1. История, развитие и типы дистрибутивов Linux.

[История Linux началась в 1991 году, когда финский студент Линус Торвальдс создал своё собственное ядро для процессора 80386, совместимое с Unix1](http://opensourcerules.net/istoriya-razvitiya-linux.html). Он опубликовал исходный код ядра в Интернете и пригласил всех желающих присоединиться к разработке. Так начался проект Linux, который стал одним из самых популярных и успешных примеров совместной работы программистов со всего мира.

Развитие Linux происходило в двух основных направлениях: создание дистрибутивов и улучшение ядра. Дистрибутивы Linux — это готовые операционные системы, состоящие из ядра Linux и набора программного обеспечения, выбранного и настроенного разработчиками дистрибутива. Дистрибутивы могут отличаться по целям, аудитории, интерфейсу, установке, обновлению, поддержке и другим параметрам. [Существует более шестисот дистрибутивов Linux, но наиболее известными и распространёнными являются такие, как Debian, Ubuntu, Fedora, Red Hat, SUSE, Slackware, Gentoo, Arch Linux и другие](http://opensourcerules.net/istoriya-razvitiya-linux.html)[2](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D1%82%D1%80%D0%B8%D0%B1%D1%83%D1%82%D0%B8%D0%B2_Linux).

Улучшение ядра Linux — это постоянный процесс добавления новых функций, исправления ошибок, оптимизации производительности и поддержки нового оборудования. Ядро Linux развивается под руководством Линуса Торвальдса, который принимает или отклоняет изменения, предлагаемые другими разработчиками. Ядро Linux имеет модульную структуру, что позволяет легко добавлять или удалять компоненты в зависимости от потребностей пользователя. Ядро Linux поддерживает множество архитектур процессоров, таких как x86, x86\_64, ARM, MIPS, PowerPC, SPARC и другие. [Ядро Linux также может работать в разных режимах, таких как монолитное, микроядерное, гибридное и другие](http://opensourcerules.net/istoriya-razvitiya-linux.html)[3](https://habr.com/ru/companies/1cloud/articles/441554/).

Типы дистрибутивов Linux можно классифицировать по разным критериям, таким как:

* Способ установки: дистрибутивы могут устанавливаться на жёсткий диск, запускаться с компакт-диска, флешки или сети, или работать в виртуальной машине.
* Способ обновления: дистрибутивы могут использовать разные системы управления пакетами, такие как dpkg, rpm, portage, pacman и другие, для установки, удаления и обновления программ.
* Способ разработки: дистрибутивы могут быть созданы коммерческими компаниями, сообществами добровольцев, или индивидуальными разработчиками.
* Способ поддержки: дистрибутивы могут предлагать разные уровни технической поддержки, документации, форумов, списков рассылки и других ресурсов для пользователей.
* Способ лицензирования: дистрибутивы могут быть полностью свободными, частично свободными, или проприетарными, в зависимости от лицензий, под которыми распространяется их программное обеспечение.
* Способ ориентации: дистрибутивы могут быть ориентированы на разные цели, такие как общее назначение, образование, наука, безопасность, разработка, игры, мультимедиа, серверы и другие.

1. Планирование и установка Linux

Планирование и установка Linux — это важный этап создания рабочей системы на базе этой операционной системы. Для успешной установки Linux вам нужно выполнить следующие шаги:

Для того, чтобы установить Linux, вам нужно выполнить несколько шагов:

* Выбрать дистрибутив Linux, который подходит для ваших целей и требований. Существует множество различных версий Linux, разработанных отдельными группами людей. Вы можете ознакомиться с рейтингом и описанием популярных дистрибутивов на сайте [DistroWatch](https://www.youtube.com/watch?v=ypEPe5Ii3Aw" \t "_blank) или воспользоваться специальными тестами, которые помогут вам определиться с выбором, например, [Linux Distribution Chooser](https://lifehacker.ru/kak-ustanovit-linux/) или [Linux Quiz](https://ru.wikihow.com/%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8%D1%82%D1%8C-Linux).
* Загрузить образ выбранного дистрибутива в формате ISO с официального сайта или другого надежного источника. Обычно на сайтах дистрибутивов есть разделы загрузок, где вы можете выбрать подходящую версию и способ загрузки (обычный или через торрент).
* Записать образ дистрибутива на носитель, с которого вы собираетесь устанавливать Linux. Это может быть CD, DVD или USB-флешка. Для записи образа на CD или DVD вы можете использовать стандартные средства вашей системы или специальные программы, такие как [ImgBurn](https://help.ubuntu.ru/wiki/ubuntu_install" \t "_blank) или [CDBurnerXP]. Для записи образа на USB-флешку вам понадобятся другие программы, такие как [Rufus] или [Etcher]. Эти программы позволяют создать загрузочную флешку с Linux, которая будет работать на большинстве современных компьютеров.
* Загрузить компьютер с носителя, на который вы записали образ дистрибутива. Для этого вам нужно изменить порядок загрузки в BIOS или UEFI вашего компьютера, чтобы он сначала пытался загрузиться с CD, DVD или USB-флешки, а потом с жесткого диска. Для этого вам нужно при включении компьютера нажать определенную клавишу (обычно это F2, F10, F12, Del или Esc), чтобы войти в настройки BIOS или UEFI. Там вы можете выбрать нужный носитель в разделе Boot или Boot Order. Сохраните настройки и перезагрузите компьютер. Если все сделано правильно, то вы увидите экран загрузки Linux.
* Выполнить установку Linux, следуя инструкциям мастера установки. Каждый дистрибутив имеет свой собственный мастер установки, который может отличаться по интерфейсу и опциям. Однако, в общем случае, вам нужно будет выбрать язык установки, часовой пояс, раскладку клавиатуры, тип установки (автоматический или ручной), разметку диска (создание и форматирование разделов), имя компьютера, имя пользователя и пароль, а также дополнительные параметры, такие как выбор программ, настройка сети, установка загрузчика и т.д. После того, как вы заполните все необходимые поля, начнется процесс копирования файлов системы на диск. Это может занять от нескольких минут до нескольких часов, в зависимости от скорости вашего компьютера и объема данных. По окончании установки вам нужно будет перезагрузить компьютер и снять носитель с образом дистрибутива. После перезагрузки вы увидите экран входа в Linux, где вы сможете ввести свое имя пользователя и пароль и начать работу с новой системой.

1. Пользователи и группы. Файлы конфигурации. Управление учетными записями пользователей.

Пользователи и группы в Linux - это способ организации доступа к файлам, каталогам и процессам на компьютере. Каждый пользователь имеет свой идентификатор (UID), имя, пароль и домашний каталог. Каждая группа имеет свой идентификатор (GID) и имя. Пользователи могут принадлежать к одной или нескольким группам, что определяет их права и обязанности. [Вы можете добавлять, удалять и изменять пользователей и группы с помощью команд useradd, userdel, usermod, groupadd, groupdel и groupmod1](https://it-tehnik.ru/windows10/nastroyka/lokalnye-polzovateli-i-gruppy.html).

Файлы конфигурации в Linux - это текстовые файлы, в которых хранятся настройки и параметры для различных программ и служб. Вы можете редактировать файлы конфигурации с помощью текстовых редакторов, таких как vi, nano или gedit. Файлы конфигурации обычно находятся в каталогах /etc, /usr/local/etc или в домашних каталогах пользователей. Файлы конфигурации могут иметь разные расширения, такие как .conf, .cfg, .ini или .rc.

Управление учетными записями пользователей в Linux - это функция безопасности, которая позволяет контролировать, какие действия могут выполнять пользователи на компьютере. Вы можете использовать команду sudo, чтобы выполнить команды от имени другого пользователя, обычно суперпользователя (root). Для этого вам нужно ввести свой пароль и подтвердить запрос. [Вы можете настроить, какие пользователи могут использовать sudo и какие команды они могут выполнять, с помощью файла /etc/sudoers](https://support.microsoft.com/ru-ru/windows/%D0%B4%D0%BE%D0%B1%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%B8-%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D1%83%D1%87%D0%B5%D1%82%D0%BD%D1%8B%D1%85-%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%B5-104dc19f-6430-4b49-6a2b-e4dbd1dcdf32)

1. Системы управления пакетами. Их использование. Основные средства управления установкой, обновлением и удалением пакетов.

Системы управления пакетами - это набор программного обеспечения, который позволяет установить, обновить и удалить различные компоненты программного обеспечения на вашем компьютере. Они используются во многих операционных системах, в том числе в Linux.

В Linux существует множество систем управления пакетами, которые отличаются форматом пакетов, способом разрешения зависимостей, интерфейсом пользователя и другими особенностями. Некоторые из наиболее популярных систем управления пакетами в Linux это:

* [**RPM и yum**: используются во множестве дистрибутивов Linux, в том числе Fedora, RHEL, ASP Linux, Mandriva, OpenMandriva Lx, openSUSE1](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8). Пакеты имеют расширение .rpm и содержат бинарные файлы, метаданные и сценарии установки и удаления. Yum - это инструмент командной строки, который позволяет управлять пакетами RPM, загружая их из репозиториев в интернете или локальной сети.
* [**dpkg и apt**: используются в Debian и в различных дистрибутивах, основанных на нём, например Ubuntu1](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8). Пакеты имеют расширение .deb и также содержат бинарные файлы, метаданные и сценарии установки и удаления. Apt - это инструмент командной строки, который позволяет управлять пакетами dpkg, загружая их из репозиториев в интернете или локальной сети. [Apt также предоставляет графический интерфейс, например Synaptic](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8" \t "_blank)[1](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8).
* [**Pacman**: используется в Arch Linux, Frugalware и DeLi Linux1](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8). Пакеты имеют расширение .pkg.tar.zst и представляют собой сжатые zstd tar архивы, содержащие бинарные файлы и метаданные. Pacman - это инструмент командной строки, который позволяет управлять пакетами, загружая их из репозиториев в интернете или локальной сети. Pacman также позволяет создавать собственные пакеты с помощью утилиты makepkg и специального типа сценария оболочки, называемого PKGBUILD.

Основные средства управления установкой, обновлением и удалением пакетов в Linux зависят от того, какая система управления пакетами используется. В общем случае, для установки пакета нужно указать его имя или путь к файлу пакета, для обновления пакета нужно указать его имя или выполнить обновление всех установленных пакетов, для удаления пакета нужно указать его имя. Например, для системы управления пакетами RPM и yum, эти операции могут выглядеть так:

* Установка пакета: yum install имя\_пакета или rpm -i путь\_к\_файлу\_пакета
* Обновление пакета: yum update имя\_пакета или yum update (для обновления всех пакетов)
* Удаление пакета: yum remove имя\_пакета или rpm -e имя\_пакета

Для системы управления пакетами dpkg и apt, эти операции могут выглядеть так:

* Установка пакета: apt install имя\_пакета или dpkg -i путь\_к\_файлу\_пакета
* Обновление пакета: apt update (для обновления списка доступных пакетов) и apt upgrade имя\_пакета или apt upgrade (для обновления всех пакетов)
* Удаление пакета: apt remove имя\_пакета или dpkg -r имя\_пакета

Для системы управления пакетами Pacman, эти операции могут выглядеть так:

* Установка пакета: pacman -S имя\_пакета или pacman -U путь\_к\_файлу\_пакета
* Обновление пакета: pacman -Sy имя\_пакета или pacman -Syu (для обновления всех пакетов)
* Удаление пакета: pacman -R имя\_пакета

Если вам нужна более подробная информация о системах управления пакетами в Linux, вы можете посетить следующие ссылки:

* [Система управления пакетами — Википедия](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8)
* [Список систем управления пакетами программного обеспечения — Википедия](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D1%8F)
* [Управление пакетами — openSUSE Wiki](https://ru.opensuse.org/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%D0%BC%D0%B8)

1. Конфигурирование сети в Linux

Конфигурирование сети в Linux - это процесс настройки параметров сетевых интерфейсов, таких как IP-адрес, маска подсети, шлюз по умолчанию, DNS-сервер и т.д. для обеспечения связи с другими устройствами в сети или в Интернете.

Существует несколько способов конфигурирования сети в Linux, в зависимости от типа сетевого интерфейса, дистрибутива Linux и желаемого режима работы. Некоторые из наиболее распространенных способов:

* Использование утилиты ifconfig для ручной настройки сетевых интерфейсов через командную строку. Этот метод подходит для временной настройки или для тестирования сетевых настроек. [Однако, утилита ifconfig считается устаревшей и заменена утилитой ip в большинстве дистрибутивов Linux1](https://help.ubuntu.ru/wiki/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_linux).
* Использование утилиты ip для ручной или автоматической настройки сетевых интерфейсов через командную строку. Этот метод является более современным и мощным, чем ifconfig, и позволяет выполнять различные операции с сетевыми интерфейсами, такие как добавление, удаление, включение, отключение, изменение параметров и т.д.
* Использование графических инструментов для настройки сети через графический интерфейс пользователя. Этот метод является наиболее простым и удобным для большинства пользователей, так как не требует знания командной строки или редактирования конфигурационных файлов. [Например, в Ubuntu можно использовать сетевой менеджер NetworkManager для настройки сети через панель управления или апплет на панели задач](https://help.ubuntu.ru/wiki/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2_linux)[2](https://blog.sedicomm.com/2020/03/16/15-poleznyh-komand-ifconfig-dlya-nastrojki-setevogo-interfejsa-v-linux/).
* Использование конфигурационных файлов для настройки сети через текстовый редактор. Этот метод является наиболее гибким и надежным, так как позволяет сохранять и восстанавливать сетевые настройки при перезагрузке системы или при изменении сетевого интерфейса. Однако, этот метод требует знания синтаксиса и расположения конфигурационных файлов, которые могут отличаться в разных дистрибутивах Linux. [Например, в Debian и Ubuntu можно использовать файл /etc/network/interfaces для настройки сети](https://help.ubuntu.ru/wiki/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_%D1%81%D0%B5%D1%82%D0%B8_%D0%B2%D1%80%D1%83%D1%87%D0%BD%D1%83%D1%8E)

1. Системы мониторинга и SNMP

[SNMP (Simple Network Management Protocol) - это протокол прикладного уровня, который обеспечивает стандартизированную структуру и общий язык для мониторинга и управления устройствами в сети1](https://selectel.ru/blog/snmp/). SNMP позволяет сетевым администраторам собирать, анализировать и изменять информацию о состоянии и производительности сетевых устройств, таких как маршрутизаторы, коммутаторы, серверы, принтеры и т.д.

Системы мониторинга - это программные или аппаратные средства, которые используют SNMP или другие протоколы для отслеживания и управления сетевыми ресурсами. Системы мониторинга могут выполнять различные функции, такие как:

* Определение и отображение топологии сети и ее компонентов;
* Сбор и хранение статистических данных о сетевом трафике, загрузке, доступности и ошибках;
* Генерация и отправка оповещений, отчетов и рекомендаций по улучшению сетевой работы;
* Выполнение диагностики и устранения неполадок в сети;
* Выполнение действий по управлению сетевыми устройствами, таких как перезагрузка, обновление, конфигурирование и т.д.

Некоторые примеры систем мониторинга, которые используют SNMP, это:

* Zabbix - это открытое программное обеспечение для мониторинга сетей и приложений, которое поддерживает различные протоколы, включая SNMP, IPMI, JMX и т.д. Zabbix может мониторить множество параметров сетевых устройств, таких как CPU, память, диск, температура, вентиляторы и т.д. [Zabbix также может создавать графики, карты, панели и триггеры для визуализации и оповещения о сетевых событиях](https://ru.wikipedia.org/wiki/SNMP" \t "_blank)[2](https://ru.wikipedia.org/wiki/SNMP).
* PRTG Network Monitor - это коммерческое программное обеспечение для мониторинга сетей и инфраструктуры, которое также поддерживает SNMP и другие протоколы. PRTG может мониторить разнообразные аспекты сетевой работы, такие как пропускная способность, доступность, SLA, QoS и т.д. [PRTG также предоставляет интуитивный веб-интерфейс, мобильные приложения и настраиваемые дашборды для управления и отчетности о сетевом состоянии](https://selectel.ru/blog/snmp/)[3](https://bing.com/search?q=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B+%D0%BC%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%D0%B0+%D0%B8+SNMP).
* Nagios - это еще одно открытое программное обеспечение для мониторинга сетей и систем, которое также поддерживает SNMP и другие протоколы. Nagios может мониторить сетевые устройства, серверы, приложения, службы и процессы, а также определять и предупреждать о сетевых проблемах и инцидентах. [Nagios также имеет веб-интерфейс, плагины, аддоны и API для расширения и интеграции с другими системами](https://fiberroad.com/ru/resources/glossary/what-is-snmp/" \t "_blank)

1. Управление дисковыми устройствами, разделами и файловыми системами в Linux

Управление дисковыми устройствами, разделами и файловыми системами в Linux - это важный аспект администрирования и настройки операционной системы. Для этого существует множество утилит и команд, которые позволяют выполнять различные операции над дисками и разделами, такие как:

* Просмотр информации о дисках, разделах и файловых системах;
* Создание, удаление, изменение размера, форматирование, копирование и перемещение разделов;
* Монтирование и размонтирование разделов и файловых систем;
* Проверка и восстановление разделов и файловых систем;
* Изменение атрибутов и флагов разделов и файловых систем;
* Управление таблицами разделов и загрузочными записями.

Некоторые из наиболее распространенных и полезных утилит и команд для управления дисковыми устройствами, разделами и файловыми системами в Linux это:

* [fdisk - утилита командной строки для создания и изменения таблиц разделов MS-DOS (MBR) и GPT](https://blog.sedicomm.com/2022/08/01/6-luchshih-menedzherov-razdelov-partition-manager-cli-gui-dlya-linux/)[1](https://blog.sedicomm.com/2022/08/01/6-luchshih-menedzherov-razdelov-partition-manager-cli-gui-dlya-linux/);
* [parted - утилита командной строки для создания и изменения таблиц разделов разных типов, включая MS-DOS, GPT, BSD и другие](https://blog.sedicomm.com/2022/08/01/6-luchshih-menedzherov-razdelov-partition-manager-cli-gui-dlya-linux/)[2](https://winitpro.ru/index.php/2020/07/09/parted-upravlenie-razdelami-linux/);
* gparted - графическая утилита для создания и изменения разделов и файловых систем, основанная на parted;
* [lsblk - команда для вывода информации о дисковых устройствах и их разделах4](https://help.sweb.ru/upravlenie-ustrojstvami-hraneniya-dannyh-v-linux_1252.html);
* [blkid - команда для вывода информации о типах файловых систем и UUID разделов](https://blog.sedicomm.com/2022/08/01/6-luchshih-menedzherov-razdelov-partition-manager-cli-gui-dlya-linux/)[5](https://pingvinus.ru/programs/system/partitioning);
* [df - команда для вывода информации об использовании дискового пространства файловыми системами](https://blog.sedicomm.com/2022/08/01/6-luchshih-menedzherov-razdelov-partition-manager-cli-gui-dlya-linux/)[6](https://bing.com/search?q=);
* du - команда для вывода информации об использовании дискового пространства директориями и файлами;
* mount - команда для монтирования файловых систем на указанные точки монтирования;
* umount - команда для размонтирования файловых систем с указанных точек монтирования;
* mkfs - утилита для создания файловых систем разных типов, таких как ext2, ext3, ext4, xfs, btrfs и другие;
* fsck - утилита для проверки и восстановления файловых систем разных типов;
* tune2fs - утилита для изменения параметров файловых систем ext2, ext3 и ext4;
* e2label - утилита для изменения меток (имен) файловых систем ext2, ext3 и ext4;
* grub - утилита для установки и настройки загрузчика GRUB, который позволяет выбирать операционную систему при запуске компьютера.

Если вы хотите узнать больше о управлении дисковыми устройствами, разделами и файловыми системами в Linux, вы можете посетить следующие ссылки:

* [Управление устройствами хранения данных в Linux](https://bing.com/search?q=)
* [Управление дисками. Программы для Linux](https://pingvinus.ru/programs/system/partitioning)
* [Parted — управление разметкой и разделами дисков в Linux](https://winitpro.ru/index.php/2020/07/09/parted-upravlenie-razdelami-linux/)

1. Резервное копирование.

Резервное копирование в Linux - это процесс создания копии ваших данных на другом носителе, например на внешнем диске, сетевом хранилище или облачном сервисе. Резервное копирование позволяет восстановить ваши данные в случае их потери, повреждения или удаления.

В Linux существует множество утилит и программ для резервного копирования, которые имеют разные функции, возможности и интерфейсы. Некоторые из наиболее популярных и полезных утилит для резервного копирования в Linux это:

* Rsync - это утилита командной строки, которая позволяет быстро и эффективно копировать файлы и каталоги между локальными и удаленными местами. Rsync поддерживает инкрементное резервное копирование, сжатие, шифрование, фильтрацию и другие опции. [Rsync также может быть автоматизирован с помощью сценариев и заданий cron](https://lifehacker.ru/linux-backup-applications/)[1](https://lifehacker.ru/linux-backup-applications/).
* Fwbackups - это кросс-платформенное графическое приложение, которое позволяет легко создавать и восстанавливать резервные копии файлов и каталогов. [Fwbackups поддерживает различные режимы резервного копирования, такие как полный, инкрементный и дифференциальный, а также различные места назначения, такие как локальные диски, сетевые папки и FTP-серверы](https://blog.sedicomm.com/2018/07/22/14-utilit-rezervnogo-kopirovaniya-dlya-linux-sistem/" \t "_blank)[2](https://blog.sedicomm.com/2018/07/22/14-utilit-rezervnogo-kopirovaniya-dlya-linux-sistem/).
* Bacula - это мощная и сложная система резервного копирования, восстановления и проверки данных, которая работает в сети и состоит из нескольких компонентов, таких как директор, консоль, файл, хранилище, каталог и монитор. [Bacula позволяет резервировать целые файловые системы, операционные системы, приложения и базы данных, а также управлять и настраивать различные аспекты процесса резервного копирования](https://lifehacker.ru/linux-backup-applications/)[3](https://siobr.ru/linux-acronis-polnoe-rukovodstvo-po-ustanovke-i-nastroyke/).
* Timeshift - это простое и удобное приложение, которое позволяет создавать «снимки» системы, то есть резервные копии всех системных файлов, настроек и приложений. Timeshift позволяет легко восстанавливать систему в рабочее состояние в случае сбоя или повреждения. [Timeshift поддерживает два типа снимков: на основе Rsync и на основе Btrfs](https://www.handybackup.ru/linux-backup.shtml" \t "_blank).

1. Процессы в Linux. Сигналы. Средства контроля и мониторинга процессов

Процессы в Linux - это программы, которые выполняются в операционной системе. Каждый процесс имеет свой уникальный идентификатор (PID), приоритет, состояние, родительский процесс и дочерние процессы. [Процессы могут быть созданы, завершены, приостановлены или возобновлены с помощью различных команд и системных вызовов1](https://rebrainme.com/blog/linux/30-instrumentov-monitoringa-sistemy-linux-kotorye-dolzhen-znat-kazhdyj-sisadmin/).

Сигналы - это способ коммуникации между процессами в Linux. Сигналы могут быть отправлены процессом самому себе, другому процессу или ядром системы. Сигналы могут сообщать о различных событиях, таких как ошибки, прерывания, завершения или запросы на остановку. Каждый сигнал имеет свое целочисленное значение и имя, например, SIGINT (2) или SIGKILL (9). [Процессы могут обрабатывать сигналы по-разному, в зависимости от того, какие функции они определили для реакции на сигналы2](https://www.opennet.ru/docs/RUS/linux_parallel/node10.html).

Средства контроля и мониторинга процессов - это программы, которые позволяют анализировать и управлять процессами в Linux. С их помощью можно получать информацию о производительности, потреблении ресурсов, состоянии и активности процессов. Некоторые из наиболее популярных и полезных средств контроля и мониторинга процессов в Linux это:

* [top: отображает процессы в реальном времени, сортируя их по различным параметрам, таким как использование процессора, памяти, диска или сети3](https://habr.com/ru/articles/423049/).
* [vmstat: отображает статистику виртуальной памяти, подкачки, блочного ввода-вывода, прерываний и активности процессора](https://rebrainme.com/blog/linux/30-instrumentov-monitoringa-sistemy-linux-kotorye-dolzhen-znat-kazhdyj-sisadmin/)[3](https://habr.com/ru/articles/423049/).
* [w: отображает информацию о пользователях, вошедших в систему, и их процессах3](https://habr.com/ru/articles/423049/).
* [ps: отображает информацию о выбранных процессах, такую как PID, PPID, состояние, приоритет, время работы и т.д.3](https://habr.com/ru/articles/423049/).
* [pstree: отображает древовидную структуру процессов, показывая их иерархические отношения](https://rebrainme.com/blog/linux/30-instrumentov-monitoringa-sistemy-linux-kotorye-dolzhen-znat-kazhdyj-sisadmin/)[3](https://habr.com/ru/articles/423049/).
* [htop: расширенная версия top, которая предоставляет больше возможностей и интерактивности](https://rebrainme.com/blog/linux/30-instrumentov-monitoringa-sistemy-linux-kotorye-dolzhen-znat-kazhdyj-sisadmin/)[4](https://veesp.com/ru/blog/linux-system-monitoring-basics/).
* strace: отслеживает системные вызовы и сигналы, которые производит процесс, полезно для отладки и решения проблем.

1. DHCP и его настройка в Linux.

[DHCP (Dynamic Host Configuration Protocol) - это протокол, который позволяет автоматически назначать IP-адреса и другие параметры сети компьютерам и устройствам, подключенным к локальной сети](https://bing.com/search?q=DHCP+%d0%b8+%d0%b5%d0%b3%d0%be+%d0%bd%d0%b0%d1%81%d1%82%d1%80%d0%be%d0%b9%d0%ba%d0%b0+%d0%b2+Linux)[1](https://bing.com/search?q=DHCP+%D0%B8+%D0%B5%D0%B3%D0%BE+%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0+%D0%B2+Linux). DHCP состоит из двух основных компонентов: DHCP-сервера и DHCP-клиентов. DHCP-сервер - это компьютер или устройство, которое хранит информацию о доступных IP-адресах и настройках сети, и выдает их по запросу DHCP-клиентов. [DHCP-клиент - это компьютер или устройство, которое запрашивает IP-адрес и настройки сети у DHCP-сервера при подключении к сети](https://bing.com/search?q=DHCP+%d0%b8+%d0%b5%d0%b3%d0%be+%d0%bd%d0%b0%d1%81%d1%82%d1%80%d0%be%d0%b9%d0%ba%d0%b0+%d0%b2+Linux)[1](https://bing.com/search?q=DHCP+%D0%B8+%D0%B5%D0%B3%D0%BE+%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0+%D0%B2+Linux).

Настройка DHCP в Linux зависит от того, какую роль вы хотите выполнить: DHCP-сервера или DHCP-клиента. [В общем случае, для настройки DHCP-сервера в Linux вам необходимо выполнить следующие шаги](https://bing.com/search?q=DHCP+%d0%b8+%d0%b5%d0%b3%d0%be+%d0%bd%d0%b0%d1%81%d1%82%d1%80%d0%be%d0%b9%d0%ba%d0%b0+%d0%b2+Linux)[2](https://siblimo.ru/kak-nastroit-dhcp-linuks/)[3](https://zvenst.ru/nastroika-dhcp-na-linux-debian/)[4](https://logi.cc/kaketo-nastrojka-dhcp-servera-na-linux/)[5](https://gatefinder.ru/nastroika-dhcp-servera/):

* Установить пакет DHCP-сервера с помощью менеджера пакетов вашей дистрибуции. Например, в Debian или Ubuntu это можно сделать с помощью команды:

sudo apt install isc-dhcp-server

* Открыть файл настроек DHCP-сервера для редактирования. Обычно он находится в /etc/dhcp/dhcpd.conf. В этом файле вы можете определить различные параметры для вашей сети, такие как диапазон IP-адресов, маска сети, шлюз, DNS-серверы и т.д. Пример:

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.100 192.168.1.200;

option routers 192.168.1.1;

option domain-name-servers 8.8.8.8, 8.8.4.4;

}

* Настроить статические IP-адреса для машин клиентов, если необходимо. Это можно сделать, добавив секцию host в файл настроек DHCP-сервера, указав MAC-адрес и желаемый IP-адрес для каждого клиента. Пример:

host printer {

hardware ethernet 00:11:22:33:44:55;

fixed-address 192.168.1.10;

}

* Перезапустить DHCP-сервер с помощью команды:

sudo systemctl restart isc-dhcp-server

[Для настройки DHCP-клиента в Linux вам необходимо выполнить следующие шаги](https://bing.com/search?q=DHCP+%d0%b8+%d0%b5%d0%b3%d0%be+%d0%bd%d0%b0%d1%81%d1%82%d1%80%d0%be%d0%b9%d0%ba%d0%b0+%d0%b2+Linux)[6](https://virtual-box.ru/nastroika-ip-dhcp-v-linux/):

* Установить пакет DHCP-клиента с помощью менеджера пакетов вашей дистрибуции. Например, в Debian или Ubuntu это можно сделать с помощью команды:

sudo apt install isc-dhcp-client

* Открыть файл настроек DHCP-клиента для редактирования. Обычно он находится в /etc/dhcp/dhclient.conf. В этом файле вы можете указать, какие параметры сети вы хотите получать от DHCP-сервера, или задать свои собственные. Пример:

request subnet-mask, broadcast-address, time-offset, routers,

domain-name, domain-name-servers, domain-search, host-name,

dhcp6.name-servers, dhcp6.domain-search;

send host-name = gethostname();

* Настроить сетевой интерфейс для использования DHCP. Это можно сделать, настроив параметры сетевого подключения в файле конфигурации, или используя специальные инструменты командной строки, такие как ipconfig или ifconfig. Пример:

sudo ip link set eth0 up

sudo dhclient eth0

1. Межсетевые экраны. Netfilter/iptables и её применение.

Межсетевые экраны - это программы или устройства, которые контролируют и фильтруют сетевой трафик, проходящий между разными сетями или хостами. [Межсетевые экраны могут использоваться для защиты сети от внешних атак, для ограничения доступа к определенным ресурсам или для реализации различных политик сетевой безопасности1](https://ruvds.com/ru/helpcenter/iptables/).

Netfilter - это модуль ядра Linux, который предоставляет функциональность межсетевого экрана на уровне пакетов. [Netfilter позволяет перехватывать, анализировать, модифицировать и принимать решения о сетевых пакетах, проходящих через разные точки сетевого стека](https://habr.com/ru/articles/684524/" \t "_blank)[2](https://habr.com/ru/articles/684524/).

iptables - это утилита командной строки, которая используется для управления правилами и таблицами Netfilter. [iptables позволяет создавать, изменять и удалять правила фильтрации, трансляции адресов (NAT), маршрутизации и других функций Netfilter](https://ru.wikipedia.org/wiki/Iptables" \t "_blank)[3](https://ru.wikipedia.org/wiki/Iptables).

Применение Netfilter/iptables может быть разным в зависимости от целей и задач сетевого администратора. Например, с помощью Netfilter/iptables можно:

* Разрешать или запрещать входящие и исходящие соединения по определенным портам, протоколам или адресам.
* Преобразовывать внутренние адреса во внешние и наоборот с помощью NAT, чтобы обеспечить доступ к Интернету или скрыть внутреннюю сеть.
* Балансировать нагрузку между несколькими серверами с помощью IP-балансировки или туннелирования.
* Отслеживать и логировать сетевую активность для анализа и отладки.
* Реализовывать сетевые зоны безопасности (DMZ) для разделения сетевых служб по уровню доверия.
* Применять различные расширения и модули Netfilter для улучшения производительности и функциональности межсетевого экрана

1. Web-сервер и его настройка.

Веб-сервер - это программа, которая обрабатывает запросы от клиентов (например, браузеров) и возвращает им ответы (например, HTML-страницы). Настройка веб-сервера в Linux зависит от того, какой веб-сервер вы хотите использовать, какие функции и службы вы хотите предоставить и какие требования к безопасности и производительности вы имеете.

Одним из наиболее популярных и мощных веб-серверов в Linux является Apache. Apache - это свободный и открытый веб-сервер, который поддерживает множество модулей и расширений, позволяющих настраивать его под различные нужды. Для работы с Apache вам потребуется установить его с помощью менеджера пакетов вашей дистрибуции, например:

sudo apt install apache2

Затем вам потребуется настроить файлы конфигурации Apache, которые обычно находятся в директории /etc/apache2. В этих файлах вы можете определить различные параметры, такие как:

* Порт, на котором Apache будет прослушивать запросы (по умолчанию 80).
* Имя сервера, которое Apache будет использовать для идентификации себя (по умолчанию localhost).
* Корневая директория, в которой Apache будет искать файлы для отдачи (по умолчанию /var/www/html).
* Виртуальные хосты, которые позволяют Apache обслуживать несколько доменов или сайтов на одном сервере.
* Модули, которые расширяют функциональность Apache, например, для работы с PHP, SSL, CGI и т.д.

После внесения изменений в файлы конфигурации Apache, вам нужно перезапустить его, чтобы они вступили в силу, например:

sudo systemctl restart apache2

1. DNS и её настройка в Linux.

DNS (Domain Name System) - это система доменных имен, которая позволяет переводить доменные имена сайтов в IP-адреса и обратно. DNS также используется для обнаружения и идентификации других устройств и сервисов в сети.

Настройка DNS в Linux зависит от типа вашего подключения и дистрибутива. В общем случае, вы можете настроить DNS в Linux двумя способами:

* С помощью меню графической оболочки. Этот способ подходит для начинающих пользователей, которые не хотят работать с консолью. Вы можете выбрать свое подключение, нажать на кнопку “Параметры соединения” и перейти к вкладке “IPv4” или “IPv6”. [Там вы можете указать способ получения DNS (автоматический или ручной) и ввести адреса серверов DNS, если нужно1](https://lumpics.ru/setup-dns-in-linux/)[2](https://habr.com/ru/articles/713156/).
* С помощью редактирования конфигурационных файлов. Этот способ подходит для опытных пользователей, которые предпочитают иметь больше контроля над настройками. Вы можете открыть файл /etc/resolv.conf и ввести адреса серверов DNS, которые вы хотите использовать. Например, если вы хотите использовать публичные серверы Google DNS, вы можете ввести следующие строки:

nameserver 8.8.8.8

nameserver 8.8.4.4

Вы также можете настроить DNS-сервер для локальной сети, если вы хотите иметь свою собственную систему доменных имен для внутренних ресурсов. [Для этого вам потребуется установить и настроить специальное программное обеспечение, например, BIND](https://pq.hosting/help/system/253-kak-nastroit-dns-v-ubuntu.html)

DNS (Domain Name System) - это система доменных имен, которая позволяет переводить доменные имена сайтов в IP-адреса и обратно. DNS также используется для обнаружения и идентификации других устройств и сервисов в сети.

Настройка DNS в Linux зависит от типа вашего подключения и дистрибутива. В общем случае, вы можете настроить DNS в Linux двумя способами:

* С помощью меню графической оболочки. Этот способ подходит для начинающих пользователей, которые не хотят работать с консолью. Вы можете выбрать свое подключение, нажать на кнопку “Параметры соединения” и перейти к вкладке “IPv4” или “IPv6”. [Там вы можете указать способ получения DNS (автоматический или ручной) и ввести адреса серверов DNS, если нужно1](https://lumpics.ru/setup-dns-in-linux/)[2](https://habr.com/ru/articles/713156/).
* С помощью редактирования конфигурационных файлов. Этот способ подходит для опытных пользователей, которые предпочитают иметь больше контроля над настройками. Вы можете открыть файл /etc/resolv.conf и ввести адреса серверов DNS, которые вы хотите использовать. Например, если вы хотите использовать публичные серверы Google DNS, вы можете ввести следующие строки:

nameserver 8.8.8.8

nameserver 8.8.4.4

Вы также можете настроить DNS-сервер для локальной сети, если вы хотите иметь свою собственную систему доменных имен для внутренних ресурсов. [Для этого вам потребуется установить и настроить специальное программное обеспечение, например, BIND](https://pq.hosting/help/system/253-kak-nastroit-dns-v-ubuntu.html)

DNS (Domain Name System) - это система доменных имен, которая позволяет переводить доменные имена сайтов в IP-адреса и обратно. DNS также используется для обнаружения и идентификации других устройств и сервисов в сети.

Настройка DNS в Linux зависит от типа вашего подключения и дистрибутива. В общем случае, вы можете настроить DNS в Linux двумя способами:

* С помощью меню графической оболочки. Этот способ подходит для начинающих пользователей, которые не хотят работать с консолью. Вы можете выбрать свое подключение, нажать на кнопку “Параметры соединения” и перейти к вкладке “IPv4” или “IPv6”. [Там вы можете указать способ получения DNS (автоматический или ручной) и ввести адреса серверов DNS, если нужно1](https://lumpics.ru/setup-dns-in-linux/)[2](https://habr.com/ru/articles/713156/).
* С помощью редактирования конфигурационных файлов. Этот способ подходит для опытных пользователей, которые предпочитают иметь больше контроля над настройками. Вы можете открыть файл /etc/resolv.conf и ввести адреса серверов DNS, которые вы хотите использовать. Например, если вы хотите использовать публичные серверы Google DNS, вы можете ввести следующие строки:

nameserver 8.8.8.8

nameserver 8.8.4.4

Вы также можете настроить DNS-сервер для локальной сети, если вы хотите иметь свою собственную систему доменных имен для внутренних ресурсов. [Для этого вам потребуется установить и настроить специальное программное обеспечение, например, BIND](https://pq.hosting/help/system/253-kak-nastroit-dns-v-ubuntu.html)

1. Электронная почта.

Электронная почта в Linux - это способ обмена сообщениями между пользователями и сервисами с помощью специальных программ - почтовых клиентов. [Почтовые клиенты позволяют отправлять и получать электронные письма по протоколам SMTP, POP3 и IMAP1](https://timeweb.com/ru/community/articles/luchshie-pochtovye-klienty-dlya-linux).

Существует множество почтовых клиентов для Linux, которые имеют разный функционал, интерфейс и способ установки. Некоторые из них работают в графическом режиме, а некоторые в консольном. Вот несколько примеров почтовых клиентов для Linux:

* [**Thunderbird** - один из самых популярных и удобных почтовых клиентов для Linux, который поддерживает множество дополнений, тем и функций2](https://habr.com/ru/articles/143570/). Установить Thunderbird можно с помощью команды sudo apt install thunderbird или через менеджер приложений.
* [**Mailspring** - простой и современный почтовый клиент, который имеет красивый дизайн и расширенные возможности, такие как уведомления о прочтении, отслеживание ссылок, шаблоны писем и т.д.3](https://bluemail.help/ru/default-email-client/). Установить Mailspring можно с помощью команды sudo snap install mailspring или через менеджер приложений.
* [**Sylpheed** - быстрый и надежный почтовый клиент, который работает в графическом режиме, но имеет простой и легкий интерфейс4](https://winitpro.ru/index.php/2021/04/21/otpravka-email-iz-konsoli-linux/). Установить Sylpheed можно с помощью команды sudo apt install sylpheed или через менеджер приложений.
* [**mutt** - мощный и гибкий почтовый клиент, который работает в консольном режиме и поддерживает множество настроек и скриптов5](https://blog.sedicomm.com/2018/10/24/4-sposoba-otpravki-vlozhenij-elektronnoj-pochty-iz-komandnoj-stroki-linux/). Установить mutt можно с помощью команды sudo apt install mutt или yum install mutt.

Если вы хотите отправить электронное письмо из командной строки Linux, вы можете использовать один из этих почтовых клиентов или другие утилиты, такие как mail, mailx или sendmail. Например, чтобы отправить письмо с вложением через mutt, вы можете использовать следующую команду:

mutt -s "Тема письма" -a "Файл вложения" "Адрес получателя" < "Файл с текстом письма"

1. FTP и настройка FTP-сервера

FTP (File Transfer Protocol) - это протокол, который позволяет передавать файлы между клиентом и сервером через сеть. FTP-сервер - это программа, которая обеспечивает функциональность FTP на компьютере с Linux. FTP-клиент - это программа, которая подключается к FTP-серверу для загрузки или скачивания файлов.

Для создания FTP-сервера в Linux вам нужно выполнить следующие шаги:

* [Установить FTP-сервер, например, vsftpd1](https://ru.wikihow.com/%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8%D1%82%D1%8C-%D0%B8-%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B8%D1%82%D1%8C-FTP-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80-%D0%BD%D0%B0-Ubuntu-Linux), который является одним из самых популярных и безопасных FTP-серверов для Linux. Вы можете установить его с помощью команды sudo apt install vsftpd в терминале.
* Отредактировать файл конфигурации FTP-сервера, который находится в /etc/vsftpd.conf. В этом файле вы можете настроить различные параметры, такие как разрешение на запись, ограничение доступа, шифрование трафика и т.д. Вы можете открыть этот файл с помощью команды sudo nano /etc/vsftpd.conf в терминале.
* Добавить пользователей, которые будут иметь доступ к FTP-серверу. Вы можете использовать существующих пользователей Linux или создать виртуальных пользователей, которые не имеют локальных учетных записей. Вы можете добавить пользователей с помощью команды sudo adduser имя\_пользователя в терминале.
* Настроить брандмауэр, чтобы разрешить входящие соединения к FTP-серверу. Это необходимо, если вы используете Ubuntu или другой дистрибутив Linux с включенным брандмауэром по умолчанию. Вы можете настроить брандмауэр с помощью команды sudo ufw allow 20/tcp и sudo ufw allow 21/tcp в терминале, чтобы разрешить порты для FTP.

[После выполнения этих шагов вы сможете подключиться к своему FTP-серверу с помощью FTP-клиента, например, FileZilla2](https://progler.ru/blog/kak-ustanovit-i-nastroit-ftp-server-v-linux), который является одним из самых удобных и многофункциональных FTP-клиентов для Linux. Вы можете установить его с помощью команды sudo apt install filezilla в терминале.

1. Прокси-сервер и его настройка

Прокси-сервер - это сервер, который выступает в качестве посредника между вашим компьютером и интернетом. Прокси-сервер может использоваться для разных целей, таких как обход блокировок, повышение анонимности, ускорение загрузки сайтов и т.д.

Для настройки прокси-сервера в Linux вам нужно определить переменные окружения для разных типов трафика, таких как http, https и ftp. Это можно сделать с помощью команды export в терминале. Например, если вы хотите использовать прокси-сервер с адресом 192.168.1.1 и портом 8080 для http-трафика, вы можете ввести следующую команду:

export http\_proxy="http://192.168.1.1:8080"

Если прокси-сервер требует аутентификации, вы можете указать имя пользователя и пароль в формате user:pass. Например:

export http\_proxy="http://user:pass@192.168.1.1:8080"

Вы можете проверить, что прокси-сервер работает, с помощью команды env | grep -i proxy, которая покажет вам текущие переменные прокси. Вы также можете использовать утилиты, такие как curl, wget, apt-get и т.д., которые будут автоматически использовать прокси-сервер для доступа к интернету.

Для отключения прокси-сервера в Linux вам нужно сбросить переменные окружения с помощью команды unset. Например:

unset http\_proxy

1. Автоматизация задач администрирования на основе скриптовых языков оболочки.\

Прокси-сервер - это сервер, который выступает в качестве посредника между вашим компьютером и интернетом. Прокси-сервер может использоваться для разных целей, таких как обход блокировок, повышение анонимности, ускорение загрузки сайтов и т.д.

Для настройки прокси-сервера в Linux вам нужно определить переменные окружения для разных типов трафика, таких как http, https и ftp. Это можно сделать с помощью команды export в терминале. Например, если вы хотите использовать прокси-сервер с адресом 192.168.1.1 и портом 8080 для http-трафика, вы можете ввести следующую команду:

export http\_proxy="http://192.168.1.1:8080"

Если прокси-сервер требует аутентификации, вы можете указать имя пользователя и пароль в формате user:pass. Например:

export http\_proxy="http://user:pass@192.168.1.1:8080"

Вы можете проверить, что прокси-сервер работает, с помощью команды env | grep -i proxy, которая покажет вам текущие переменные прокси. Вы также можете использовать утилиты, такие как curl, wget, apt-get и т.д., которые будут автоматически использовать прокси-сервер для доступа к интернету.

Для отключения прокси-сервера в Linux вам нужно сбросить переменные окружения с помощью команды unset. Например:

unset http\_proxy

Если вы хотите настроить прокси-сервер для графического интерфейса, вы можете использовать меню настроек сети в вашем дистрибутиве Linux. [Там вы можете выбрать тип прокси, ввести адрес и порт прокси-сервера и применить изменения](https://youproxy.io/blog/how_to_setup_a_proxy_server_on_linux/)

1. Взаимодействие с OC Windows. Разделение и доступ к ресурсам в Windows-сетях.

Взаимодействие с OC Windows - это процесс обмена данными и командами между программами и операционной системой. [Операционная система Windows предоставляет различные интерфейсы для взаимодействия с ней, такие как графический пользовательский интерфейс (GUI), командная строка, PowerShell, API и т.д1](https://learn.microsoft.com/ru-ru/windows/security/identity-protection/access-control/access-control)

Разделение и доступ к ресурсам в Windows-сетях - это процесс управления правами и разрешениями пользователей и групп на файлы, папки, принтеры и другие объекты, доступные по сети. Для этого используются списки управления доступом (ACL), которые содержат записи управления доступом (ACE), определяющие, кто и как может получать доступ к ресурсу. В Windows существуют два типа разрешений: разрешения для общего доступа и разрешения NTFS. [Разрешения для общего доступа применяются к ресурсам, к которым можно получить доступ по сети, а разрешения NTFS применяются к ресурсам, хранящимся на диске с файловой системой NTFS2](https://support.microsoft.com/ru-ru/windows/%D0%BF%D1%80%D0%B5%D0%B4%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BE%D0%B1%D1%89%D0%B5%D0%B3%D0%BE-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0-%D0%BA-%D1%84%D0%B0%D0%B9%D0%BB%D0%B0%D0%BC-%D0%BF%D0%BE-%D1%81%D0%B5%D1%82%D0%B8-%D0%B2-windows-b58704b2-f53a-4b82-7bc1-80f9994725bf)[3](https://learn.microsoft.com/ru-ru/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions)

Linux - это семейство операционных систем, основанных на ядре Linux, которое является свободным и открытым программным обеспечением. Linux поддерживает множество архитектур, протоколов и стандартов, что делает его гибким и совместимым с различными устройствами и сетями. [Linux также предлагает разнообразие дистрибутивов, которые предоставляют различные наборы программ, интерфейсов и настроек для разных потребностей пользователе](https://altarena.ru/kak-nastroit-rabochuyu-gruppu-v-windows-10/)

1. Аудит и система регистрации событий

Аудит и система регистрации событий в Linux - это процесс отслеживания и записи важных событий, связанных с безопасностью и работой операционной системы. Для этого используется демон auditd, который позволяет настраивать правила фильтрации, управления и анализа событий. [С помощью утилит auditctl, ausearch, aureport и других можно управлять подсистемой аудита и просматривать журналы аудита1](https://habr.com/ru/companies/selectel/articles/267833/)[2](https://xakep.ru/2021/09/16/linux-audit/)

Для установки и настройки подсистемы аудита в Linux вам потребуется выполнить следующие шаги:

* Установить пакет audit с помощью команды sudo dnf install audit или аналогичной для вашего дистрибутива.
* Включить и запустить демон auditd с помощью команды sudo systemctl enable --now auditd.
* Настроить правила фильтрации событий в файле /etc/audit/audit.rules или с помощью команды sudo auditctl -a ....
* Проверить статус работы подсистемы аудита с помощью команды sudo auditctl -s.
* Просмотреть журнал аудита в файле /var/log/audit/audit.log или с помощью команд sudo ausearch ..., sudo aureport ... и других.

1. SSH

**SSH** - (**Secure** **Shell**) - это протокол удаленного управления компьютером с операционной системой **Linux**. В основном **ssh** используется для удаленного управления серверами через терминал. Если вы администратор нескольких серверов или даже продвинутый веб-мастер, то наверное, вы часто сталкиваетесь с необходимостью работать с тем или иным компьютером по **ssh**.

**SSH (Secure SHell - защищенная оболочка)** — сетевой **протокол** прикладного уровня, предназначенный для безопасного удаленного доступа к **различным системам (Linux, Windows, Mac)**.

Данный протокол шифрует всю передаваемую информацию по сети. По умолчанию, используется **22-й порт**. В основном он нужен для **удаленного управления** данными пользователя на сервере, запуска служебных команд, работы в консольном режиме с базами данных.

Эта служба была создана в качестве замены не зашифрованному [Telnet](https://ru.wikipedia.org/wiki/Telnet) и использует криптографические техники, чтобы обеспечить, что всё сообщение между сервером и пользователем было зашифровано.

Чтобы установить SSH-соединение, необходимы два компонента: SSH-сервер и SSH-клиент. Сервер прослушивает определенный порт (по умолчанию это порт 22) и при успешной аутентификации дает доступ пользователю. Все команды, которые используются на SSH-клиенте, отправляются через защищенный канал связи на SSH-сервер, на котором они выполняются и откуда отправляют результат работы обратно клиенту.

#### SSH-сервер

Устанавливается на управляемой операционной системе и принимает входящие подключения от клиентских машин, проверяя соединение одним из способов:

* по IP-адресу клиента, что не слишком безопасно из-за риска подмены;
* по публичному ключу клиента и имени пользователя. Нужно создать приватный (закрытый) и публичный (открытый) ключ. Зашифровав информацию одним ключом, можно расшифровать ее только другим;
* по паролю клиента, который передается в зашифрованном виде. Это один из наиболее распространенных вариантов. Вводить его нужно при каждом подключении.

Платные и бесплатные SSH-серверы есть для всех распространенных ОС:

* BSD — OpenSSH;
* Linux — dropbear, lsh-server, openssh-server;
* Windows — freeSSHd, copssh, WinSSHD, OpenSSH и т. д.

#### SSH-клиент

Используется для входа на удаленный сервер и выполнения команд. Через клиент выполняется управление удаленным компьютером.

SSH-клиенты разработаны для всех ОС. Имеют платные и бесплатные версии:

* Linux/BSD — openssh-client, putty, ssh, Vinagre;
* Windows — PuTTY, SecureCRT, ShellGuard;
* Android — connectBot.

Встроенный SSH-клиент Windows, основанный на OpenSSH, предустановлен в ОС, начиная с Windows 10 1809.

### Установка OpenSSH на Ubuntu

Установка с помощью менеджера пакетов apt-get:

sudo apt-get install openssh-server

### Проверка SELinux

Security Enhanced Linux, или SELinux – это усовершенствованный механизм контроля доступа, встроенный в большинство современных дистрибутивов Linux. Первоначально он был разработан Агентством национальной безопасности США **для защиты компьютерных систем от вторжения злоумышленников и взлома**. SELinux также может помешать работе с ssh. Поэтому необходимо убедиться, что он отключен, либо [отключить его](https://support.kaspersky.com/KWTS/6.1/ru-RU/165993.htm).

Устанавливаем доп. инструменты для работы с сетью и настройками безопасности:

sudo apt-get install policycoreutils

sudo apt-get install net-tools

Проверяем статус SELinux. Состояние должно быть disable.

sestatus

### Подключение к виртуальной машине с типом подключения NAT

Если виртуальная машина использует тип сетевого подключения [NAT](https://wiki.merionet.ru/seti/13/nat-na-palcax-chto-eto/), то первоначально необходимо настроить проброс портов. Пробросим порт хоста 2222 (или любой свободный) на гостевой порт виртуальной машины номер 22 (порт ssh по умолчанию).

После этого мы можем подключиться из Windows к нашей виртуальной машине.

#### Подключение по ssh через PuTTY

Т.к. в качестве сетевого подключения у виртуальной машины используется NAT, при подключении мы будем указывать петлевой адрес [localhost](http://localhost/) (127.0.0.1) c портом, на который был назначен проброс.

### Заключение

Несмотря на высокую защиту протокола, использование стандартного порта значительно повышает риск взлома сервера. Например, это можно сделать при помощи **brute-force** (атака полным перебором). Порт 22 — открытый, поэтому злоумышленнику нужно только подобрать логин и пароль к серверу. Это сложно, но возможно. Чтобы максимально ограничить доступ к серверу для злоумышленников (настроить брандмауэр, iptables), можно сменить SSH-порты.

## **Коротко о принципе работы SSH**

Рассмотрим, как работает подключение через SSH в Linuxи других ОС.

Сервер ожидает подключений на порту, который используется демоном sshd (чаще всего — 22). Клиент, в свою очередь,  создаёт подключение и определяет метод шифрования.

Когда между устанавливается TCP-соединение, стороны обмениваются различной вспомогательной информацией — поддерживаемыми методами шифрования, ключом public host и проч.

Далее ключ генерируется по алгориутму Диффи-Хеллмана, путём объединения ключей. Механизм работы алгоритма:

1. Стороны генерируют одинаковое число и выбирают стандарт шифрования.
2. Далее обе стороны выбирают новое число и не сообщают друг другу о нём.
3. Сгенерированное на шаге 2 число используется в качестве приватного ключа, а число из пункта 1 — публичного.
4. Стороны передают публичные ключи друг другу.
5. Вычисляя общий секрет, каждая сторона использует свой приватный ключ и чужой публичный. Его используют для симметричного шифрования.

Основное преимущество этого процесса — ни клиент, ни сервер не контролируют генерацию ключа, хотя участвуют в процессе оба.

## **Настройка SSH на стороне сервера**

Чтобы без проблем подключаться к удалённому устройству по SSH, нужно, чтобы и клиент, и сервер были корректно сконфигурированы. Рассмотрим, как обеспечить на сервере Linux доступ по SSH.

1. В первую очередь нужно обновить репозиторий с помощью apt:

sudo apt update

2. Далее устанавливаем набор программ OpenSSH:

sudo apt install openssh-server ssh

3. Запускаем sshd и добавляем в автозагрузку с помощью systemd:

sudo systemctl enable sshd

4. Проверям. Для этого, во-первых, смотрим статус работы sshd:

sudo systemctl sshd status

5. Во-вторых, пробуем подключиться к самому серверу:

ssh localhost

Если вы видите предложение добавить отпечаток и диалоговое окно с вопросом, продолжать ли соединение, то всё настроено корректно. Далее разберёмся, что это значит.

Стандартная настройка на этом завершена. Однако рекомендуется выполнить ещё несколько простых шагов для повышения безопасности.

Настройка SSH задаётся в файле/etc/ssh/sshd\_config.

### Замена стандартного порта

Порт SSH по умолчанию — 22. Многие специалисты рекомендуют менять это значение на любое другое (можно выбрать любой порт от 50000 до 65000). Причина в том, что, если устройство находится в общей сети и доступен из интернета, он неизбежно будет подвергаться атакам и автоматическим попыткам взлома. Даже если механизм авторизации надёжен, сервер всё равно выполняет немало работы: журналирование попыток входа, установление соединения, генерация ключа и так далее.

Если заменить порт или закрыть его с помощью [таблиц маршрутизации iptables](https://timeweb.cloud/docs/unix-guides/iptables-setup), нагрузка существенно снизится — соединения с 25 портом будут отсекаться ещё на этапе установки соединения.

Для замены откроем файл:

sudo nano /etc/ssh/sshd\_config

Находим переменную Port 22 и заменяем 22 на, например, 55222. Если настройки SSH стандартные, не забудьте раскоментировать строку.

### Отключение доступа root

Смена стандартного порта повышает безопасность, но не гарантирует то, что злоумышленники не узнают, какое значение вы указали в файле конфигурации, — существует программное обеспечение, которое сканирует порты сервера.

В качестве ещё одной меры безопасности закроем удалённый доступ учётной записи root, так как иначе злоумышленники при попадании в систему получат неограниченные полномочия.

Ограничим доступ, установив флаг переменной PermitRootLogin на no.

### Ограничение авторизации по паролю

Следующий шаг — запрет входа по паролю. Вместо этого включим принудительное использование ключей, присвоив переменной PasswordAuthentication флаг no.

Затем перезапустите демон sshd:

sudo systemctl restart sshd

### Ограничение доступа по IP

Вы также имеете возможность ограничить SSH-соединение Linux-сервера, дав доступ ограниченному диапазону IP-адресов. Чтобы это сделать, откройте файл/etc/hosts.deny:

sudo nano /etc/hosts.deny

… и добавьте строку sshd: ALL.

В конфиге /etc/hosts.allow укажите разрешённые IP-адреса:

sudo nano /etc/hosts.allow

sshd: 182.10.0.1 182.10.0.10

## **SSH-клиенты**

Если вы подключаетесь с Windows-устройств, можете использовать специальные приложения. Например, PuTTY, WinSCP или Termius. Если работаете в unix-системах, вам доступноподключение по SSH из консоли Linux или terminal напрямую.

## **Авторизация**

Рассмотрим, как выполнить подключение по SSH в Linux. Самый простой способ авторизации на сервере — войти с помощью пароля, который передаётся по защищённому соединению. Однако, рекомендуется не использовать этот метод, поскольку пароль может быть скомпрометирован, утерян или подобран злоумышленником перебором (брутфорс-атака).

В качестве альтернативы рекомендуется использовать вход по ключам.

### По паролю

Чтобы подключиться к серверу, воспользуйтесь командой:

ssh username@host, где username — имя пользователя, а host — сервер.

Выше  — подключение с настройками по умолчанию, т. е. к 22 порту. В примере ниже мы изменили это значение на то, которое указали в конфигурации:

ssh -p 55222 username@host

Если не указывать учётную запись и написать просто ssh host, попытка соединения будет устанавливаться с использованием имени текущего пользователя.

### По ключам

Ключ должен быть сгенерирован на стороне клиента. Для этого воспользуйтесь утилитой ssh-keygen:

ssh-keygen -t rsa

В папке ~/.ssh будет сгенерировано два файла:

1. id\_rsa — приватный ключ, на это намекают права: только владелец файла может читать и редактировать.
2. id\_rsa.pub — публичный ключ, об этом говорит и расширение, и права: доступен для чтения всем.

Далее нужно передать id\_rsa.pub на сервер. Для этих целей воспользуйтесь утилитой ssh-copy-id:, указав имя сервера вместо host:

ssh-copy-id host

## **Заключение**

SSH — незаменимый протокол для специалистов, работающих с удалёнными устройствами. Он позволяет настраивать серверы, размещать и забирать файлы. И всё это по защищённому каналу.

Чтобы разобраться, как работает протокол, рассмотрели подключение по SSH Linux-устройств и с паролем, и с ключами доступа. В этих целях арендовали сервер с ОС Ubuntu на [Timeweb Cloud](https://timeweb.cloud/), настроили на нём протокол и авторизовались на сервере с удалённого компьютера через командную строку.