**Администрирование учётных записей пользователей и групп.**

Отправной точкой реализации управления доступом в ASTRA LINUX SE являлось унаследованное от ОС семейства Linux дискреционное управление доступом. Поэтому, несмотря на то что в настоящее время в ASTRA LINUX SE используются мандатные управление доступом и контроль целостности, а в перспективе ролевое управление доступом, целесообразно рассмотреть основные элементы дискреционного управления доступом, не утратившие своей актуальности в современных релизах ASTRA LINUX SE.

Дискреционное управление доступом в ОС семейства Linux базируется на понятии владения (использовании права доступа владения) файлом, каталогом, процессом (сущностями и субъект-сессиями). Так в файловых системах семейства extfs, которые по умолчанию используются в ASTRA LINUX SE, для каждого файла или каталога обязательно задана учётная запись пользователя — их владелец. Процесс, функционирующий от имени такой учётной записи-владельца сущности, имеет право изменять дискреционные права доступа к ней, например назначать их учётным записям других пользователей ASTRA LINUX SE на основе стандарта POSIX ACL .

**Access Control List или ACL** — список контроля доступа, который определяет, кто или что может получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом. Списки контроля доступа являются основой систем с избирательным управлением доступа.

Для оптимизации и облегчения администрирования дискреционного управления доступом в случаях, когда к одним и тем же файлам или каталогам требуется установить одинаковые права доступа более чем для одной учётной записи пользователя, в ASTRA LINUX SE применяются группы учётных записей пользователей. В результате для файлов и каталогов владельцем (обладателем к ним правом доступа владения) может быть задана группа. При этом для них остаются владельцами и соответствующие учётные записи пользователей. В перспективе при реализации в ASTRA LINUX SE ролевого управления доступом вместо учётных записей пользователей и групп владельцами будут задаваться роли или административные роли.

Таким образом, при управлении доступом в ASTRA LINUX SE, в том числе дискреционным, администрируют следующие его элементы:

* учётные записи пользователей (account);
* группы (логические объединения учётных записей пользователей с равными дискреционными правами доступа);
* права доступа к файлам, каталогам, другим объектам доступа (сущностям и субъект-сессиям);
* режимы доступа, обеспечивающие возможность учета ряда особенностей управления доступом.

Утилиты администрирования учётных записей пользователей и групп реализованы в пакете Shadow Suite.

Кроме них для этого используется ряд системных файлов, которые конфигурируются администратором системы. Такие файлы в рамках МРОСЛ ДП -модели рассматриваются как сущности, параметрически ассоциированные с учётными записями пользователей.

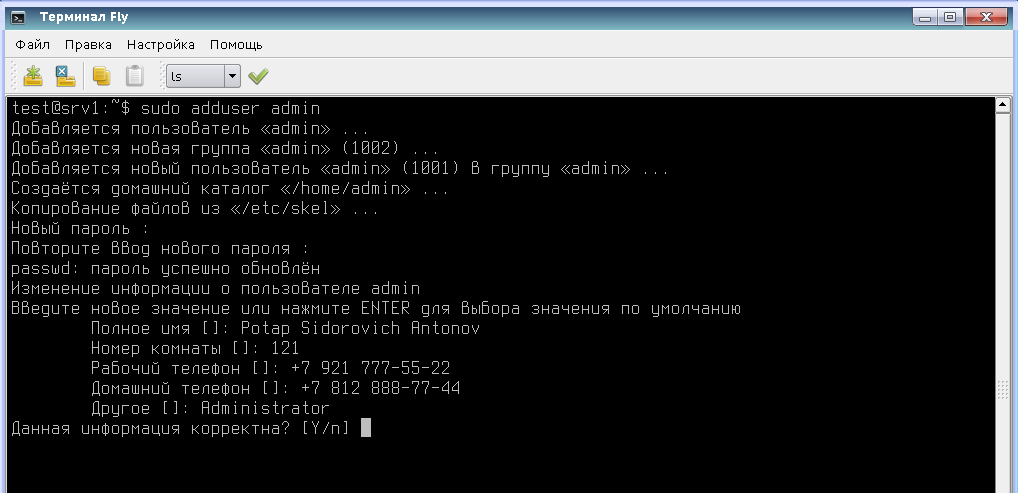
Основой для задания учётных записей пользователей и групп являются их идентификаторы:

* uid (User ID) — число, уникально идентифицирующее учётную запись пользователя в ASTRA LINUX SE;
* gid (Group ID) — число, уникально идентифицирующее группу пользователей ASTRA LINUX SE.

Эти идентификаторы хранятся в следующих конфигурационных файлах, которые используется специальным процессом login, реализующим вход пользователя в ASTRA LINUX SE — его идентификацию и аутентификацию:

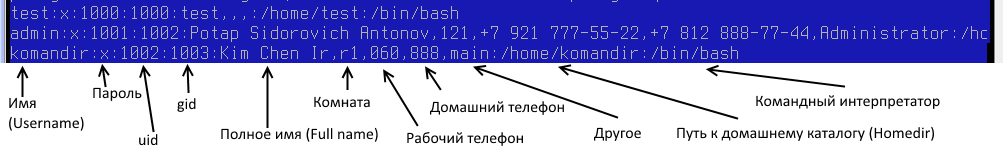
* /etc/passwd — файл с данными об учётных записях пользователей;
* /etc/group — файл с данными об учётных записях групп пользователей.

учётная запись каждого пользователя представляет одну строку в файле/etc/passwd. Таким образом, регистрация новой учётной записи пользователя в системе, фактически, является добавлением соответствующей строки в этот файл.



Добавим пользователя admin.

Откроем файл /etc/passwd в редакторе mc



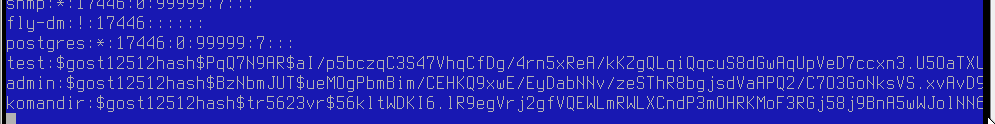
Разделителем полей данных в строке, соответствующей учётной записи пользователя, является символ «:». В результате у администратора с помощью команды grep есть возможность фильтрации требуемых данных об учётной записи пользователя, которая состоит из следующих элементов:

• username — уникальное символьное имя, присваиваемое каждой учётной записи пользователя (при выборе имени могут использоваться буквы и цифры, а также знак подчёркивания и точка);

• uid — уникальный идентификатор учётной записи пользователя (представлен числом);

• gid — уникальный идентификатор первичной группы, в которую входит учётная запись пользователя (представлен числом);

• password — пароль, который может храниться в зашифрованном виде непосредственно в рассматриваемой строке (если вместо пароля задан символ «х»), то он хранится в доступном для чтения и записи только администратору системном файле /etc/shadow в зашифрованном виде):



•full name — полное имя учётной записи пользователя (например, пользователь с username равным sidor может иметь полное имя «Ivan Sidorov», а также в этом же элементе через запятую могут перечисляться дополнительные сведения о пользователе: домашний и рабочий номера телефонов, адрес и т.д.);

• home directory — домашний каталог учётной записи пользователя, находящийся в каталоге /home;

• login shell — командный интерпретатор (shell), который запускается при входе пользователя в ASTRA LINUX SE, по умолчанию это интерпретатор bash (/bin/bash).

Создание, удаление и изменение учётных записей пользователей осуществляется администратором (в рамках МРОСЛ ДП-модели ему соответствует доверенная субъект-сессия, обладающая соответствующими текущими специальными административными ролями) с использованием следующих приёмов:

• непосредственное редактирование файла /etc/passwd;

• с применением утилит из пакетов passwd и adduser;

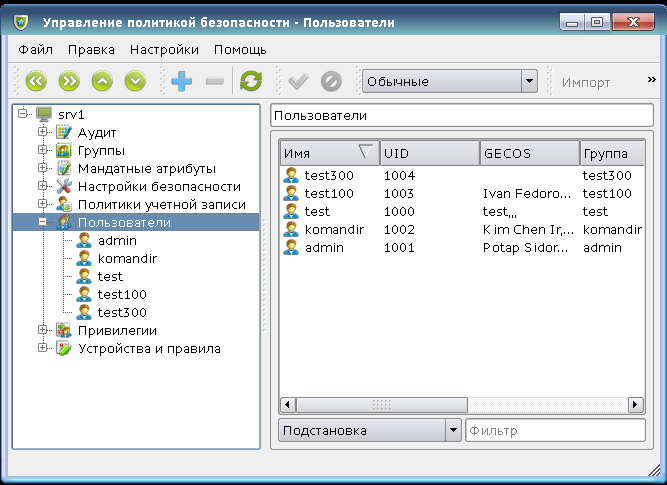
• с активизацией из меню «Пользователи и группы» утилиты с графическим интерфейсом «Управление политикой безопасности».

(МРОСЛ ДП-модель — мандатная сущностно-ролевая ДП-модель).

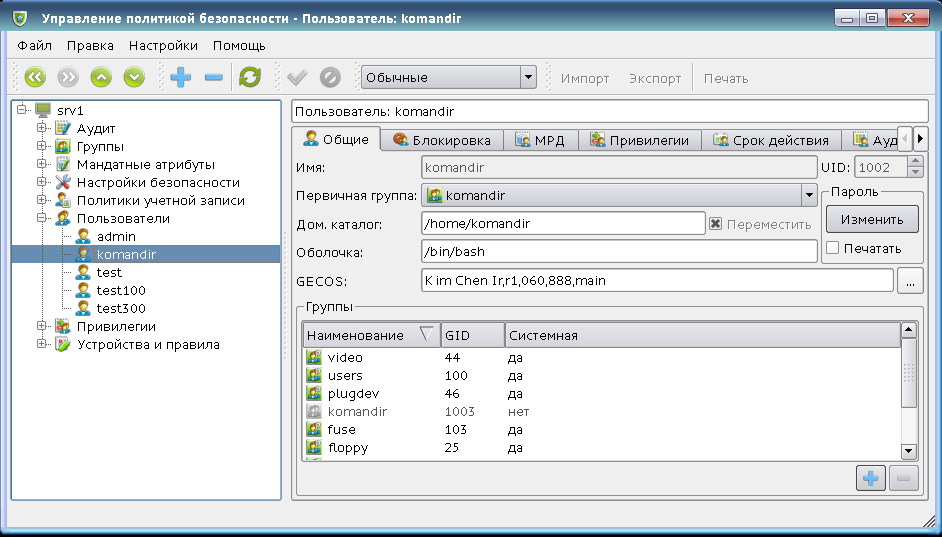
В ASTRA LINUX SE получение идентификатора учётной записи пользователя (uid), а также других связанных с ним наборов параметров, возможно с помощью команд whoami, id, who. Для изменения пароля учётной записи пользователя используется команда passwd, которая проверяет заданные правила формирования пароля, например, его минимальную длину, или же создан ли он на основе предыдущего пароля.

Для корректного администрирования учётной записи пользователя (в том числе с добавлением при её создании в домашний каталог необходимых конфигурационных файлов) администратор может использовать команды adduser, useradd (создание), usermod (модификация параметров) и userdel (удаление). В рамках МРОСЛ ДП-модели этим командам соответствуют де-юре правила вида create\_ user, set-user\_labels и delete-user.

В то же время для администрирования учётных записей пользователей целесообразно использовать утилиту с графическим интерфейсом «Управление политикой безопасности» (утилиту flу-admin-smc), доступную из элемента «Настройки» главного пользовательского меню.



Учётные записи пользователей, зарегистрированных на рабочей станции локально, администрируются с использованием утилиты «Управление политикой безопасности» из раздела «Пользователи и группы» вкладки «Локальная политика». Выбрав какую-либо учётную запись, администратор ASTRA LINUX SE может просмотреть и изменить её параметры, которые считываются из файла /etc/passwd .



Добавление учётной записи пользователя также осуществляется администратором с использованием утилиты «Управление политикой безопасности».

Для безопасности ASTRA LINUX SE важна регулярная проверка корректности параметров учётных записей пользователей, для чего администратор может использовать команду pwck (от password check), которая проверяет целостность данных и правильность формата записей в файлах /etc/passwd и /etc/shadow, при этом проверяются:

* корректность количества полей в записях этих файлов;
* уникальность имён учётных записей пользователей;
* уникальность идентификаторов учётных записей пользователей;
* корректность принадлежности каждой учётной записи пользователя её первичной группе;
* корректность пути к домашнему каталогу каждой учётной записи пользователя;
* корректность сведений об используемом интерпретаторе по умолчанию.

Исправление выявленных командой pwck ошибок администратор может осуществить с помощью команды usermod.

Данные о каждой группе учётных записей пользователей находятся в системном файле /etc/group в строке формата «groupname: password:gid:other members», которая состоит из следующих элемента

• groupname — имя группы;

• password — пароль, установленный для группы;

• gid — идентификатор группы (аналогичный полю gid в учётной записи пользователя);

• other members — другие пользователи, входящие в состав группы.

Как и в случае системного файла /etc/passwd право на запись в файл /etc/group (который является сущностью, параметрически ассоциированной с учётными записями доверенных и недоверенных пользователей) имеет только администратор, остальные пользователи могут только просматривать его содержимое.

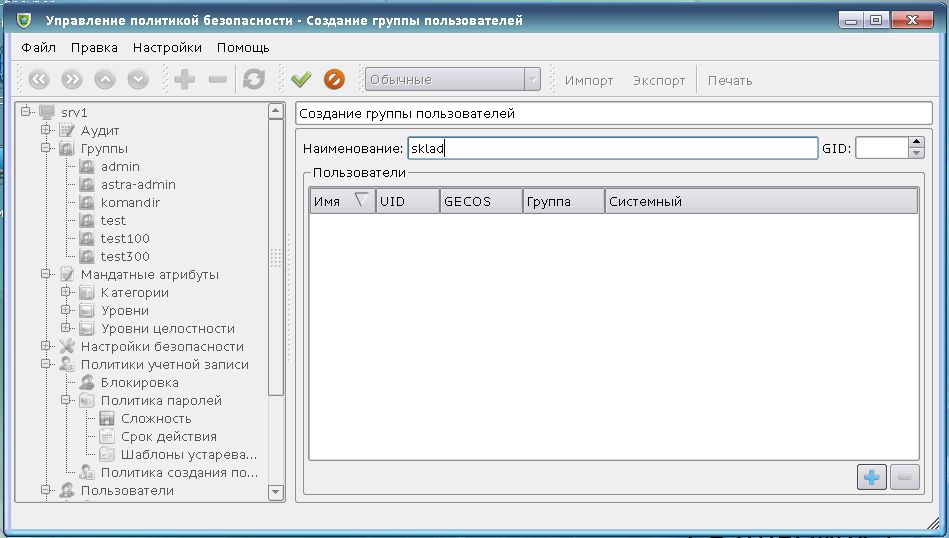
Пользователь может получить данные о своей принадлежности к группам с помощью команд id и groups. Администратор может создавать, удалять или изменять параметры групп учётных записей пользователей:

• непосредственно редактируя файл /etc/group’

• редактируя файлы /etc/group и /etc/gshadow (назначение последнего аналогично назначению файла /etc/shadow) командой gpasswd;

• используя команды groupadd и groupdel;

• изменяя параметры групп учётных записей пользователей командой groupmod;



* используя утилиту «Управление политикой безопасности».

Для проверки корректности параметров групп учётных запиcей пользователей используется аналогичная команде pwck команда grpck, которая анализирует данные файлов /etc/group и /etc/gshadow, дополнительно используя для этого данные из файла /etc/passwd. При этом проверяются:

• корректность количества полей в записях этих файлов;

• уникальность имён групп;

• уникальность идентификаторов групп;

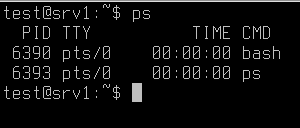
• корректность состава учётных записей пользователей и администраторов каждой группы.

Исправление выявленных командой grpck ошибок администратор может осуществить с помощью команды groupmod.

Так как в перспективе на смену группам в ASTRA LINUX SE придут роли или административные роли, то в рамках МРОСЛ ДП-модели к командам администрирования групп учётных записей пользователей соответствуют де-юре правила вида grant\_admin\_rights, remove\_admin\_rights, create-role, delete\_role, create\_hard\_link\_role, delete\_hard\_link\_role, rename\_role, get\_role\_attr, set\_role\_labels.

**Администрирование процессов.**

Администратору ASTRA LINUX SE требуется контролировать и управлять выполнением совокупности процессов (доверенных или недоверенных субъект-сессий в рамках МРОСЛ ДП-модели), которые были запущены пользователями в рмчках своих сеансов, а также ядром ASTRA LINUX SE, системными и прикладными сервисами.



Основной командой для мониторинга состояния процессов в ASTRA LINUX SE является команда ps. Запущенная без опций и аргументов команда ps выводит на экран список процессов, выполняемых на активном терминале (tty) или псевдотерминале (pts), при этом для каждого процесса указываются:

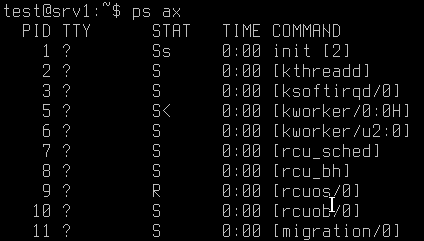
PID — идентификатор процесса, который присваивается при его г гарте из числа свободных PID в диапазоне значений от 0 до (232 – 1);

TTY— терминал (tty) или псевдотерминал (pts), в котором выполняется процесс;

TIME — время выполнения процесса процессором;

CMD — имя программы, соответствующей выполняющемуся процессу.

Использование параметров с командой ps позволяет просмотреть более детальную информацию о процессах.



Опции, отбирающие процессы для отчёта:

-A : все процессы;

-a : связанные с конкретным терминалом, кроме главных системных процессов сеанса, часто используемая опция;

-N : отрицание выбора;

-d : все процессы, кроме главных системных процессов сеанса;

-e : все процессы;

-f : расширение информации

T : все процессы на конкретном терминале;

a : процессы, связанные с текущим терминалом, а также процессы других пользователей;

r : информация только о работающих процессах;

x : процессы, отсоединённые от терминала.

Параметры STAT

R : процесс выполняется в данный момент

S : процесс ожидает (т.е. спит менее 20 секунд)

I : процесс бездействует (т.е. спит больше 20 секунд)

D : процесс ожидает ввода-вывода (или другого недолгого события), непрерываемый

Z : zombie или defunct процесс, то есть завершившийся процесс, код возврата которого пока не считан родителем

T : процесс остановлен

W : процесс в свопе

< : процесс в приоритетном режиме.

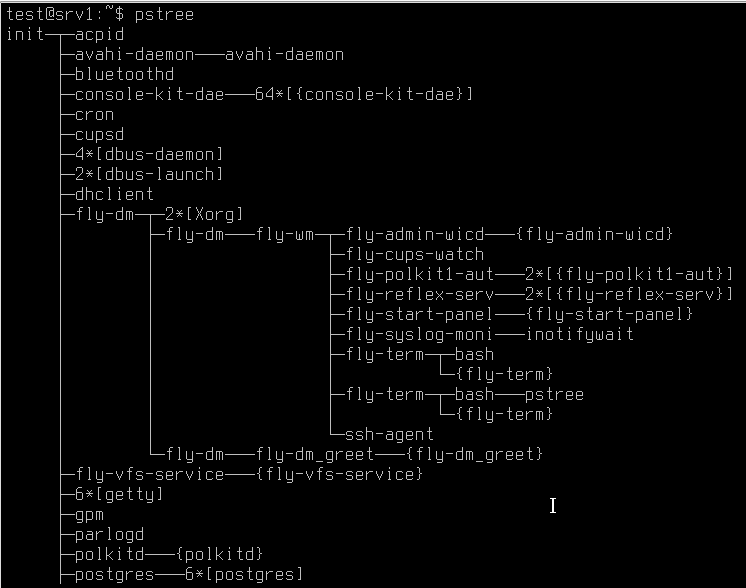
N : процесс в режиме низкого приоритета

L : real-time процесс, имеются страницы, заблокированные в памяти.

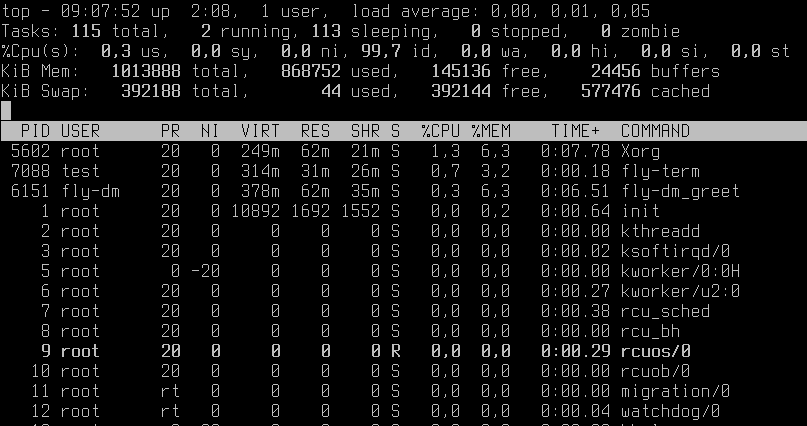
s : лидер сессии

Прототипом команды ps, позволяющим моделировать получении данных о процессах (субъект-сессиях), в рамках МРОСЛ ДП-модели является де-юре правило вида get-subject-attr.

Команда pstree дополняет команду ps, с её помощью можно отобразить дерево процессов, функционирующих на всех терминалах, в формате «предок-потомок». Это позволяет проследить, цепочку порождения исследуемого процесса и получить возможность корректного управления им (особенно это касается его завершения) с учётом его «родственных связей». Без использования параметров команда pstree выводит дерево процессов, где каждый процесс идентифицируется именем соответствующей ему программы.



Команды ps и pstree позволяют получить сведения о запущенных процессах, отследить их текущее состояние и взаимосвязи друг с другом. Для того чтобы получать данные о процессах, собранные за некоторый интервал времени, используется команда top. Принцип ее работы основан на периодическом анализе обновлений таблицы процессов ASTRA LINUX SE, что позволяет отследить изменение их параметров.



Информация, выводимая командой top, содержит общие данные о процессах и ресурсах ASTRA LINUX SE:

число пользовательских сеансов (user);

усреднённая загруженность ресурсов системы (load average);

общее число процессов (total task) и число процессов, находящихся в разных состояниях (running, sleeping, stopped и zombie);

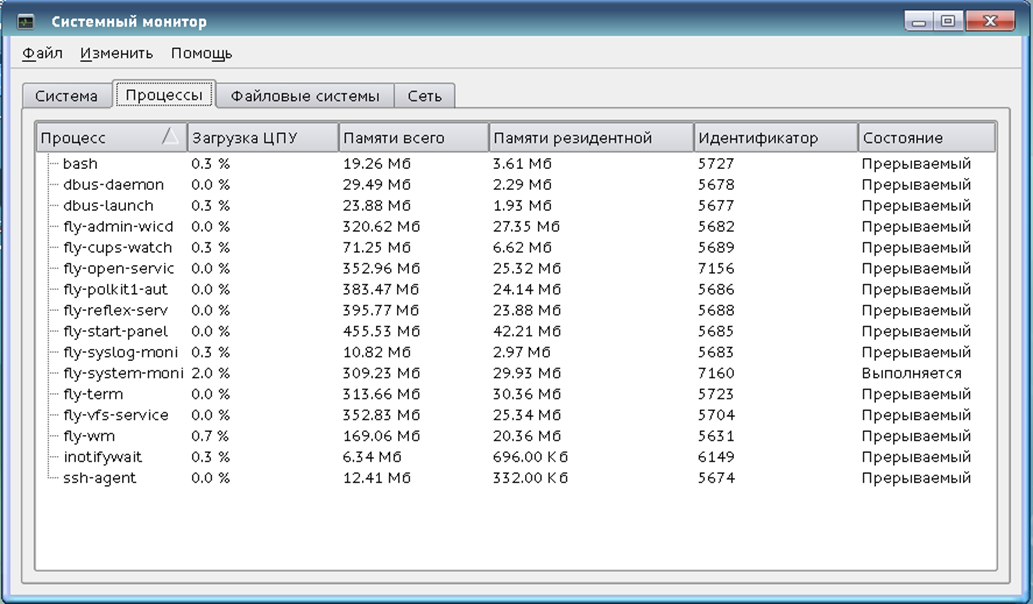
загруженность процессора (%Cpu);

распределение оперативной памяти между процессами (KiB Mem);

используемые области подкачки страниц (KiB Swap).

Кроме того, команда top выводит в терминал все данные, выдаваемые командой ps в режиме детализированного вывода.

При работе в защищённой графической подсистеме Fly информацию, аналогичную выводимой командой top, можно получить с использованием графической утилиты «Системный монитор» меню Системные» главного меню.



Дополнительно графическая утилита «Системный монитор» может осуществлять управление процессами, при этом доступны следующие функции:

• остановки/возобновления работы процессов;

• прерывания (для допускающих прерывания процессов);

• завершения процессов.

В ASTRA LINUX SE администратор может управлять запущенными процессами, передавая им сигналы с использованием команды kill (в рамках МРОСЛ ДП-модели ей соответствует де-юре правило вида delete\_session). Процесс, получив сигнал, может отреагировать на него либо по умолчанию, заданному ядром ASTRA LINUX SE, либо использовать собственную функцию обработки сигнала. В основном сигналы команды kill предназначены для реализации различных режимов прерывания, завершения, приостановления или возобновления работы процессов. Команда killall является расширением команды kill и отличается от нее тем, что посылает сигналы всем процессам, запущенным при выполнении одной программы.

Также администратор и пользователи ASTRA LINUX SE имеют возможность влиять (например, с помощью команды nice) на использование выполняющимися процессами ресурса времени центрального процессора путём изменения их приоритета, указывающего ядру ASTRA LINUX SE, где расположить процесс в общей очереди готовых к выполнению на центральном процессоре процессов.