Лекция14 **Особенности аутентификации и аудита в ОССН Astra Linux**

**1. Особенности аутентификации**

Подобно другим современным Linux-системам, подсистема аутентификации ОССН построена на основе архитектуры PAM.

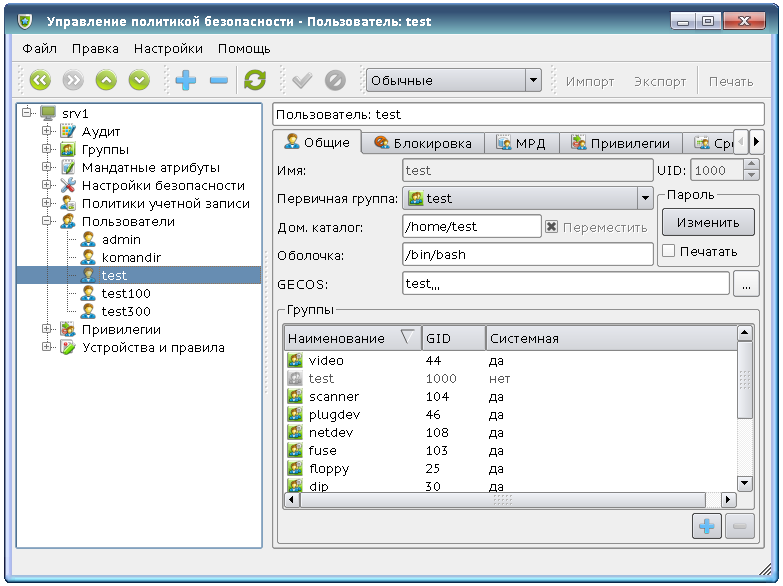
PAM — Pluggable Authentication Modules (Подключаемы Модули Безопасности).

В прошлом если приложению Linux требовалось запросить аутентификацию пользователя, то ему приходилось обращаться к файлам /etc/passwd и /etc/shadow. Такой подход был прост, но при этом разработчикам приходилось думать не только о работе с файлами, но и о вопросах безопасности. В связи с этим возникла необходимость разработки прозрачного механизма аутентификации пользователей, не зависящего от способа хранения информации об их учетных записях.

Решение этой задачи было предложено в проекте Linux-PAM. Архитектура PAM была впервые предложена компанией Sun в октябре 1995 года, а в августе 1996 года инфраструктура Linux-PAM была включена в дистрибутив Red Hat Linux.

В Astra Linux SE к стандартному набору модулей PAM добавлены четыре дополнительных модуля, реализующие назначение мандатных атрибутов, уровня целостности и специфических привилегий ОССН первому процессу в сеансе работы пользователя с ОССН. Если клиентская программа РАМ в ходе аутентификации не обращается к перечисленным модулям, сеанс пользователя, аутентифицированного данной программой, получает низкий уровень целостности и нулевые мандатные атрибуты, не дающие никаких прав доступа к конфиденциальным данным.

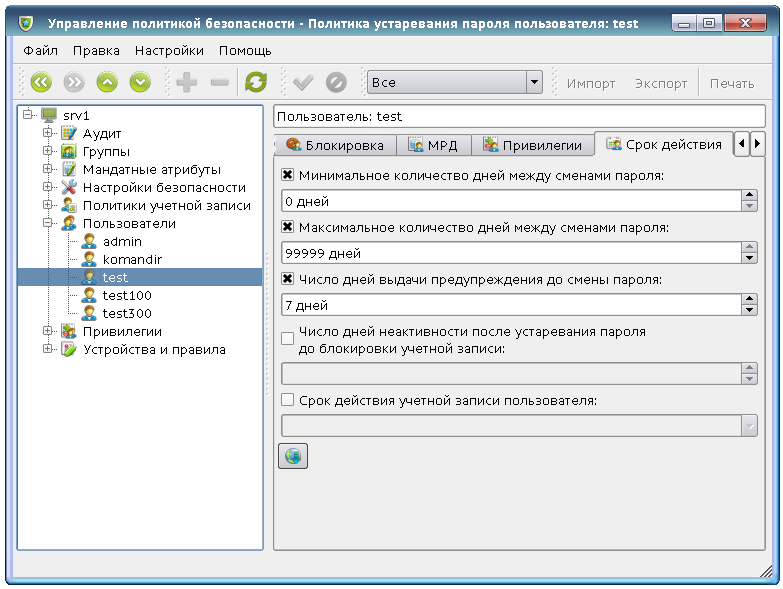
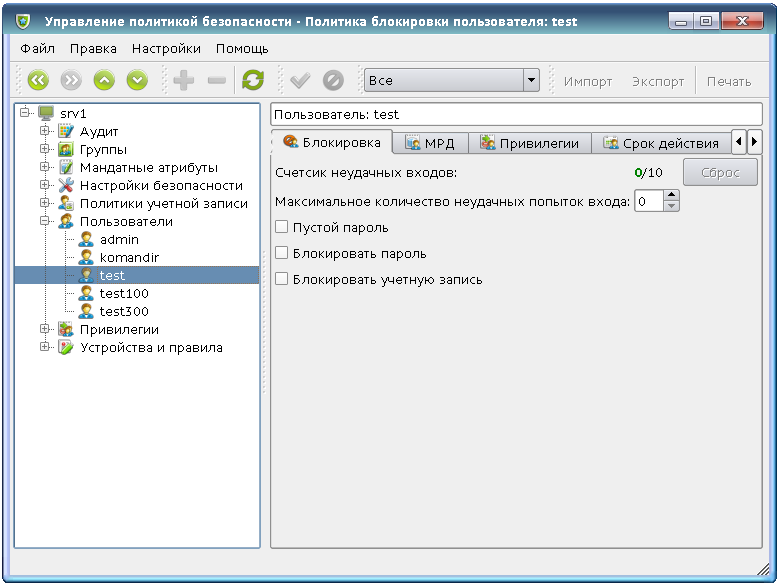
В ОССН не предъявляется никаких специальных требований к РАМ-модулям. Любой такой модуль, разработанный для любой *Linux-*системы, должен корректно функционировать в ОССН. В файл **/etc/pamd/common-password** по умолчанию включён **РАМ-** модуль **pam-cracklib.so**, запрещающий назначать пользователям простые пароли, нестойкие к подбору.



Администрирование подсистемы аутентификации осуществляется с использованием графической утилиты **fly-admin-smc** («Управление политикой безопасности»). Пароль и основные параметры аутентификации для пользователя задаются при регистрации учётной записи на вкладках «Общие», «Блокировка», «Срок действия» элемента меню «Пользователи»/ <имя пользователя>» (рис. ).

Рис. 3.17. Основные настройки учётной записи пользователя

Основные элементы вкладок имеют следующее назначение.

* Пароль: изменить — позволяет администратору ОССН принудительно назначить пользователю новый пароль. Это самый простой способ устранить проблему, если пользователь забыл свой пароль.
* Срок действия учётной записи пользователя — если заполнено, по достижении указанной даты учётная запись данного пользователя будет автоматически заблокирована. Пользователь, учётная запись которого заблокирована, не может входить в систему до тех пор, пока администратор ОССН не снимет блокировку.  
  
* 
* Блокировать учётную запись — позволяет администратору ОССН заблокировать учётную запись пользователя или снять ранее наложенную блокировку.
* UID — внутренний числовой идентификатор учётной записи пользователя, назначается при регистрации, в дальнейшем, как правило, не изменяется. Указывается справочно, так как это может пригодиться при анализе системных журналов, локализации и устранении проблем функционирования системного и прикладного ПО и т.п., но в повседневной работе не используется. Чаще всего администратор даже не знает, каким учётным записям сопоставлены какие числовые идентификаторы. Обычно первый зарегистрированный в системе пользователь получает идентификатор 1000, второй зарегистрированный пользователь — 1001 и т. д.
* Первичная группа — группа пользователей, внутренний числовой идентификатор которой назначается в качестве идентификатора GID процессам, запускаемым от имени данной учётной записи пользователя. По умолчанию каждой учётной записи пользователя назначается фиктивная группа, включающая только саму учётную запись пользователя. Каждой учётной записи пользователя назначается одна и только одна первичная группа. Первичная группа не может быть одной из предопределённых системных групп.
* GID — внутренний числовой идентификатор первичной группы учётной записи пользователя. Аналогично UID, приводится справочно, в повседневной работе не используется.
* Вторичные группы — перечень групп, в которые входит учётная запись пользователя. Заметим, что для предоставления учётной записи пользователя административных полномочий необходимо и достаточно включить её в группу **astra-admin** либо с помощью данной вкладки, либо сделав группу **astra-admin** первичной группой пользователя.
* Неуспешных входов — количество неуспешных входов в систему, которые пытался совершить пользователь с момента последнего обнуления счётчика неуспешных входов либо с момента регистрации учётной записи пользователя, если счётчик ни разу не обнулялся.
* Сброс — кнопка обнуления счётчика неуспешных входов для данной учётной записи пользователя.
* Максимальное — максимально допустимое для данной учётной записи пользователя значение счётчика неуспешных входов. При превышении данного значения учётная запись пользователя автоматически блокируется. Специальное значение 0 означает, что данная функция отключена.
* Период блокировки — длина в секундах паузы после каждой неуспешной попытки входа пользователя в систему перед проверкой пароля в ходе следующей аутентификации. Специальное значение 0 означает, что данная функция отключена.

Чаще всего все вышеперечисленные свойства учётной записи пользователя однократно задаются при её регистрации и более не изменяются, однако при необходимости администратор ОССН может в любой момент изменить любое её свойство.

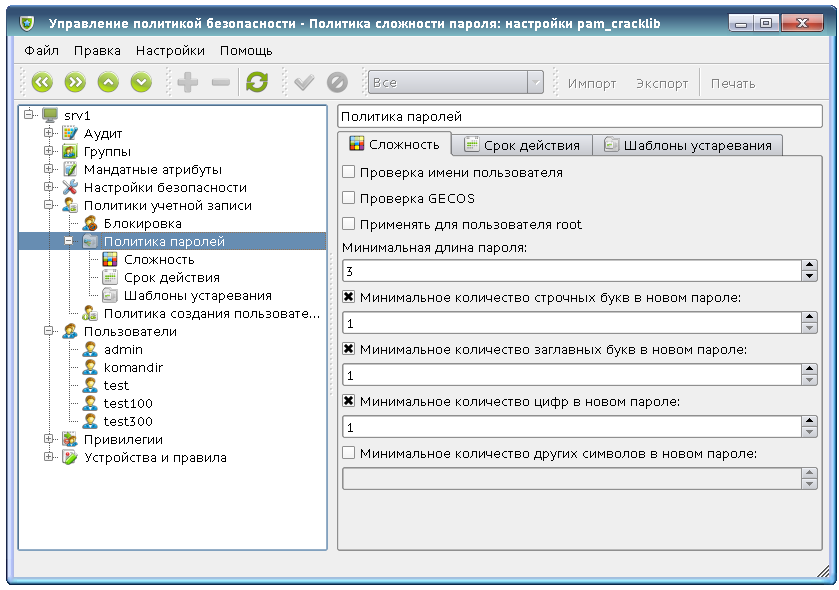


Рис. 3.18. Вкладка «Параметры пароля» графической утилиты fly-admin-smc

Политики паролей задаются в разделе «Политики паролей» графической утилиты **fly-admin-smc**. Политика паролей разделена на три части, размещённые в окне графической утилиты fly-admin-smc на трёх вкладках.

Основные элементы вкладок имеют следующее назначение.

* Число дней неактивности после устаревания пароля до блокировки учётной записи пользователя — описывает поведение ОССН в случае, если устаревание пароля произошло в период долгой неактивности пользователя, когда пользователь не входил в систему много дней подряд, обычно такие ситуации связаны с отпуском, командировкой или болезнью. Если значение данного поля равно ***N***, ОССН разрешает единственный вход по устаревшему паролю в течение **N** дней после устаревания, затем учётная запись блокируется. Специальное значение — 1 (установлено по умолчанию) требует блокировать учётную запись пользователя немедленно после устаревания пароля.
* Минимальное количество дней между сменой пароля — описывает минимальный интервал времени между двумя последовательными сменами пароля. Специальное значение 0 (задано по умолчанию) разрешает менять пароль немедленно после предыдущего изменения.
* Максимальное число дней работоспособности пароля — описывает максимальный срок действия пароля, по истечении которого пароль устаревает. По умолчанию задан максимально допустимый для ввода в окне срок 99999 дней, что составляет немногим менее 274 лет и фактически отключает данную политику.
* Число дней выдачи предупреждения до смены пароля — описывает поведение ОССН, когда пароль учётной записи пользователя вот-вот устареет. Если значение данного поля равно ЛГ, то за N дней до устаревания пароля при каждом успешном входе в систему пользователю выдаётся предупреждение, что его пароль скоро устареет.
* Минимальная длина пароля — устанавливает минимально допустимую длину пароля. При попытке назначить новым паролем более короткую строку пользователь получит отказ. Поскольку пароли учётных записей пользователей хранятся в ОССН в виде хеш-функций, не допускающих обратное преобразование за полиномиальное время, пароль может быть проверен на соответствие данному параметру только в момент установки или проверки. Поэтому изменение данного параметра политики паролей не влияет на уже установленные пароли, они продолжают действовать, даже если они противоречат новой политике паролей.
* Максимальное количество символов в нижнем регистре, Максимальное количество символов в верхнем регистре, Максимальное количество цифр, Максимальное количество других знаков — позволяют администратору ОССН требовать от пользователей, чтобы те использовали трудноподбираемые пароли, составленные из символов, принадлежащих к различным классам. Данные параметры политики позволяет запрещать применение длинных, но нестойких паролей, наподобие «аааааааааааааааа» или «1234567890123456». Специальное значение —1 означает, что данный элемент политики паролей отключён.

Вторая часть политики паролей администрируется с помощью второй вкладки — «Управление блокировками» (рис. 3.19).

Основные элементы второй вкладки имеют следующее назначение.

* Использовать индивидуальные настройки — разрешает или запрещает вводить для отдельных учётных записей пользователей индивидуальные параметры управления блокировками.
* Не использовать счетчик для пользователя с uid = 0 — запрещает или разрешает применять автоматическое блокирование

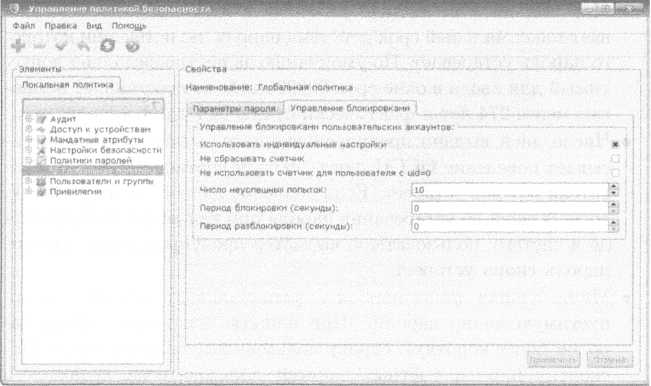


Рис. 3.19. Раздел «Управление блокировками» политики паролей

для учётной записи пользователя с UID = 0 (обычно это суперпользователь root). Если автоматическое блокирование запрещено для данной учётной записи пользователя, это фактически разрешает нарушителю подбирать её пароль сколько угодно долго. Если же блокирование разрешено, это позволяет нарушителю временно запрещать суперпользователю вход в систему, имитируя попытки подбора пароля суперпользователя, что в отдельных конфигурациях ОССН может нарушить её работоспособность. По умолчанию автоматическое блокирование учётной записи пользователя с UID = 0 разрешено.

* Число неуспешных попыток — максимально допустимое количество неуспешных попыток входа в систему, после превышения которого учётная запись пользователя автоматически блокируется.
* Период блокировки — длительность в секундах периода времени, на который блокируется учётная запись пользователя, превысившего максимально допустимое количество неуспешных попыток входа в систему.
* Период разблокировки — длительность в секундах периода времени, по истечении которого отменяется блокировка, наложенная на учётную запись пользователя, превысившего максимально допустимое количество неуспешных попыток входа в систему. Помимо глобальной политики паролей, в системе могут существовать другие политики. Для создания новой политики паролей еле-

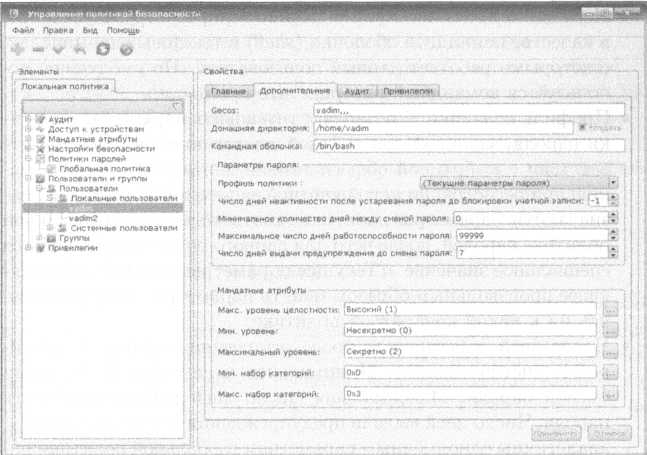


Рис. 3.20. Дополнительные настройки учётной записи пользователя

дует воспользоваться контекстным меню раздела «Политики паролей» или любого его подраздела. Если политика паролей не является глобальной, то в соответствующем окне имеется возможность записать текущее состояние политики паролей в глобальную политику.

Параметры пароля, действующие в отношении конкретной учётной записи пользователя, задаются на вкладке «Дополнительные» элемента «Пользователи и группы / Пользователи / Локальные пользователи / <имя пользователя>» (рис. 3.20).

Основные элементы вкладки имеют следующее назначение:

* Gecos — значение элемента GECOS учётной записи пользователя. Данный элемент используется некоторым устаревшим ПО для хранения дополнительной информации о учётной записи пользователя (полное имя, должность, номер комнаты, номер телефона и т. д.), не имеет отношения к обеспечению безопасности. По умолчанию имеет вид «%username%„,».
* Домашняя директория — каталог, в котором будут размещаться документы и настройки данной учётной записи пользователя. По умолчанию имя домашнего каталога имеет вид «/home/ %username%».
* Создать — если опция включена (по умолчанию), домашний каталог учётной записи пользователя автоматически создаётся при её регистрации.
* Командная оболочка — командный интерпретатор, запускаемый в качестве командной оболочки (shell) в текстовых терминалах, с которыми работает данный пользователь. По умолчанию используется командный интерпретатор / bin/bash.
* Профиль политики — позволяет установить параметры политики пароля, заданной для учётной записи пользователя, в соответствии с выбранной общесистемной политикой. По умолчанию при регистрации новой учётной записи пользователя ей назначаются параметры политики, соответствующие глобальной политике паролей, после чего для данного поля устанавливается специальное значение «(Текущие параметры пароля)», позволяющее произвольным образом менять параметры, не привязываясь ни к какой конкретной политике.
* Число дней неактивности после устаревания пароля до блокировки учётной записи, Минимальное количество дней между сменой пароля, Максимальное число дней работоспособности пароля, Число дней выдачи предупреждения до смены пароля — аналогичны одноимённым параметрам глобальной политики паролей. Заметим, что не все параметры глобальной политики паролей допускают переопределение для конкретных учётных записей пользователей.
* Мандатные атрибуты — мандатные атрибуты учётной записи пользователя, их назначение было описано ранее.

Наряду с графической утилитой fly-admin-smc, для администрирования подсистемы аутентификации ОССН могут применяться, например, следующие команды, аналогичные соответствующим командам Debian GNU/Linux:

* addgroup, groupadd — создают группу пользователей;
* adduser, user add — создают учётную запись пользователя;
* chfn — изменяет элемент GECOS учётной записи пользователя;
* chpasswd — позволяет последовательно поменять пароли нескольким учётным записям пользователя, применяется в скриптах, реализующих регистрацию учётных записей пользователей в пакетном режиме;
* chsh — изменяет командный интерпретатор (shell), выбранный для учётной записи пользователя;
* delgroup, groupdel — удаляют группу пользователей;
* deluser, userdel — удаляют учётную запись пользователя;
* gpasswd — позволяет управлять членством учётных записей пользователей в группах;
* groupmod — позволяет переименовать группу пользователей или изменить её внутренний числовой идентификатор;
* grpck — проверяет корректность формата и содержания файлов, хранящих информацию о группах пользователей;
* newgrp — добавляет учётную запись пользователя в группу;
* newusers — позволяет одновременно создать или обновить несколько учётных записей пользователей в пакетном режиме;
* passwd — меняет пароль учётной записи пользователя;
* pwck — проверяет корректность формата и содержания файлов, хранящих информацию о учётных записях пользователей;
* usermod — изменяет свойства учётной записи пользователя.

**4. Особенности аудита**

Помимо стандартного для Debian GNU/Linux демона rsyslogd, в ОССН также имеется собственная система аудита, реализуемая подсистемой безопасности PARSEC, позволяющая более эффективно управлять регистрацией событий, непосредственно связанных с безопасностью ОССН. Архитектура аудита PARSEC показана на рис. 3.21.

Зарегистрированные события записывают в файлы kernel.mlog и user.mlog, по умолчанию размещаемые в каталоге /var/log/ parsec. Каждая запись файла соответствует одному зарегистрированному событию и содержит следующие данные:

* имя учётной записи пользователя;
* источник события;
* время регистрации события;
* имя процесса;
* статус выполнения системного вызова, приведшего к регистрации события: успех ([s]) или отказ ([/]);
* имя, параметры и возвращаемое значение системного вызова, приведшего к регистрации события.



Рис. 3.21. Архитектура аудита PARSEC

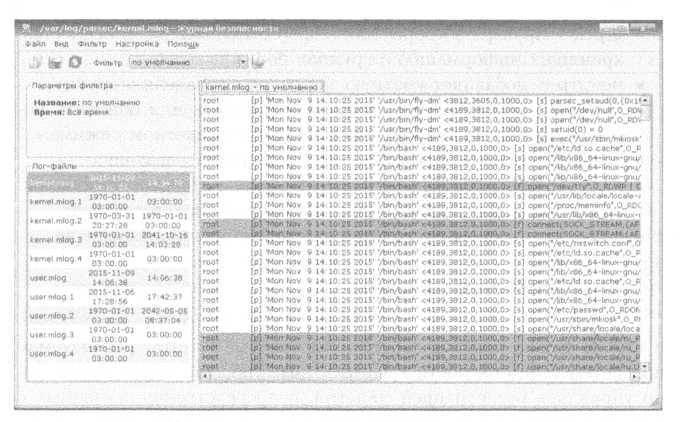


Рис. 3.22. Утилита просмотра журналов аудита

Для просмотра зарегистрированных событий аудита используется графическая утилита fly-admin-viewaudit, интерфейс которой показан на рис. 3.22.

В левой части окна интерфейса перечислены текущие параметры фильтрации отображаемых событий, а также перечень файлов, доступных для просмотра. В правой части окна интерфейса отображаются события, зарегистрированные в выбранном файле аудита и удовлетворяющие текущим параметрам фильтрации. События, связанные с успешными обращениями к данным, отображаются белым цветом, события связанные с неуспешными обращениями, — красным.

Управление фильтрацией событий аудита осуществляется по команде меню «Фильтр / Изменить» с использованием интерфейса, показанного на рис. 3.23.

Основные элементы интерфейса имеют следующее назначение:

* Заголовок интерфейса содержит имя редактируемого фильтра.
* Время — позволяет задать интервал времени, к которому должны принадлежать отображаемые события аудита. Можно указать в явном виде начальный и конечный моменты, воспользоваться одним из предопределённых значений, либо отключить фильтрацию событий аудита по времени.

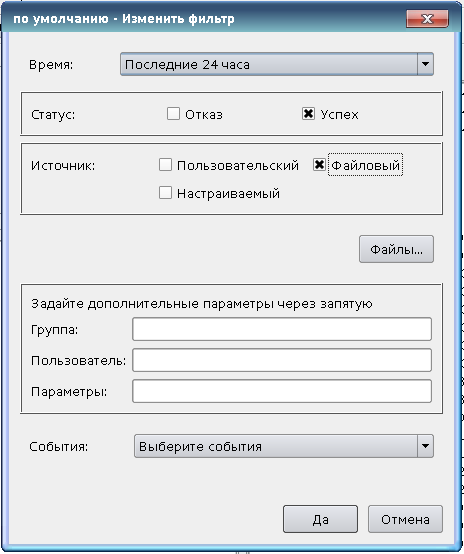
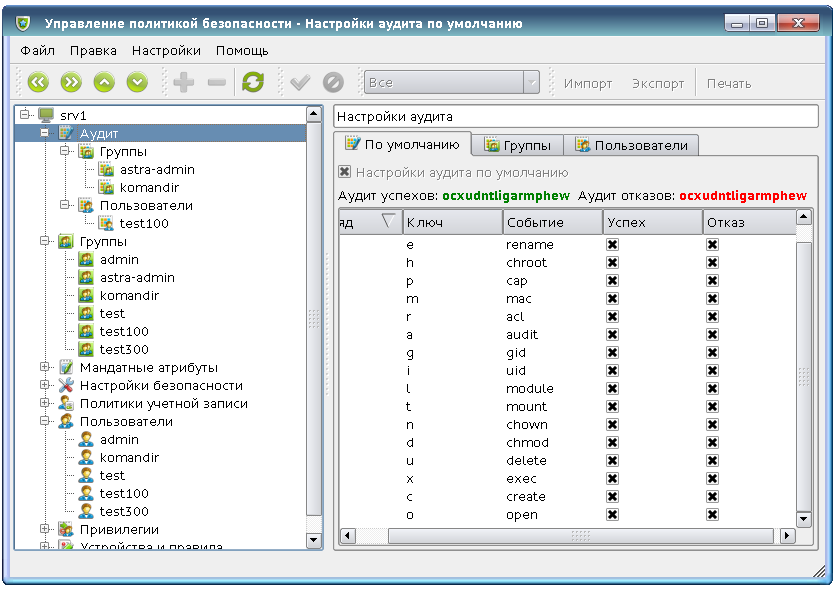


Рис. 3.23. Управление фильтрацией событий аудита

* Статус — позволяет фильтровать отображаемые события аудита по статусу выполнения системного вызова. Если в фильтре выбран только один статус, в окно утилиты выводятся только события аудита с этим статусом, если выбраны или не выбраны оба статуса, фильтрация событий аудита по статусу отключена.
* Источник — позволяет фильтровать отображаемые события аудита по источнику. Если в фильтре не выбран ни один источник, фильтрация по источнику отключена, и в окно утилиты выводятся события аудита с любым источником, так же как когда выбраны все три источника.
* Файлы — позволяет ограничить отображаемые события аудита определённой областью файловой системы ОССН.
* Дополнительные параметры — позволяет фильтровать события аудита, содержащие заданные подстроки в соответствующих полях строки, описывающей событие.
* События — позволяет фильтровать отображаемые события аудита по типу системного вызова, с которым оно связано.

Политикой аудита удобнее всего управлять с помощью графической утилиты fly-admin-smc («Управление политикой безопасности»). Аналогично политикам паролей в ОССН может одновременно действовать несколько политик аудита.

* 
* Рис. 3.24. Настройка политики аудита
* Каждая политика аудита может быть применена к конкретной учётной записи пользователя или к группе пользователей, кроме того, существует общесистемная политика, действующая по умолчанию. Создание и редактирование политик аудита осуществляется разделе «Аудит» (рис. 3.24).

Политика аудита кодируется двумя битовыми масками, в которых каждый бит соответствует категории событий, регистрируемых подсистемой аудита. Одна маска перечисляет успешные события (т. е. события, соответствующие успешным попыткам доступа субъектов к сущностям), другая — неуспешные события. Каждая категория событий аудита соответствует одному или нескольким системным вызовам, при реализации которых, если соответствующая категория включена, то генерируется событие аудита. В ОССН версии 1.4 реализуются следующие категории событий аудита:

* open — открытие файловой сущности (файла или каталога);
* create — создание файловой сущности;
* ехес — выполнение программного файла;
* delete — удаление файловой сущности;
* chmod — изменение дискреционных атрибутов файловой сущности (типичного для ОС семейства Linux вектора прав доступа);
* chown — изменение владельца файловой сущности;
* mount — монтирование или размонтирование внешнего носителя данных;
* module — загрузка или выгрузка модуля расширения ядра ОССН;
* uid — смена идентификатора учётной записи пользователя для процесса;
* gid — смена идентификатора группы для процесса;
* audit — изменение политики аудита;
* a cl — изменение дискреционных атрибутов файловой сущности;
* mac — изменение мандатных атрибутов файловой сущности;
* cap — изменение привилегий учётной записи пользователя или группы;
* chroot — смена корня файловой системы ОССН для процесса;
* rename — переименование файловой сущности;
* net — некоторые сетевые операции.

Каждой учётной записи пользователя и группе ОССН может быть сопоставлена своя политика аудита. Для создания новой политики аудита используются контекстные меню разделов «Аудит/ Группы пользователей» или «Аудит/Пользователи» соответственно.