

Дисциплина «Защита в операционных системах»

Лабораторная работа № 7

Тема: Администрирование локальных учётных записей пользователей и групп пользователей, конфигурирование политики безопасности в ОССН Astra Linux Special Edition.

Цель: Изучить возможности ОССН Astra Linux Special Edition при администрировании локальных учётных записей пользователей и групп с использованием командной строки и графического интерфейса, конфигурирование политики безопасности.

Порядок выполнения лабораторной работы: работа выполняется самостоятельно под руководством преподавателя.

Время выполнения лабораторной работы (аудиторные часы) – 4 часа.

Оборудование и программное обеспечение: работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОС Linux.

1. Теоретические сведения

1.1 Работа с пользователями и группами в ОССН Astra Linux Special Edition

Операционная система специального назначения (ОССН) Astra Linux Special Edition – многопользовательская ОС, потому учётная запись пользователя – ключевой элемент всей системы управления доступом. Для идентификации учётных записей пользователей и групп в ОССН как во всех ОС семейства Linux используются UID и GID соответственно.

В ОС семейства UNIX пользователей можно условно разделить на три группы:

- специальные пользователи;
- системные пользователи;
- стандартные пользователи.

. К *специальным пользователям* относятся **root** (суперпользователь) и **nobody** (с группами **root** и **nogroup** соответственно). Пользователь **root** имеет наименьшие **UID** и **GID** - **0** и является обладателем неограниченных прав, он имеет доступ к любому объекту системы и может выполнять любые настройки.

Пользователь **nobody** (никто) - имеет наибольший идентификатор - **65534** и не может являться владельцем ни одного файла в системе, не состоит ни в одной привилегированной группе и не имеет никаких полномочий кроме стандартных. Используется для запуска от его имени процессов с низким уровнем доверия, чтобы ограничить их доступ к системе в случае возможной

компрометации. Фактически к nobody будут всегда применяться права для "остальных" и при стандартных наборах привилегий 644 на файлы и 755 на директории он будет иметь возможность исключительно чтения и просмотра содержимого каталогов. Для чувствительных конфигурационных файлов, ключей и сертификатов используются более ограниченные наборы прав 640 или 600, к таким файлам nobody доступа не имеет.

Следующая условная группа - **системные пользователи**, которые используются для запуска служб и доступа к устройствам, например, www-data для веб-сервера или systemd-network для управления сетью через systemd. Первоначально для них выделялись идентификаторы от 1 до 100, но в связи с большим количеством служб в современных системах этот диапазон расширен до **499** в RHEL и производных от него, и до **999** в системах, основанных на Debian.

Третья условная группа - **стандартные пользователи** - идентификаторы зарезервированы в диапазоне от 1000 до 65533.

Это разделение на три группы достаточно условное и предназначено для повышения удобства администрирования ОС. Например, встретив в незнакомой системе пользователя с UID до 999, администратор большой долей вероятности предположит, что это служба.

Когда пользователь регистрируется в системе (проходит процедуру авторизации, например, вводя системное имя и пароль), он идентифицируется с учётной записью, в которой система хранит информацию о каждом пользователе: его системное имя и некоторые другие сведения, необходимые для работы с ним. Именно с учётными записями, а не с самими пользователями, и работает система. Ниже приведён список этих сведений.

Системное имя (user name)

Это то имя, которое вводит пользователь в ответ на приглашение login:. Оно может содержать только латинские буквы и знак "_". Это имя используется также в качестве имени учётной записи.

Идентификатор пользователя (UID)

Linux связывает системное имя с идентификатором пользователя в системе — UID (User ID). UID — это положительное целое число, по которому система и отслеживает пользователей. Обычно это число выбирается автоматически при регистрации учётной записи, однако оно не может быть совершенно произвольным. В Linux есть некоторые соглашения относительно того, каким типам пользователей могут быть выданы идентификаторы из того или иного диапазона. В частности, UID от "0" до "100" зарезервированы для псевдопользователей.

Идентификатор группы (GID)

Кроме идентификационного номера пользователя с учётной записью связан идентификатор группы. Группы пользователей применяются для организации доступа нескольких пользователей к некоторым ресурсам. У группы, так же, как и у пользователя, есть имя и идентификационный номер — GID (Group ID). В Linux каждый пользователь должен принадлежать как минимум к одной группе — группе по умолчанию. При создании учётной записи

пользователя обычно создаётся и группа, имя которой совпадает с системным именем, именно эта группа будет использоваться как группа по умолчанию для этого пользователя. Пользователь может входить более чем в одну группу, но в учётной записи указывается только номер группы по умолчанию. Группы позволяют регулировать доступ нескольких пользователей к различным ресурсам.

Полное имя (full name)

Помимо системного имени в учётной записи содержится и полное имя (имя и фамилия) использующего данную учётную запись человека. Конечно, пользователь может указать что угодно в качестве своего имени и фамилии. Полное имя необходимо не столько системе, сколько людям — чтобы иметь возможность определить, кому принадлежит учётная запись.

Домашний каталог (home directory)

Файлы всех пользователей в Linux хранятся отдельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен. Информация о домашнем каталоге обязательно должна присутствовать в учётной записи, потому что именно с него начинает работу пользователь, зарегистрировавшийся в системе.

Начальная оболочка (login shell)

Важнейший способ взаимодействовать с системой Linux — командная строка, которая позволяет пользователю вести «диалог» с системой: передавать ей команды и получать её ответы. Для этой цели служит специальная программа — командная оболочка (или интерпретатор командной строки), по-английски — shell. Начальная оболочка (login shell) запускается при входе пользователя в систему в текстовом режиме (например, на виртуальной консоли). Поскольку в Linux доступно несколько разных командных оболочек, в учётной записи указано, какую из командных оболочек нужно запустить для данного пользователя. Если специально не указывать начальную оболочку при создании учётной записи, она будет назначена по умолчанию, вероятнее всего это будет bash.

Каждый пользователь должен принадлежать как минимум к одной группе — первичной группе. При создании учётной записи пользователя командой `adduser` или с использованием графической утилиты `fly-admin-smc` создаётся группа, имя которой совпадает с системным именем учётной записи пользователя. Данная группа применяется как первичная группа и будет задана идентификатором в учётной записи пользователя, расположенной в файле `/etc/passwd`. Учётная запись пользователя может входить более чем в одну группу, тогда имена таких групп (в ОССН данные группы называются вторичными) будут находиться в файле `/etc/group`.

Как правило, файлы, владельцами которых являются учётные записи пользователей, хранятся в соответствующих им домашних каталогах, находящихся в каталоге `/home`. При этом во время первого входа в ОССН с

заданными уровнем доступа (Num1), уровнем целостности (Num2) и набором неиерархических категорий (Num3) создаётся уникальный каталог с именем вида:

```
/home /.pdp / имя_пользователя /Num1:Num2:Num2:0,
```

что позволяет распределить по каталогам файлы (в том числе документы) в зависимости от их уровней конфиденциальности и целостности. Доступ субъект-сессий (процессов), функционирующих от имени других учётных записей пользователей, к домашнему каталогу в ОССН версии 1.5 может быть ограничен с использованием как параметров (меток конфиденциальности) мандатного управления доступом, так и дискреционных прав доступа.

Данные об учётных записях пользователей и группах хранятся в файлах `/etc/passwd` и `/etc/group` соответственно.

Формат `/etc/passwd`

Файл `/etc/passwd` - текстовый файл с одной записью в строке, представляющей учетную запись пользователя. Чтобы просмотреть содержимое файла, используется текстовый редактор или, например, команду `cat` (`less`):

```
adminastra@astra:~$ less /etc/passwd
```

Обычно первая строка описывает пользователя `root`, за которым следуют системные и обычные учетные записи пользователей. Новые записи добавляются в конец файла.

Каждая строка файла `/etc/passwd` содержит семь полей, разделенных двоеточием:

```
mark:x:1001:1001:mark,,,:/home/mark:/bin/bash
[--] - [--] [--] [-----] [-----] [-----]
|   |   |   |   |   |   |
|   |   |   |   |   |   |   +--> 7. Login shell
|   |   |   |   |   |   |   +-----> 6. Home directory
|   |   |   |   |   |   |   +-----> 5. GECOS
|   |   |   |   |   |   |   +-----> 4. GID
|   |   |   |   |   |   |   +-----> 3. UID
|   |   |   |   |   |   |   +-----> 2. Password
|   |   |   |   |   |   |   +-----> 1. Username
```

Username. Строка, которую вы вводите при входе в систему. Каждое имя пользователя должно быть уникальной строкой на компьютере. Максимальная длина имени пользователя ограничена 32 символами.

Password. В старых системах Linux зашифрованный пароль пользователя хранился в файле `/etc/passwd`. В большинстве современных систем это поле имеет значение `x`, и пароль пользователя сохраняется в файле `/etc/shadow` (состав файла `/etc/shadow` будет рассмотрен ниже).

UID. Идентификатор пользователя — это номер, назначенный каждому пользователю. Он используется операционной системой для обращения к пользователю.

GID. Номер идентификатора группы пользователя, относящийся к основной группе пользователя. Когда пользователь создает файл, группа файла устанавливается на эту группу. Как правило, имя группы совпадает с именем пользователя. Пользователя вторичные группы перечислены в файле `/etc/groups`.

GECOS или полное имя пользователя. Это поле содержит список значений через запятую со следующей информацией:

- Полное имя пользователя или название приложения.
- Номер комнаты.
- Рабочий номер телефона.
- Домашний телефон.
- Другая контактная информация.

Home directory. Абсолютный путь к домашнему каталогу пользователя. Он содержит файлы пользователя и конфигурации. По умолчанию домашние каталоги пользователей именуются по имени пользователя и создаются в каталоге `/home`.

Login shell. Абсолютный путь к оболочке входа пользователя. Это оболочка, которая запускается, когда пользователь входит в систему. В большинстве дистрибутивов Linux оболочкой входа по умолчанию является Bash.

Все учетные записи в Linux — или, по крайней мере те, что соответствуют реальным пользователям — защищены паролями. Когда пользователь задает пароль, криптографическая свертка пароля (хэш) записывается в строку учетной записи пользователя в файле `/etc/shadow`. Входя в систему, пользователь вводит пароль, который снова хэшируется, и свертка сравнивается со сверткой в файле `shadow`. В открытом виде пароли не хранятся нигде.

Формат `/etc/shadow`

Файл `/etc/shadow` - текстовый файл с одной записью в строке, представляющей криптографическую свертку пароля (хэш) учетной записи пользователя. Чтобы просмотреть содержимое файла, используйте текстовый редактор или, например, команду `cat (less)`:

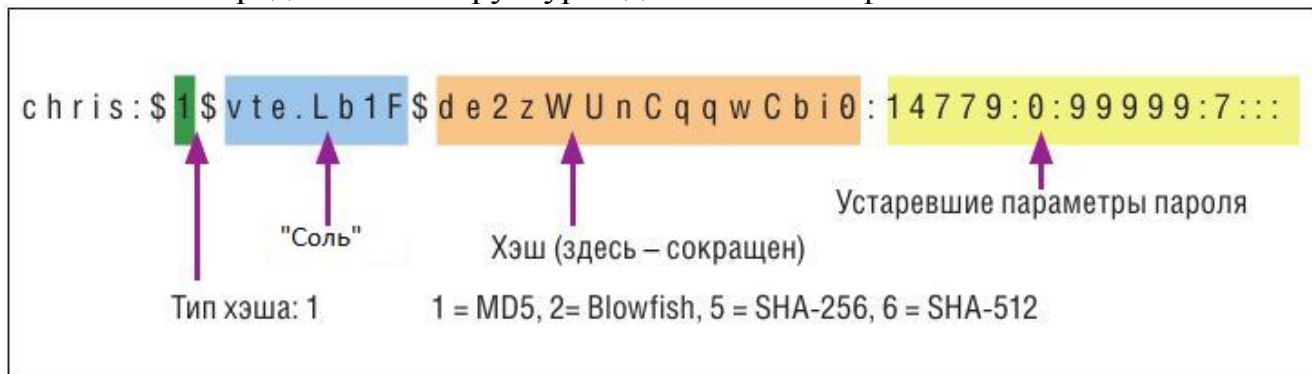
```
root@astra:~# cat /etc/shadow
```

Входя в систему, пользователь вводит пароль, который снова хэшируется, и свертка сравнивается со сверткой в файле `shadow`. В открытом виде пароли **НЕ ХРАНЯТСЯ**.

При хешировании паролей в ОСН используется [криптографические алгоритмы с «солью»](#).

В ОС Linux использовались различные алгоритмы хэширования. Самый ранний был основан на алгоритме DES и использовал только пароли из восьми символов – по семь бит от каждого символа образовывали 56-битный ключ DES. В дальнейших версиях была добавлена поддержка хэширования на основе алгоритма MD5 и поддержка сверток SHA-256 и SHA-512. Они поддерживают более длинные пароли и используют более длинные свертки.

Ниже представлена структура одной записи в файле shadow:



Хэширование по определенному алгоритму выполняется процедурой *crypt library*.

Для администрирования параметров учётных записей пользователей используются следующие команды и утилиты:

user add и adduser – команды добавления учётной записи пользователя;

passwd – команда смены пароля учётной записи пользователя;

usermod – команда модификации параметров уже существующей учётной записи;

userdel – команда удаления учётной записи пользователя;

groupadd – команда управления группами;

addgroup – команда создания группы;

delgroup – команда удаления группы;

fly-admin-smc – графическая утилита, позволяющая решать комплекс задач по администрированию учётных записей пользователей и групп, в том числе администрировать параметры мандатного управления доступом и мандатного контроля целостности.

Управление пользователями с использованием графической оболочки «Политика безопасности»

Доступ к графической оболочке ОСН «Политика безопасности» можно получить через терминал Fly, введя команду fly-admin-smc с правами суперпользователя или перейдя по следующему пути: **Пуск → Панель управления → Безопасность → Политика безопасности → компонент «Пользователи»** (см. рисунок 1).

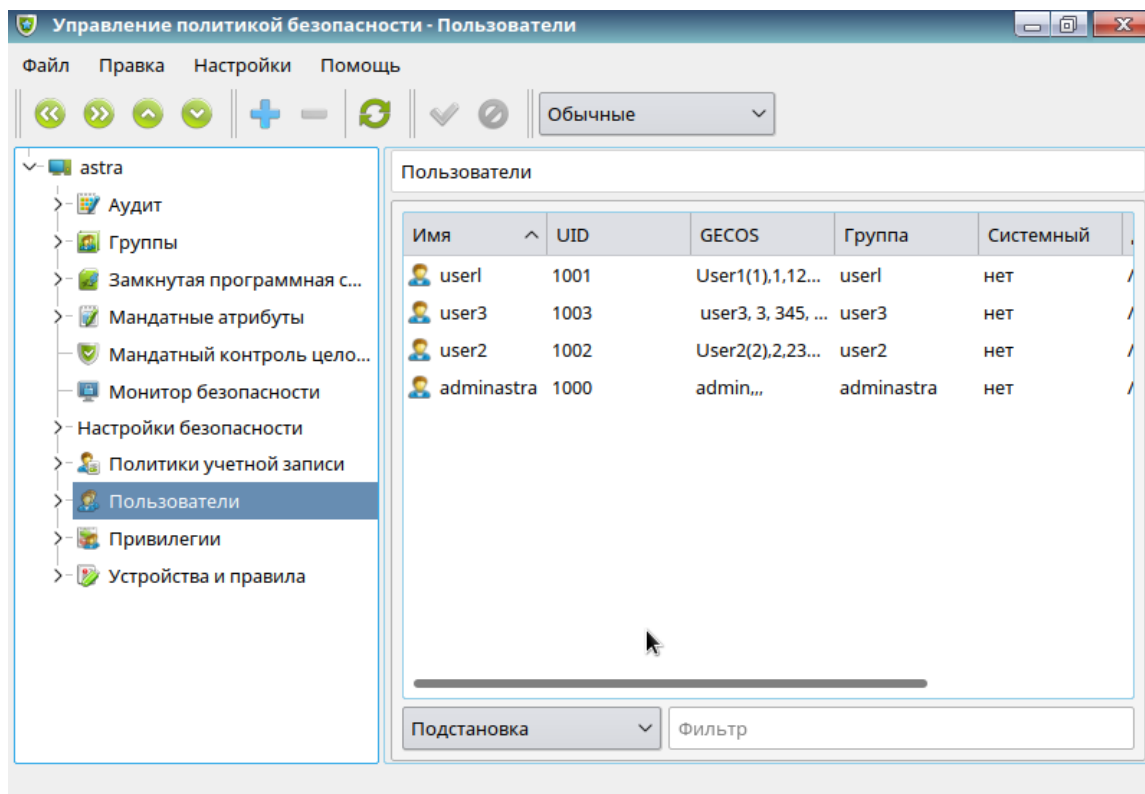



Рисунок 1 – Редактирование пользователей с использованием графической оболочки ОССН «Политика безопасности»

Для добавления нового пользователя в дерево консоли (слева) выберите компонент «Пользователи».

Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду «Создать». Появится новое окно создания пользователя (см. рисунок 2). В появившемся окне необходимо ввести имя нового пользователя, выбрать первичную группу пользователя (для выбора снять выделитель «новая» напротив соответствующего окна), выбрать домашний каталог или использовать уже существующий, отредактировать дополнительную информацию о пользователе и нажать кнопку  в верхней части окна.

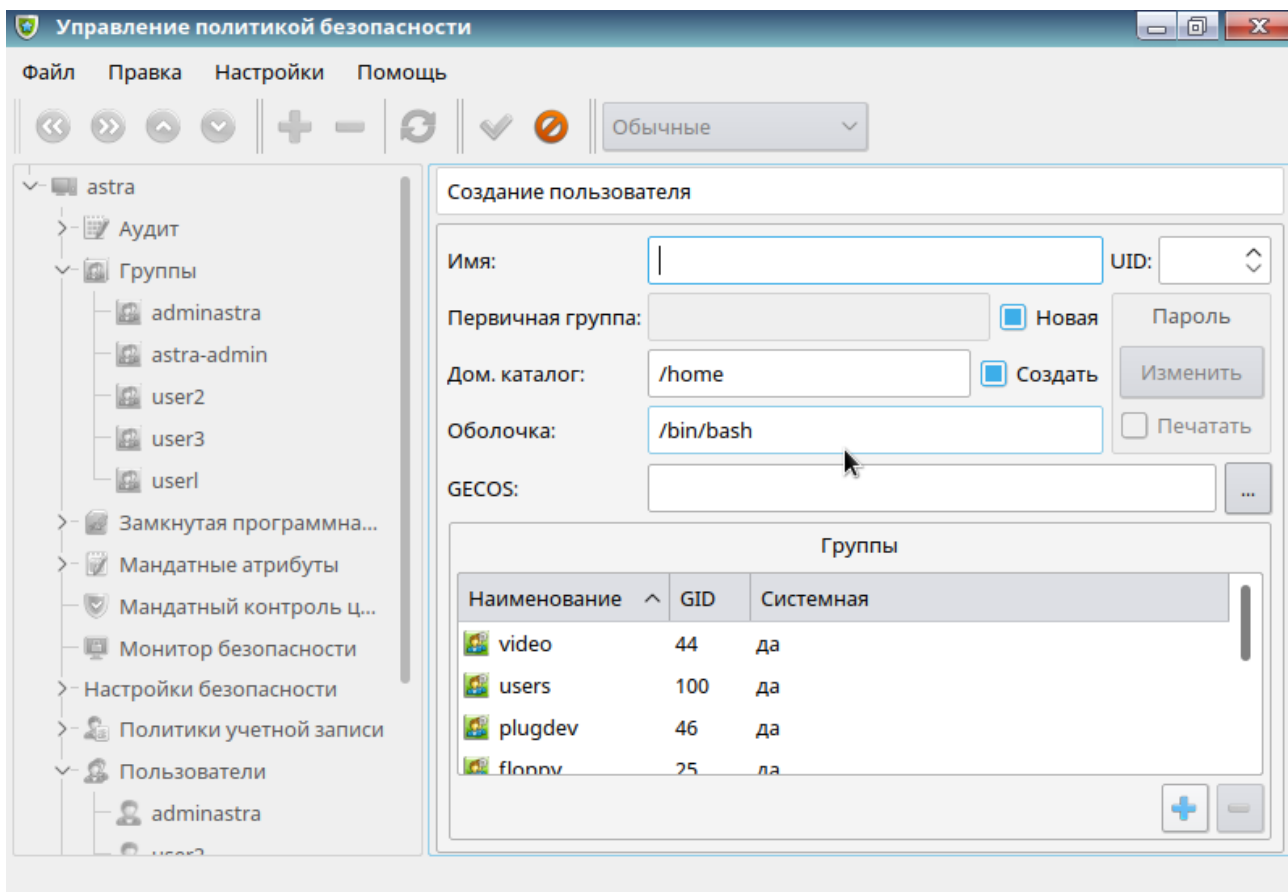


Рисунок 2 – Окно создания нового пользователя

После добавления нового пользователя кнопка можно добавить пароль пользователя (кнопка «Изменить» поля «Пароль»).

Управление группами с использованием графической оболочки «Политика безопасности»

На рабочей панели в табличном виде отображается список групп пользователей, для получения доступа к которому необходимо выбрать компонент «Группы» утилиты «Политика безопасности» (см. рисунок 3).

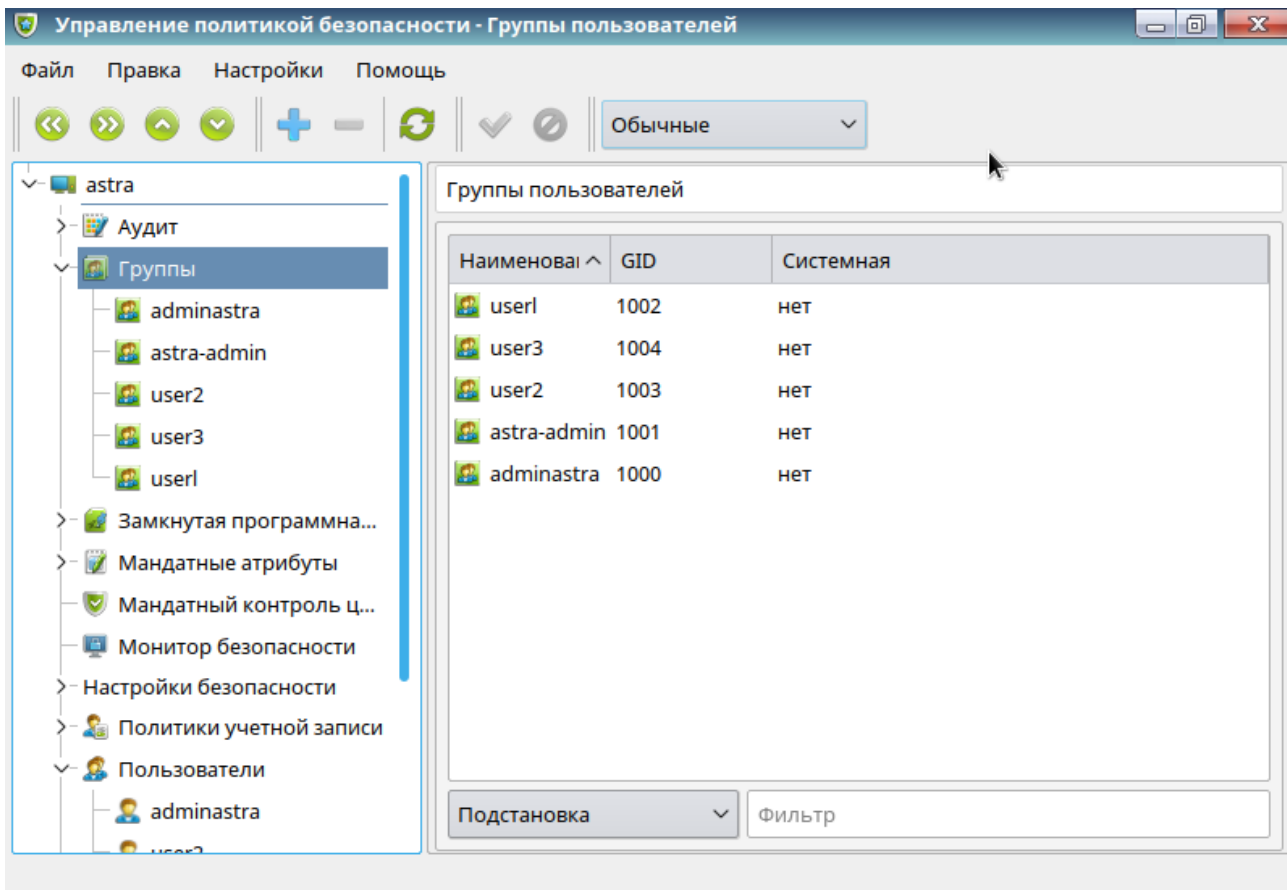


Рисунок 3 – Редактирование групп пользователей

Столбцы: «Наименование» (со значком порядка сортировки справа) - имя группы; «Gid» - идентификационный номер группы; «Системная» - отметка для системных групп.

Двойным щелчком левой кнопки мыши на названии группы в таблице открывается раздел этой группы в дереве навигации, а на рабочей панели появляются вкладки:

1) вкладка «Общие» (см. рисунок 4):

- «Имя» - отображается имя члена группы;
- «UID» - отображается идентификационный номер члена группы;
- «GECOS» - отображается информация из учетной записи члена группы;
- «Группа» - отображается имя группы
- «Системный» - отметка для членов системных групп;
- кнопки управления списком (внизу):

- [Добавить] — открывается окно со списком пользователей. Элемент списка выделяется щелчком левой кнопки мыши на нем. [Да] - окно закрывается, и имя выделенного пользователя отображается в поле «Пользователи», [Отмена] - окно закрывается;

- [Удалить из группы] - выделенный в поле «Имя» элемент удаляется;

2) вкладка «Аудит» - настройки аудита группы (см. рисунок 5):

- «Настройка аудита по умолчанию» — флаг включения аудита по умолчанию;

- «Аудит успехов» и «Аудит отказов» — список флагов включения регистрации событий в журнале операций, в случае их, соответственно,

успешного и неуспешного выполнения членом группы. Флаг переключается щелчком левой кнопки мыши на нем.

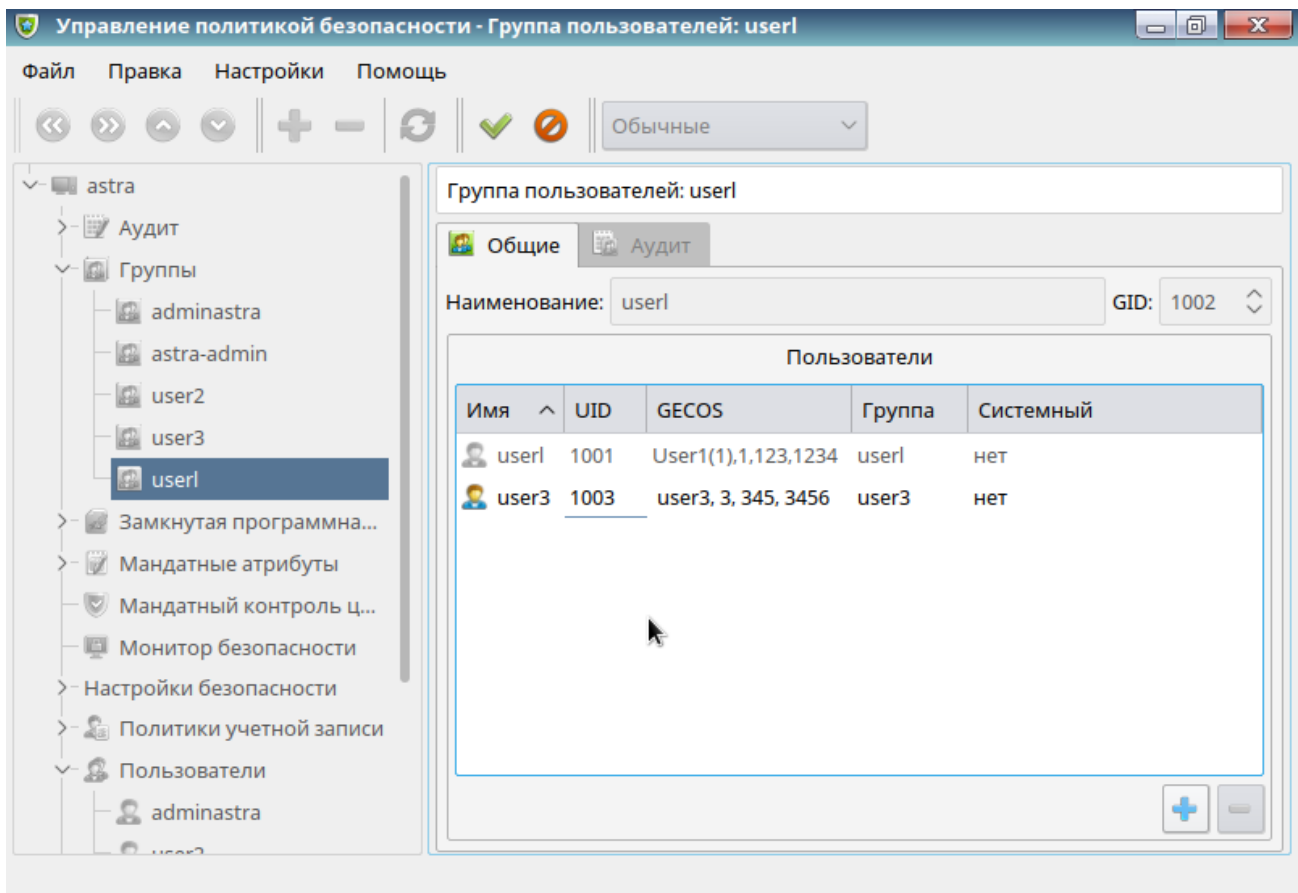


Рисунок 4 – Вкладка «Общие» в окне редактирования групп пользователей

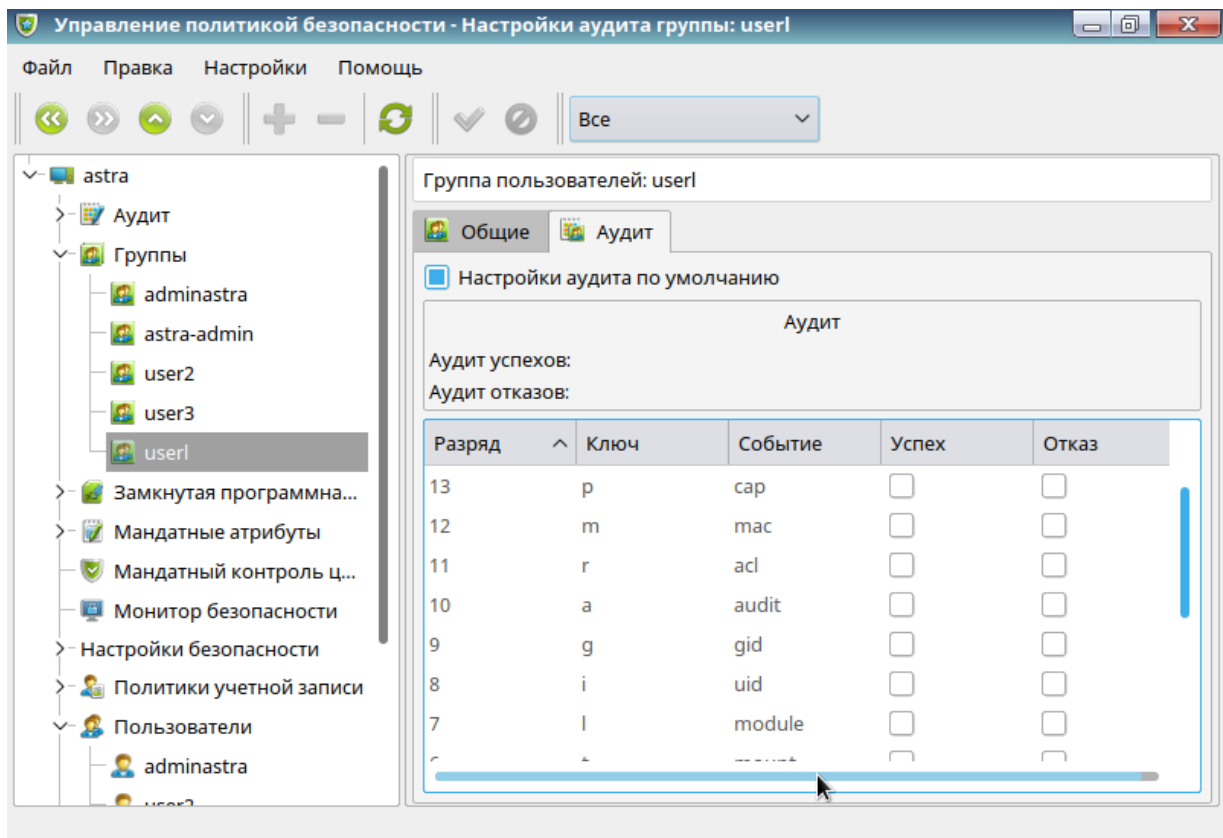


Рисунок 5 - Вкладка «Аудит» в окне редактирования групп пользователей

1.2 Аудит событий в ОССН Astra Linux Special Edition

Для аудита ОС могут использоваться системные лог-файлы различных служб и программ. Основное расположение этих файлов — системный каталог `/var/log`.

Аудит событий постановки/снятия с контроля целостности исполняемых модулей и файлов данных, а также событий неудачного запуска неподписанных файлов осуществляется в системном журнале `/var/log/kern.log` и `fly-admin-viewaudit`.

Аудит событий создания/удаления/изменения настроек учетных записей пользователей и начала/окончания сеансов работы учетных записей пользователей осуществляется в системном журнале `/var/log/auth.log`.

Аудит событий изменения полномочий для учетных записей по доступу к информации осуществляется в системном журнале `/var/log/auth.log` и `fly-admin-viewaudit`.

Аудит событий смены аутентифицирующей информации учетных записей осуществляется в системном журнале `/var/log/auth.log`.

Аудит событий выдачи печатных (графических) документов на бумажный носитель осуществляется в системных журналах `/var/log/cups/page_log` и `/var/spool/cups/parsec`.

Аудит отслеживания удаления журналов аудита parsec отображается первой записью в том же файле журнала `fly-admin-viewaudit`.

Настройка событий, подлежащих аудиту, осуществляется с помощью графической оболочки ОССН «Политика безопасности», запустить которую можно через терминал Fly, введя команду `fly-admin-smc` с правами суперпользователя или перейдя по следующему пути: **Пуск** → **Панель управления** → **Безопасность** → **Политика безопасности** → компонент **«Пользователи»** (см. рисунок 10).

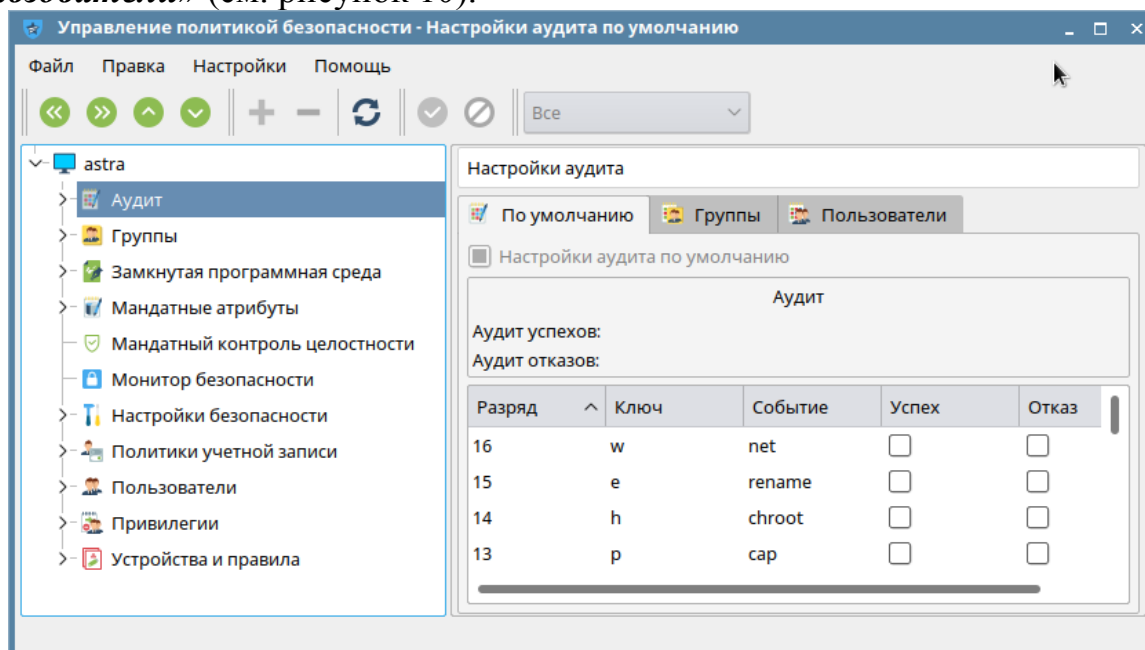


Рисунок 10 – Компонент «Аудит» безопасности ОССН

Неудачный вход в систему

Команда faillog показывает содержимое журнала неудачных попыток (файл /var/log/faillog) входа в систему. Также она может быть использована для управления счетчиком неудачных попыток и их ограничением. При запуске faillog без параметров выводятся записи faillog только тех пользователей, у которых имеется хотя бы одна неудачная попытка входа.

Предельное число попыток входа для каждой учетной записи равно 10. Для сброса неудачных попыток входа необходимо пользоваться параметром -г.

Описание команды, а также файла /var/log/faillog приведено в man faillog и man 5 faillog.

1.3 Политика безопасности в ОССН Astra Linux Special Edition

Безопасность операционной системы основана на правилах, регулирующих разные аспекты ее работы. Вместе эти правила составляют единую политику безопасности.

Настройки политики безопасности по своему функциональному и смысловому значению объединяются в группы и структурно организуются в дереве настроек политики безопасности, которая отображается на боковой панели навигации (см. рис. 6): «Аудит», «Группы», «Мандатные атрибуты», «Замкнутая программная среда», «Мандатные атрибуты», «Мандатный контроль целостности», «Монитор безопасности», «Настройки безопасности», «Политики учетной записи», «Пользователи», «Привилегии» и «Устройства и правила».

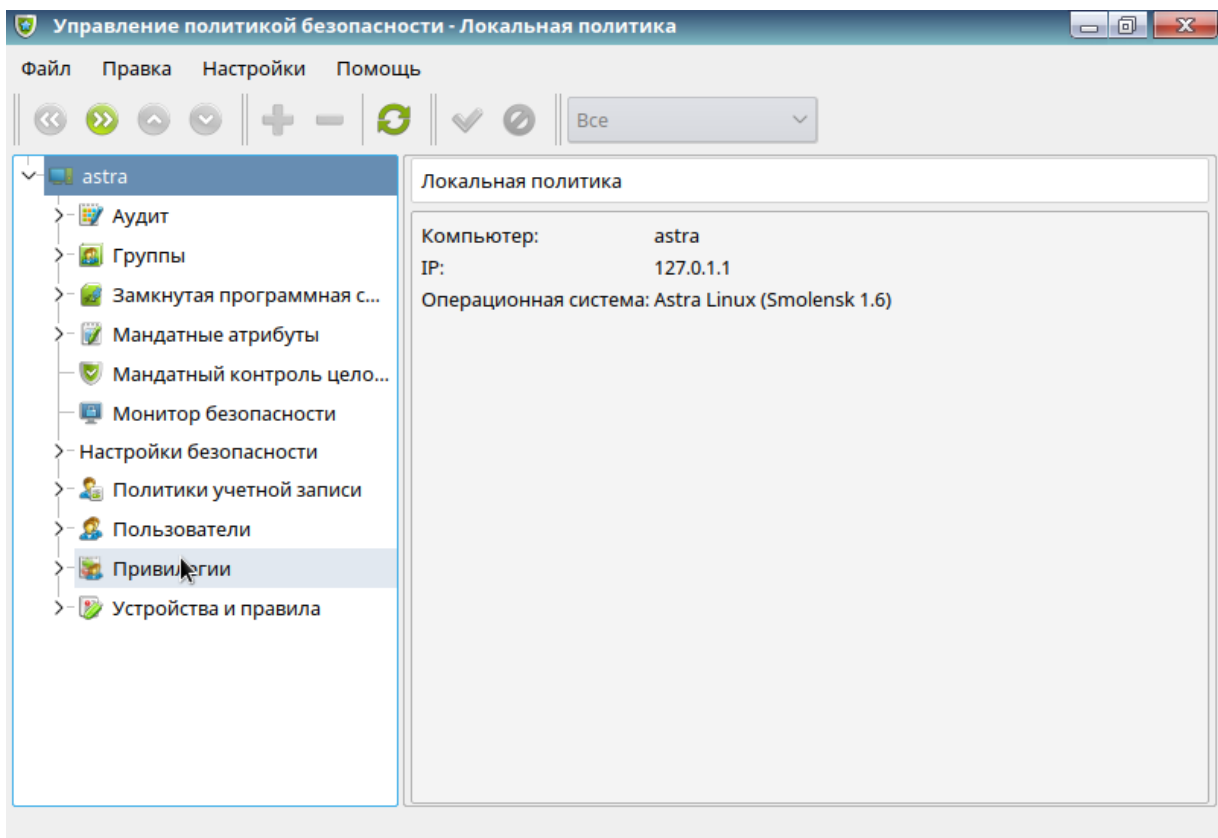


Рисунок 6 – Окно настроек политики безопасности ОССН

Терминальная вершина дерева настроек политики безопасности называется разделом, а нетерминальная вершина - сводом разделов. Раздел или свод разделов выделяется щелчком левой кнопки мыши на нем. После выделения справа появляется соответствующая форма рабочей панели с элементами для настройки соответствующих параметров политики безопасности. При наведении курсора на элемент управления появляется подсказка.

Значения параметров устанавливаются в режиме администратора.

Далее рассматриваются порядок администрирования группы политики безопасности - «Политики учетной записи».

Группа настроек включает:

раздел «Блокировка» (рис. 7) - политика блокировки учетной записи: настройки `pam_tally`.

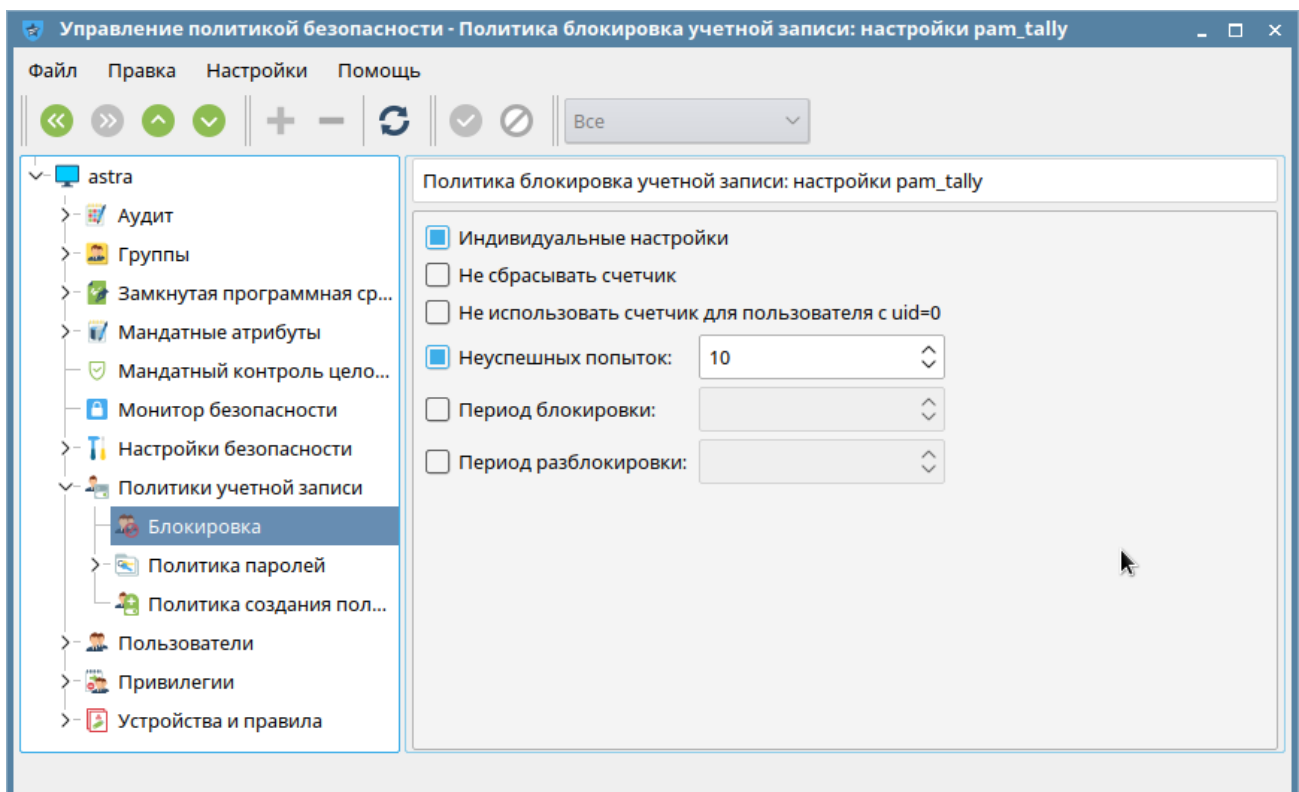


Рисунок 7 – Раздел «Блокировка» группы «Политики учетной записи»

Рабочая панель содержит элементы настройки:

- флаг «Индивидуальные настройки» - разрешает использование индивидуальных настроек;
- флаг «Не сбрасывать счетчик» - отменяет сброс счетчика;
- флаг «Не использовать счетчик для пользователя с uid=0» - отменяет счетчик для суперпользователя;
- «Неуспешных попыток» - в числовом поле устанавливается максимально допустимое количество некорректных попыток входа пользователя в систему (неудачных попыток ввода пароля) до автоматической блокировки учетной записи;
- «Период блокировки (секунды)» - в числовом поле устанавливается продолжительность (в сек.) запрета на повторный вход в систему после неуспешного входа;

- «Период разблокировки (секунды)» - в числовом поле устанавливается период времени (в сек.) по истечению которого отменяется автоматическая блокировка, установленная после достижения максимального количества неудачных попыток входа.

Свод разделов «**Политики паролей**» (рис. 8) содержит:

- **раздел «Сложность»** - вкладка «Сложность» рабочей панели содержит элементы настройки:

- флаг «Проверка имени пользователя» - включает проверку имени пользователя;
- флаг «Проверка GECOS» - включает проверку информации из учетной записи пользователя;
- флаг «Применять для пользователя root» - включает применение для суперпользователя;
- «Минимальное длина пароля» - в числовом поле устанавливается минимальная длина пароля;
- флаг «Минимальное количество строчных букв в новом пароле» - активирует числовое поля для установки минимального количества строчных букв в новом пароле;
- флаг «Минимальное количество заглавных букв в новом пароле» - активирует числовое поля для установки минимального количества заглавных букв в новом пароле;
- флаг «Минимальное количество цифр в новом пароле» - активирует числовое поля для установки минимального количества цифр в новом пароле;
- флаг «Минимальное количество других символов в новом пароле» - активирует числовое поля для установки минимального количества других символов в новом пароле;

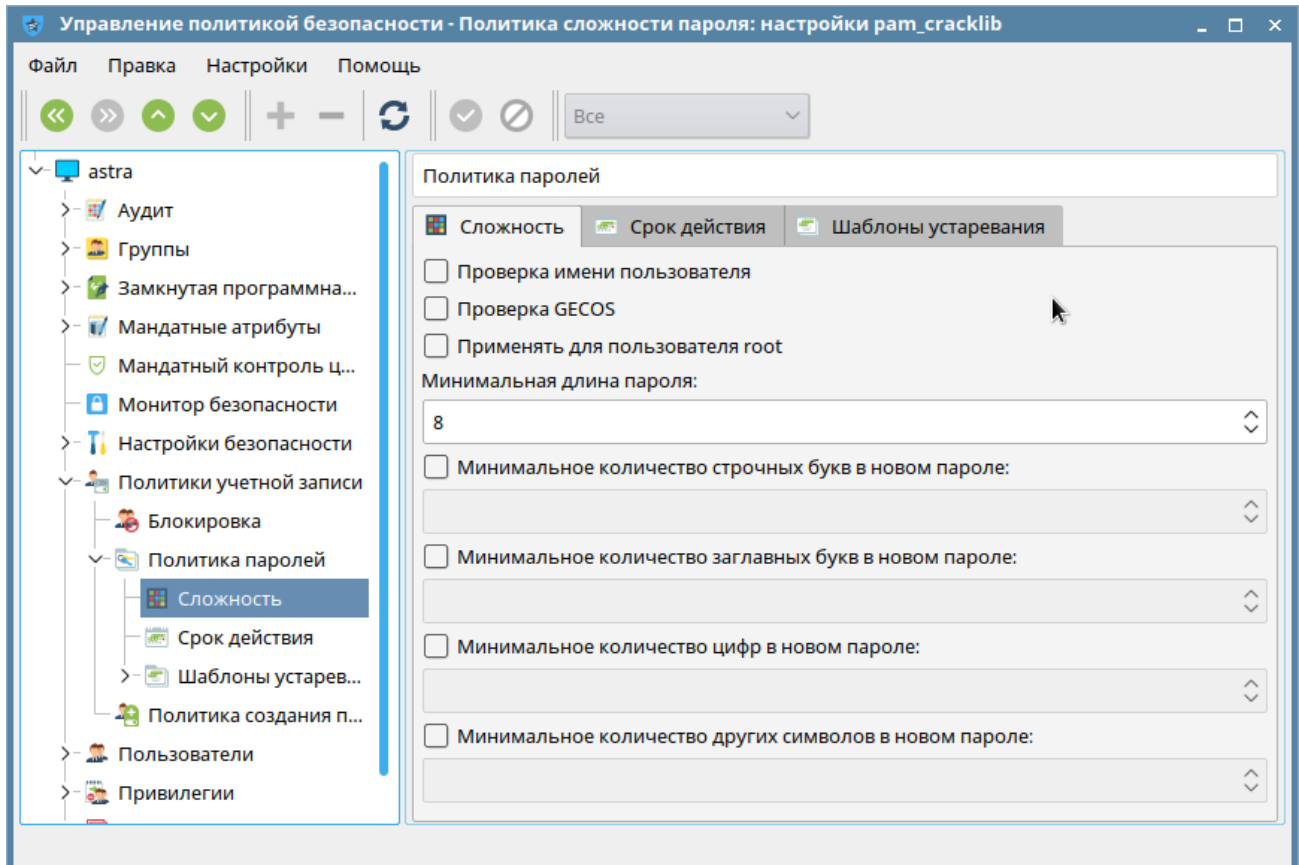



Рисунок 8 – Окно настройки сложности пароля

- раздел «Срок действия» (см. рис. 9) - вкладка «Срок действия» рабочей панели содержит элементы настройки:

- флаг «Минимальное количество дней между сменами пароля» - активирует числовое поля для установки минимального количества дней для смены пароля;
- флаг «Максимальное количество дней между сменами пароля» - активирует числовое поля для установки максимального количества дней для смены пароля;
- флаг «Число дней выдачи предупреждения до смены пароля» - активирует числовое поля для установки количества дней для выдачи предупреждения до смены пароля;
- флаг «Число дней неактивности после устаревания пароля до блокировки учетной записи» - активирует числовое поля для установки числа дней неактивности поле устаревания пароля до блокировки учетной записи;
- флаг «Срок действия учетной записи» - активирует числовое поля для установки срока действия учетной записи;
- [ - Импорт из шаблона] - открывается окно для установки шаблона политики пароля и последующего импорта параметров из установленного шаблона;

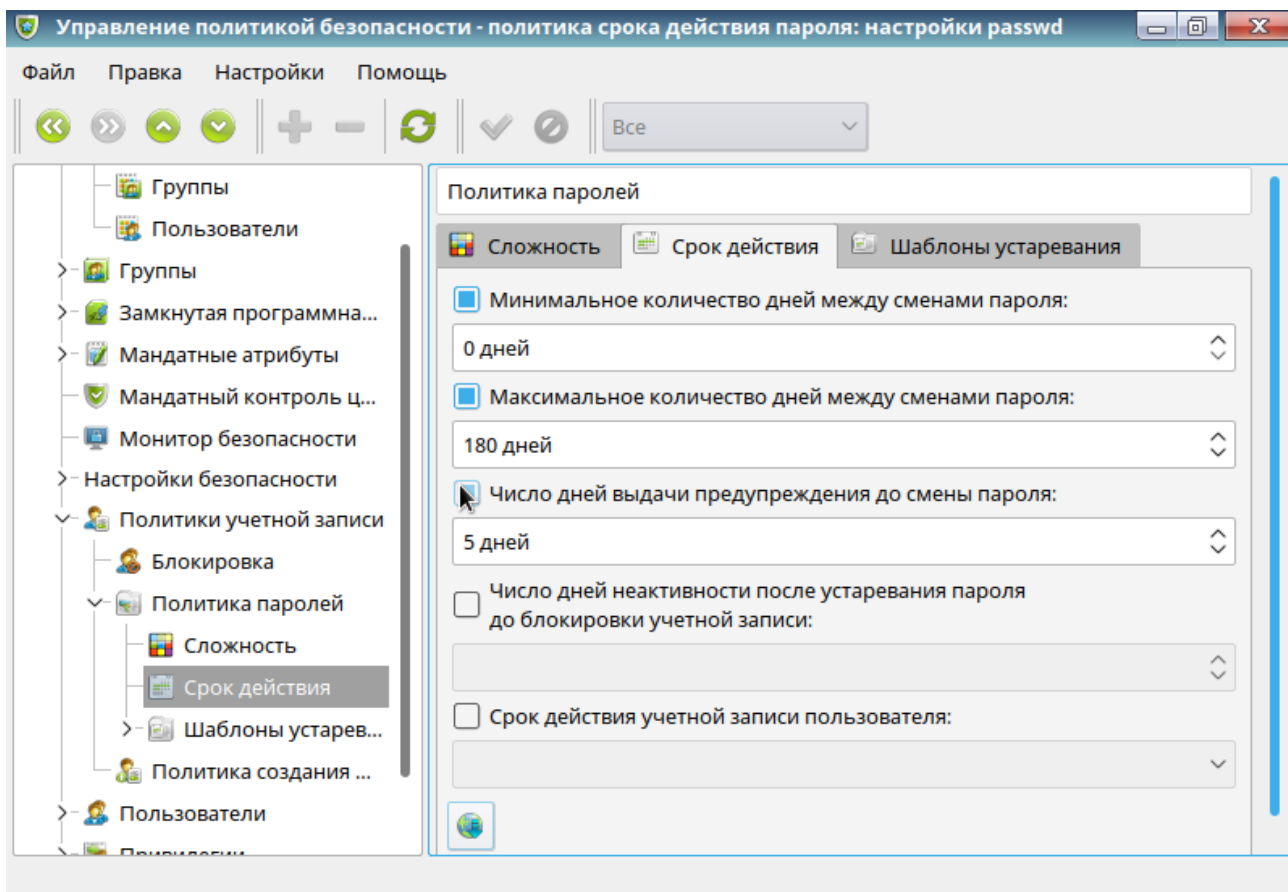


Рисунок 9 – Окно настройки политики срока действия пароля

- свод разделов «Шаблоны устаревания» - в табличном виде отображается список установленных шаблонов политики пароля. Двойным щелчком левой кнопки мыши на названии шаблона в таблице открываются разделы с шаблонами в дереве навигации, а на рабочей панели отображается соответствующая выделенному шаблону вкладка с информацией о значениях настроек.

2 Задание

Работа с пользователями и группами в ОССН Astra Linux Special Edition

В ходе выполнения заданий лабораторной работы результаты выполнения команд должны быть отражены в отчете в виде скриншотов экрана с пояснениями.

1. Авторизоваться в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).
2. Запустить терминал Fly.
3. Определить текущую учётную запись пользователя с использованием команды whoami.

4. Проверить наличие права доступа на чтение к файлу `/etc/passwd` и получить следующие данные, выполнив команды `cat /etc/passwd` или `less /etc/passwd`:

- количество параметров учётных записей пользователей;
- количество параметров, совпадающих у всех учётных записей пользователей;
- текущее число учётных записей пользователей;
- количество различных используемых командных интерпретаторов.

5. Вывести строку, соответствующую текущей учётной записи пользователя, из файла `/etc/passwd` с использованием команды `cat /etc/passwd | grep "^$(whoami)"`, при этом получить следующие данные:

- наличие пароля или свёртки пароля (вывести эти данные командой)
`cat /etc/passwd | grep "^$(whoami)" | cut -d : -f 2`
- группа и идентификатор текущей учётной записи пользователя;
- командный интерпретатор по умолчанию для текущей учётной записи пользователя.

6. Настроить политику безопасности в соответствии со следующими требованиями:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия (срок действия пароля не более 90 суток), длиной не менее 6 буквенно-цифровых символов;
- вновь создаваемый пароль субъектов доступа должен удовлетворять требованиям уникальности, т.е. отличаться не менее чем на 5 символов;
- субъект доступа должен быть предупрежден о необходимости смены пароля не менее чем за 7 дней;
- после 4 неудачных попыток аутентификации учетная запись субъекта доступа должны быть заблокирована на срок не менее 35 минут (настройки применимы для всех субъекта доступа).

7. Создать учётную запись пользователя `user1` (с соответствующим домашним каталогом) с использованием графического интерфейса, установить пароль, соответствующий требованиям политики информационной безопасности. С помощью системного журнала `/var/log/auth.log` определить все записи, касающиеся рассматриваемого события.

8. Добавить учётную запись пользователя `user2` с использованием команды `adduser user2`, без использования команды `sudo`, проанализировать и объяснить результат. Выполнить те же действия с применением команды `sudo`. Установить учётной записи пользователя `user2` пароль, соответствующий требованиям политики информационной безопасности. С помощью системного журнала `/var/log/auth.log` определить все записи, касающиеся рассматриваемого события.

9. Проанализировать изменения в ОССН, связанные с добавлением новых учётных записей пользователей, для чего определить:

- домашние каталоги учётных записей пользователей по данным файла `/etc/passwd`;
- содержимое файла `/etc/shadow`;
- алгоритм хеширования пароля, используемый в ОССН;
- скрипты, которые были перемещены в домашние каталоги учётных записей пользователей из каталога `/etc/skel`, при этом сравнить файлы в каталоге `/etc/skel` с файлами домашних каталогов учётных записей пользователей с использованием команды `sudo diff -s /etc/skel /home/user | grep "идентичны"`;
- новые группы в файле `/etc/group`;
- идентификаторы новых учётных записей пользователей и групп в файлах `/etc/group` и `/etc/passwd`.

10. Создать учётные записи пользователей `user3`, `user4` любым возможным способом (с помощью графического интерфейса или команды `adduser`).

11. Задать пароли для учётных записей пользователей `user3` и `user4`, соответствующие требованию политики безопасности, с использованием команд `passwd user3` без использования команды `sudo`, проанализировать и объяснить результат. Выполнить те же действия с применением команды `sudo`, после чего определить:

- домашние каталоги учётных записей пользователей по файлу `/etc/passwd`;
- наличие свёрток паролей учётных записей пользователей по файлам `/etc/passwd` и `/etc/shadow`;
- новые группы в файле `/etc/group`
- идентификаторы новых учётных записей пользователей в файле `/etc/passwd`;
- командный интерпретатор по умолчанию для созданных учётных записей пользователей, используя команду:
`tail -1 /etc/passwd|cut -d: -f7`
- определить алгоритм свёртки пароля этих учётных записей пользователей по файлу `/etc/shadow`.

С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

12. С использованием графической утилиты «Политика безопасности» заблокировать пароль учётной записи пользователя `user1`. Проверить изменения файлов `/etc/passwd` и `/etc/shadow`, осуществив следующие действия:

- в терминале Fly выполнить команды `sudo cat /etc/passwd` и `sudo cat /etc/shadow`;
- проверить наличие блокировки учётной записи пользователя по файлу `/etc/shadow` (должен быть установлен знак «!» в начале свёртки пароля);
- проверить функционирование блокировки путём осуществления попытки входа в ОССН в отдельном сеансе от имени учётной записи пользователя `user1`;

- снять блокировку (выполнить удаление пароля и блокировки входа, задать повторно пароль) и проверить возможность входа в ОССН с учётной записью пользователя `user1`.

С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

13. Выполнить удаление учётных записей пользователей:

- удалить учётную запись пользователя `user1` с использованием графической утилиты «Политика безопасности»;

- удалить учётную запись пользователя `user2` командой `sudo deluser user2`;

- проверить наличие домашних каталогов учётных записей пользователей `user1` и `user2`, после чего с использованием справочной информации по команде `userdel` определить её параметры, позволяющие удалять содержимое домашнего каталога учётной записи пользователя;

- удалить домашние каталоги учётных записей пользователей `user1` и `user2` непосредственно командами `rm -r /home/userone` и `rm -r /home/usertwo`, осуществив попытки удаления без использования и с использованием команды `sudo`;

- проверить наличие домашних каталогов учётных записей пользователей `user1`, `user2` в каталоге `/home/.pdp`.

С помощью соответствующего системного журнала аудита определить все записи, касающиеся рассматриваемого события.

14. Создать новую группу `group3` (с использованием графической утилиты «Политика безопасности») и группу `group4` (командой `sudo addgroup group4`, выполненной в терминале `Fly`).

15. Добавить учётную запись пользователя `user3` во вторичную группу `group3` командой `usermod -a -G group3 user3` и во вторичную группу `group4` с помощью графической утилиты «Политика безопасности». Проверить включение учётной записи пользователя `user3` в группы `group3` и `group4` путем просмотра содержимого файла `/etc/group` командами `cat /etc/group | grep "^group3"` и `cat /etc/group | grep "^group4"`.

16. Выполнить удаление учётной записи пользователя `user3` из группы `group3` с использованием графической утилиты «Политика безопасности» и из группы `group4` командой `gpasswd -d user3 group4`.

17. Удалить группу `group3` командой `sudo delgroup group3` в терминале `Fly` и группу `group4` с помощью графической утилиты «Политика безопасности».

3. Контрольные вопросы

1. Что такое идентификационные номера пользователей и групп в ОССН Astra Linux?

2. Какие файлы ОССН Astra Linux содержат информацию о пользователях и группах системы?
3. Какие поля содержит каждая строка файла `/etc/passwd`, кратко охарактеризуйте их?
4. В каком файле ОССН Astra Linux хранятся пароли, в каком виде они представлены?
5. Формат записи в файле `/etc/shadow`, что означает каждое поле?
6. Назовите команды и утилиты, используемые для администрирования параметров учётных записей пользователей.
7. Как осуществляется аудит событий в ОССН Astra Linux? Как настроить перечень событий, подлежащих аудиту?
8. Какие настройки содержит раздел «Блокировка» в политиках учётной записи?
9. Опишите требования, предъявляемые к паролю. Как реализовано конфигурирование этих требований в ОССН Astra Linux?

4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате `.doc` и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (образец титульного листа представлен в приложении 1).

Отчет должен содержать:

- титульный лист;
- цель работы;
- краткие теоретические сведения, ответы на контрольные вопросы;
- описание хода выполнения работы со скриншотами;
- выводы.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

Лабораторная работа № _____
на тему «_____»

Выполнил обучающийся гр. _____

(Фамилия, Имя, Отчество)

Проверил:

(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону

20__