1. Дискреционное управление доступом

В Astra Linux предусмотрено три режима работы — базовый («Орёл»), усиленный («Воронеж») и максимальный («Смоленск»). Они отличаются наличием средств защиты информации. Дискреционное управление доступом доступно уже в базовом режиме работы.

Функции подсистемы безопасности и их состояния определяются следующим образом:

- значения «по умолчанию» задаются при выборе режима работы в процессе установки ОС;
- значения «по умолчанию», определенные режимом работы, могут быть изменены в процессе установки ОС;
- функции подсистемы безопасности могут быть включены и выключены в процессе эксплуатации ОС.

При изменении уровня защищенности (режимов работы ОС):

- в сторону снижения уровня защищенности — автоматически отключаются функции безопасности, которые для данного уровня защищенности недоступны;
- в сторону увеличения уровня защищенности — состояние функций безопасности автоматически не меняется. Функции безопасности становятся доступными для включения.

Режим работы ОС указывается в файле /etc/astra_license:

```
MODE=2
DESCRIPTION=maximum(smolensk)
URL=https://astralinux.ru/information/licenses
```

где 0 — базовый, 1 — усиленный, 2 — максимальный.

Дискреционное управление доступом подразумевает разграничение доступа на основе списков управления или матрицы доступа. Параметры доступа указываются в индексном

дескрипторе файла (inode), в котором содержатся:

- идентификатор пользователя (UID);
- идентификатор группы (GID);
- права доступа к файлу, под которые выделено 12 бит.

Права доступа к файлам могут назначаться для трёх классов пользователей:

☐. Владелец файла — пользователь, чей UID указан в inode файла. По умолчанию — пользователь, создавший файл.
☐. Группа-владелец файла — это пользователи, входящие в группу, чей GID указан в inode файла.
☐. Все остальные пользователи – это пользователи, у которых UID не совпадает с UID из inode и которые не входят в группу-владелец файла.

2. Права доступа

Для каждого класса пользователей в отношении файлов и каталогов могут быть назначены 3 права доступа (3 стандартных бита защиты):

- read (r);
- write (w);
- eXecute (x).

Для файлов стандартные биты защиты трактуются следующим образом:

- r — право на чтение данных в файле;
- w — право на изменение данных в файле;
- x — право на выполнение файла (программы).

Для каталогов стандартные биты защиты трактуются следующим образом:

- r — право просмотра содержимого каталога;
- w — возможность создания или удаления файлов в данном каталоге;
- x — право доступа к каталогу (т.н. право поиска).

Если право x на каталог не установлено, то блокируется доступ ко всему, что находится в этом каталоге и ниже.

Часто права доступа к файлу записываются в следующем виде:

Первый символ строки обозначает тип файла:

- дефис — обычный файл;
- буква d — каталог (directory);
- буква l — ссылка, ярлык (link).

Далее права указываются в трёх триплетах — для пользователя-владельца файла, для группы-владельца, и для остальных пользователей.

В примере выше всем пользователям предоставлен полный доступ к файлу (чтение, запись и исполнение). Если бы потребовалось разрешить владельцу файла полный доступ, а остальным только чтение, то права доступа имели бы следующий вид:

```
-rwxr--r--
```

То есть, символ дефиса указывает на отсутствие того или иного права.

Кроме стандартных 9-ти битов защиты в inode также хранятся три дополнительных бита защиты:

- SetUID (suid) — если установлен этот бит, то запускаемый процесс будет работать от имени владельца файла-программы, а не от имени владельца сеанса (процесса, который порождает данный новый процесс). Установка этого бита на каталог не имеет смысла;
- SetGID (sgid) — если установлен sgid, то процесс, запускаемый программой, получает привилегии группы-владельца программы. Создаваемые файлы в каталоге с этим битом будут наследовать группу этой папки, а вложенные папки, в том числе, и этот бит;
- Sticky-бит —устанавливается на каталоги с правами rwxrwxrwx, в таких каталогах любой пользователь может создать файл, но удалить файл может только владелец (если не установлен sticky-бит, то любой пользователь может удалить любой файл). Установка этого бита на файлы не имеет смысла.

Дополнительные биты защиты sgid и suid указываются как буква s в правах доступа. Sticky-бит обозначается как буква t. Эти буквы стоят на месте буквы x. При этом, если установлены одновременно права на исполнение и дополнительные биты защиты, буквы s или t становятся прописными.

Например, если на файл установлен suid, sgid, а также право на исполнение для группы, то права доступа будут иметь следующий вид:

```
-rwsrwSr--
```

Каталог, имеющий Sticky-бит, а также право доступа, записи и чтения для всех пользователей, выглядит следующим образом:

```
drwxrwxrwT
```

Рассмотренная выше форма записи прав доступа называется символьной. Она позволяет быстро понять, какие права установлены на файл или каталог. Но, также существует и другая форма записи — абсолютная (числовая). Она короче, чем символьная, но сложнее для восприятия человеком.

В абсолютной нотации права доступа к файлам представлены четырёхзначными числами:

- самая левая цифра соответствует специальным битам защитам (suid, sgid, sticky bit);
- следующие три цифры обозначают права (rwx) для владельца, группы и всех остальных, соответственно.

Каждая цифра в абсолютной нотации является суммой двоичного представления битов:

- suid, r = 4;
- sgid, w = 2;
- sticky bit, x = 1;
- отсутствие права = 0.

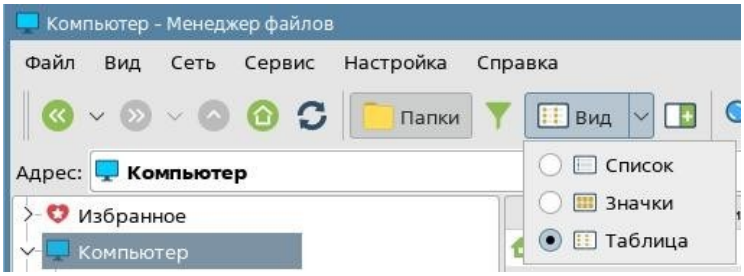
Пример преобразования символьной записи прав доступа к абсолютной приведён в таблице ниже.

Доп. бит			Владелец			Группа			Остальные		
suid	sgid	sticky	r	w	x	r	w	x	r	w	x
0	1	1	1	1	1	1	1	0	1	0	0
0+2+1			4+2+1			4+2+0			4+0+0		
3			7			6			4		

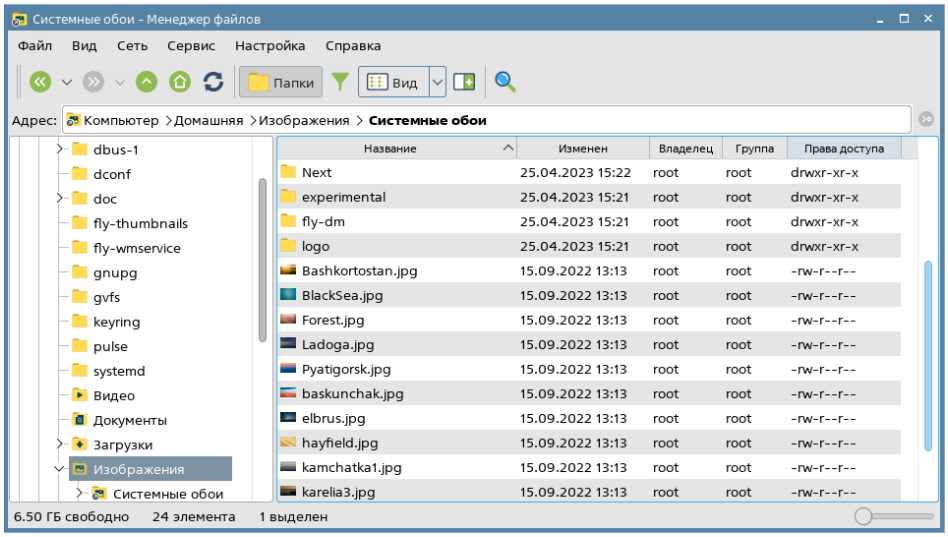
3. Управление правами доступа

Просмотреть и задать права доступа к файлу позволяет **Менеджер файлов**. Увидеть права доступа при просмотре

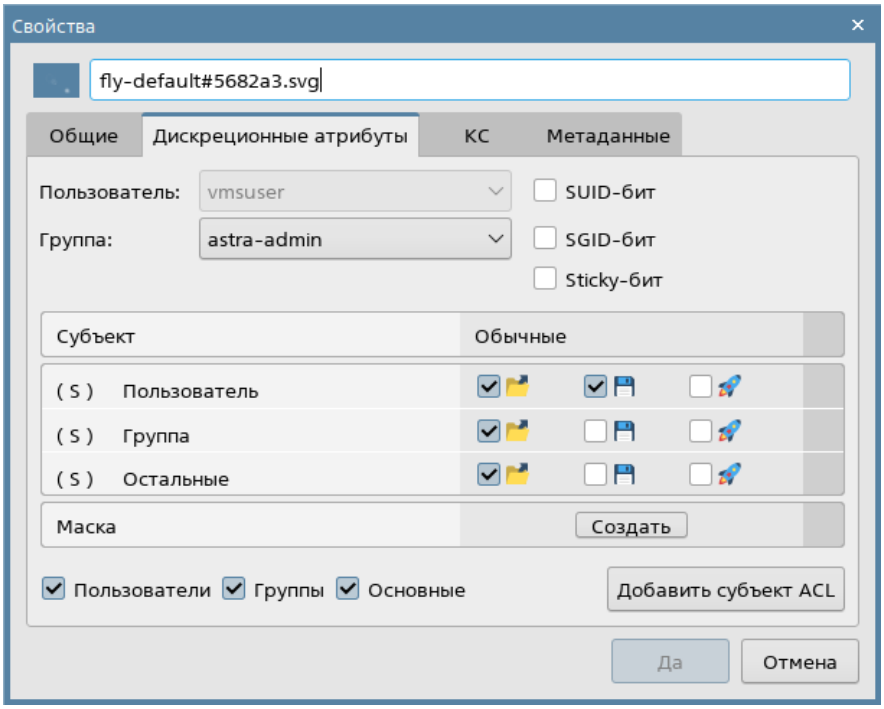
каталога позволяет табличный вид, который можно включить с помощью соответствующей кнопки на панели инструментов.



При просмотре каталога в табличном виде права доступа отображаются в символьной форме.



Также просмотреть установленные права доступа можно в свойствах файла или каталога, на вкладке **Дискреционные атрибуты**.



В верхней части вкладки можно указать владельца, группу, а также дополнительные биты защиты.

Изменять владельца у файла может только администратор системы root (сам владелец не может отказаться от файла).

Менять группу может root или владелец файла, если владелец передает файл в группу, в которой он сам состоит.

В центральной части вкладки отображаются права доступа в табличном виде, где в первом столбце указывается субъект, к которому применяются правила. В последующих столбцах отмечаются права на чтение, запись и исполнение. Для каталога также будут отображаться дополнительные столбцы — **По умолчанию**. В этих столбцах указываются права, присваиваемые создаваемым в этом каталоге объектам.

Изменить права доступа может владелец файла или root.

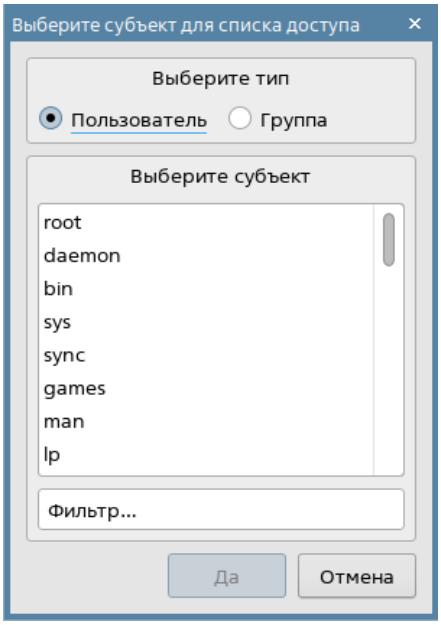
Ниже можно указать маску, которая переопределит права. Например, добавив маску, в которой предоставлены все права, можно предоставить полный доступ, независимо от того, входит ли пользователь в группу.

В нижней части окна отображаются флаги, которые позволяют скрыть или отобразить субъекты соответствующего типа в таблице.

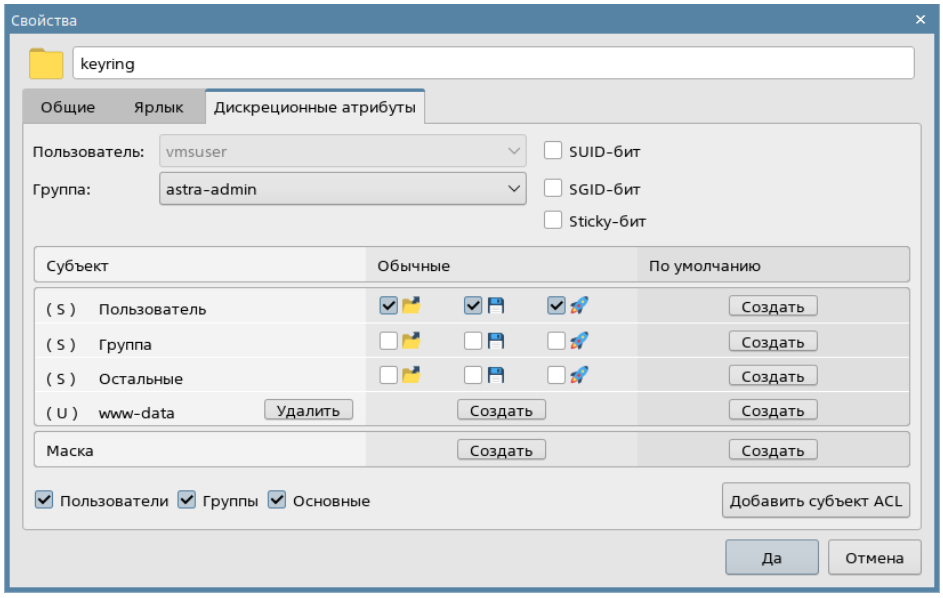
Также внизу расположена кнопка **Добавить субъект ACL**. С её помощью можно добавить дополнительное правило ACL (Access Control List — список управления доступом).

Списки управления доступом позволяют определять стандартные права (read, write, execute) на файлы и каталоги для указанных в списке пользователей и групп. Можно использовать следующие типы списков управления доступа:

- ACL для пользователя;
- ACL для группы;
- маска, которая определяет максимально возможные права для пользователей и групп.



При нажатии кнопки **Добавить субъект ACL** отобразится окно, в котором следует выбрать, для какого типа субъекта будет установлено правило — пользователь или группа. Затем необходимо выбрать непосредственно пользователя или группу (можно воспользоваться фильтром внизу окна) и нажать кнопку **Да**. На вкладке **Дискреционные атрибуты** появится строка с выбранным субъектом. Для установки особых прав в строке с этим субъектом потребуется нажать кнопку **Создать**.



Установленная на объект маска отменяет действие прав субъекта ACL.

ПРИМЕЧАНИЕ
Определить тип субъекта позволяет буква, указанная в скобках в начале строки: S — основной, U — пользователь, G — группа.