ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа

«Блокхост-Сеть 4»

Руководство администратора безопасности

Часть 7. Консоль управления клиентом в ОС Linux

Санкт-Петербург, 2024

Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» (далее по тексту – СЗИ от НСД «Блокхост-Сеть 4», СЗИ или средство).

В документе содержатся сведения о консоли, предназначенной для управления контролем целостности файлов и каталогов, и очисткой памяти рабочих станций под управлением ОС Linux:

- назначение консоли и ее основные функциональные возможности;
- описание интерфейса консоли и основные принципы работы с ней;
- управление механизмом контроля целостности;
- настройка механизма очистки памяти.

В разделе «Подсистема ГУПТ» содержится информация о действиях администратора безопасности по управлению подсистемой гарантированного удаления по требованию в ОС Linux.

В конце документа приведен список использованных сокращений.

Содержание

Введение

Настоящее руководство администратора безопасности СЗИ от НСД «Блокхост-Сеть 4» является эксплуатационным документом, содержащим информацию о действиях администратора безопасности по работе с консолью управления клиентом: подсистемой гарантированного удаления по требованию (подсистемой ГУПТ), механизмом контроля целостности файлов и каталогов (подсистемой КЦ), механизмом очистки памяти рабочих станций (подсистемой ОП) под управлением ОС Linux.

Степени важности примечаний:

Важная информация

Указания, требующие особого внимания.

Дополнительная информация

Указания, позволяющие упростить работу с консолью.

1 Назначение подсистем ГУПТ, КЦ и ОП

Подсистема управления контролем целостности файлов и каталогов рабочих станций под управлением ОС Linux предназначена для:

– формирования перечня файлов и каталогов для постановки на контроль;

– формирования перечня файлов и каталогов для исключения отслеживания контроля целостности;

– формирования отчетов при выявлении нарушения целостности файлов и каталогов, установленных на контроль.

Подсистема очистки памяти предназначена для удаления остаточной информации после завершения поставленных на контроль процессов.

Процесс перезаписи оперативной памяти происходит по следующей схеме: по окончании работы контролируемого процесса механизм очистки памяти производит захват всей свободной оперативной памяти, включая и область, освобожденную контролируемым процессом. Захваченные области оперативной памяти перезаписываются маскирующими данными. По мере перезаписи механизм очистки высвобождает перезаписанную область.

Подсистема гарантированного удаления по требованию предназначена для осуществления гарантированного удаления выбранных объектов файловой системы с носителя информации (за исключением оптических дисков) без возможности их дальнейшего восстановления на рабочих станциях под управлением ОС семейств Linux.

Удаление выбранных файлов происходит троекратным затиранием содержимого кластеров носителя информации по специальному алгоритму, исключающему считывание остаточной информации на диске после их удаления.

2 Общий порядок работы в консоли

Консоль управления клиентом в ОС Linux устанавливается на рабочую станцию при установке клиента управления средства защиты от несанкционированного доступа «Блокхост-Сеть 4» (подробное описание установки описано в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux»).

Если клиентская рабочая станция не находится под управлением сервера «СЗИ от НСД «Блокхост-Сеть 4», при первом запуске консоли управления, для последующего входа в консоль, предлагается задать пароль для учетной записи пользователя ***«admin»*** (рисунок 2.1):

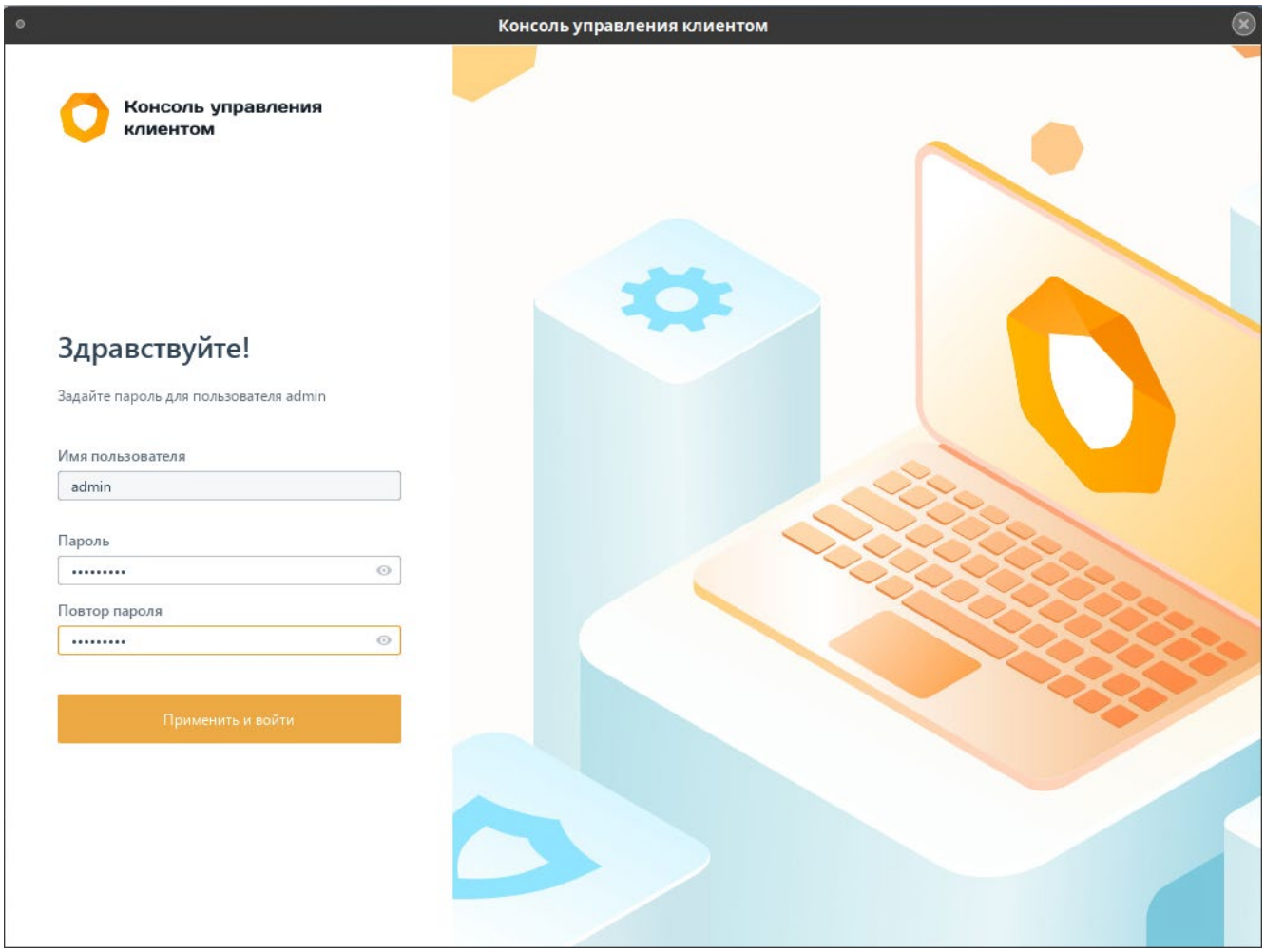


Рисунок 2.1 – Первый вход в консоль управление клиентом

При вводе пароля необходимо учитывать следующие ограничения:

– пароль должен содержать от 8 до 16 символов;

– сложность пароля учетных записей пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля (пароль должен включать символы как минимум из 3 групп):

Заглавные буквы	A…Z	26
Строчные буквы	a…z	26
Цифры	0…9	10
Специальные символы	@ # $ % ^ & * - _ ! + = [ ] { } < > | : ` , . ? / ‘ ~ ( ) ; “	31

При последующем запуске консоли управления необходимо ввести аутентификационные данные пользователя (рисунок 2.2):

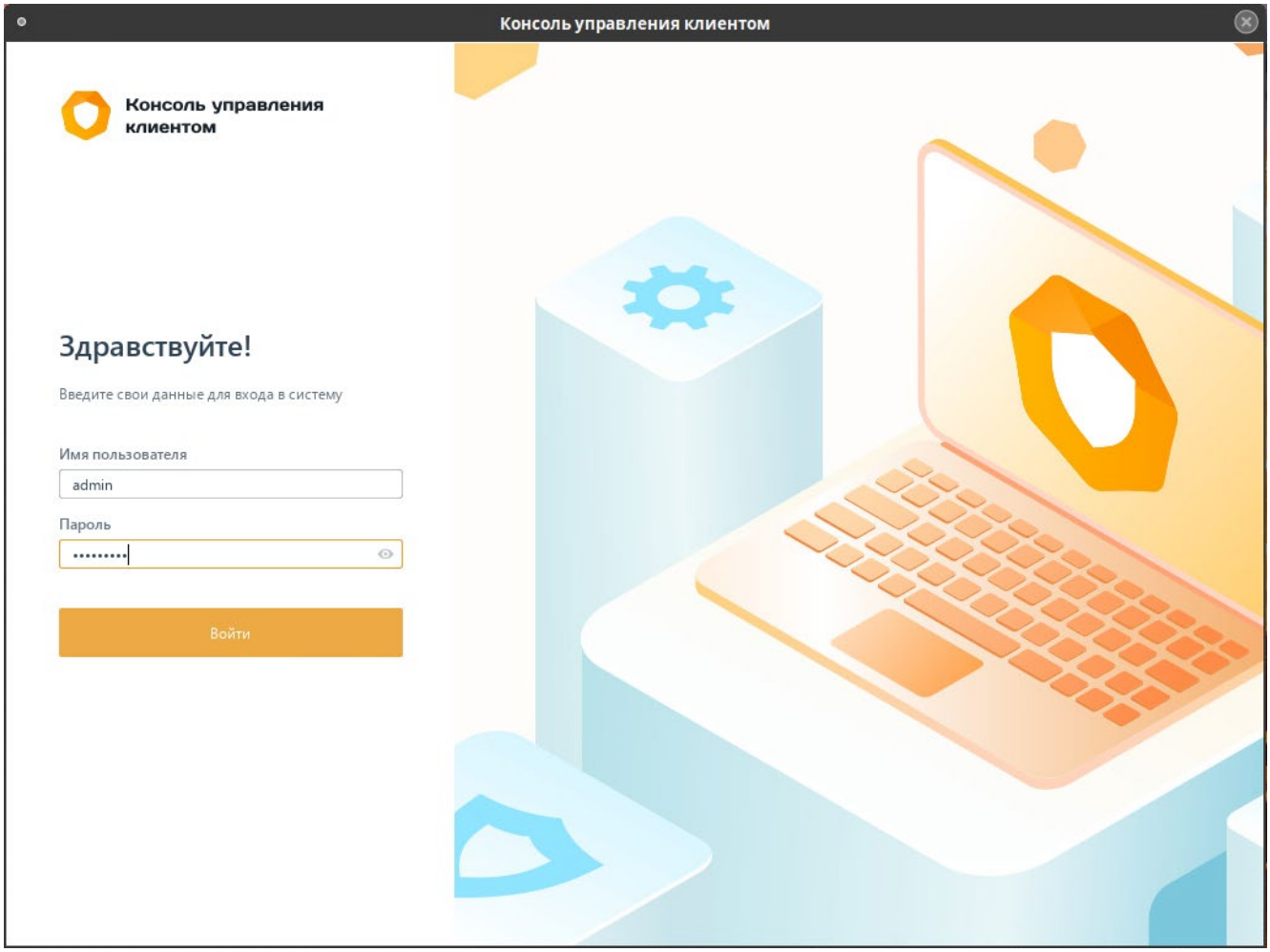


Рисунок 2.2 – Аутентификация в локальной консоли

После успешного прохождения аутентификации будет доступен основной интерфейс консоли (рисунок 2.3).

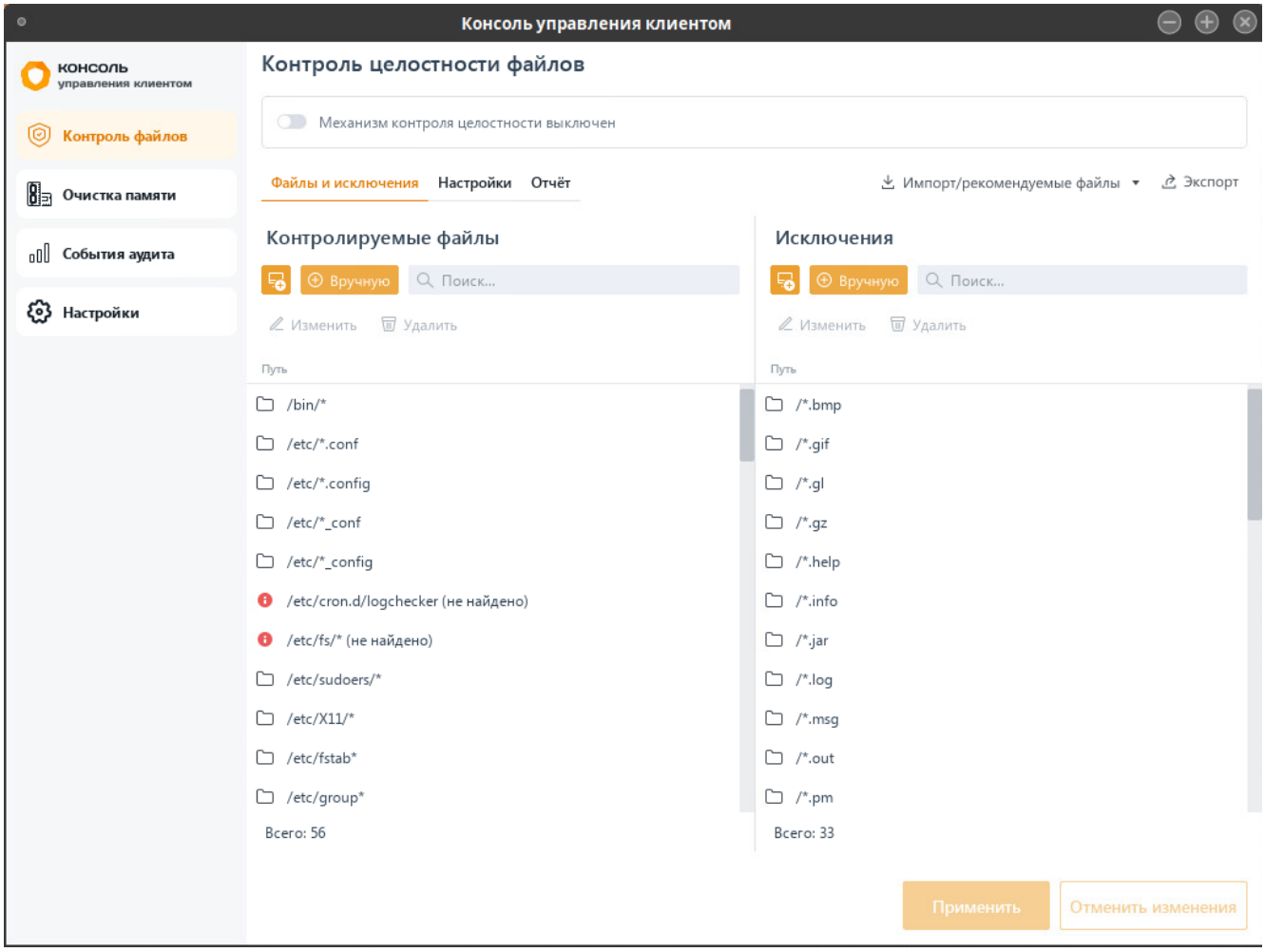


Рисунок 2.3 – Основной интерфейс консоли управления клиентом

3 Удаленное управление клиентом

Удаленное управление клиентской рабочей станцией с помощью сервера СЗИ от НСД «Блокхост-Сеть 4» предполагает возможность дистанционного изменения настроек клиентских рабочих станций под управлением ОС Linux при помощи политик.

Если клиентская рабочая станция взята под управление сервера СЗИ от НСД «Блокхост-Сеть 4», получение параметров механизмов выполняется во время подключения рабочей станции к серверу.

На рабочих станциях под управлением сервера СЗИ от НСД «Блокхост-Сеть 4», параметры и настройки механизмов будут недоступны для редактирования на локальной машине локальному администратору.

Если клиентская рабочая станция находится под управлением сервера «СЗИ от НСД «Блокхост-Сеть 4», вход в консоль управления клиентом невозможен. При попытке входа в консоль появится сообщение, что подключение клиента к консоли управления не поддерживается (рисунок 3.1).

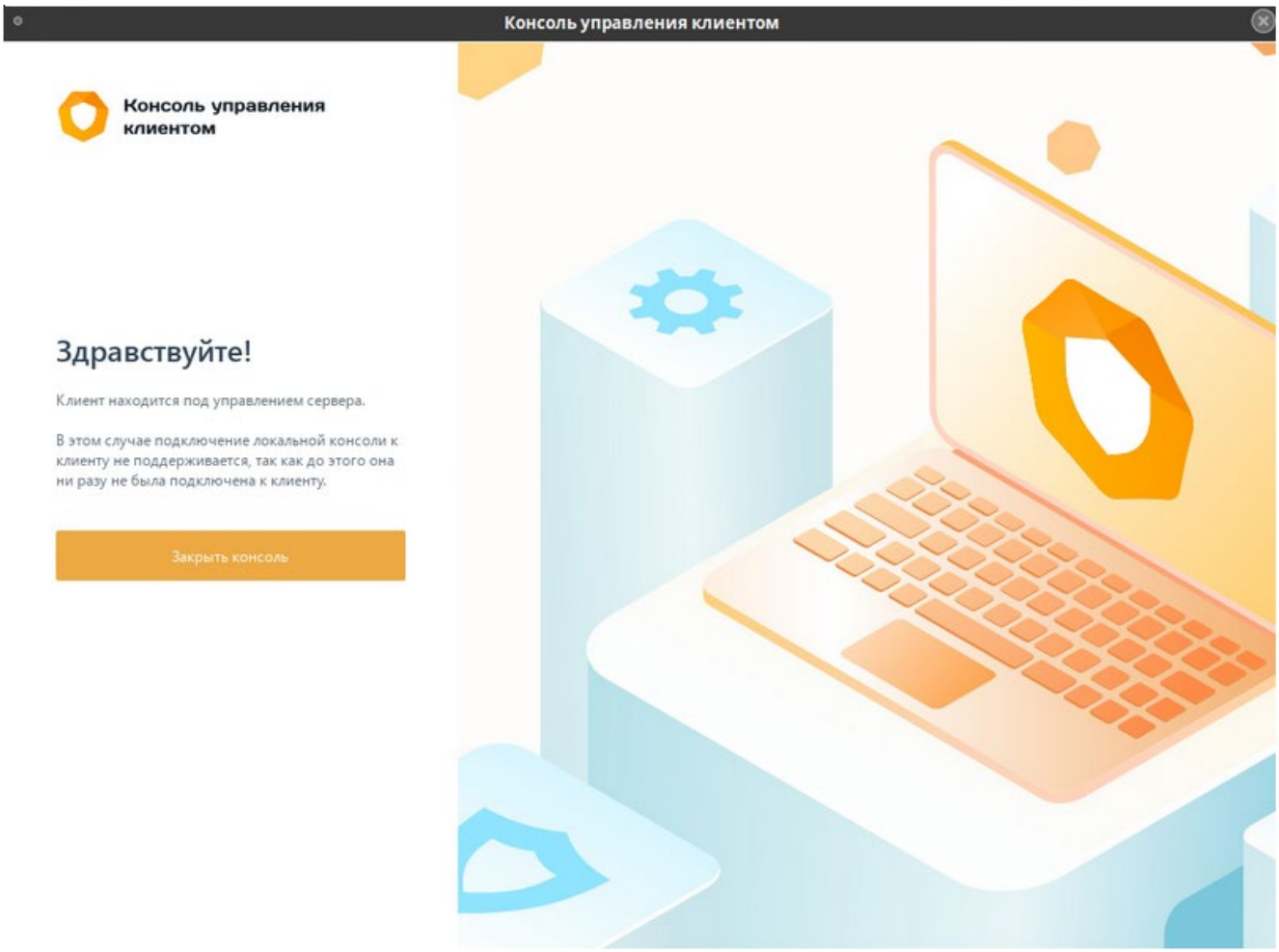


Рисунок 3.1 – Недоступно изменение настроек механизмов рабочей станции

4 Контроль целостности файлов в ОС Linux

«**Контроль целостности файлов»** предназначен для слежения за неизменностью поставленных на КЦ файлов и каталогов загружаемой ОС, а также файлов и каталогов пользователя, целостность которых имеет критическое значение для безопасного функционирования ОС.

Администратор может устанавливать на контроль файлы и каталоги рабочей станции и (или) формировать список исключений файлов и каталогов, контроль целостности которых не будет отслеживаться.

При нарушении целостности файлов и каталогов, установленных на контроль, в случае установки параметра ***Формировать события аудита при нарушении целостности файлов*** в настройках, в журнале аудита фиксируется событие о выявленном нарушении.

4.1 Формирование перечня файлов для постановки на КЦ и списка исключений

Необходимо учитывать, что на контроль целостности могут быть установлены только объекты типа «обычный файл» (S_ISREG). Другие типы файлов игнорируются.

Для постановки файлов на КЦ или формирования списка исключений перейдите во вкладку «**Контроль целостности файлов**» (рисунок 4.1).

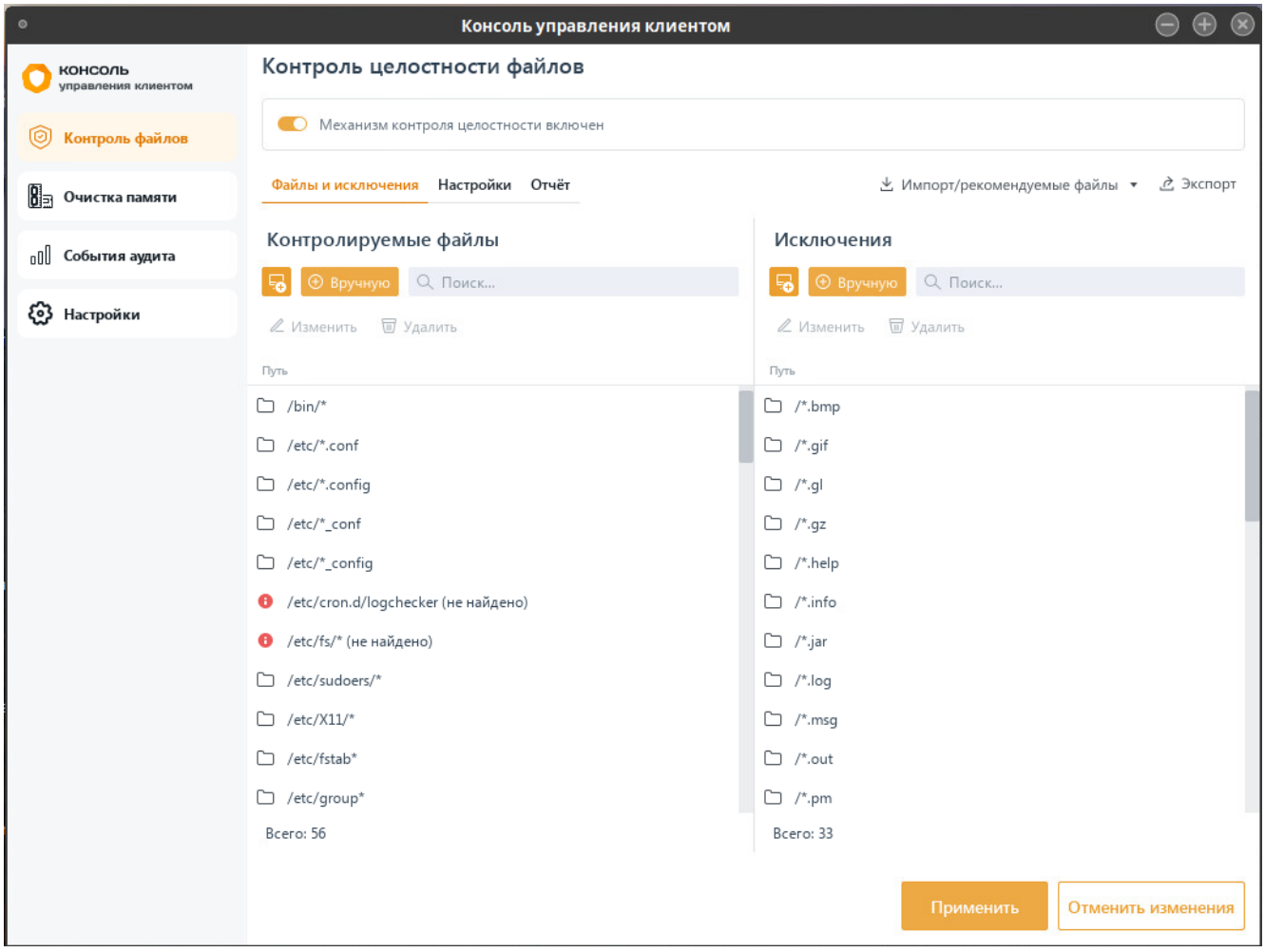


Рисунок 4.1 – Постановка файлов на КЦ/Формирование списка исключений

Включите механизм КЦ файлов, установив переключатель в положение  , и сформируйте перечень файлов и каталогов ОС Linux для постановки на КЦ в левой части вкладки в области ***Контролируемые файлы***, и добавьте файлы и каталоги, которые будут исключены при проверке КЦ, в правой части вкладки в области ***Исключения*** (рисунок 4.2).

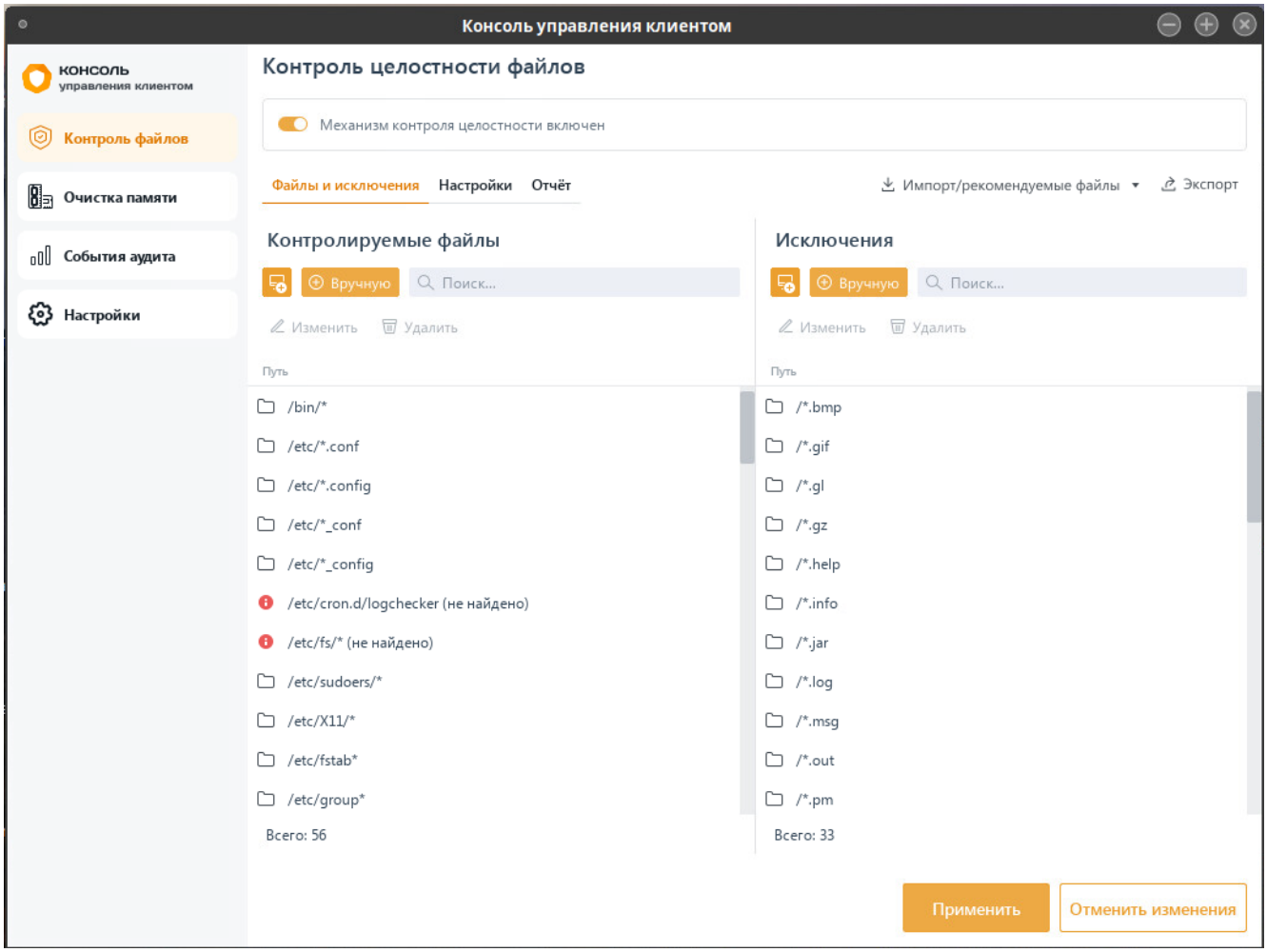


Рисунок 4.2 – Добавление файлов на КЦ/Формирование списка исключений

По умолчанию в области добавления файлов и каталогов на контроль и в области добавления исключений при проверке КЦ уже содержится перечень масок для файлов и каталогов, рекомендуемых к постановке на КЦ. При необходимости каждый пункт в перечне можно изменить или удалить.

Добавление в список файлов для постановки на КЦ/в список исключений возможно несколькими способами:

– вручную по кнопке Вручную, с последующим вводом полного пути к файлу/каталогу (рисунок 4.3) (также доступен ввод масок для файлов и каталогов);

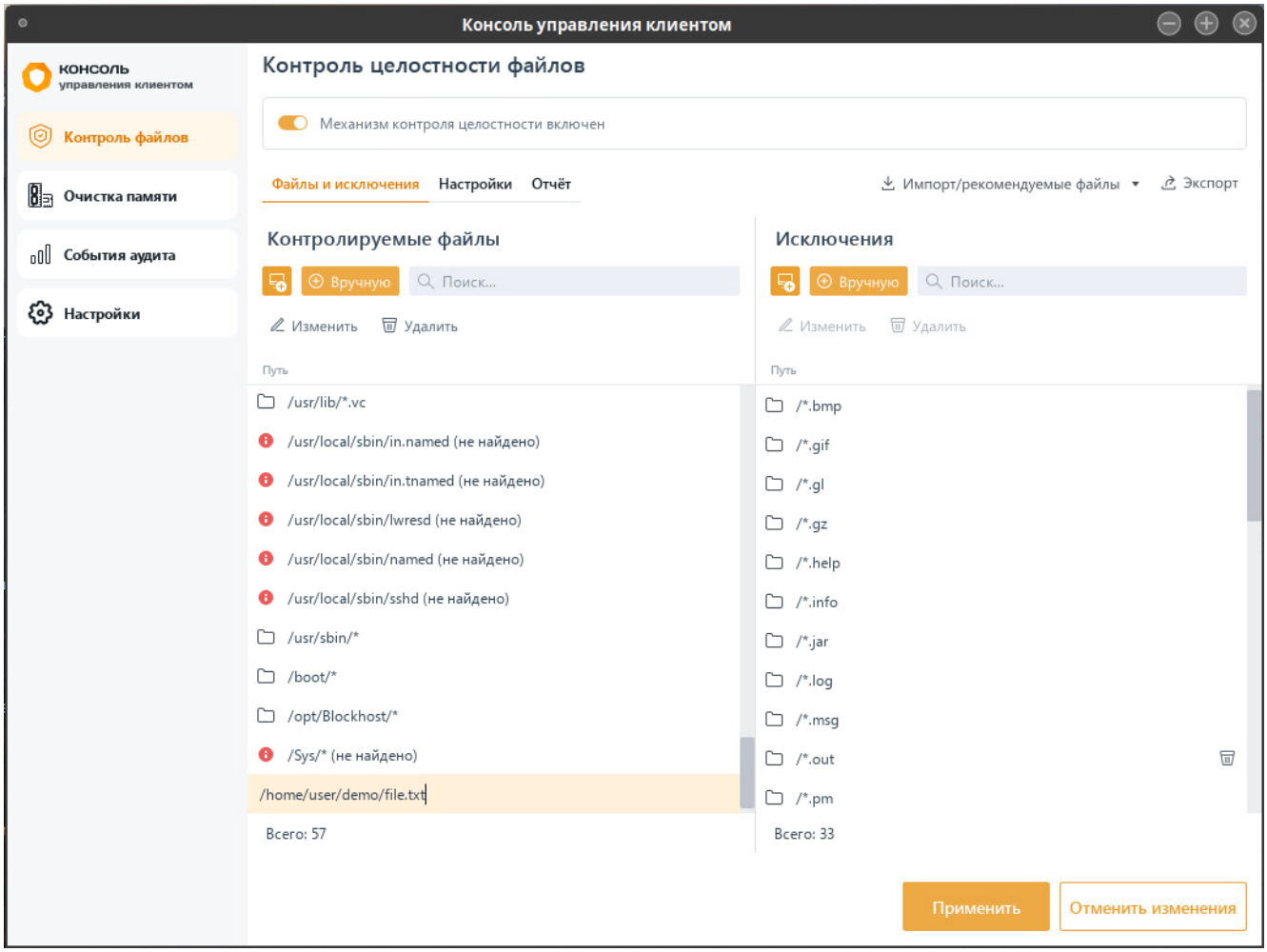


Рисунок 4.3 – Добавление файлов на КЦ/в список исключений вручную

– из файловой системы рабочей станции по кнопке .

При добавлении файла или каталога вручную, если заданный путь не обнаружен на рабочей станции, в строке с указанной директорией появится индикация « » и уточнение, что путь не найден.

4.1.1 Добавление в список файлов для постановки на КЦ/в список исключений из файловой системы

Для добавления в список файлов для постановки на КЦ/в список исключений из файловой системы рабочей станции перейдите по кнопке в окно добавления файлов/каталогов на контроль (рисунок 4.4). В окне добавления директорий/файлов появится файловая система рабочей станции.

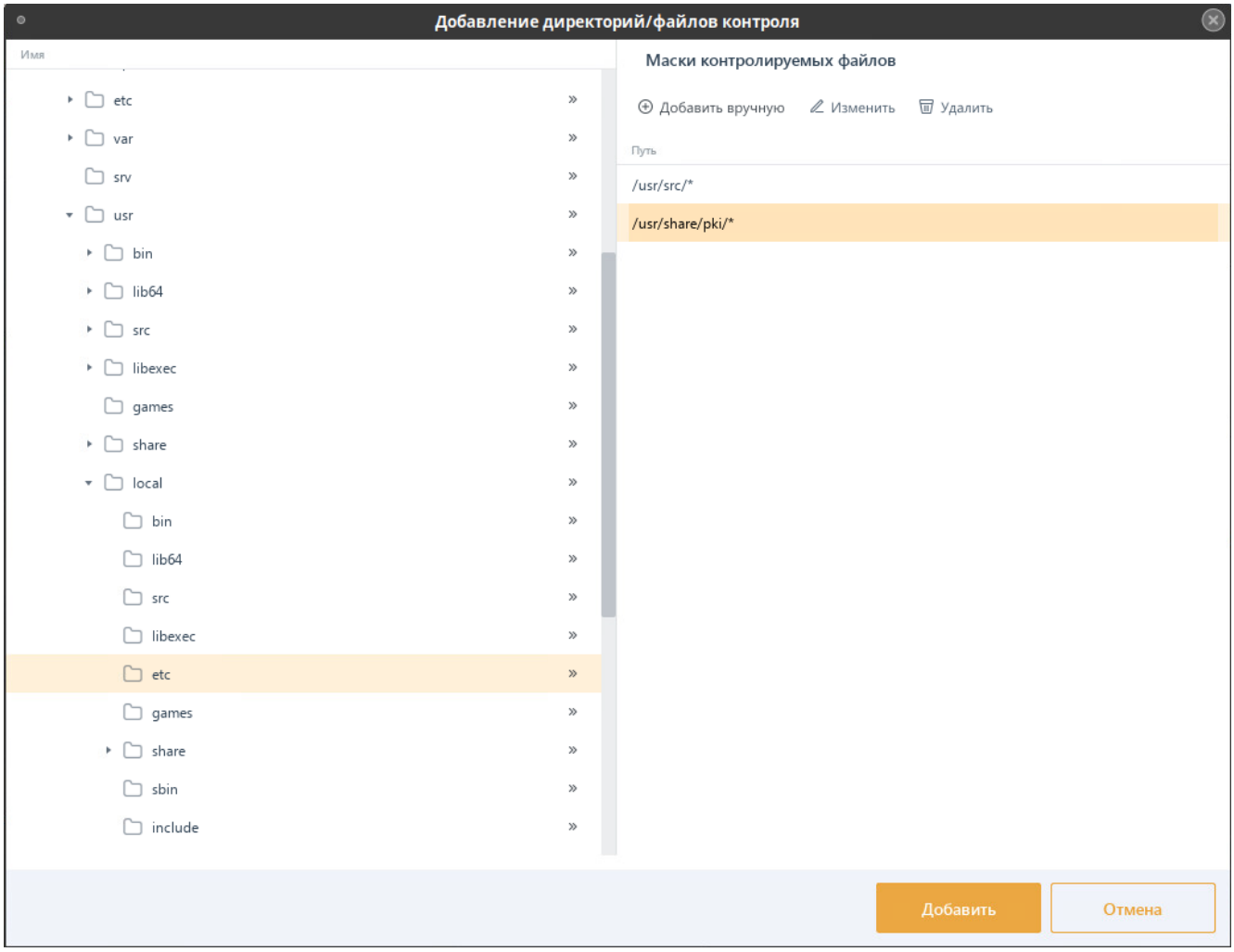


Рисунок 4.4 – Добавление директорий/файлов из файловой системы

Добавьте все файлы/каталоги в правую область окна ***Маски контролируемых файлов*** путем нажатия » в строке требуемого к установке файла/каталога.

В правой области окна ***Маски контролируемых файлов*** можно изменять уже добавленные маски контролируемых файлов по кнопке Изменить или добавлять маски вручную.

После нажатия ***Добавить*** в перечне файлов для постановки на КЦ/исключений появятся объекты, добавленные из всех файловых систем рабочих станций (рисунок 4.3).

4.2 Формирование отчета при выявлении нарушений КЦ

При необходимости просмотра выявленных изменений в файлах и каталогах, установленных на контроль, перейдите во вкладку ***Отчет*** (рисунок 4.5).

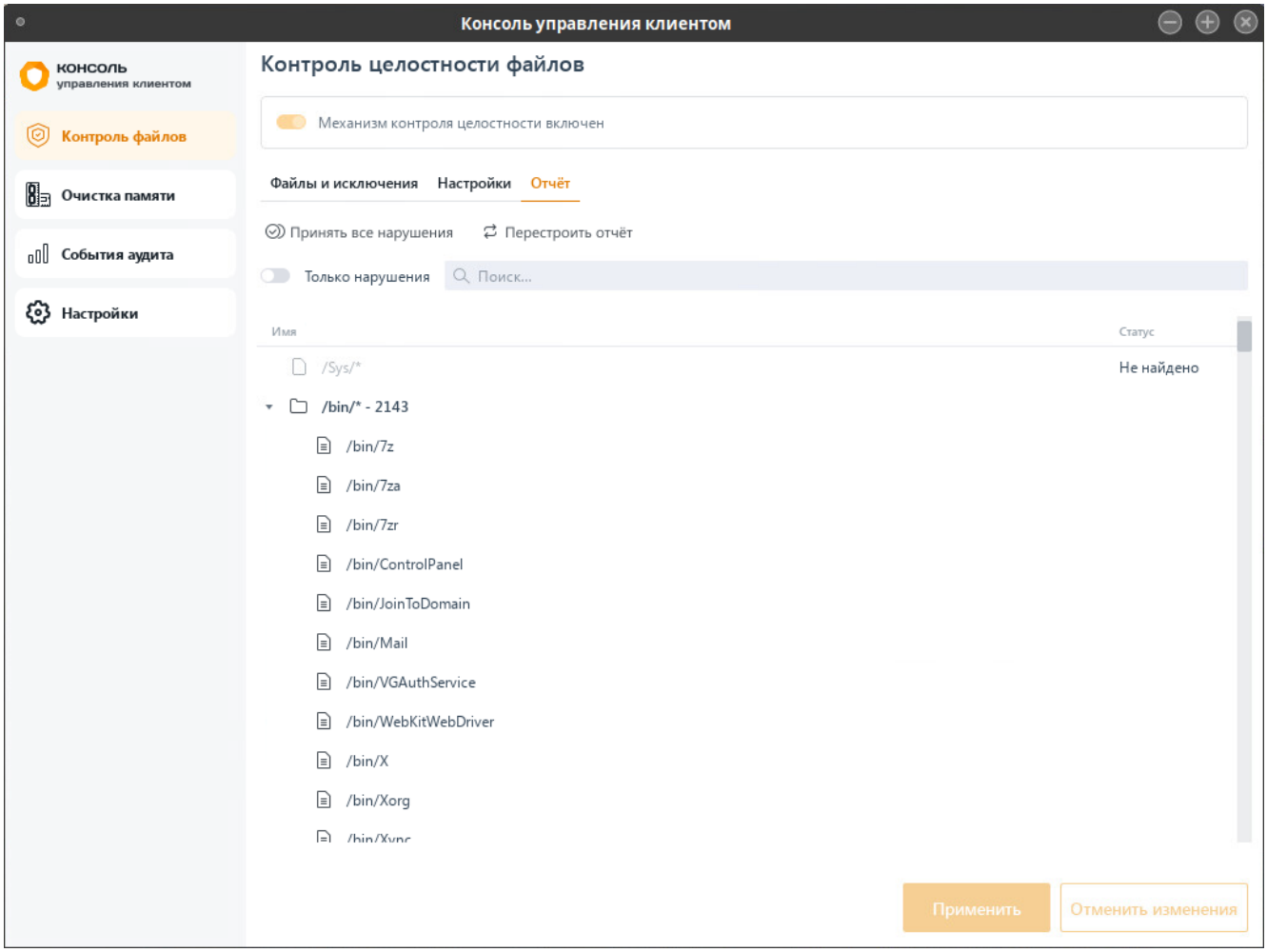


Рисунок 4.5 – Вкладка ***Отчет***

Во вкладке ***Отчет*** отображаются все файлы, установленные на контроль, с учетом каталогов, масок файлов и исключений, добавленных в перечень во вкладке ***Файлы и исключения***.

При обнаружении нарушений в поставленных на контроль файлах и каталогах отчет будет обновлен с периодичностью, установленной во вкладке ***Настройки*** в параметре ***Выполнять построение отчета каждые (часы:минуты)*** (рисунок 4.8).

Для внепланового обновления отчета воспользуйтесь кнопкой Перестроить отчёт (рисунок 4.5).

После обновления отчета в перечне файлов и каталогов, поставленных на контроль, отобразятся все выявленные нарушения целостности (рисунок 4.6).

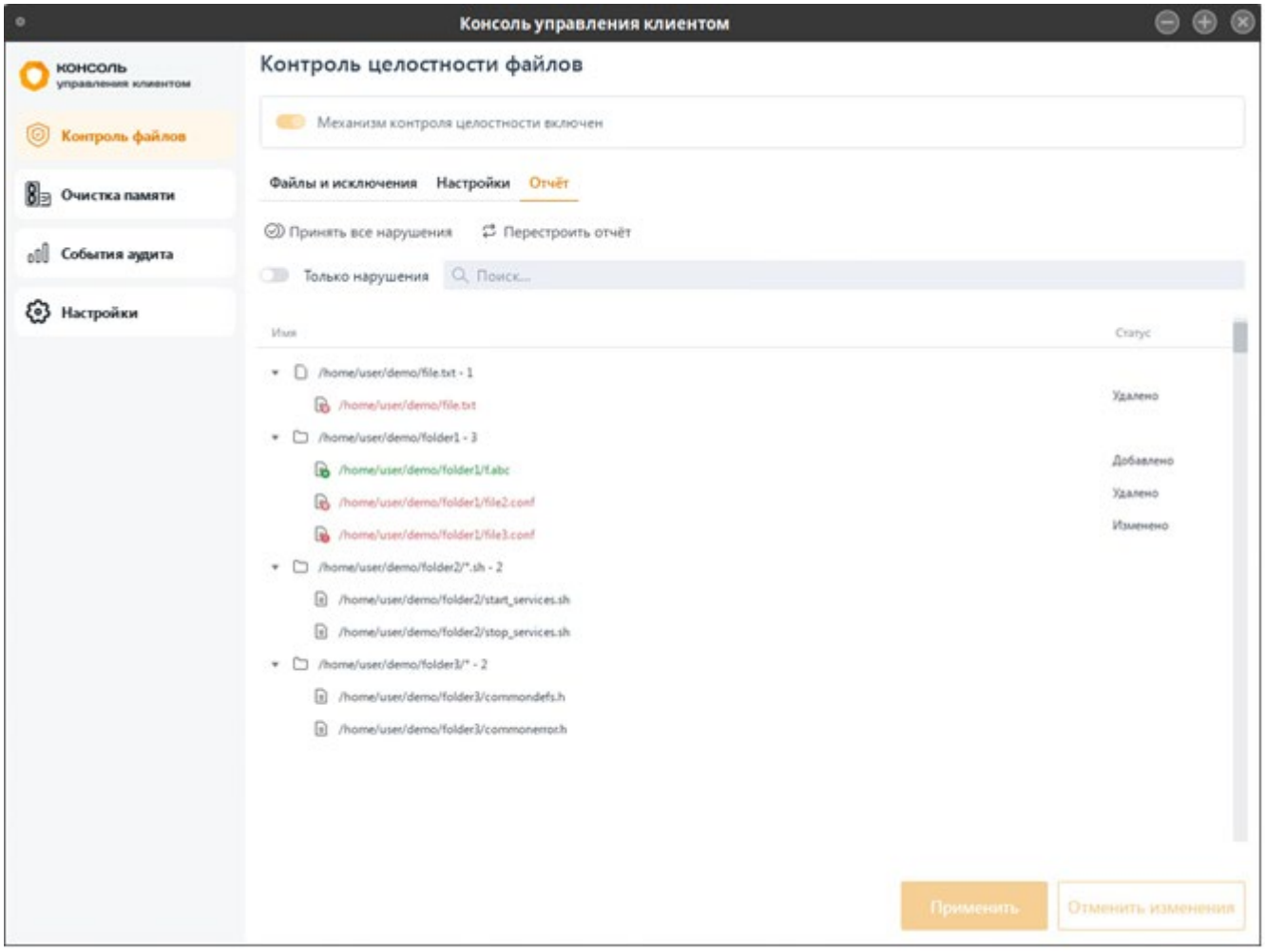


Рисунок 4.6 – Выявление нарушений контроля целостности

Если выявленные нарушения целостности согласованы и не имеют критического значения для безопасного функционирования ОС, администратор может принять изменения по кнопке Принять все нарушения (рисунок 4.7).

При этом контрольные суммы объектов, поставленных на контроль, будут пересчитаны, и слежение за контролем целостности данных объектов будет продолжено до момента исключения их из списка.

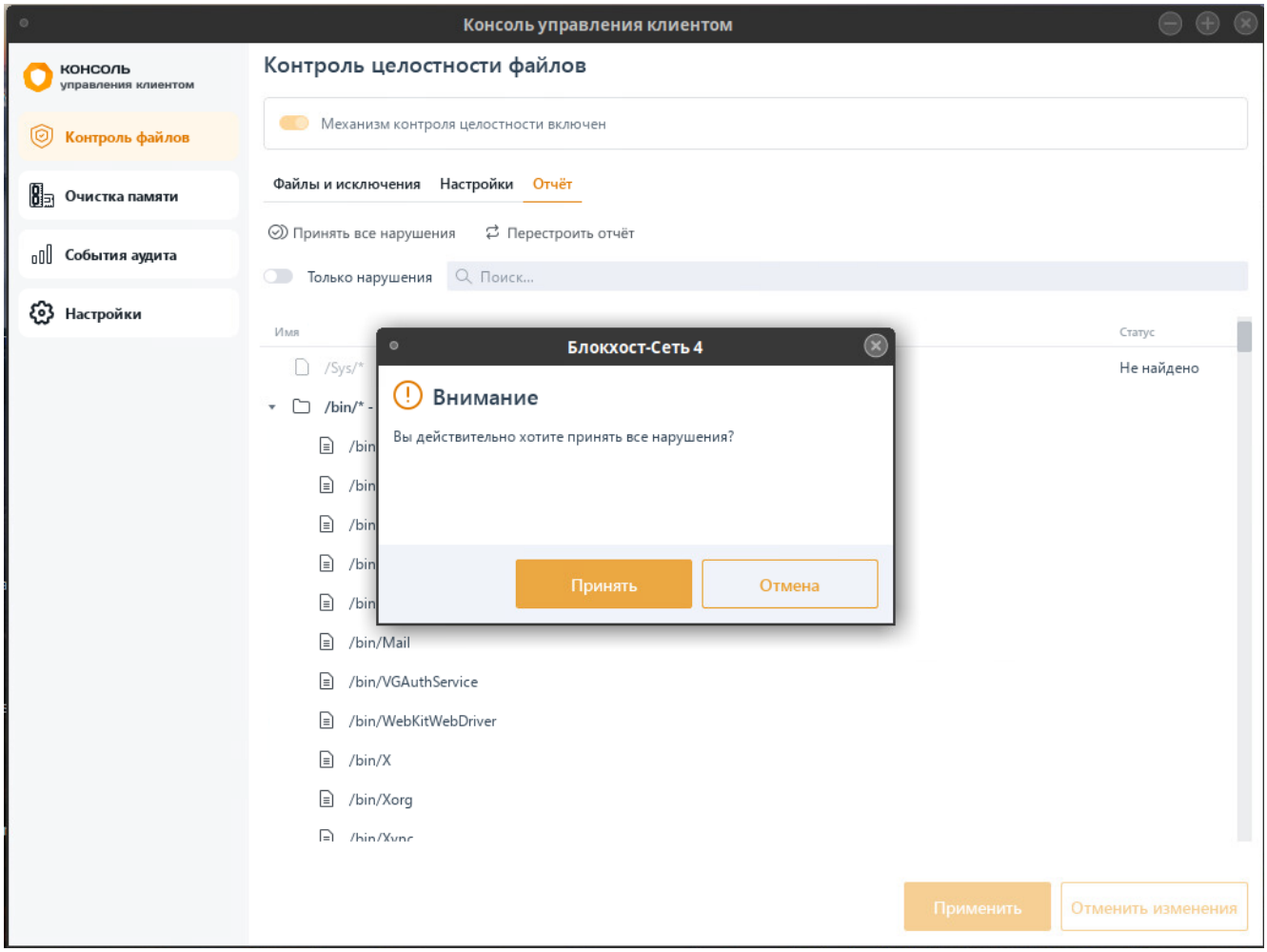


Рисунок 4.7 – Принятие нарушений и пересчет контрольных сумм объектов

4.3 Настройки контроля целостности файлов в ОС Linux

Во вкладке ***Настройки*** доступно изменение периодичности проверки целостности файлов, установленных на контроль, и настройка формирования событий аудита при нарушении целостности (рисунок 4.8).

Задайте периодичность проверки целостности файлов, установив время в параметре ***Выполнять построение отчета каждые (часы:минуты)***. По умолчанию проверка целостности осуществляется каждые 2 часа.

При необходимости фиксировать в журнале аудита выявленные изменения в контролируемых файлах, установите параметр ***Формировать события аудита при обнаружении изменения файлов.***

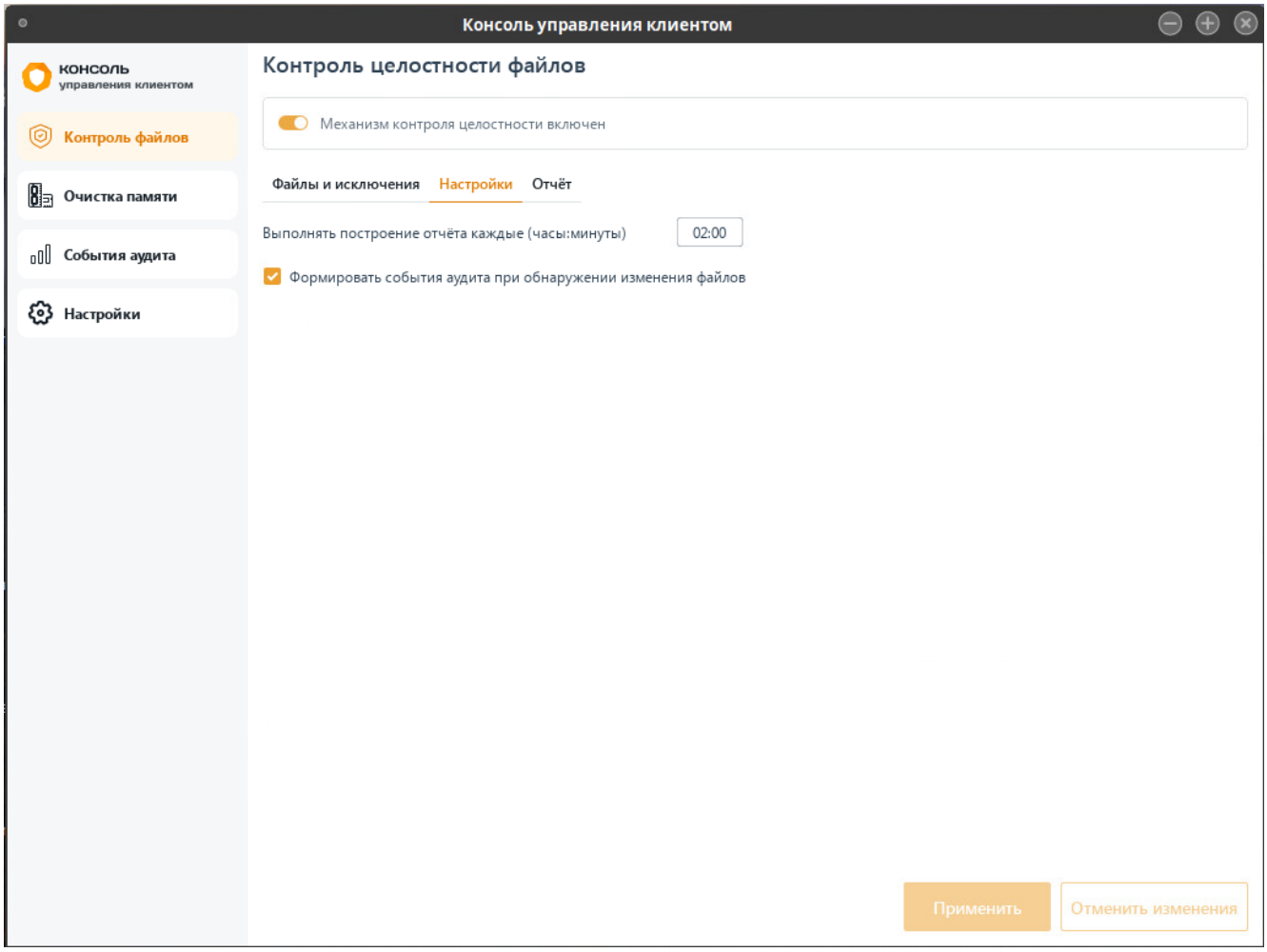


Рисунок 4.8 – Настройки контроля целостности файлов в ОС Linux

5 Очистка памяти в ОС Linux

Механизм очистки оперативной памяти доступен только для РЕД ОС.

Необходимо учитывать, что механизм очистки памяти поддерживает символьные ссылки (SymLink) только на пакет и файл. SymLink на объекты, заданные масками не поддерживаются.

Очистка памяти выполняется с целью удаления остаточной информации после завершения поставленных на контроль процессов.

Процесс перезаписи оперативной памяти происходит по следующей схеме: по окончании работы контролируемого процесса механизм очистки памяти производит захват всей свободной оперативной памяти, включая и область, освобожденную контролируемым процессом. Захваченные области оперативной памяти перезаписываются маскирующими данными. По мере перезаписи механизм очистки высвобождает перезаписанную область.

Если ОС имеет поддерживаемое СЗИ ядро, после установки клиента Блокхост-Сеть и включения механизма очистки памяти, проверка работы механизма очистки памяти будет фиксироваться в журнале событий аудита.

Если ОС имеет не поддерживаемое СЗИ ядро после установки клиента Блокхост-Сеть возможны следующие ситуации:

– механизм очистки памяти выключен – события механизма очистки памяти не фиксируются в журнале событий аудита;

– механизм очистки памяти включен – в журнале событий аудита фиксируется сообщение от механизма очистки памяти о несовместимом ядре;

– механизм очистки памяти включен – установка клиента Блокхост-Сеть производилась на поддерживаемом СЗИ ядре, но при очередном обновлении ОС обновилась до не поддерживаемого ядра, в журнале событий аудита фиксируется сообщение от механизма очистки памяти о несовместимом ядре.

5.1 Формирование перечня файлов и списка исключений

Для настройки параметров механизма очистки оперативной памяти перейдите во вкладку **«Очистка памяти»** (рисунок 5.1).

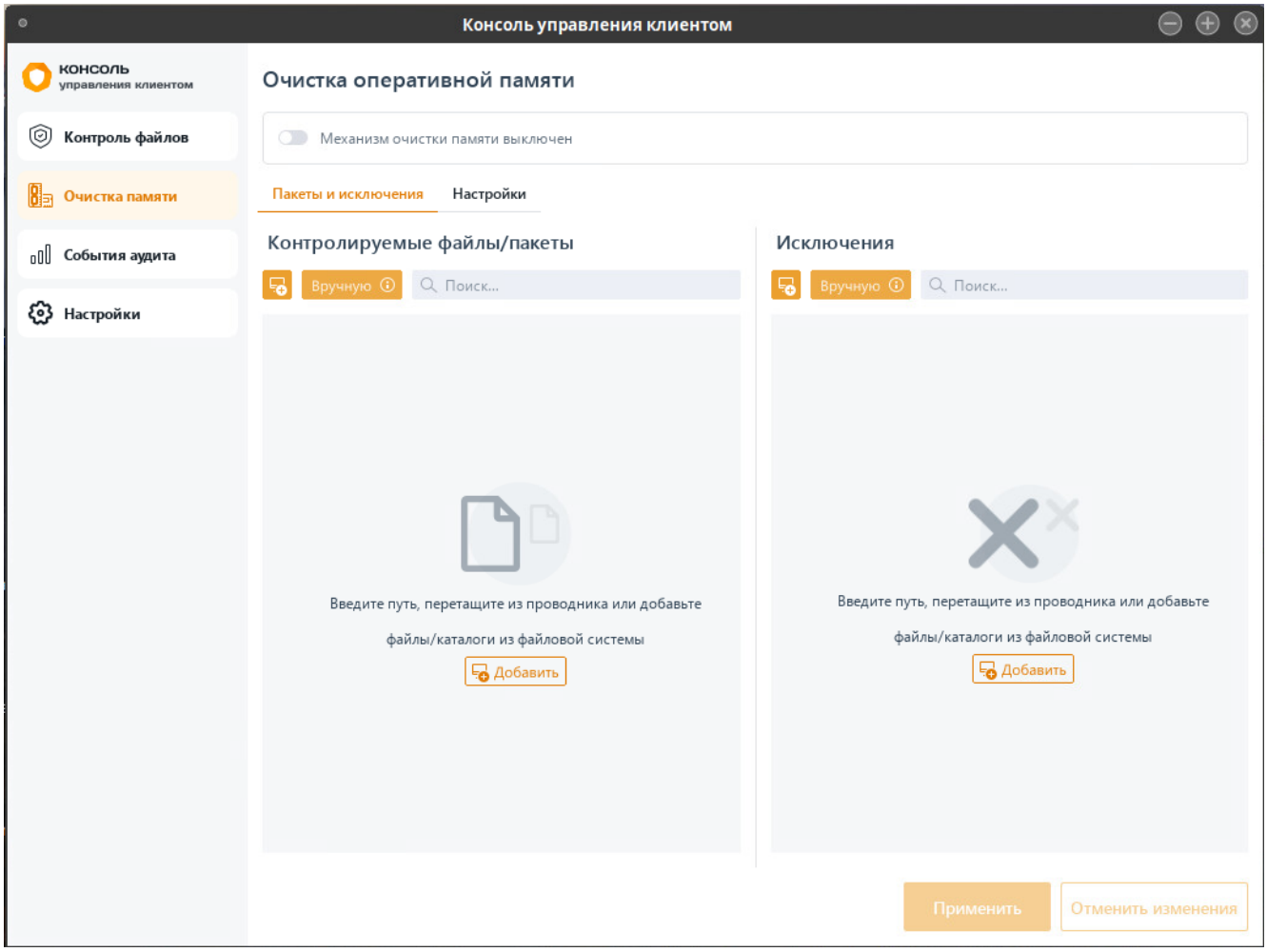


Рисунок 5.1 – Механизм очистки оперативной памяти

Включите механизм очистки оперативной памяти, установив переключатель в положение 

, и сформируйте перечень файлов/пакетов ОС Linux с целью удаления остаточной информации после завершения поставленных на контроль процессов в левой части вкладки, и добавьте файлы/пакеты, которые будут исключены при удалении остаточной информации, в правой части вкладки в области ***Исключения*** (рисунок 5.1).

Добавление файлов/пакетов в список контролируемых файлов/в список исключений возможно несколькими способами:

– вручную по кнопке 

, с последующим вводом полного пути к файлу/пакету (также доступен ввод масок):

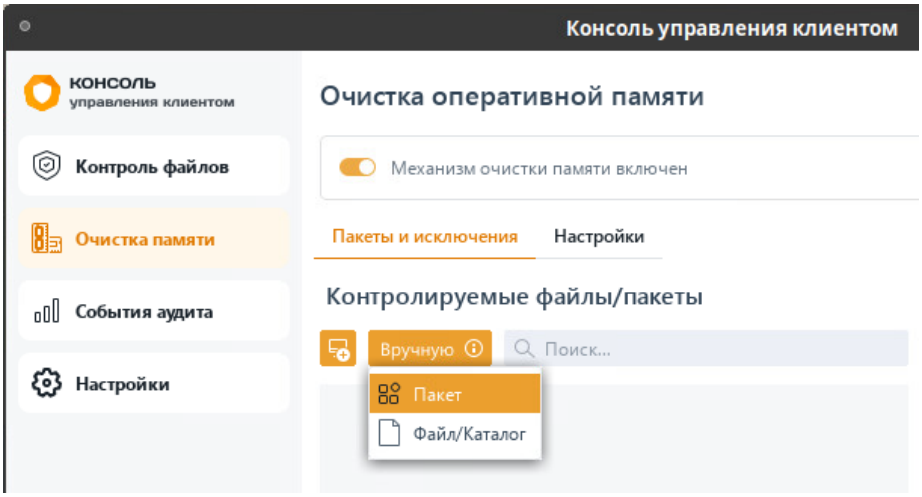


Рисунок 5.2 – Добавление вручную файла или пакета

При ручном вводе допускается применение следующих масок:

* – любое количество любых символов;
? – любой одиночный символ;
\ – символ-исключение (при этом в маске «*», символ «*» будет являться именно символом, а не маской).

– из файловой системы одной или нескольких удалённых клиентских рабочих станций под управлением ОС Linux по кнопке  с выбором:

- добавления в список из файловой системы клиентских рабочих станций под управлением ОС Linux (описано в разделе ***Добавление в список файлов для постановки на КЦ/в список исключений из файловой системы***);
- добавления в список пакетов клиентских рабочих станций под управлением ОС Linux.

5.1.1 Добавление пакетов в список файлов/в список исключений из файловой системы клиентских рабочих станций

Для добавления пакетов в список файлов/в список исключений из файловой системы рабочей станции перейдите по кнопке  в окно добавления файлов/пакетов на контроль во вкладку ***Пакеты*** (рисунок 5.3).

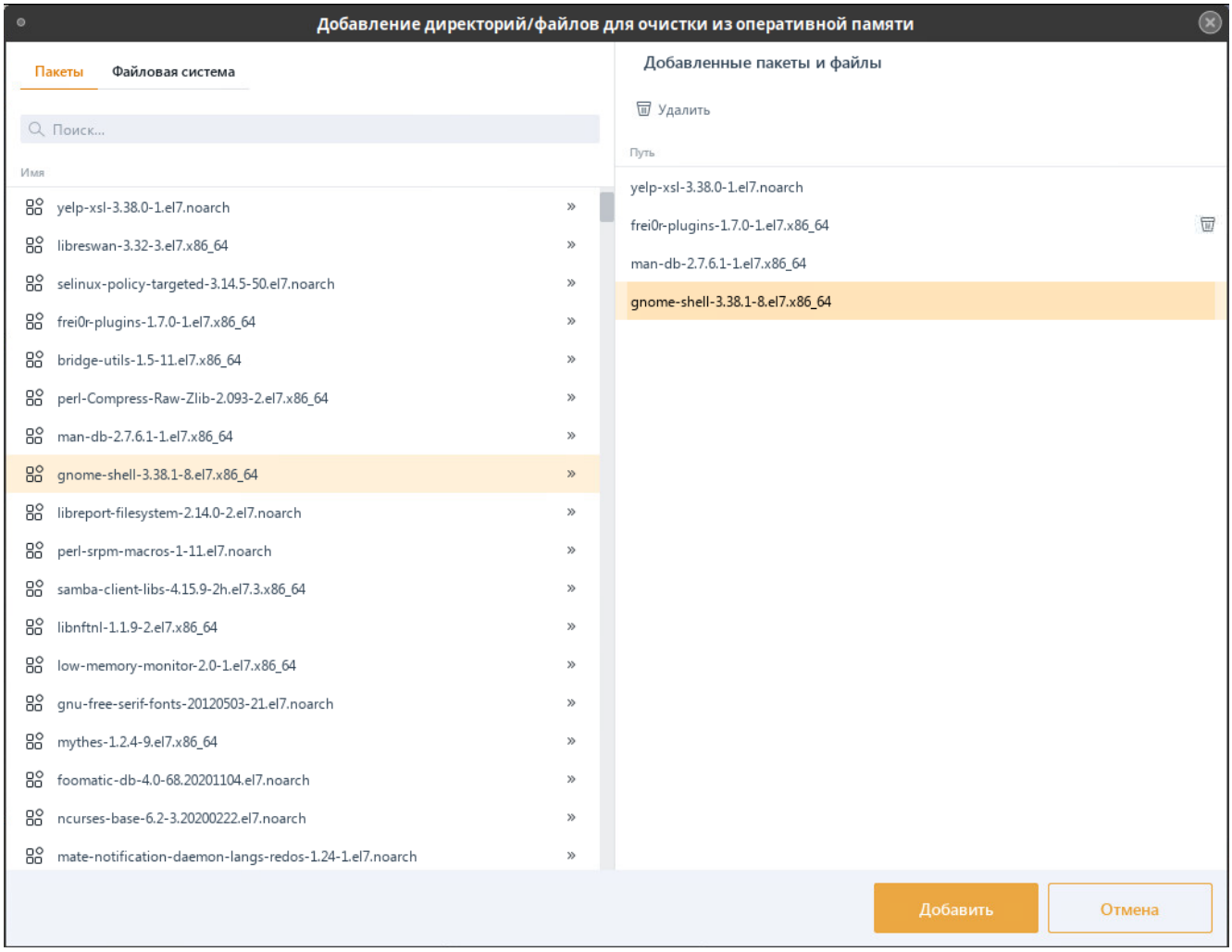


Рисунок 5.3 – Добавление пакетов/файлов из файловой системы

Добавьте все пакеты в правую область окна ***Добавленные пакеты и маски*** путем нажатия » в строке требуемого к установке пакета.

После нажатия ***Добавить*** в перечне файлов для постановки на КЦ/исключений появятся объекты, добавленные из всех файловых систем рабочих станций (рисунок 5.4).

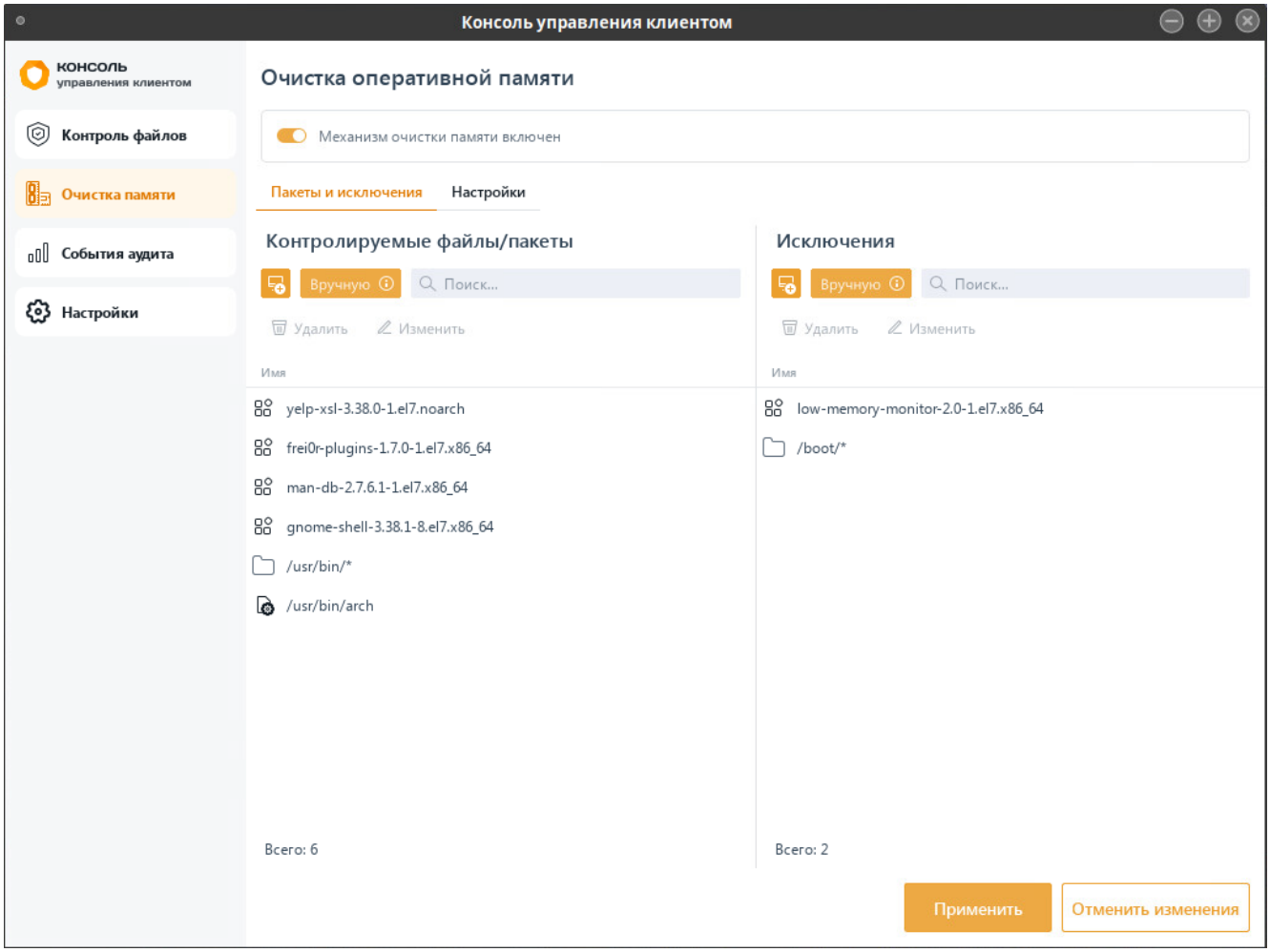


Рисунок 5.4 – Добавленные на контроль очистки памяти объекты

5.2 Настройки очистки памяти в ОС Linux

Во вкладке ***Настройки*** доступна настройка формирования событий аудита при очистке памяти (рисунок 5.5).

При необходимости фиксировать в журнале аудита события, поставленные на контроль при очистке памяти, установите параметр ***Формировать события аудита.*** При этом для дочерних процессов память будет очищаться, но события формироваться не будут.

Для формирования событий аудита при очистке памяти дочерних процессов контролируемых файлов установите параметр ***Формировать события аудита при очистке памяти для дочерних процессов.***

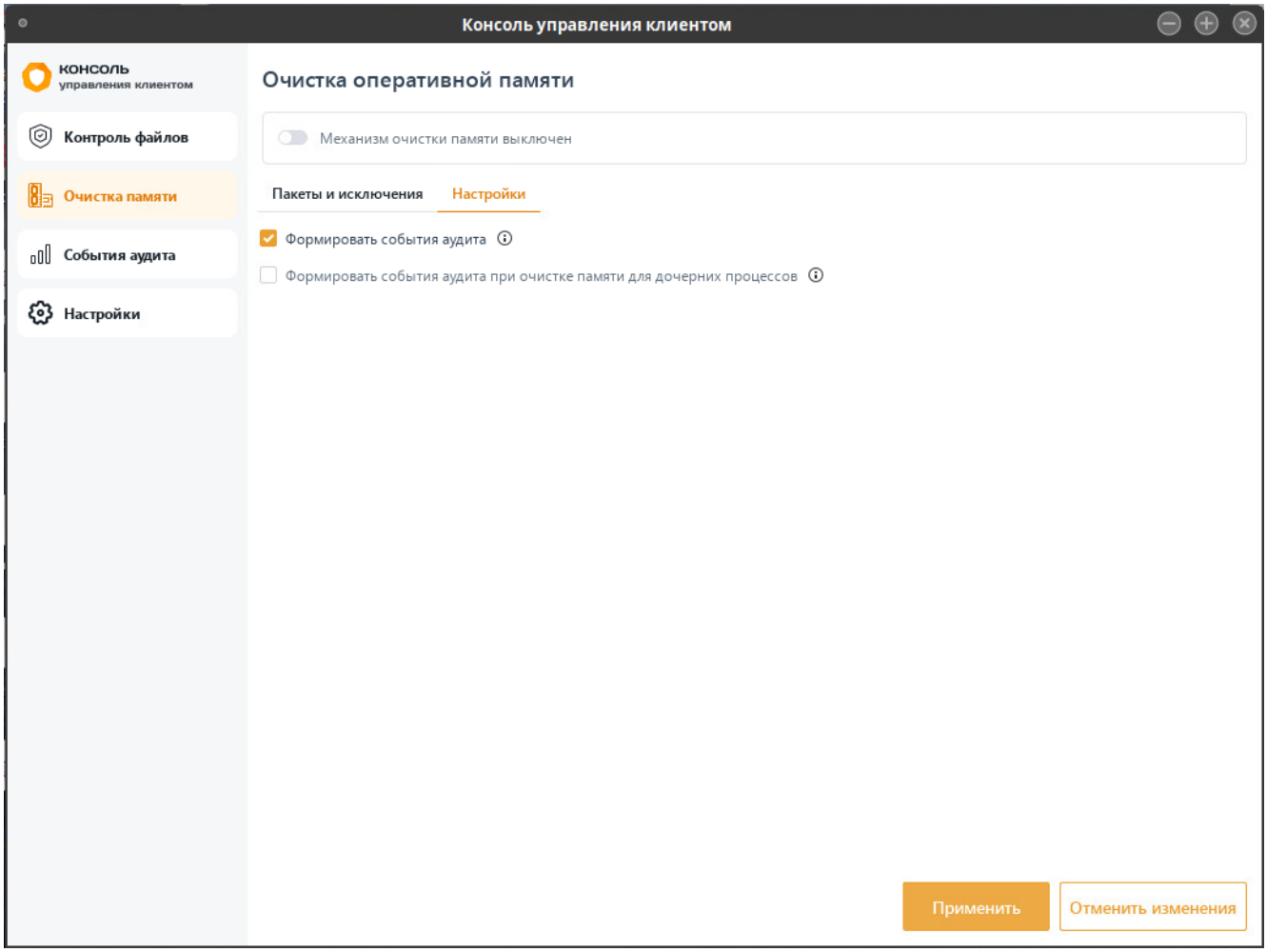


Рисунок 5.5 – Настройки очистки памяти

6 События аудита

Сбор событий аудита предназначен для сбора событий аудита с рабочей станции, формирования сводного отчета, просмотра и фильтрации событий аудита.

Вкладка ***События аудита*** предназначена для отслеживания событий на рабочей станции (рисунок 6.1). В верхней части вкладки доступны параметры для фильтрации всех событий по заданным значениям.

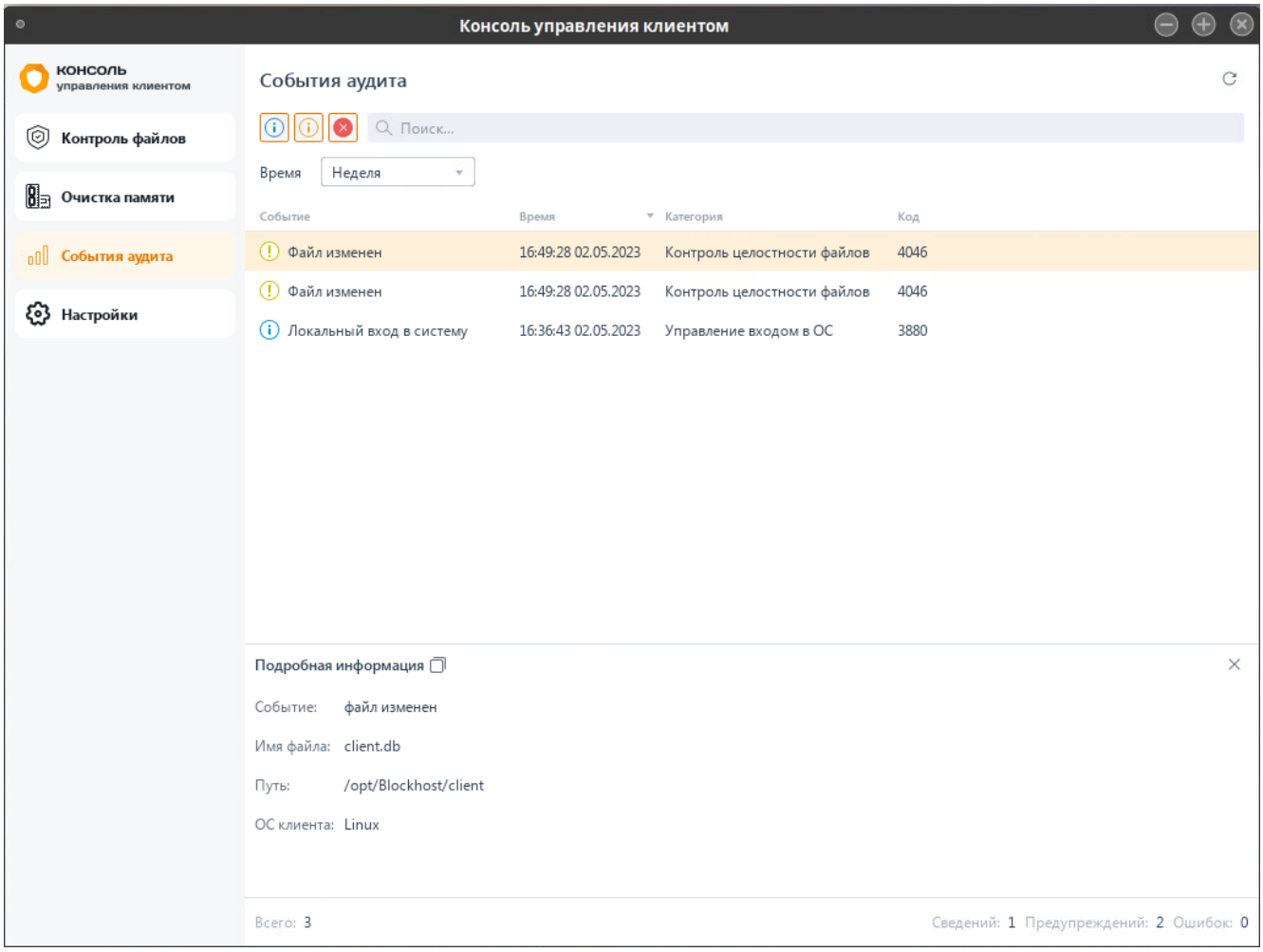


Рисунок 6.1 – События аудита

В списке событий содержится информация:

– ***Уровень важности*** – уровень важности зафиксированного события (сведения, предупреждения или ошибка);

– ***Событие*** – краткое описание зафиксированного события (полный перечень фиксируемых событий приведен в Приложении 1 к настоящему документу);

– ***Время*** – дата и время момента фиксации произошедшего события;

– ***Категория*** – категория, которой принадлежит зафиксированное событие;

– ***Код*** – код события.

Возможно отфильтровать события аудита по следующим параметрам:

– ***По уровню важности*** – выборка событий по уровню важности ;

– ***По времени*** – выборка событий за определенный период времени:

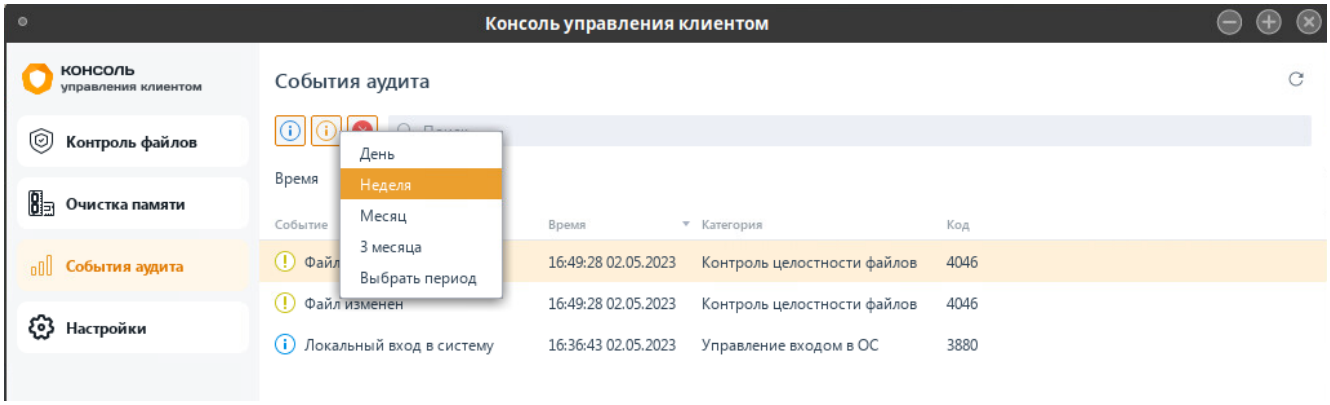


Рисунок 6.2 – Фильтр по времени

При выборе фильтра по времени ***Выбрать период*** (рисунок 6.2) вводится дата и время начала выборки событий и вводится дата и время окончания выборки (рисунок 6.3).

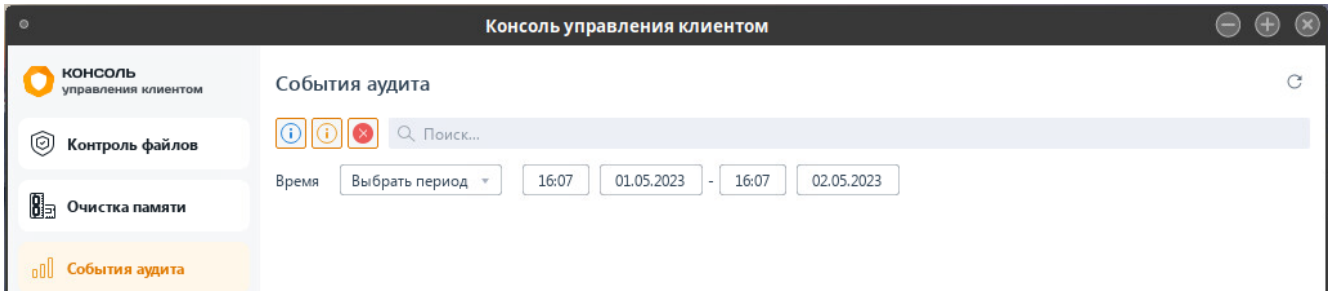


Рисунок 6.3 – Фильтр по времени ***Выбрать период***

7 Настройки доступа к консоли управления клиентом

Для добавления учетных записей пользователей, которым будет предоставлен доступ к настройкам механизмов с помощью консоли управления клиентом, перейдите во вкладку ***Доступ к приложению*** (рисунок 7.1).

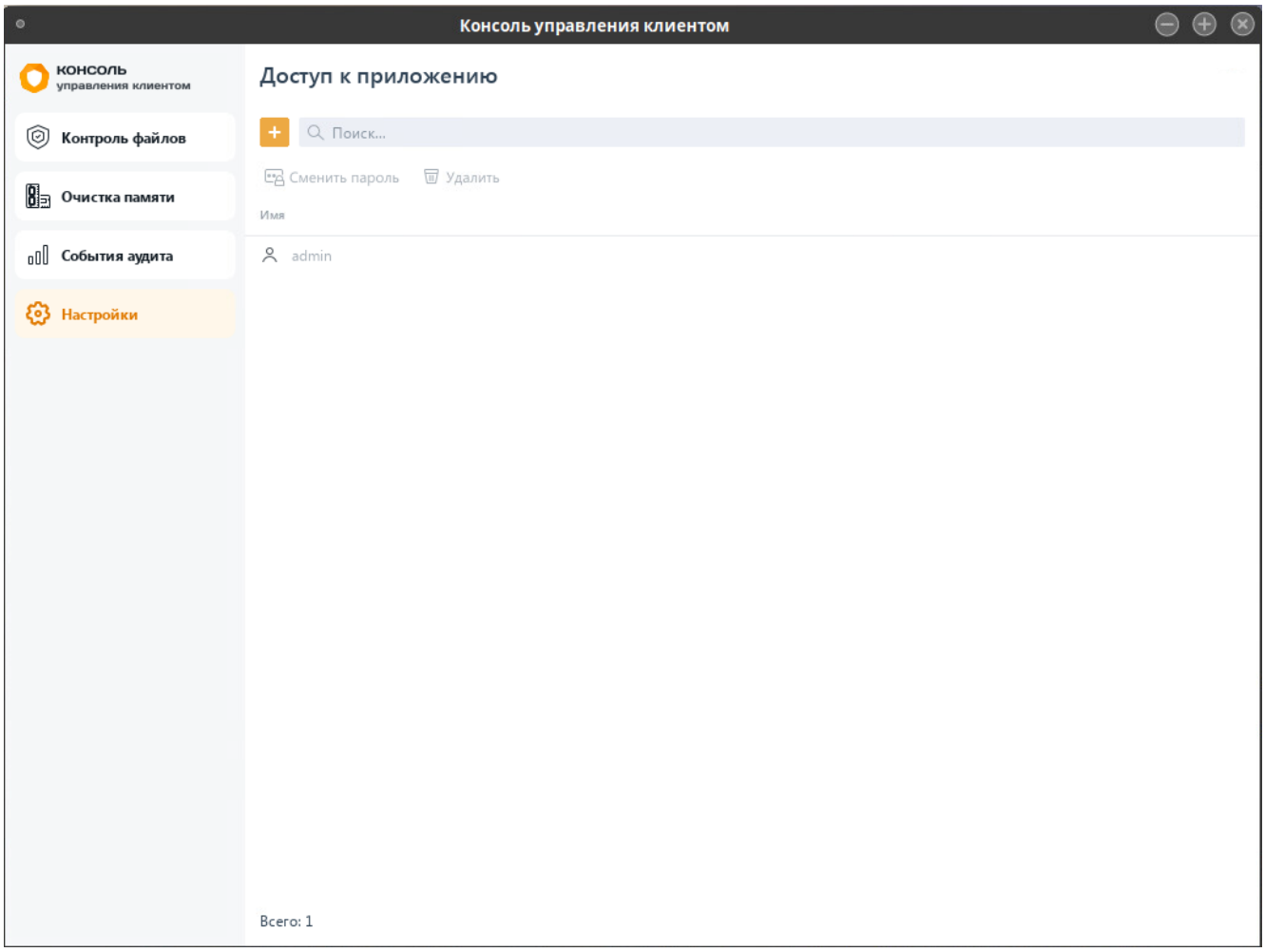


Рисунок 7.1 – Настройка доступа к консоли управления клиентом

Во вкладке отображен перечень учетных записей пользователей, имеющих доступ к настройкам механизмов консоли управления клиентом.

По умолчанию после установки консоли в перечень учетных записей добавляется пользователь: имя пользователя ***«admin»*** с заданным при первом входе в консоль паролем. Данная учетная запись может быть удалена или изменена администратором.

Для добавления новой учетной записи нажмите кнопку  и введите в появившемся окне (рисунок 7.2):

– имя учетной записи пользователя (ограничения, которые необходимо учитывать при задании имени, приведены ниже);

– пароль для доступа пользователя к консоли (ограничения, которые необходимо учитывать при задании пароля, приведены ниже);

– повторите ввод введенного пароля.

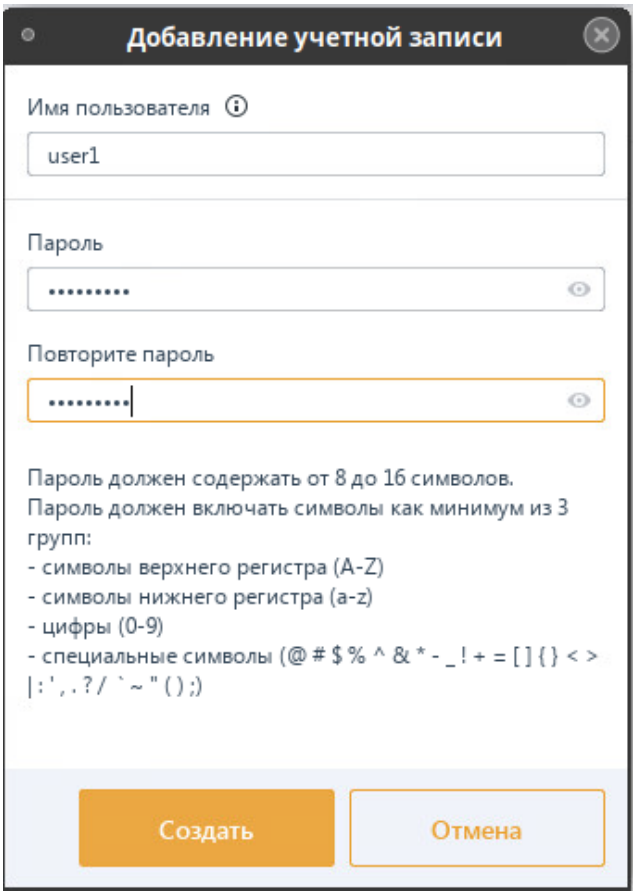


Рисунок 7.2 – Добавление учетной записи пользователя

Необходимо учитывать следующие ограничения:

– ***имя пользователя*** должно содержать от 3 до 30 символов. Не должно содержать пробелы, специальные символы @ # $ % ^ & * ! + = ( ) [ ] { } < > | : ' , / \ ` ~ ; ", несколько точек подряд;

– ***пароль*** должен содержать от 8 до 16 символов. Сложность пароля учетных записей пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля (пароль должен включать символы как минимум из 3 групп):

Заглавные буквы	A…Z	26
Строчные буквы	a…z	26
Цифры	0…9	10
Специальные символы	@ # $ % ^ & * - _ ! + = [ ] { } < > | : ` , . ? / ‘ ~ ( ) ; “	31

8 Подсистема ГУПТ

8.1 Запуск подсистемы ГУПТ

Для начала работы необходимо выполнить запуск подсистемы ГУПТ под учетной записью администратора с помощью команды ***sudo***.

Запуск подсистемы ГУПТ без параметров невозможен:

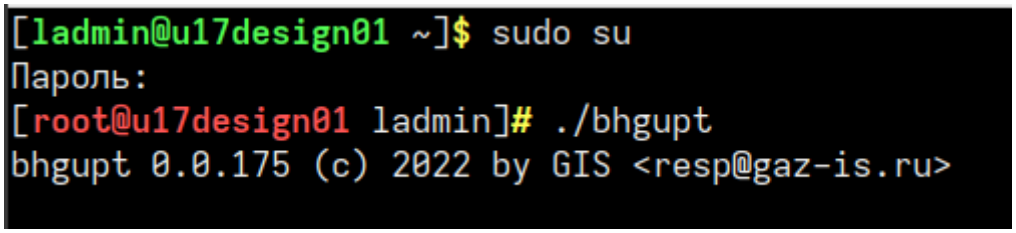


Рисунок 8.1 – Запуск подсистемы ГУПТ

Команды подсистемы ГУПТ позволяют выполнять следующие действия:

- формировать список файлов и папок, подлежащих гарантированному удалению;
- определять размер псевдослучайной последовательности символов, которыми будут заполняться кластеры носителей информации при выполнении гарантированного удаления;
- гарантированно удалять выбранные файлы и папки;
- гарантированно очищать (заполнять псевдослучайной последовательностью символов) свободное пространство разделов жестких дисков.

В данной версии поддерживается работа с файловыми системами EXT 2/3/4, FAT 12/16/32 и exFAT.

8.2 Команды подсистемы ГУПТ

Синтаксис подсистемы ГУПТ имеет следующий вид:

```
Синтаксис: bhgupt [опции] [force]/[noforce] пути к файлу(ам) и/или каталогу(ам) etc.
```

```
bhgupt [-опция] [-параметр] <полный путь к файлу>/
<полный путь к файлу 2>…<полный путь к файлу N> /
<полный путь к папке>
```

Опции команды *bhgupt* необходимо вводить с учетом регистра.

Команду можно применять сразу к нескольким объектам, указав их через пробел или к директории с объектами.

Особенности применения:

1) В опции `[-a]` в качестве параметра можно указать имя файла, в который будет выводится журнал. В случае указания параметра `[none]` вывод аудита будет отключен.
2) Опция `[-H]` используется в комбинации с параметром *[force]\[noforce]*.
3) В опции `[-d]` в качестве параметра необходимо указать точку монтирования раздела.
4) В опции `[-D]` в качестве параметра необходимо указать точку монтирования раздела.
5) В опции `[-f]` в качестве параметра необходимо указать путь к файлу, в котором перечислены пути к файлам и каталогам.
6) В опции `[-l]` в качестве параметра необходимо указать путь к файлу лога.
7) В опции `[-n]` в качестве параметра необходимо указать количество проходов затирания.
8) В опции `[-s]` в качестве параметра необходимо указать путь к файлу со случайной последовательностью.

В подсистеме ГУПТ доступны следующие команды:

- *bhgupt <путь к файлу>* – гарантированное удаление файлов/папок;

Например:

```
[root@u17design01 ladmin]# ./bhgupt ./file1.txt
Тип: Файл Время: 25/5/2023 10:46:5  Имя пользователя: root Объект:
 ./file1.txt Результат: Успех Описание: Файл ./file1.txt удален.


Working time : 3 sec.
```

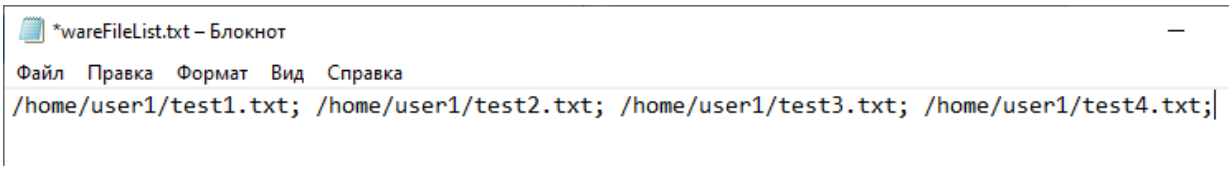
Рисунок 8.2 – Пример команды подсистемы ГУПТ

Параметры команды *bhgupt*:

- `-a` – (audit) настройка политики аудита. По умолчанию осуществляется вывод в консоль. Если в опции указать параметр [none], то вывод осуществляться не будет. При необходимости вывода в отдельный файл нужно указать в параметрах имя файла;

- `-b` – (block level) гарантированное удаление объектов на уровне блочных устройств;
- `-c` – (clear-attributes) сброс атрибутов, защищающих объект файловой системы;
- `-d` – (device free space) затирание свободного пространства на указанном устройстве. В опции необходимо указать точку монтирования раздела;
- `-D` – (device-root-block) затирание блоков, зарезервированных для суперпользователя на устройстве. В опции необходимо указать точку монтирования раздела;
- `-f` – (files list) текстовый файл, содержащий список путей к файлам и каталогам для удаления;

В текстовом файле пути до объектов указываются без кавычек. Пути разделены точкой с запятой «;» или символом новой строки «\n»:



- `-j` – (journal clear) затирание в журнале блоков, которые использовались для журналирования файла;
- `-l` – (log file) файл лога. В параметре необходимо указать путь к файлу лога;

Например:

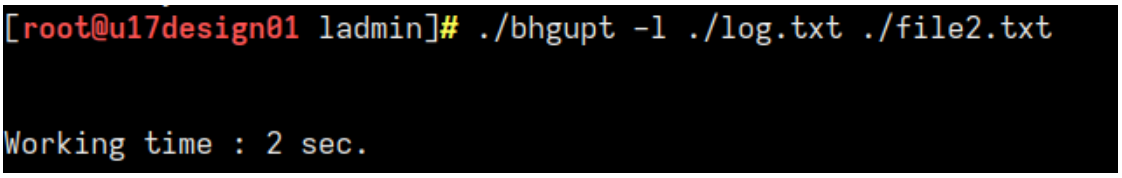


Рисунок 8.3 – Пример команды с указанием пути к файлу лога

- `-e` – (loggin levels) уровень логирования. Предусмотрено два уровня логирования 1 – user mode (по умолчанию) и 2 – service mode;
- `-L` – (low reliability node) режим низкой надежности;
- `-n` – (number of passes) количество проходов затирания. В параметре необходимо указать количество проходов затирания;
- `-r` – (recursive mode) рекурсивный обход каталогов. Не используется для файлов;
- `-R` – (random device) использовать устройство /dev/urandom для получения

случайной последовательности;

- `-H` – (rm-hardlinks [no]force) удалять содержимое файла, который имеет жесткие ссылки. С аргументом *force* все жесткие ссылки на этот файл удаляются. С аргументом *noforce* все жесткие ссылки на этот файл игнорируются. Если данная опция указана с каталогом, то механизм обработки применяется ко всем файлам, которые находятся в каталоге;

Например:

```
[root@u17design01 ladmin]# ./bhgupt -H force ./file3.txt
Тип: Файл Время: 25/5/2023 10:50:50  Имя пользователя: root Объект
: ./file3.txt Результат: Успех Описание: Файл ./file3.txt удален.


Working time : 3 sec.

События аудита созданы.
```

Рисунок 8.4 – Пример команды удаления содержимого файла с жесткими ссылками

- `-s` – (sequence source) источник последовательности (если необходимо задать другой источник последовательности, отличный от используемого по умолчанию /dev/urandom). В параметре необходимо указать путь к файлу со случайной последовательностью;

Например:

```
[root@u17design01 ladmin]# ./bhgupt -s ./2431235421 ./file.txt
Тип: Файл Время: 25/5/2023 10:53:22  Имя пользователя: root Объект
: ./file.txt Результат: Успех Описание: Файл ./file.txt удален.


Working time : 2 sec.

События аудита созданы.
```

Рисунок 8.5 – Пример команды с указанием источника последовательности

- `-h` – (help) помощь;

Например:

```
[ladmin@u17design01 ~]$ ./bhgupt -h
bhgupt 0.0.194 (c) 2022 by GIS <resp@gaz-is.ru>

Синтаксис: bhgupt [опции] [force]/[noforce] пути к файлу(ам) и/или каталогу(ам) etc.


Опции:
        a   --audit                     Настройка политики аудита.
                                        По умолчанию вывод происходит в консоль.Если указан параметр none вывод аудита отключен.
                                        Любой другой параметр воспринимается как имя файла, в который производится вывод аудита.
        h   --help                      Помощь.
        b   --block-level               Гарантированное удаление объектов на уровне блочных устройств.
        c   --clear-attributes          Сброс атрибутов, защищающих объект файловой системы.
        d   --device-free-space         Затирание свободного пространства на указанном устройстве. В параметре необходимо указать точку монтирования раздела.
        D   --device-root-block         Затирание свободного пространства и блоков, зарезервированных для суперпользователя, на указанном устройстве.
                                        В параметре необходимо указать точку монтирования раздела.
        f   --files-list                Файл, содержащий список путей к файлам и каталогам для удаления. В параметре необходимо указать путь к файлу,
                                        в котором перечисленны пути к файлам и каталогам.
                                        Пути разделены точкой с запятой <<;>> или символом новой строки <<\n>>.
        j   --journal-clear             Затереть в журнале блоки, которые использовались для журналирования файла.
        l   --log-file                  Файл лога. В параметре необходимо указать путь к файлу лога.
        e   --logging-levels            Уровень логирования. Существует два уровня логирования 1- user mode (по умолчанию) и 2 - service mode.
        L   --low-reliability-mode      Режим низкой надежности.
        n   --number-of-passes          Количество проходов затирания. В параметре необходимо указать количество проходов затирания
        r   --recursive-mode            Рекурсивный обход каталогов.
        R   --random-device             Использовать устройство /dev/urandom для получения случайной поледовательности.
        H   --rm-hardlinks [no]force    Удалять содержимое файла, который имеет жесткие ссылки.
                                        С аргументом force все жесткие ссылки на этот файл удаляются.
                                        С аргументом noforce все жесткие ссылки на этот файл игнорируются.
                                        Если данная опция указана с каталогом, то механизм обработки применяется ко всем файлам,
                                        которые находяться в каталоге.
        s   --sequence-source           Источник последовательности. В параметре необходимо указать путь к файлу со случайной последовательностью.
```

Рисунок 8.6 – Пример вызова справки

Перечень сокращений

EXT	–	Extended File System
FAT	–	File Allocation Table
ГУПТ	–	Гарантированное удаление по требованию
КЦ	–	Контроль целостности
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПО	–	Программное обеспечение
СЗИ	–	Средство защиты информации