1. Учётные записи

Основа распределения прав доступа в операционной системе Linux лежит на понятии пользователь. Пользователю-владельцу файла выдаются определенные полномочия для работы с ним, а именно: на чтение, запись и выполнение. Также отдельно устанавливаются полномочия на чтение, запись и выполнение для всех остальных пользователей. Поскольку в Linux всё есть файл, то такая система позволяет регулировать доступ к любому действию в этой операционной системе с помощью установки прав доступа на файлы. Но еще при создании Linux, разработчики поняли, что этого явно недостаточно.

Поэтому были придуманы группы пользователей. Пользователи могут объединяться в группы, чтобы уже группам выдавать нужные полномочия на доступ к тем или иным файлам и, соответственно, и действиям.

Каждой группе присваивается идентификатор (GroupID, далее - GID). GID от 0 до 99 используются самой системой. GID от 100 до 999 используются службами и создаются динамически.

Идентификаторы для пользовательских групп распределяются динамически в диапазоне от 1000 до 59999.

В Linux предусмотрено три типа пользователей:

☐. Суперпользователь (root) — имеет полный доступ к системе.

☐. Обычные пользователи — разрешён терминальный вход в систему.

☐. Системные пользователи — учётные записи, которые необходимы для функционирования операционной системы и служб.

Пользователи, как и группы, имеют свой идентификатор (UserID, далее — UID). Суперпользователь всегда имеет UID равный нулю. Идентификаторы для пользователей распределяются аналогично таковым для групп:

- от 0 до 99 — используются самой системой;
- от 100 до 999 — используются службами;
- от 1000 до 59999 — используются пользователями.

> **ПРИМЕЧАНИЕ**
> в Linux используются и другие идентификаторы пользователей и групп. Они используются в особых случаях и в данном курсе рассмотрены не будут. Ознакомиться с политикой распределения идентификаторов можно по ссылке https://www.debian.org/doc/debian-policy/ch-opersys.html#users-and-groups.

Информация об учётных записях хранится в файле /etc/passwd. Каждая строка в файле соответствует одной учётной записи. Параметры учётной записи в строке разделены двоеточием и имеют следующий набор:

- имя учётной записи (логин);
- пароль в зашифрованном виде. Символ X означает, что пароль хранится в отдельном файле - /etc/shadow;
- идентификатор пользователя (UID);
- идентификатор группы (GID), которой принадлежит пользователь;
- подробная информация о пользователе (поле GECOS). Значения записываются через запятую, без использования символа двоеточие. Обычно значения идут в следующем порядке:
  - полное имя пользователя;
  - адрес;
  - номер рабочего телефона;
  - номер домашнего телефона;
  - прочая информация (например, электронная почта);
- абсолютный путь к домашнему каталогу пользователя;
- первая программа, выполняемая сразу после входа пользователя в систему. Обычно это командный интерпретатор (shell), например, /bin/bash. Если указать специальное значение /bin/false (которое ничего не делает и возвращает контроль системе немедленно), то пользователь не сможет войти в систему.

```
tester:x:210:8:Edward Chernenko,Marx Street 10,4554391,5454221:/home/ed:/bin/bash
dbus:x:81:81:System Message Bus:/:/usr/bin/nologin
```

Файл /etc/passwd может быть прочитан обычным пользователем, что является уязвимым местом в безопасности. Получив этот файл, можно попытаться подобрать пароль к учётной записи. Поэтому пароли в зашифрованном виде хранятся в отдельном файле - /etc/shadow, доступ к которому обычный пользователь не имеет. Каждая строка файла содержит девять полей, разделённых двоеточием:

- имя пользователя (username);
- закодированный пароль (encrypted password);
- дата последнего изменения пароля (last password change): в днях, отсчитываемых с 1 января 1970 года (дата эпохи);
- минимальное число дней между изменениями пароля (minimum password age). Это количество дней, которое должно пройти прежде, чем можно будет изменить пароль пользователя. Значение «0» означает отсутствие данного ограничения;
- максимальное число дней между изменениями пароля (maximum password age). Это количество дней до

необходимости смены пароля. Значение 99999 указывает на то, что ограничение не установлено;

- период предупреждения (warning period). Количество дней до истечения срока действия пароля, в течение которых пользователя предупреждают о необходимости изменения пароля;
- период бездействия (inactivity period). Количество дней бездействия пользователя после истечения срока действия пароля до блокировки учетной записи пользователя;
- срок действия учетной записи (expiraion date). Дата, когда учетная запись была отключена;
- не используется (unused).

В Astra Linux для шифрования паролей используется алгоритм gost12_512 (ГОСТ Р 34.11-2012).

Информация о группах содержится в файле /etc/group. Каждая строка в файле несколько значений, разделённых двоеточием:

- имя группы (groupname);
- пароль в зашифрованном виде. Символ X означает, что пароль хранится в отдельном файле - /etc/gshadow;
- идентификатор группы (GID);
- список пользователей (username-list), разделенных запятой, для которых данная группа является дополнительной (вторичной).

Пароль для группы используется в случае, если пользователь, не являющийся членом группы, хочет получить членство в данной группе. Пустое значение в поле пароля группы означает, что только члены группы могут использовать ее для получения доступа к файлам. Как и в случае с пользователями, пароли для групп хранятся в отдельном файле - /etc/gshadow. Для каждой группы — отдельная строка, содержащая значения, разделённые двоеточием:

- имя группы;
- зашифрованный пароль группы;
- администраторы группы — члены группы, перечисленные через запятую, которые могут менять пароль или членство в группе;
- члены группы — члены группы, перечисленные в этом поле, являются обычными пользователями данной группы.

Перед созданием учётных записей рекомендуется решить несколько организационных вопросов:

- Выработать правила формирования имен учетных записей пользователей и групп;
- Решить, как будут распределяться идентификаторы учетных записей пользователей и групп (UID, GID);

- Определить основную (первичную) и дополнительные (вторичные) группы для учетных записей пользователей;
- Решить, где будут располагаться домашние каталоги пользователей;
- Решить, какой командный интерпретатор будет использоваться по умолчанию;
- Определить правила формирования и политику использования паролей.

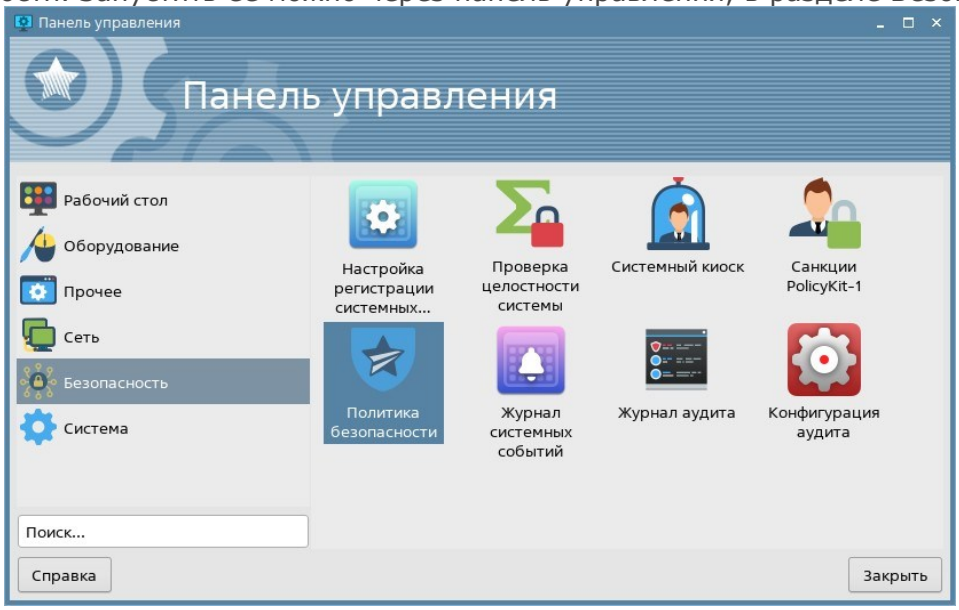
В случае, если для учетной записи пользователя явно не задается первичная группа, то возможен выбор одной из двух стандартных политик:

- для учетных записей пользователей определяется общая первичная группа (по умолчанию, группа users, GID 100)
- для каждой учетной записи пользователя создается своя первичная группа (приватная), имя которой совпадает с именем пользователя

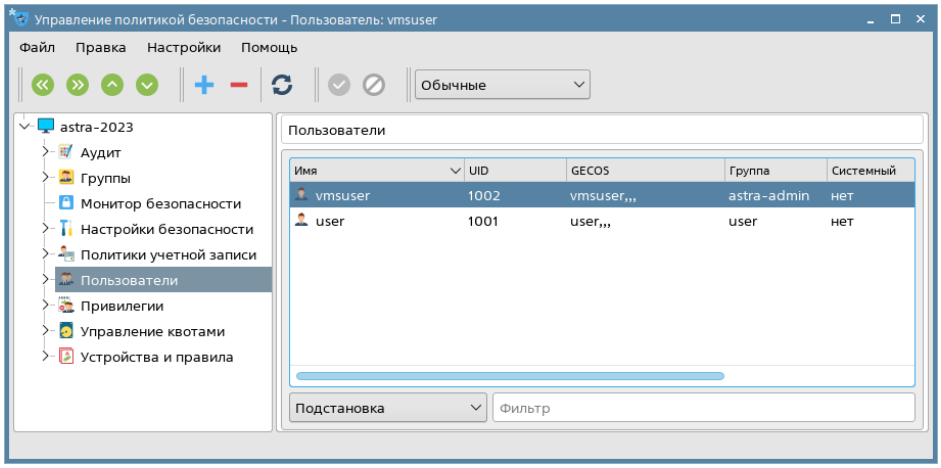
Политика с приватной первичной группой считается более безопасной и является политикой по умолчанию в Astra Linux.

2. Управление учётными записями

Управление учётными записями и группами в Astra Linux осуществляется в утилите Политика безопасности. Запустить её можно через панель управления, в разделе Безопасность.



Работа с утилитой требует повышенных привилегий, поэтому при её запуске потребуется ввести пароль суперпользователя.



В левой части окна отображается панель навигации, с помощью которой можно перейти к различным настройкам безопасности системы. Работа с пользователями и группам осуществляется в соответствующих разделах.

В верхней части окна отображается панель инструментов. Кнопка в виде синего плюса позволяет создать новую группу или учётную запись. Кнопка в виде красного минуса позволяет удалить группу или пользователя (активна только при выбранном пользователе или группе). Круглая зелёная кнопка с галочкой позволяет применить (сохранить) внесённые изменения (активна только в случае внесения изменений). Рядом расположена круглая кнопка с диагональной линией — она позволяет отменить внесённые изменения.

Двойное нажатие на пользователе или группе позволит перейти к редактированию соответствующих параметров.

Атрибуты и другие параметры учетной записи пользователя распределены по вкладкам:

- Общие — основные атрибуты учетной записи пользователя и задание пароля;
- Блокировка — блокировка пароля и учетной записи;
- Аудит — настройки аудита событий, вызванных действиями пользователя;
- Привилегии — установка привилегий пользователя;
- МРД — установка мандатных атрибутов пользователя;
- Срок действия — сроки действия пароля и учетной записи;
- Графический киоск — настройка работы пользователя с ограниченным набором приложений (режим графического киоска);
- Квоты — настройка дисковых квот для пользователя.

Параметры группы также распределены по вкладкам:

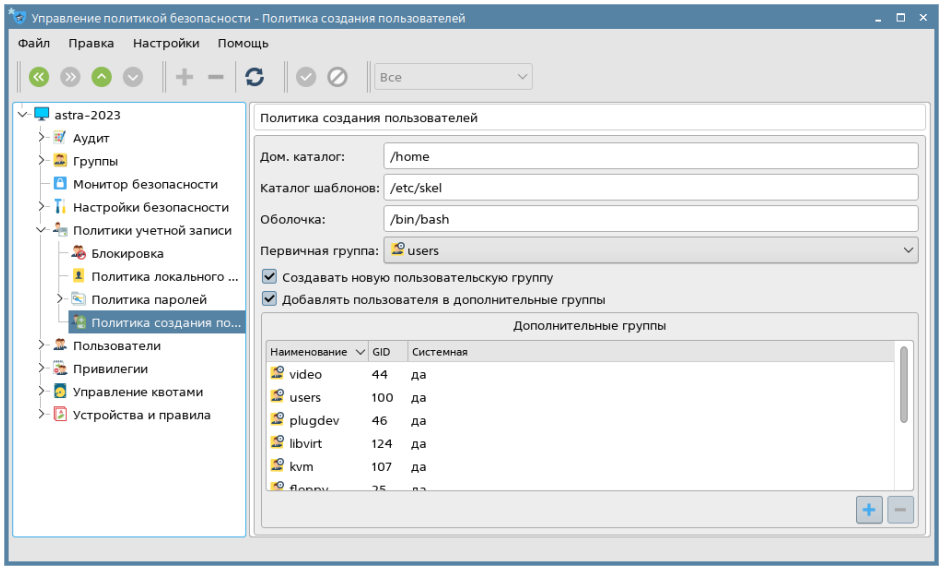
- Общие — позволяет добавить пользователей в группу;
- Аудит — редактирование правил аудита для пользователей, входящих в группу;
- Квоты — настройка дисковых квот для пользователей из группы;

- Графический киоск — настройка работы пользователей, входящих в группу, с ограниченным набором приложений.

В разделе параметры, как:

Политики учетной записи

- Блокировка — условия автоматической блокировки пользователя;
- Политика паролей — параметры сложности пароля, срок действия, история паролей;
- Политика создания пользователей — параметры по умолчанию для создаваемых пользователей (первичная группа, дополнительные группы, присваиваемые по умолчанию, домашний каталог, и прочие);
- Политика локального входа — выбор пользователей, которым разрешён вход.



Ярлыки установленных графических приложений (файлы с суффиксом .desktop) находятся в каталоге /usr/share/applications. Настройки рабочего стола для новых пользователей хранятся в каталоге /usr/share/fly-wm:

- подкаталог Меню Пуск — настройки меню «Пуск»;
- подкаталог Рабочие столы — настройки рабочих столов;
- theme/default.themerc — тема оформления (в частности, обои).

Текущие настройки рабочего стола пользователя ~/.fly:

- Меню Пуск — меню «Пуск»;
- theme/current.themerc — текущая тема оформления.

Файлы с рабочих столов пользователей располагаются в каталогах ~/Рабочие столы/Рабочий стол{1..4}

Если требуется немедленно разместить ярлык на рабочих столах всех пользователей, то следует скопировать файл ярлыка из каталога /usr/share/applications в каталог /usr/share/applications/flydesktop.

Ярлыки и папки для немедленного их появления в меню**Пуск** следует помещать в каталог /usr/share/applications/flystartmenu.

Описания папок, которые помещаются в меню **Пуск** или автоматически создаются в домашних каталогах пользователя, размещаются в файлах .directory внутри папок (для просмотра в менеджере файлов, необходимо в менюпараметр Отображать скрытые).