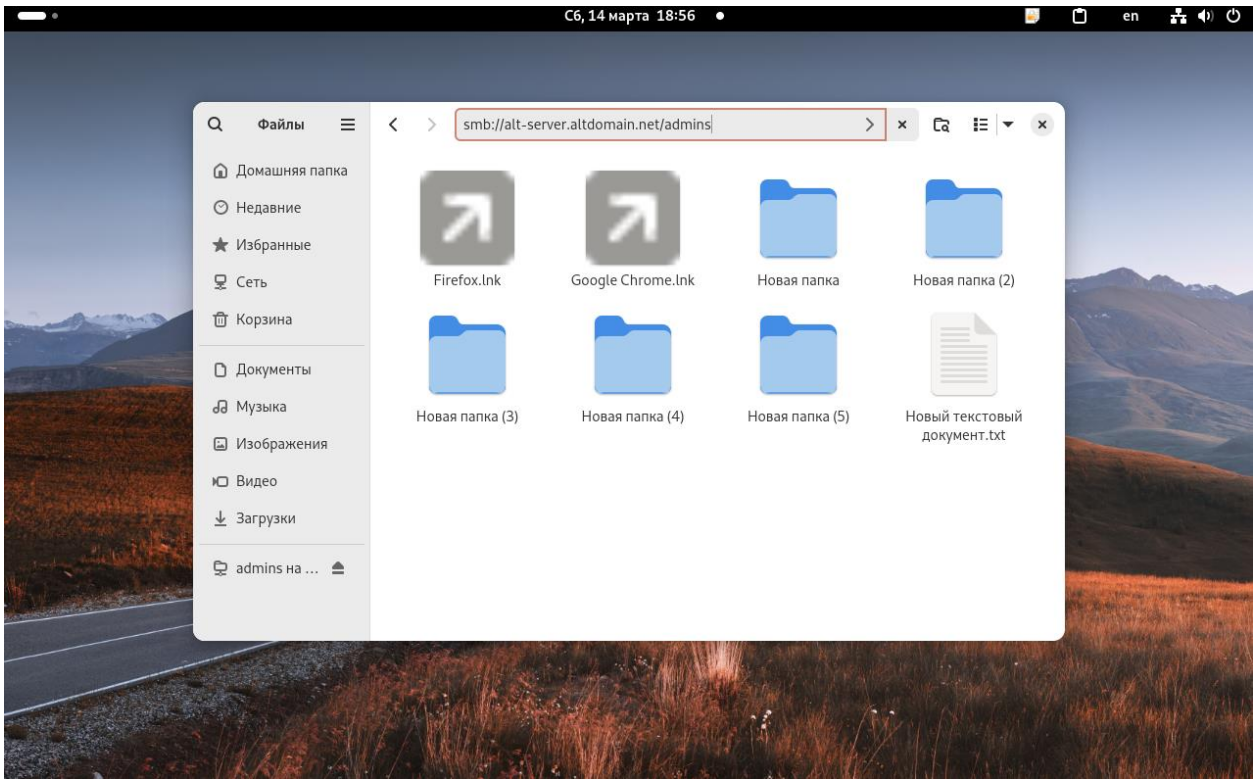

Рис. 4.41.2. Подключение к конкретному ресурсу на файловом сервере

Примечание 31. Список файлов на файловом сервере должен совпадать с содержанием при открытии файлового сервера на операционной системе windows, подключение к которому приводится в разделе 4.1.3 настоящего методического пособия.

4.2.4. Проверка доступности сети Интернет в среде ОС Linux (тестирование программного прокси-сервера squid)

Для проверки доступности сети Интернет через прокси-сервер, развернутый в разделе 2.5 настоящего методического пособия воспользуемся любым интернет-браузером, доступным на вашем клиенте.

Без предварительной настройки сети на клиенте у вас будет либо бесконечная загрузка страницы (рис. 4.25) либо ошибка подключения/соединения (рис. 4.26) чтобы такого не возникало необходимо настроить клиентскую ОС на работу с программным прокси-сервером, развернутым ранее – это требование является одинаковым как для рабочих станций windows клиентов, так и для рабочих станций linux.

В случае с linux указать прокси-сервер нужно прописать в настройках системы. Для этого откроем параметры системы из меню приложений, попасть в которое можно нажатие на «ползунок» в левом верхнем углу экрана. Меню приложений и приложение настроек показаны на рисунке 4.42.

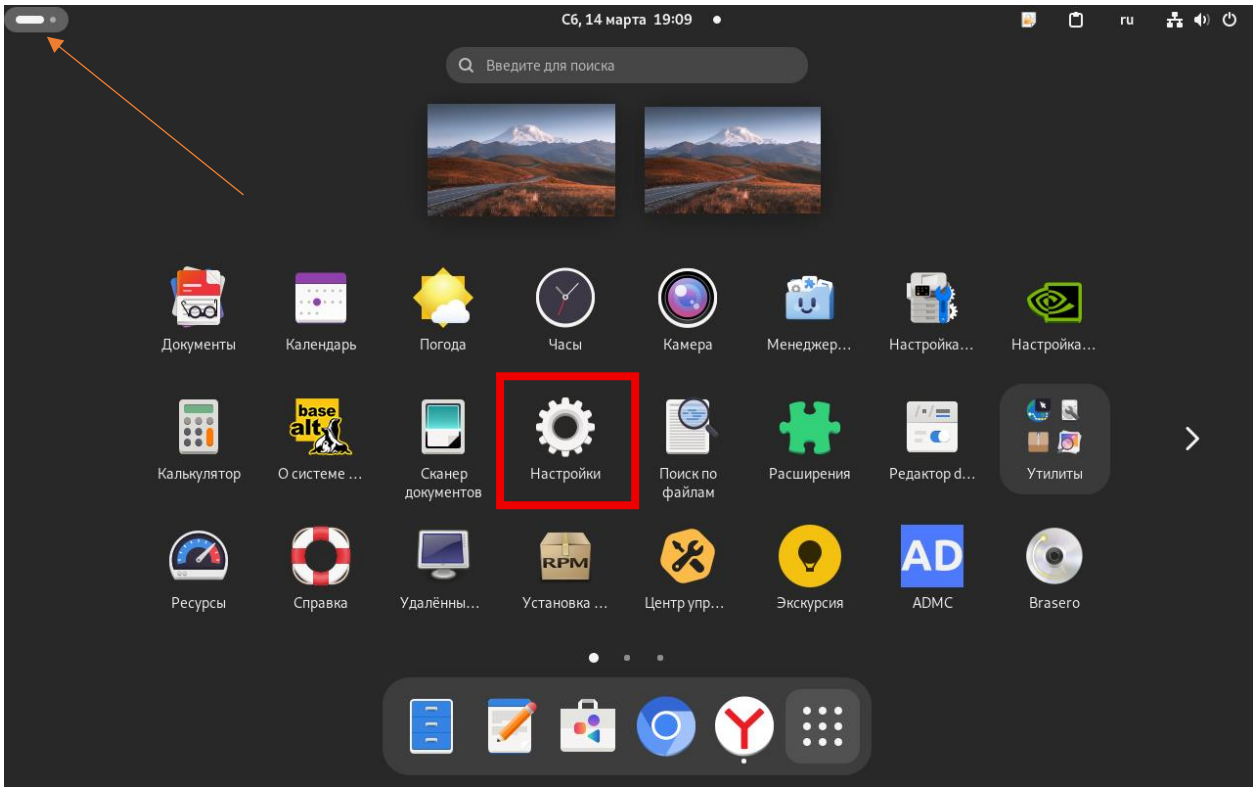

Рис. 4.42. Меню приложений графической оболочки GNOME

Нажмите на него и перед вами откроется окно настроек системы, перейдите в раздел «Сеть» (показано синим), затем откройте окно настроек Прокси (показано красным) на рисунке 4.43.

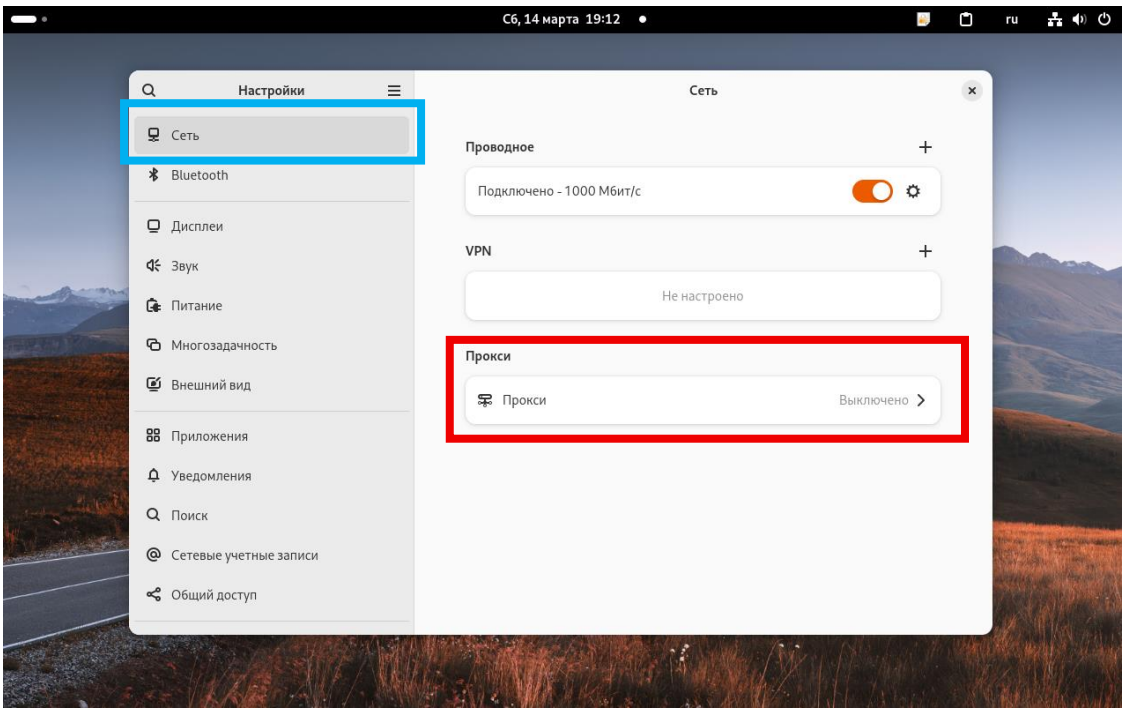

Рис. 4.43. Окно приложения «Настройки»

Активируем функцию прокси и заполним поля http- и https-прокси, с использованием конфигурации прокси-сервера из раздела 2.5 конфигурация ftp и socks прокси не обязательна. Пример готовой конфигурации приводится на рисунке 4.44.

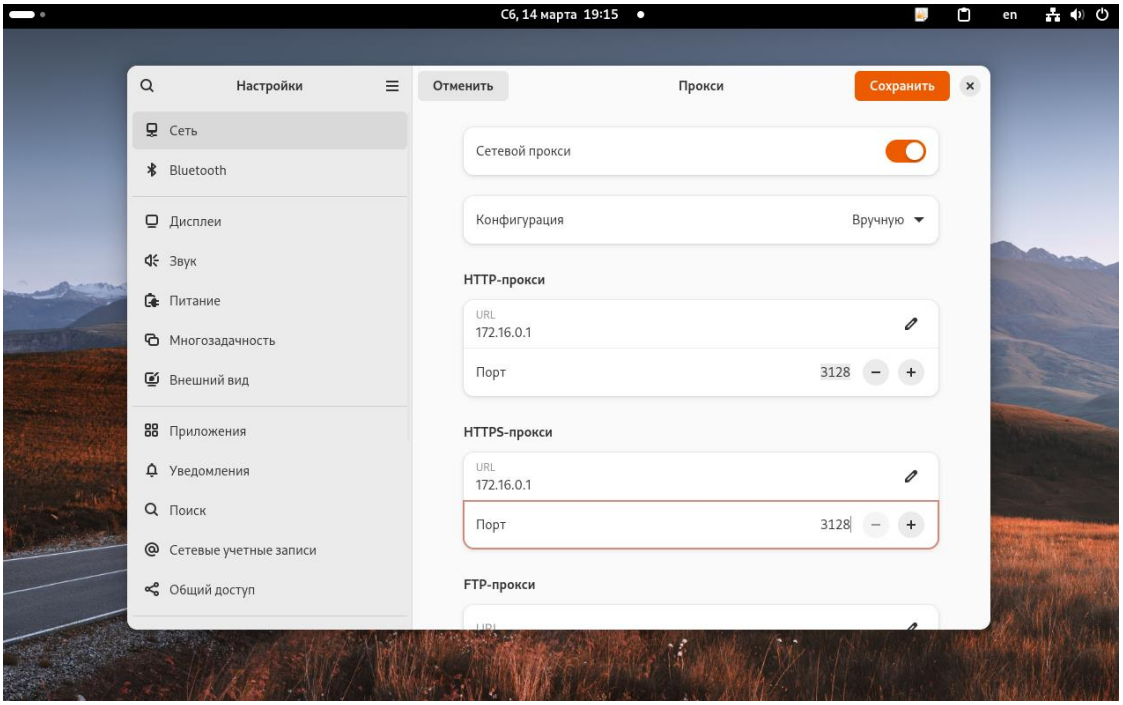

Рис. 4.44. Настройки прокси-сервера на стороне клиента linux

После продленных манипуляций на стороне клиента, проверим доступ к сети Интернет аналогичным пункту 4.1.4 образом. (рис. 4.45, рис. 4.46, рис. 4.47, рис. 4.48)

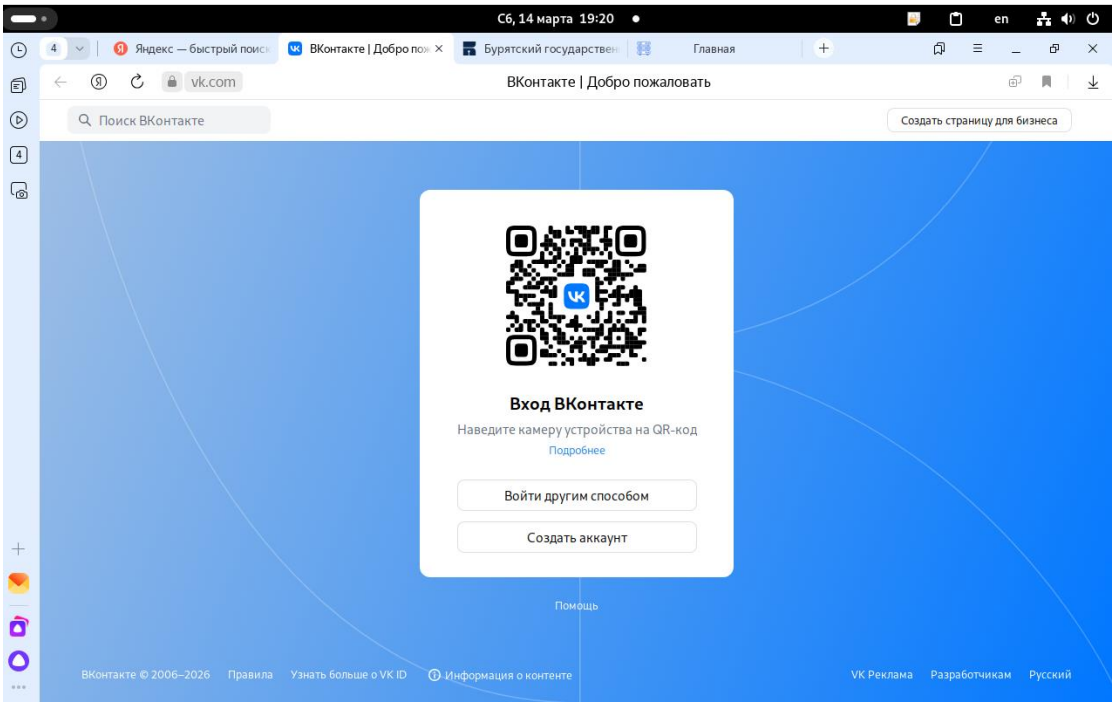

Рис. 4.45. Доступность сервисов ВК

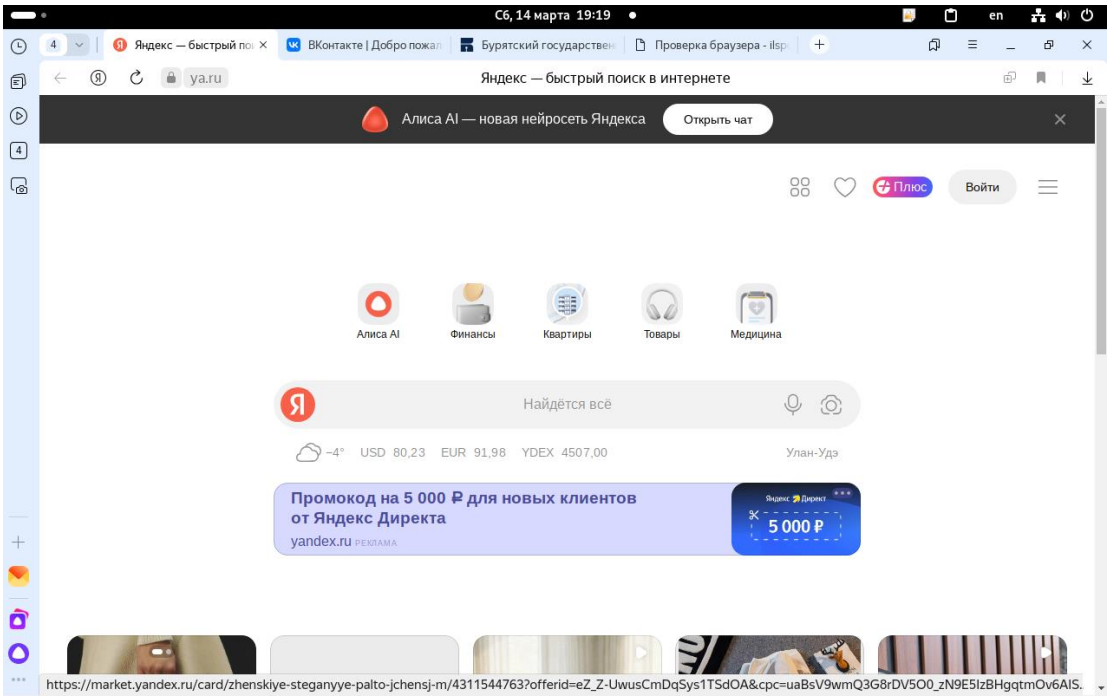

Рис. 4.46. Доступность сервисов Яндекс

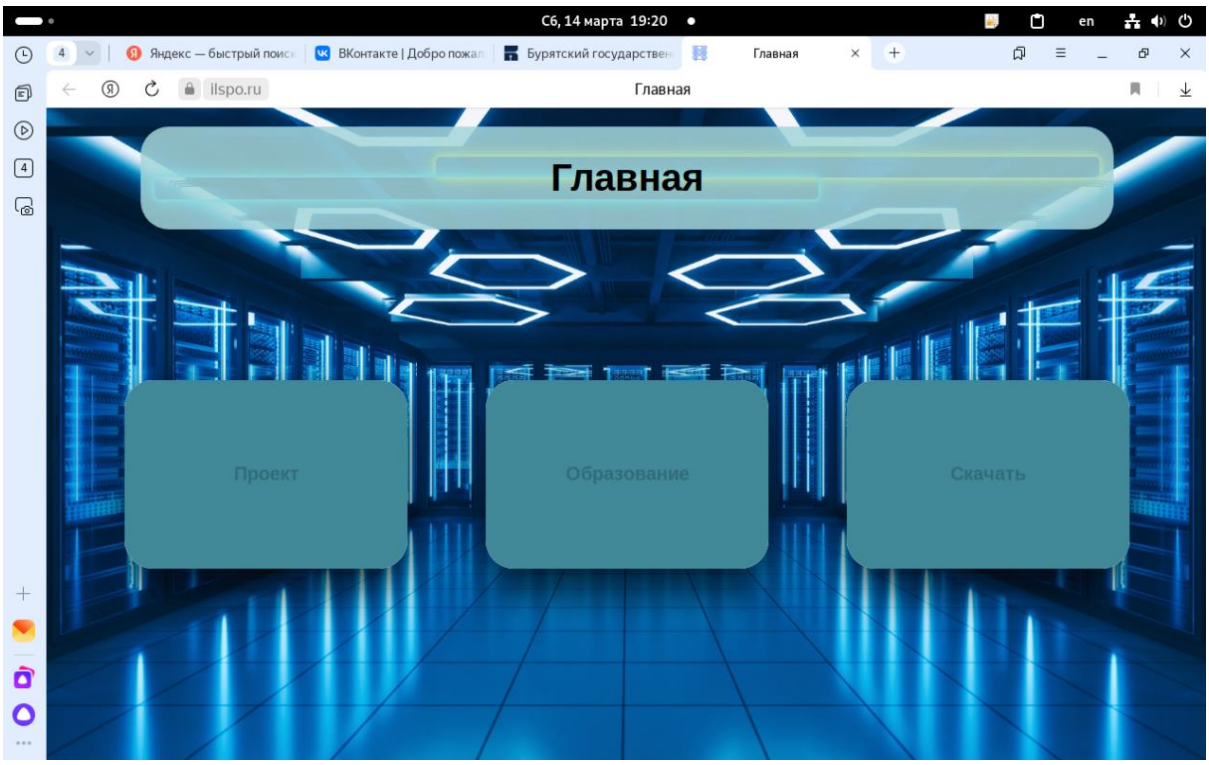

Рис. 4.45. Доступность сервисов ВК

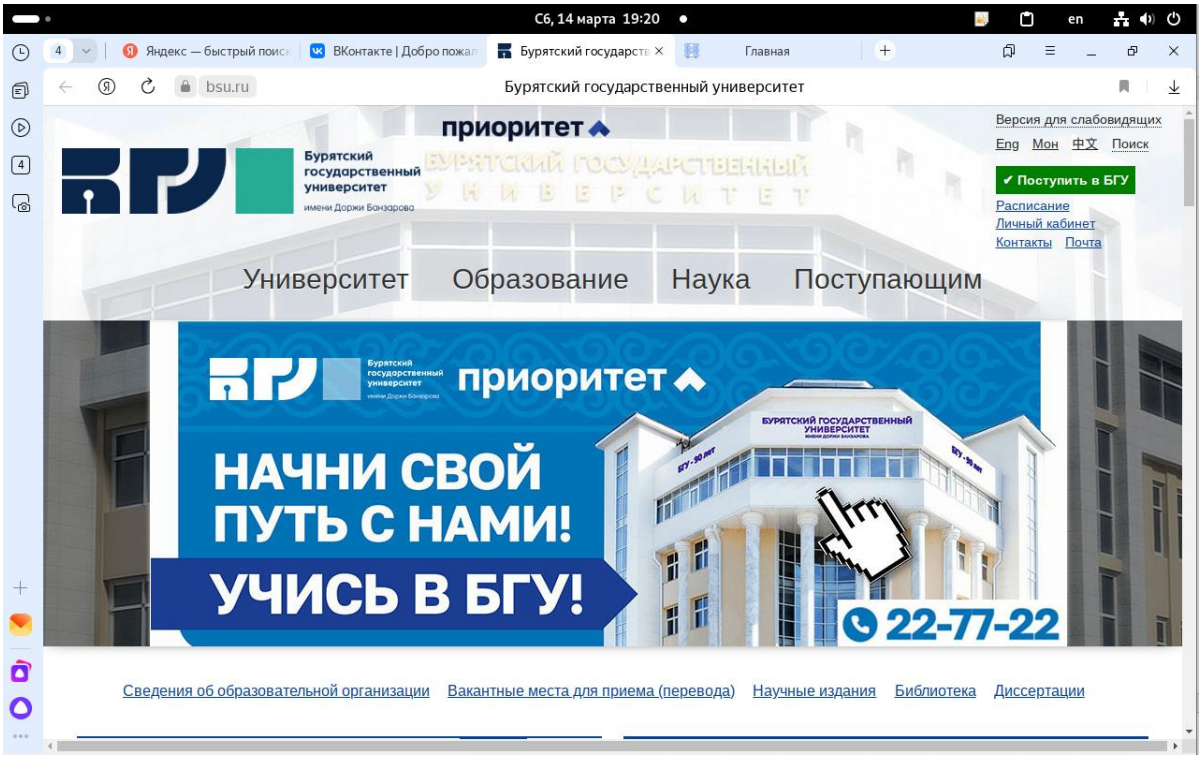

Рис. 4.45. Доступность ресурса Бурятского ГосУниверситета

Некоторые выводы из Раздела 4. «Интеграция клиентских станций в серверную инфраструктуру на базе ранее развернутых служб»

Практическая значимость выполненных действий заключается в обеспечении сквозной аутентификации и авторизации пользователей в гетерогенной сети. Посредством введения клиентских машин в домен на базе службы каталогов (AD DC) была реализована централизованная система идентификации, что является необходимым условием для дальнейшего применения групповых политик и разграничения прав доступа. Успешное взаимодействие клиентов со службами DHCP и DNS подтвердило корректность конфигурации сетевой инфраструктуры и обеспечило прозрачное для пользователя разрешение имен и получение сетевых параметров.

Кроме того, результатом раздела стала практическая реализация политик безопасности и контроля доступа к сетевым ресурсам. Настройка клиентских устройств на использование прокси-сервера (Squid) и подключение файловых ресурсов (SMB) ознаменовали собой переход серверных служб из состояния «в ожидании подключения» в режим активного обслуживания запросов. Таким образом, созданная инфраструктура обрела целостность и функциональность, став пригодной для выполнения базовых задач, характерных для реального корпоративного сегмента. Дальнейшее развитие системы будет связано с углубленной настройкой политик безопасности и оптимизацией производительности развернутых служб.

Дополнительная информация

Используя домен на базе BaseALT Server администраторам доступна возможность управления групповыми политиками через инструменты ADMC и GPUI: первое подразумевает управление пользователями и группами в графической среде без использования терминала, инструмент gpui предназначен для управления групповыми политиками по аналогии с Microsoft Active Directory.

Примечание 32. Групповые политики (Group Policy) — это механизм централизованного управления настройками операционной системы и приложений в среде Active Directory. Если объяснять технически, это инструмент, позволяющий администратору задавать правила работы для компьютеров и пользователей домена и принудительно применять их на всех устройствах сети без необходимости ходить к каждому ПК с отверткой и флешкой. Простыми словами, это "шаблон начальника": вы один раз прописали, что пользователь не может менять обои, отключать брандмауэр или устанавливать софт, и система сама следит за выполнением этих требований на всех тысячах машин.

Политики хранятся на контроллере домена и применяются по цепочке: сначала на весь компьютер (общесистемные настройки), потом на весь домен (влияет на всех в домене), потом на организационные подразделения (OU — виртуальные папки с юзерами/компьютерами, например "Бухгалтерия" или "Торговый зал"). Настройки нижестоящего уровня перезаписывают вышестоящие, если это разрешено.

Типы настроек:

- ***Computer Configuration (Конфигурация компьютера)** Влияет на саму машину (например, политика паролей локального администратора, параметры безопасности, скрипты запуска/выключения).*
- ***User Configuration (Конфигурация пользователя)** Влияет на окружение конкретного человека (например, перенаправление папки "Документы" на сервер, ограничение доступа к Панели управления, назначение домашней страницы в браузере).*

Механизм применения (обновления): Клиентская машина проверяет обновления политик каждые 90–120 минут (или при перезагрузке/входе пользователя). Она стягивает с контроллера домена актуальные настройки и применяет их к реестру и системе безопасности.

Контрольные вопросы для самопроверки

1. Общее понятие виртуальной машины.

2. Основные моменты установки операционной системы на виртуальную машину в среде VirtualBox.

3. Что входит в первоначальную настройку операционной системы ALT Server 11?

4. Чем отличаются доменные сети от рабочей группы?

5. Основные серверные роли. Краткая характеристика.

6. Стандартные группы пользователей в Active Directory. Какие полномочия получает пользователь при включении его в группу "Администраторы домена"?

7. Понятие DHCP сервера. В каких случаях требуется авто-назначение IP адресов в сети?

8. Назначение DNS сервера.

9. Как добавить компьютер в домен?

10. Что такое файловый сервер? Основные моменты при развертывании файлового сервера.

11. Понятие программного прокси-сервера. Для каких целей разворачивается корпоративный прокси-сервер?

12. Понятие групповых политик.

Методические рекомендации для студентов

Для успешного освоения знаний и применения их на практике необходимо наличие персонального компьютера или ноутбука с объемом оперативной памяти не менее 4 Гб и доступом в сеть интернет (для проверки работы программного прокси-сервера, а также для работы пакетных менеджеров в ОС Linux).

Образы операционных систем можно взять с сайта разработчика https://www.microsoft.com/ru-ru/download/default.aspx или через репозиторий-зеркало htpps://ftp.ilspo.ru/iso, расположенное на территории РФ.

Бесплатную среду для развертывания виртуальных машин можно скачать с сайта https://www.virtualbox.org/wiki/Downloads . Там выбираем нужную версию для вашей операционной системы.

При наличии необходимого аппаратного и программного обеспечения не составит большого труда пройти все этапы настройки виртуальных машин и выполнить итоговое контрольное задание.

Для переноса виртуальной машины, сконфигурированной самостоятельно дома на персональный компьютер, находящийся в компьютерном классе, необходимо выполнить экспорт конфигурации виртуальной машины через специальное меню VirtualBox, затем скопировать на носитель информации (флеш-накопитель достаточной емкости, переносной жесткий диск и т.п.) полученный в результате экспорта образ виртуальной машины и при открытии гипервизора в новом месте выполнить импорт конфигурации на новое место – такой перенос, в отличии от простого копирования образа жесткого диска ОС, позволит избежать проблем совместимости между различными версиями VirtualBox.

Пример итогового контрольного задания по теме

1. В организацию, в которой вы работаете системным администратором, устроился новый сотрудник в отдел статистики. Необходимо создать пользовательскую среду для нового сотрудника:

- Учетную запись пользователя в домене. Добавить в группу пользователей "Статистика".

- Доступ к файловому серверу (в папку "Public" с правом на чтение и "Архив" с полным доступом).

- Предоставить доступ в сеть интернет с ежемесячным лимитом в 1 ГБ трафика. Ограничить доступ в социальные сети "Вконтакте" и "Одноклассники".

2. Средствами управления пользователями (графическими или терминальными) выполните разграничение прав администрирования: администратор windows машин и администратор linux машин, у которых права администратора действительны лишь на указанной ОС, на остальных он работает как обычный пользователь.

Библиографический список

1. Колисниченко, Д.Н. Linux : полное руководство по работе и администрированию / Д. Н. Колисниченко. — Санкт-Петербург: Наука и Техника, 2021. — 480 с.: ил.. — (Полное руководство). — ISBN 978-5-94387-608-0
2. Hacker, R. Active directory глазами хакера / R. Hacker. — Санкт-Петербург : БХВ-Петербург, 2022. — 176 с.. — (Глазами хакера). — ISBN 978-5-9775-6783-1.
3. Колисниченко, Д.Н. Linux / Д. Н. Колисниченко. — 7-е изд., перераб. и доп.. — Санкт-Петербург : БХВ-Петербург, 2021. — 672 с.. — ISBN 978-5-9775-6649-0.
4. Войтов, Н.М. Основы работы с Linux / Н. М. Войтов. — Москва : ДМК Пресс, 2010. — 216 с.. — ISBN 978-5-94074-148-0.
5. Колисниченко, Д.Н. Серверное применение Linux / Д. Н. Колисниченко. — 3-е изд., перераб. и доп.. — Санкт-Петербург : БХВ-Петербург, 2011. — 512 с.. — (Системный администратор). — ISBN 978-5-9775-0652-6.
6. Матвеев, М.Д. Ядро Linux / М. Д. Матвеев. — Санкт-Петербург : Наука и Техника, 2023. — 352 с.. — ISBN 978-5-907592-14-8.
7. Коэн, Д. Linux для разработчиков / Д. Коэн, К. Штурм. — Астана : Спринт Бук, 2025. — 304 с.. — (Expert insight). — ISBN 978-601-08-4837-5.
8. Ванденбринк, Р. Linux для сетевых инженеров / Р. Ванденбринк. — Санкт-Петербург : Питер, 2024. — 492 с.. — (Библиотека программиста). — ISBN 978-5-4461-2275-2.
9. Барретт, Д.Д. Linux. Командная строка / Д. Д. Барретт. — Санкт-Петербург : Питер, 2024. — 253 с.. — (Бестселлеры O'Reilly). — ISBN 978-5-4461-2300-1.
10. Цыдыпов, С. Г. Администрирование локально-вычислительных сетей под управлением MS Windows Server : учебное пособие / С. Г. Цыдыпов. — Улан-Удэ : Изд-во Бурятского госуниверситета, 2019. — 75 с. — УДК 004.451.9 ББК 32.972

Учебное издание

Илья Сергеевич Поломошнов

Администрирование локально-вычислительных сетей под управлением BaseALT Linux Server

Учебное пособие

Компьютерная верстка _____

Свидетельство о государственной регистрации
№2670 от 11 августа 2017 г.

Подписано в печать «__»_____ 2026 г. Формат _____
Уч.-изд. л. ____ Усл. печ. л. ____ Тираж ___ экз. Зака ___
Цена свободная.

Издательство Бурятского госуниверситета имени Доржи Банзарова
670000, г. Улан-Удэ, ул. Смолина, 24а
rio@bsu.ru

Отпечатано в типографии Издательства
Бурятского госуниверситета имени Доржи Банзарова
67000, г. Улан-Удэ, ул. Сухэ-Батора, 3а