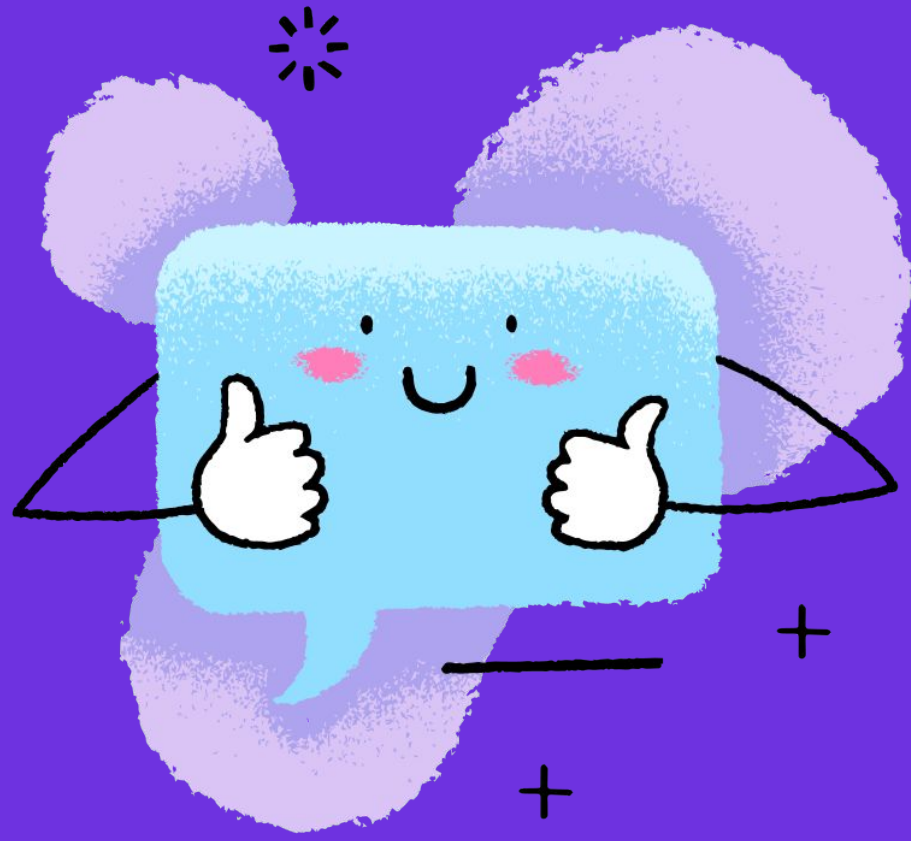
GeekBrains

Урок 3

Управление пользователями. Процессы. Права доступа. Репозитории.

Linux

Вопросы по практическому заданию и предыдущему уроку



План урока

1. Пользователи и группы пользователей
2. Процессы
3. Файловая система, права доступа к файлам
4. Репозитории

Пользователи и группы

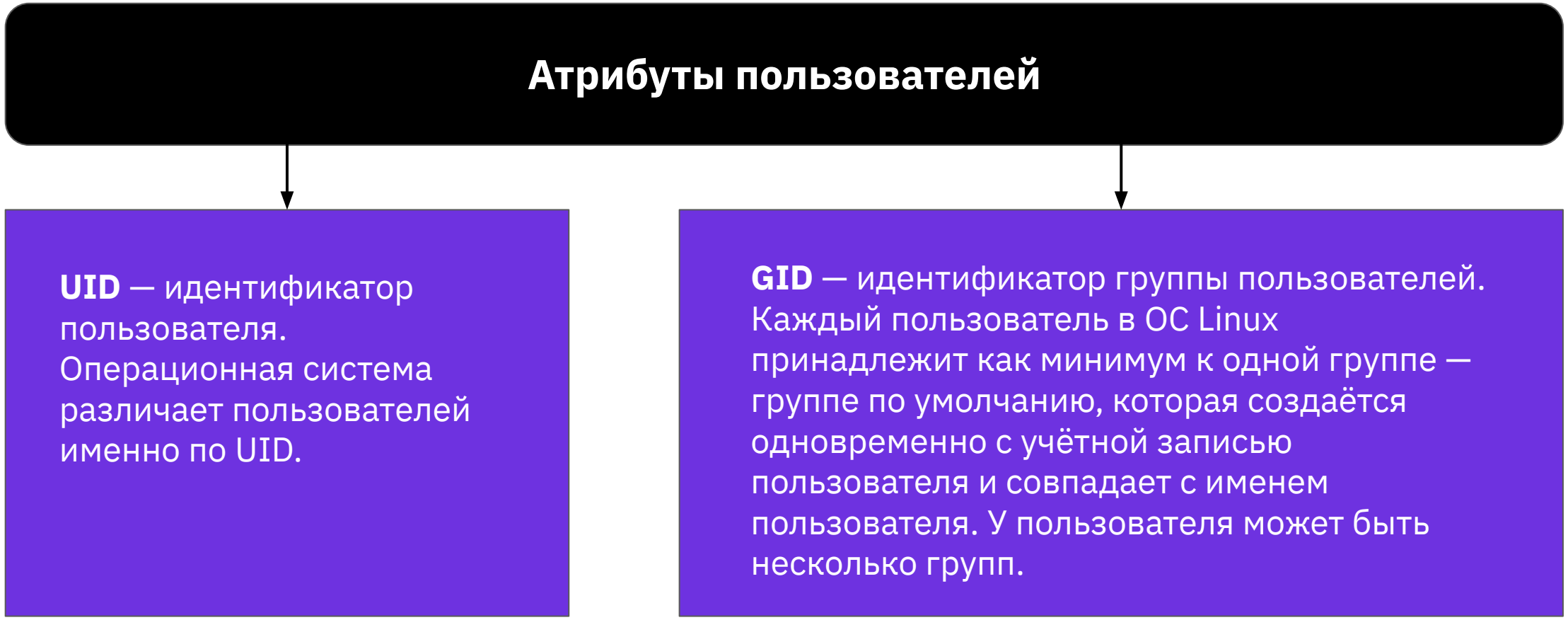
Мы освоим управление пользователями и группами. Узнаем, как применять штатные утилиты и вручную добавлять пользователей, редактируя соответствующие файлы. А также научимся изменять владельца и группу владельца файлов и каталогов.

1. Типы пользователей.
2. Управление пользователями и группами.
3. Утилиты sudo, su.

Типы пользователей

Пользователь — ключевое понятие организации системы доступа к ресурсам ОС Linux. У пользователей есть два основных атрибута: UID и GID.

Типы пользователей



Типы пользователей

ТЕМА

Типы пользователей

01

GeekBrains

Суперпользователь (root) — это пользователь с неограниченными правами. Он имеет UID и GID, равные 0. В системе больше не должно быть пользователей с таким UID, но другие пользователи могут входить в группу суперпользователя.

Этот пользователь предназначен для выполнения команд и действий с файлами, которые могут влиять на работу как отдельных служб, так и всей системы.

ТЕМА

Типы пользователей

02

GeekBrains

Системные пользователи (пользователи-демоны, технологические пользователи) предназначены для обеспечения работы запущенных процессов. Обычно такие пользователи не имеют оболочки, а также не могут никаким образом авторизоваться в системе.

ТЕМА

Типы пользователей

03

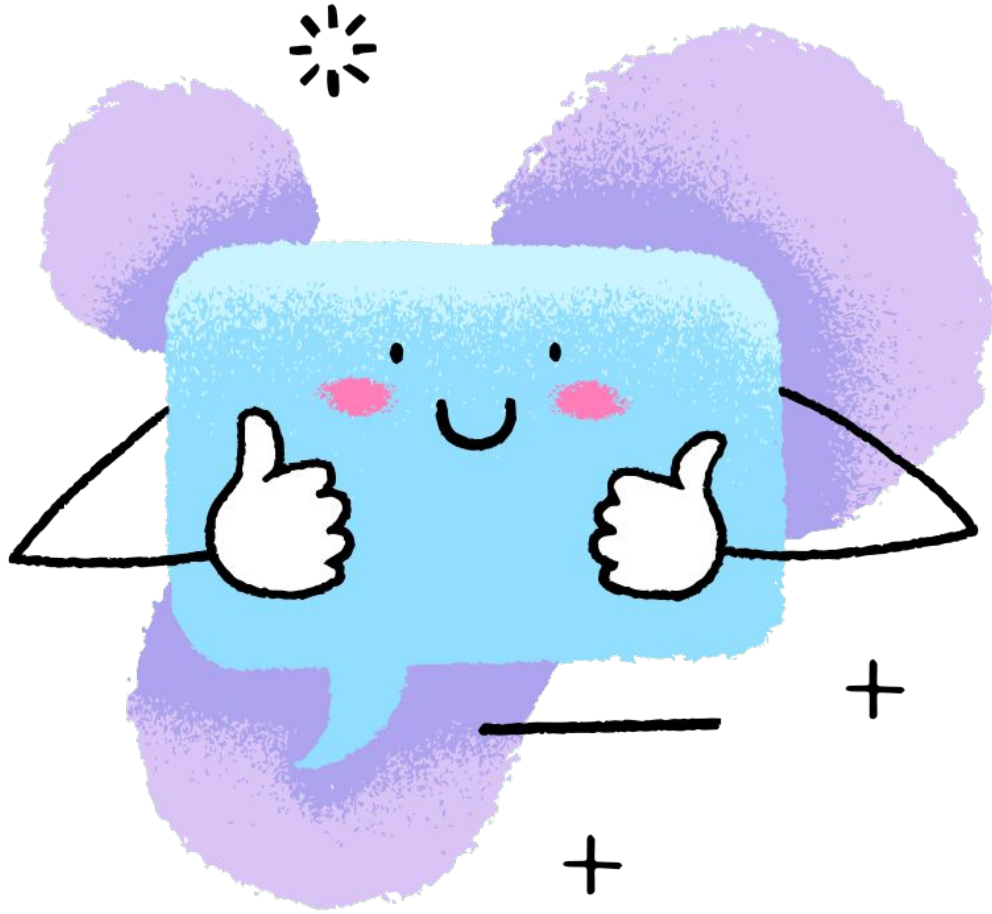
GeekBrains

Обычные пользователи — это учётные записи, которые используются для работы в ОС и создаются администратором системы.

Они могут быть локальными — созданными непосредственно на сервере, либо сетевыми, например если сведения об учётной записи хранятся в домене LDAP (аналог службы Active Directory в Windows).

Такой тип учётных записей может использоваться не только людьми, но и программным обеспечением, предназначенным для управления конфигурациями (например, Ansible).

Управление пользователями и группами



Файл **/etc/passwd** предназначен для хранения списка учётных записей (аккаунтов) в текстовом виде.

01

Файл **/etc/group** хранит информацию о группах и пользователях, состоящих в этих группах.

02

Файл **/etc/shadow** хранит информацию о паролях пользователей из файла etc/passwd. Во многих системах файл доступен только для чтения пользователю root.

03

Управление пользователями и группами

useradd — стандартная команда Linux, она предназначена для создания пользователя в системе.

adduser — Perl-скрипт, реализующий в более удобном и интерактивном виде функционал команды useradd. Он рекомендуется к использованию в Debian-подобных системах. Одна из особенностей этой команды — отсутствие каких-либо дополнительных действий с учётной записью после её создания.

Управление пользователями и группами

groupadd — стандартная утилита Linux, предназначенная для создания групп. Обычно группы создаются сразу при создании пользователя. Но довольно часто бывают ситуации, когда в одну группу должны входить сразу несколько пользователей. Здесь на выручку придёт команда groupadd.

addgroup — скрипт, использующий функционал команды groupadd.

Сравнение или перечисление

passwd user_name
изменит пароль пользователя с именем user_name.

passwd
без указания пользователя изменит или задаст пароль текущему пользователю.

chage user_name
позволит изменить политики для паролей конкретного пользователя. Действие требует прав суперпользователя, поэтому данная команда также используется с командой sudo.

usermod
изменяет атрибуты пользователя.

Утилиты sudo, su

Для выполнения административных действий обычным пользователем используют две утилиты: su и sudo.

TEMA

Утилиты sudo, su

01

GeekBrains

su — команда, которая позволяет сменить ID пользователя или делает пользователя суперпользователем, при этом не завершая сеанс пользователя.

su без параметров переключит текущего пользователя в суперпользователя. Этот метод работы под суперпользователем не очень хорош, так как нет никаких ограничений.

ТЕМА

Утилиты sudo, su

02

GeekBrains

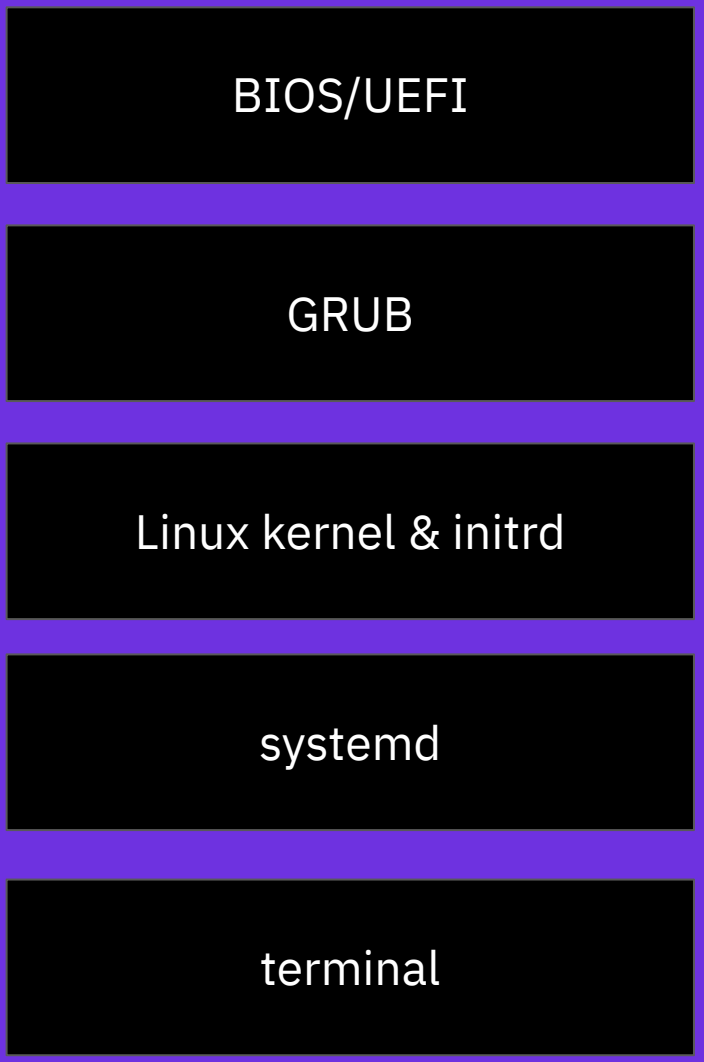
sudo — утилита, которая позволит выполнять административные действия в системе согласно настройкам в файле /etc/sudoers.

Файл /etc/sudoers редактируется только пользователем, имеющим права администратора системы.

Процессы

1. Загрузка операционной системы.
2. Процесс. Управление процессами.
3. Атрибуты процессов.
4. Управление процессами.
5. Мониторинг процессов и состояния компьютера.

Загрузка операционной системы



Что такое процесс

Процесс — одно из основополагающих понятий в ОС Linux. По сути, это совокупность какого-то кода, выполняющегося в памяти компьютера. Но есть приложения, которые могут создавать в результате своей работы не один, а несколько процессов.

Каждая команда, которую мы выполняем в терминале, или приложение, которое мы запускаем в графической оболочке, также порождает процессы.

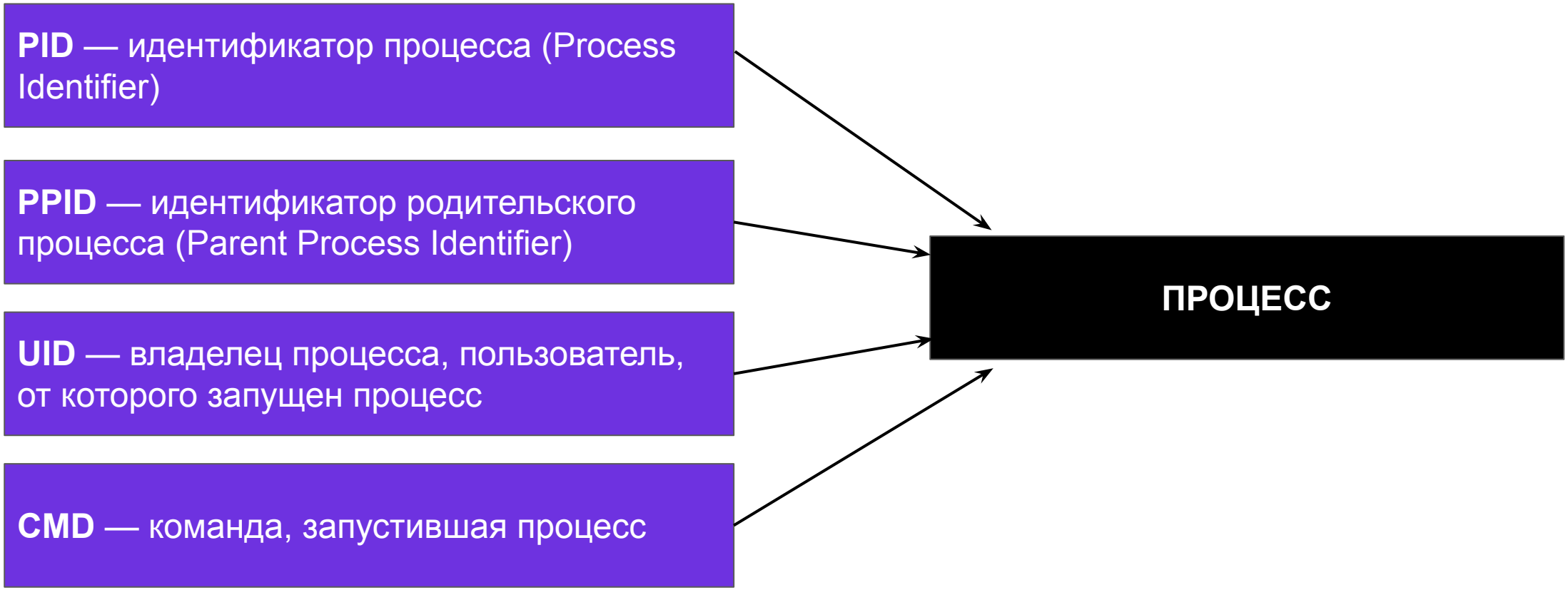
Некоторые состояния процесса

Процесс работает

Процесс спит

Процесс-зомби

Атрибуты процессов



Управление процессами (systemctl)

Управление процессами осуществляется через утилиту systemctl.

systemctl — основная команда для управления и мониторинга systemd. Позволяет получать информацию о состоянии системы и запущенных службах, а также управлять службами. Более подробную информацию можно получить на страницах справочного руководства man systemctl.

Основные параметры systemctl

1. **systemctl status** выведет на экран состояние системы.
2. **systemctl** выведет список запущенных юнитов. С точки зрения systemctl, юнитом может быть служба, точка монтирования дискового устройства.
3. **systemctl [start|stop|status|restart|reload] service_name** позволит запустить службу (start), остановить (stop), получить информацию о службе (status), перезапустить службу (restart), перечитать конфигурационный файл службы (reload).
4. **systemctl [enable|disable] service_name** позволит добавить (enable) или убрать (disable) службу из автозагрузки.

Управление процессами (kill)

Существуют специальные сигналы, которые мы можем передать процессу, используя команду **kill**. Полный список сигналов можно получить, выполнив команду **kill -l**.

Команда **kill** работает с процессом через его PID.

Стандартные потоки

Файловый дескриптор	Открытые файлы
0	Стандартный поток ввода (**STDIN**). Файл, из которого осуществляется чтение данных.
1	Стандартный поток вывода (**STDOUT**). Файл, в который осуществляется запись данных.
2	Стандартный поток ошибок (**STDERR**). Файл, в который осуществляется запись об ошибках или сообщения, которые не могут быть записаны в стандартный поток вывода.

Конвейер (pipeline)

Стандартные потоки можно перенаправлять не только в файлы, но и на ввод другим процессам. Такое перенаправление называют конвейером (pipeline). В нём используется специальный символ «|» (вертикальная черта).

Например, command-1 | command-2|...|command-n перенаправит результат работы команды command-1 на ввод другой команде — command-2, которая в свою очередь перенаправит результат своей работы на ввод следующей команде.

Мониторинг процессов и состояния компьютера

ps

Покажет список запущенных процессов в операционной системе. Эта команда в сочетании с **grep** — утилитой, осуществляющей поиск по строкам согласно заданному шаблону, — позволяет найти и получить следующую информацию о процессе: PID, PPID, статус процесса.

top
(table of process)

Выведет список запущенных в системе процессов и информацию о них. Строка load average покажет общую загрузку системы.

При этом важно понимать, что значения load average бóльшие, чем количество доступных ядер процессора, говорят о высокой нагрузке на сервер. Также программа по умолчанию сортирует процессы по нагрузке на процессор в режиме реального времени.

Права доступа к файлам

1. Права доступа к файлам и каталогам.
2. Ссылки (жесткие, символьные)

Типы файлов в Linux

Файл — ключевое понятие в Linux. Посредством файлов операционная система взаимодействует с пользователем, процессы взаимодействуют между собой и с пользователем, ядро операционной системы взаимодействует с устройствами компьютера.

Права доступа к файлам и каталогам

У файлов и каталогов есть ряд атрибутов, хранящихся в inode. Полный вывод атрибутов мы можем посмотреть, выполнив команду ls -l.

Первый столбец вывода покажет права доступа к файлу или каталогу. Символы столбца можно условно разделить на четыре группы:

Права доступа к файлам и каталогам

Тип файла	Права доступа для владельца	Права доступа для группы	Права доступа для всех остальных
- — обычный файл; d — каталог; b — файл блочного устройства; c — файл символьного устройства; s — socket; p — именованный канал (pipe); l — символическая ссылка (link).	r (read) — чтение w (write) — запись x (execute) — выполнение	r (read) — чтение w (write) — запись x (execute) — выполнение	r (read) — чтение w (write) — запись x (execute) — выполнение

Права доступа к файлам и каталогам

r (read)
Возможность открытия и чтения файла или просмотр содержимого каталога.

w (write)
Возможность изменить содержимое файла или возможность создавать, удалять или переименовывать объекты в каталоге.

x (execute)
Возможность выполнить файл (запустить программу, скрипт) или возможность войти в каталог и получить атрибуты объектов.

Права доступа к файлам и каталогам

Права доступа можно представить в численном виде, используя восьмеричную систему счисления, согласно таблице:

Восьмеричная	Символьная	Права на файл	Права на каталог
0	---	Нет	Нет
1	--x	Выполнение	Возможность зайти в каталог и прочитать атрибуты
2	-w-	Изменение содержимого файла	Возможность изменить содержимое каталога (создать файл или каталог)

Права доступа к файлам и каталогам

3	-wx	Изменение и выполнение	Возможность изменить содержимое каталога и прочитать атрибуты
4	r--	Чтение	Просмотр содержимого каталога
5	r-x	Чтение и выполнение	Просмотр содержимого каталога и атрибутов
6	rw-	Чтение и запись	Чтение и изменение содержимого каталога
7	rwx	Полные права	Полные права

Специальные биты

SUID (set user ID upon execution) — установка ID пользователя во время выполнения. Разрешает пользователям запускать файл на исполнение с правами того пользователя, которому принадлежит данный файл. SUID работает с файлами.

SGID (set group ID upon execution) — установка ID группы во время выполнения, применяется преимущественно к каталогам. Этот атрибут устанавливает идентификатор группы каталога, а не группы владельца, который создал файл в этом каталоге.

Sticky — дополнительный атрибут, который устанавливается для каталогов. Файлы из каталога с таким битом может удалить только владелец (пользователь, создавший этот файл).

Жёсткие и символические ссылки

Ссылки — это особенность файловой системы, которая позволяет размещать один и тот же файл в разных каталогах.

Жёсткая ссылка — это запись в каталоге, указывающая на inode. Создаётся только для файлов, за исключением специальных записей, указывающих на саму директорию (.) и родительскую директорию (..). Жёсткие ссылки используются только в пределах одного раздела.

Символическая ссылка — это запись в каталоге, указывающая на имя объекта с другим inode. Наиболее близка к ярлыку в Windows. Она может ссылаться на файл и на каталог. Символические ссылки могут существовать на разных разделах.

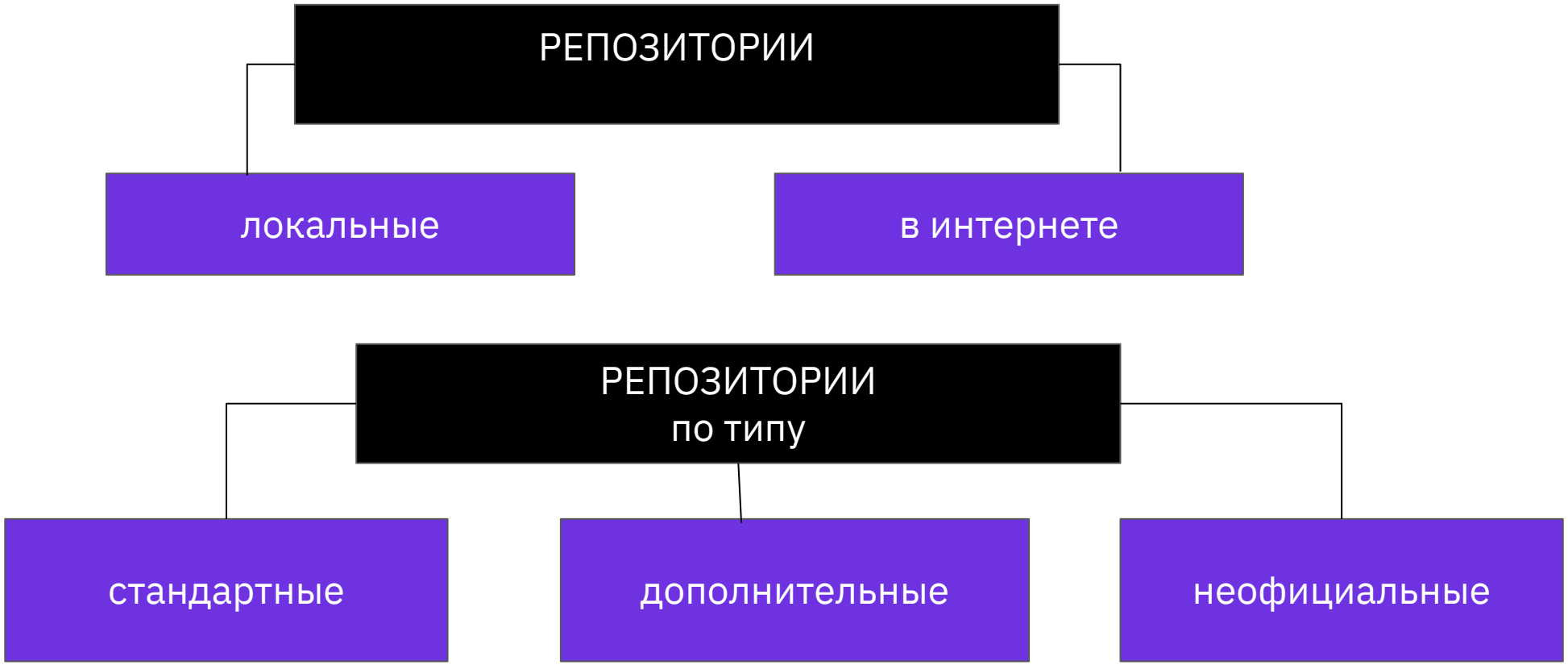
Репозитории

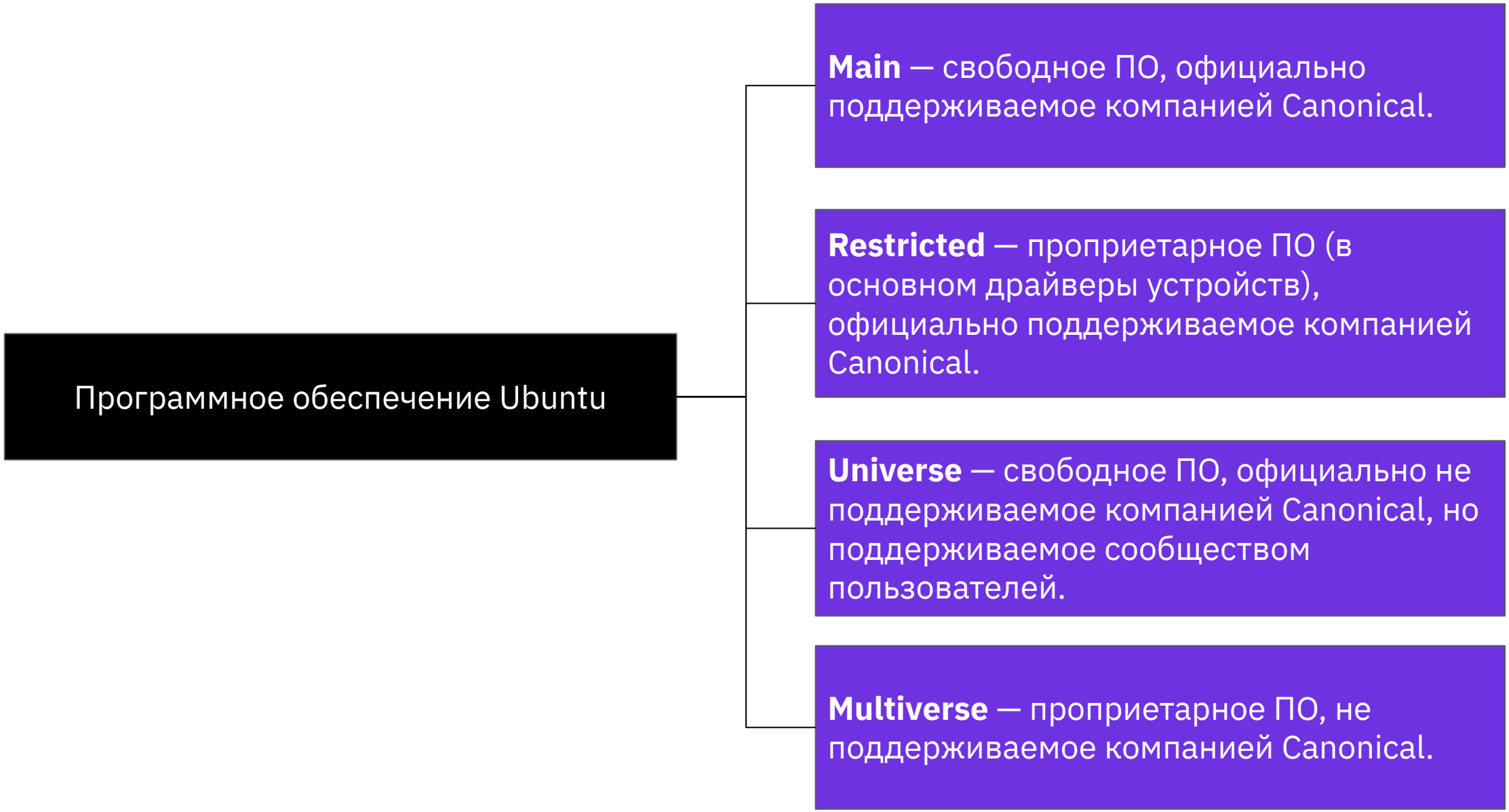
1. Репозитории и управление репозиториями.
2. Подключение репозиториев.
3. Управление пакетами.

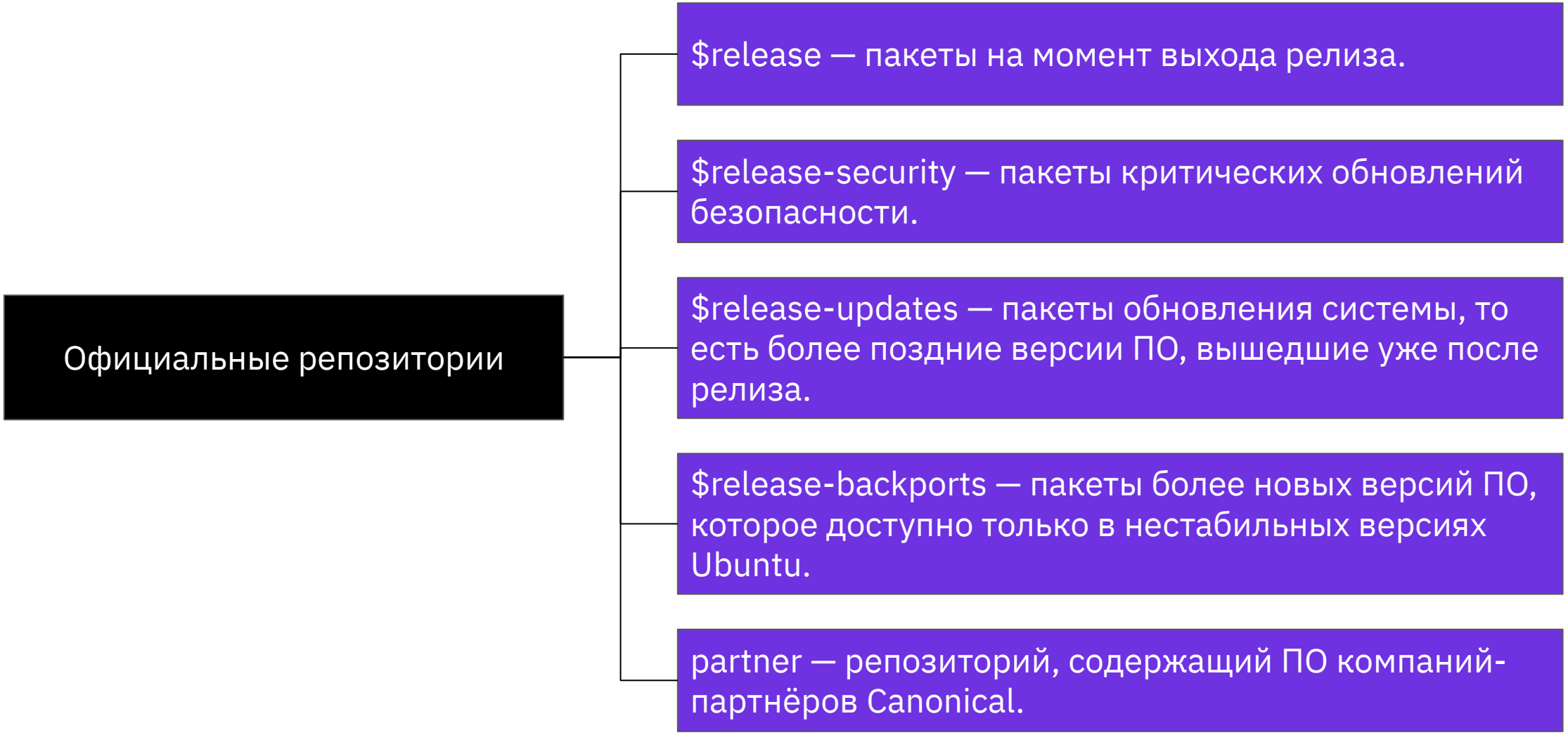
Репозитории и управление репозиториями

Пакет — под пакетами в Linux подразумевается программное обеспечение, которое можно установить, то есть набор файлов, объединённых для выполнения определённого функционала. Пакеты, как правило, хранятся в репозиториях.

Репозиторий — место, где хранятся и поддерживаются какие-либо данные. Чаще всего данные в репозитории хранятся в виде файлов, доступных для дальнейшего распространения по сети.


РЕПОЗИТОРИИ
локальные
в интернете
РЕПОЗИТОРИИ
по типу
стандартные
дополнительные
неофициальные


Программное обеспечение Ubuntu
Main — свободное ПО, официально поддерживаемое компанией Canonical.
Restricted — проприетарное ПО (в основном драйверы устройств), официально поддерживаемое компанией Canonical.
Universe — свободное ПО, официально не поддерживаемое компанией Canonical, но поддерживаемое сообществом пользователей.
Multiverse — проприетарное ПО, не поддерживаемое компанией Canonical.


Официальные репозитории
$release — пакеты на момент выхода релиза.
$release-security — пакеты критических обновлений безопасности.
$release-updates — пакеты обновления системы, то есть более поздние версии ПО, вышедшие уже после релиза.
$release-backports — пакеты более новых версий ПО, которое доступно только в нестабильных версиях Ubuntu.
partner — репозиторий, содержащий ПО компаний-партнёров Canonical.

Способы подключения репозиториев в системе

1. Редактирование файла /etc/apt/source.list.
2. Команда apt-add-repositroy.

ВАЖНО: после подключения репозитория не забудьте обновить информацию о пакетах, выполнив sudo apt update!

apt — это пакетный менеджер, который включает в себя набор утилит для управления пакетами. Он позволяет осуществлять поиск, установку и удаление пакетов, обновлять операционную систему, подключать репозитории.

dpkg — пакетный менеджер в Debian-подобных системах. Главное отличие от утилиты apt состоит в том, что dpkg работает только с локальными пакетами, он не умеет искать и устанавливать пакеты с репозиториев.

snap — это пакет, который, помимо готовой сборки самого приложения, включает в себя все необходимые зависимости и может работать почти в любом дистрибутиве Linux. В какой-то степени можно считать, что пакеты, установленные при помощи snap, — альтернатива самостоятельной сборке пакета.

Спасибо!

Каждый день вы становитесь лучше :)