УТВЕРЖДЕН
ПФНА.501410.002 РЭ-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux

Руководство по эксплуатации

ПФНА.501410.002 РЭ

Листов 233

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее руководство по эксплуатации (РЭ) распространяется на изделие «**Система защиты информации от несанкционированного доступа Dallas Lock Linux**» (далее по тексту — **СЗИ НСД Dallas Lock Linux**, **СЗИ НСД** или изделие).

Изделие рассчитано на обслуживание и эксплуатацию персоналом со среднетехническим образованием.

Обозначение изделия: **СЗИ НСД DLL**.

Децимальный номер изделия: ПФНА.501410.002.

Предприятие-изготовитель: Общество с ограниченной ответственностью «**Конфидент**» (**ООО** «**Конфидент**»). Подразделение: Центр защиты информации (**ЦЗИ**) **ООО** «**Конфидент**». Адрес предприятия-изготовителя: 192029, г. Санкт-Петербург, пр. Обуховской Обороны, д. 51, лит. К, телефон/факс: (812) 325-1037.

Документ состоит из следующих разделов:

- «Описание и работа»;
- «Ограничения по эксплуатации и установке»;
- «Установка и удаление системы защиты»;
- «Управление и настройка системы защиты»;
- «Хранение и транспортирование изделия».

1 ОПИСАНИЕ И РАБОТА

1.1 Описание изделия

1.1.1 Назначение изделия

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), государственных информационных системах (ГИС) и при защите значимых объектов критической информационной инфраструктуры (КИИ).

Изделие соответствует требованиям документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — по 5 классу защищенности;
- «Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ» (ФСТЭК России, 2020) — по 4 уровню доверия;
- «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ;
- «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) — по 4 классу защиты;
- «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты» ИТ.МЭ.В4.ПЗ;
- «Требования к межсетевым экранам» (ФСТЭК России, 2016) – по 4 классу защиты;
- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) – по 4 классу защиты;
- «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ.

При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.501410.002 ФО), изделие может быть использовано:

- В автоматизированных системах до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- В информационных системах персональных данных до 1 уровня защищенности персональных данных включительно (Руководящий документ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2013));
- В государственных информационных системах до 1 класса защищенности информационных систем включительно (Руководящий документ «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (ФСТЭК России, 2013));
- В автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно (Руководящий документ «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (ФСТЭК России, 2014));
- В критических информационных инфраструктурах до 1 категории значимости объекта включительно (Руководящий документ «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (ФСТЭК России, 2017)).

1.1.2 Состав изделия

Изделие поставляется в составе, указанном в Таблица 1.

Таблица 1

№	Наименование	Обозначение	Кол-во шт.	Примечание
1	Компакт-диск		1	
2	Программное обеспечение **СЗИ НСД Dallas Lock Linux**	ПФНА.501410.002	1	На компакт-диске
3	Описание применения	ПФНА.501410.002 31	1	На компакт-диске
4	Руководство оператора (пользователя)	ПФНА.501410.002 34	1	На компакт-диске
5	Комплектность программных средств **СЗИ НСД**	ПФНА.501410.002 КПС	1	На компакт-диске
6	Руководство по эксплуатации	ПФНА.501410.002 РЭ	1	На компакт-диске
7	Формуляр		1	Печатный вариант
8	Краткое руководство пользователя		1	Печатный вариант
9	Программа подсчета контрольных сумм		1	На компакт-диске
10	Копия сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00		1	Печатный вариант
11	Идентификатор **СЗИ**		1	Вклеен в раздел 6 формуляра на изделие
12	Футляр для компакт-диска		1	

При поставке более чем одного изделия комплектность определяется договором.

Поставка модулей «Средство контроля съемных машинных носителей информации», «Персональный межсетевой экран» и «Единый центр управления Dallas Lock» (файлы uccInst.exe, uccInst, uccAgentInst.exe и uccAgentInst) определяется договором.

1.1.3 Маркировка и упаковка изделия

Информация по маркировке указана в подразделе 1.8 документа «Технические условия» ПФНА.501410.002 ТУ на данное изделие.

Свидетельство об упаковке и маркировке находится в разделе 6 документа «Формуляр» ПФНА.501410.002 ФО на данное изделие.

1.2 Описание и работа программного обеспечения изделия

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа на технических средствах, работающих под управлением операционных систем семейства Linux (x64). Поддерживаются такие ОС[1]:

[1] Модуль «Персональный межсетевой экран» может использоваться на операционных системах семейства Linux с ядром версии 5.6 и выше. Для использования модуля «Персональный межсетевой экран» на операционных системах семейства Linux с ядром версии ниже 5.6 необходимо использовать версию изделия 3.31.58.

- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- Альт Рабочая Станция 9.0, 9.1, 9.2, 10.0, 10.1, 10.2;
- Альт Сервер 10;
- Astra Linux Common Edition 2.12;
- Astra Linux Special Edition 1.7;
- Debian 10, 11;
- Red Hat Enterprise Linux 7;
- Ubuntu-desktop 18.04, 20.04;
- РЕД ОС 7.1[2], 7.2[2], 7.3 Муром;
- РЕД ОС 8;
- РОСА «КОБАЛЬТ» 7.9 (Рабочая станция, Сервер);
- ROSA Enterprise Linux Desktop/Server 7.3[2];
- CentOS 7[2].

СЗИ НСД поддерживает 64-разрядные версии ОС архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).

СЗИ НСД поддерживает следующие типы файловой системы: ext2, ext3, ext4, JFS, ReiserFS.

Директория “/usr” не должна быть на отдельном от корневого каталога “/” разделе ФС (это касается всех дистрибутивов).

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

Для размещения файлов **СЗИ НСД** требуется 9 Гб пространства на корневом каталоге жесткого диска:

- в каталоге «/boot» (или «/boot/efi») должно быть не менее 300 Мб свободного пространства;
- в каталоге «/dllx» должно быть не менее 530 Мб свободного пространства;
- в каталоге «/dllibckp» должно быть не менее 374 Мб свободного пространства;
- в каталоге «/lib/modules» должно быть не менее 4,2 Гб свободного пространства;
- в каталоге «/tmp» должно быть не менее 3 Гб свободного пространства.

СЗИ НСД успешно устанавливается на АРМ как с UEFI/GPT, так и с BIOS/MBR на автоматически размеченный жесткий диск (разметка жесткого диска по умолчанию при установке ОС). При условии, что для всех каталогов есть необходимое свободное место.

Минимальный объем оперативной памяти, занимаемый компонентами **СЗИ НСД**, составляет 500 Мб. При высокой интенсивности файловых операций потребление может доходить до 3 Гб.

СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети.

Для обеспечения интеграции с доменом[3], изделие поддерживает работу со следующими компонентами:

- SSSD 2.6.3 и старше;
- Winbind 4.13.17 и старше;
- Kerberos 5 и старше;
- OpenLDAP 2.6.1 и старше;
- Samba 4 и старше;
- FreeIPA 3 и старше.

Поддерживаемые внешние устройства:

- USB-накопители, внешние жесткие диски, накопители на оптических дисках;
- принтеры;
- беспроводные устройства.

[2] Для защиты ТС, работающих под управлением ОС CentOS 7, РЕД ОС 7.1 и 7.2, ROSA Enterprise Linux Desktop/Server 7.3, необходимо использовать версию изделия 3.34.44 совместно с локальными репозиториями, предоставляемыми предприятием-изготовителем.

[3] Microsoft Directory — служба каталогов корпорации Microsoft для операционных систем семейства Windows Server. FreeIPA — открытый проект для создания централизованной системы по управлению идентификацией пользователей, задания политик доступа и аудита для сетей на базе Linux и Unix. Samba — программное обеспечение для реализации файлового сервера. Устанавливается на Windows, Linux/FreeBSD.

2 ОГРАНИЧЕНИЯ ПО ЭКСПЛУАТАЦИИ И УСТАНОВКЕ

2.1 Ограничения по эксплуатации

При создании защищенных автоматизированных систем до класса защищенности 1Г включительно в **СЗИ НСД** на ТС, на котором выполняется обработка защищаемой информации, необходимо включить опции, отвечающие за выполнение следующих условий:

- Осуществление идентификации при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.
- Включение регистрации входов (выходов) пользователей в систему (из системы).
- Включение регистрации выдачи печатных (графических) документов на «твердую» копию.
- Включение регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.
- Включение регистрации попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, узлам сети, каналам связи, внешним устройствам, программам, томам, каталогам, файлам, записям).
- Осуществление проверки целостности **СЗИ НСД** при загрузке операционной системы.
- Отключение аутентификации по SSH.

Установка, подключение, ввод в эксплуатацию и эксплуатация изделия должны производиться в соответствии с документами «Руководство по эксплуатации» ПФНА.501410.002 РЭ и «Руководство системного программиста (администратора)» ПФНА.501410.002 32.

Использование аппаратных идентификаторов в процессе эксплуатации изделия должно осуществляться в соответствии с эксплуатационной документацией на данные аппаратные идентификаторы.

Все сервисы, которые требуют создания пользователей в системе, рекомендуется устанавливать до установки **СЗИ НСД**.

После установки **СЗИ НСД** изменять домашние директории учетным записям пользователей будет невозможно.

Для корректной работы графической оболочки ОС автоматический вход для всех пользователей ОС должен быть отключен.

В случае обновления ядра необходимо выключить политику «**Проверять целостность прогр.апп. среды при загрузке ОС**». Далее, после обновления ядра, необходимо пересчитать контрольную сумму аппаратной целостности, подробнее — в разделе Настройка политик безопасности.

При эксплуатации **СЗИ НСД** должны быть приняты меры, исключающие доступ пользователя к ресурсам компьютера в обход его механизмов защиты, то есть проведение организационно-технических мероприятий для исключения нештатной загрузки ОС ТС.

Установка **СЗИ НСД** полностью отменяет все доменные учетные записи, которые доступны в ОС до установки **СЗИ НСД**. После установки **СЗИ** необходимо зарегистрировать в **СЗИ НСД Dallas Lock Linux** учетные записи доменных пользователей, подробнее — в разделе Регистрация учетных записей доменных пользователей.

2.2 Ограничения по установке

Установку программных модулей **СЗИ НСД** необходимо производить в соответствии с договором и отгрузочными документами (накладная, акт передачи прав и т. д.) с обязательной соответствующей записью в разделе 13 «Особые отметки» формуляра на изделие.

Дополнительная установка **СЗИ НСД** (сверх указанного количества) допускается только при переносе **СЗИ НСД** на другое ТС или его восстановлении.

В процессе эксплуатации изделия необходимо использовать сертифицированные обновления по результатам испытаний, вызванных внесением изменений в **СЗИ НСД**.

Доступ к сертифицированным обновлениям по результатам испытаний, вызванных внесением изменений в **СЗИ НСД**, возможен только в рамках действующего технического сопровождения.

В процессе эксплуатации **СЗИ НСД** запрещается:

- коммерческое тиражирование **СЗИ НСД**;
- модификация, декомпиляция или дизассемблирование **СЗИ НСД**;
- обработка компакт-диска с **СЗИ НСД** системными программами и утилитами, работающими на низком уровне.

3 УСТАНОВКА И УДАЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ

СЗИ НСД представляет собой программный комплекс средств защиты информации в ОС семейства Linux с возможностью подключения аппаратных идентификаторов. Для функционирования **СЗИ НСД** необходимо произвести установку и настройку программных компонентов системы защиты.

3.1 Подготовка к установке

При установке **СЗИ НСД** требуется скачивание пакетов из глобальной сети. Для автономных компьютеров, не подключенных к глобальной сети, необходимо, чтобы в локальной сети был расположен официальный репозиторий соответствующего дистрибутива ОС и были выполнены соответствующие настройки инфраструктуры. Следует обратить внимание, что корректная работа **СЗИ НСД** гарантируется только с официальными репозиториями, подключение к которым осуществляется сразу после установки ОС.

Необходимым условием установки является доступность официального репозитория соответствующего дистрибутива ОС.

Подготовка к установке должна осуществляться только с правами суперпользователя (*root*), обладающего правами администратора на данном ТС.

Суперпользователь (root) и пользователи с аналогичными правами обладают привилегиями, с помощью которых могут внести изменения в **СЗИ НСД** и ее настройки, способные нарушить корректность выполнения функций **СЗИ НСД** вплоть до неработоспособности **СЗИ НСД**. Контроль привилегированных пользователей должен осуществляться посредством применения организационных мер защиты.

В случае если пароль суперпользователя (*root*) не был задан до установки **СЗИ НСД**, то после установки **СЗИ НСД** суперпользователь (*root*) будет заблокирован до смены пароля средствами **СЗИ**. В дальнейшем пароль суперпользователя (*root*) можно задать только средствами **СЗИ НСД**.

Подробная информация о блокировке суперпользователя (*root*) — в разделе Подсистема журналирования.

Рекомендуется до или сразу после установки **СЗИ НСД** задать пароль для суперпользователя (*root*). В случае нарушения аппаратной целостности и при этом отсутствия пароля суперпользователя (root) возможность авторизоваться в ОС не будет предоставлена ни одному зарегистрированному пользователю ОС, в том числе суперпользователю (root).

Перед установкой **СЗИ НСД** необходимо выполнить нижеперечисленные действия:

1. Убедиться, что на ТС не установлена система защиты. Если система защиты установлена, ее необходимо удалить.

2. Проверить состояние файловой системы ПК при помощи специальной утилиты из состава ОС (например, fsck) и устранить выявленные дефекты.

3. Проверить состояние жестких дисков при помощи специальной утилиты из состава ОС (например, smartctl или hdparm) и устранить выявленные дефекты.

4. Убедиться, что на корневом каталоге жесткого диска имеется свободное пространство для размещения файлов **СЗИ НСД** в объеме 9 Гб:

- в каталоге «/boot» (или «/boot/efi») должно быть не менее 300 Мб свободного пространства;
- в каталоге «/dllx» должно быть не менее 530 Мб свободного пространства;
- в каталоге «/dllibckp» должно быть не менее 374 Мб свободного пространства;
- в каталоге «/lib/modules» должно быть не менее 4,2 Гб свободного пространства;
- в каталоге «/tmp» должно быть не менее 3 Гб свободного пространства.

СЗИ НСД успешно устанавливается на АРМ как с UEFI/GPT, так и с BIOS/MBR на автоматически размеченный жесткий диск (разметка жесткого диска по умолчанию при установке ОС). При условии, что для всех каталогов есть необходимое свободное место.

5. Перед началом установки убедиться, что отключена блокировка экрана. Установка системы защиты должна выполняться непрерывно, так как процедура установки включает в себя замену PAM-модуля, при блокировке экрана авторизация станет невозможной.

6. Закрыть все запущенные приложения, так как установка системы защиты потребует принудительной перезагрузки.

7. На время установки **СЗИ** отключить автоматическое обновление ОС.

До установки **СЗИ НСД** необходимо вручную отключить SELinux и AppArmor.

Для отключения SELinux необходимо:

1. Открыть файл */etc/selinux/config* с правами суперпользователя (root).
2. В файле */etc/selinux/config* заменить строку *SELINUX=enforcing* на *SELINUX=disabled*.
3. Выполнить перезагрузку ОС.

Для отключения AppArmor необходимо в терминале с правами суперпользователя (root) выполнить команды:

1. *systemctl stop apparmor*;
2. *systemctl disable apparmor*;

Выполнить перезагрузку ОС.

При замене AppArmor на SELinux для ОС Ubuntu корректная установка **СЗИ НСД Dallas Lock Linux** не гарантируется

До установки **СЗИ НСД** для Debian[4], Ubuntu, Astra Linux, Альт Рабочая Станция, Альт Сервер необходимо в терминале выполнить команду:

apt-get update

До установки **СЗИ НСД** для CentOS, Red Hat Enterprise Linux, РЕД ОС, РОСА «КОБАЛЬТ» Desktop/Server 7.9, ROSA Enterprise Linux Desktop/Server необходимо в терминале выполнить команду:

yum repolist ; yum makecache.

Для CentOS 7[2], ROSA Enterprise Linux Desktop/Server 7.3[2], РЕД ОС 7.1[2], 7.2[2], 7.3, 8 при использовании менеджера пакетов YUM, необходимо отключить плагин *refresh-packagekit*:

1. Открыть файл */etc/yum/pluginconf.d/refresh-packagekit.conf* с правами суперпользователя (root).
2. В файле */etc/yum/pluginconf.d/refresh-packagekit.conf* выставить строку *enabled=0.*

Перед установкой **СЗИ НСД** для Red Hat Enterprise Linux 7 следует включить репозиторий *rhel-7-server-optional-rpms*. Для этого необходимо выполнить с правами суперпользователя (root) команду в терминале: *yum-config-manager --enable rhel-7-server-optional-rpms*

[4] В случае если в качестве обновления пакетного репозитория для Debian 10/11 источником указан CD-ROM, необходимо в конфигурационном файле */etc/apt/sources.list* раскомментировать строки: “deb cdrom:” и “deb-src cdrom:”.

Перед установкой **СЗИ НСД** на Astra Linux Special Edition 1.7 следует включить необходимые пакетные репозитории. Для этого необходимо:

1. Открыть в терминале конфигурационный файл */etc/apt/sources.list* с правами суперпользователя (*root*).
2. В файле */etc/apt/sources.list* закомментировать строку: “*deb cdrom*“.
3. Раскомментировать строки сетевых репозиторий в файле */etc/apt/sources.list*.
4. Сохранить файл.

При централизованном развертывании **СЗИ НСД** с помощью Сервера безопасности **Dallas Lock** на ТС необходимо предварительно установить и настроить сервер OpenSSH[5].

По умолчанию пользователь *root* не имеет права на вход по SSH. Для того чтобы разрешить ему вход, необходимо отредактировать конфигурационный файл sshd.

1. Для Ubuntu, Debian, CentOS, RHEL, Astra Linux. Необходимо открыть на редактирование файл /etc/ssh/sshd_config, найти строку *PermitRootLogin no* и изменить значение на *yes*. Далее нужно перезапустить демон sshd (для Ubuntu, Debian, Astra Linux командой *systemctl restart ssh*, для CentOS, RHEL).

2. Для Альт Рабочая Станция, Альт Сервер. Необходимо открыть на редактирование файл /etc/openssh/sshd_config, найти строку с параметром *PermitRootLogin*. Если строка закомментирована (*#PermitRootLogin without-password*), нужно снять знак комментария # и изменить значение на *yes*. Если строка не закомментирована, нужно изменить значение на *yes*. Далее следует перезапустить демон sshd (команда *systemctl restart ssh*).

Перед установкой клиентской части с помощью **СБ Dallas Lock** необходимо проверить список поддерживаемых протоколов шифрования по ssh. Для проверки необходимо выполнить команду *ssh –Q cipher*. Если в списке поддерживаемых протоколов нет следующих алгоритмов: 3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour, то в конфигурационный файл необходимо прописать *Ciphers +3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour*[6] и сохранить его после внесенных изменений.

Сервер безопасности **Dallas Lock** для связи с Linux-клиентом использует алгоритмы шифрования «3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour», на стороне Linux-клиента список поддерживаемых алгоритмов может несущественно отличаться, и при этом удаленная установка **СЗИ НСД Dallas Lock Linux** все равно будет возможна.

После выполнения всех настроек в конфигурационном файле демон sshd необходимо перезапустить ОС.

Более подробно централизованная установка **СЗИ НСД** описана в Руководстве по эксплуатации «Система защиты информации от несанкционированного доступа **Dallas Lock 8.0**» раздел «Централизованная установка **Dallas Lock Linux**».

3.2 Установка системы защиты

Следует обратить внимание, что после начала установки **СЗИ НСД** до перезагрузки ОС отключается возможность авторизации в новом сеансе либо смены пользователя в текущем.

Графическая оболочка администрирования устанавливается отдельно от СЗИ НСД. Установку **СЗИ НСД** и графической консоли необходимо проводить от имени пользователя с правами, аналогичными правам администратора (*root*) на данном ТС.

Во время установки **СЗИ НСД** устанавливается также программа по созданию сертификатов OpenSSL. Использование программы описано в разделе Управление сертификатами системы защиты.

[5] OpenSSH — свободно распространяемая версия семейства инструментов для удаленного управления компьютерами и передачи файлов с использованием протокола безопасной оболочки (SSH).

[6] В ряде ОС символ «+» может не восприниматься, и строка будет считаться некорректной.

После После успешной установки системы защиты на ТС рекомендуется скопировать каталог */dllibckp* на USB-флеш-накопитель, выполнив команду *cp --archive --force /dllibckp /mnt/backup/*. USB-флеш-накопитель должен быть предварительно отформатирован и смонтирован следующими командами:

mkdir --parents /mnt/backup

mount /dev/sdXY /mnt/backup,

где в качестве «*XY*» необходимо указать букву и номер раздела.

Каталог */dllibckp* предназначен для хранения резервной копии целевой системы до установки системы защиты. В случае аварийного удаления **СЗИ НСД** систему можно будет восстановить.

После восстановления системы необходимо удалить файлы **СЗИ НСД**, выполнив следующие команды:

rm --force --recursive /mnt/sysroot/dll

rm --force --recursive /mnt/sysroot/dllibckp

rm --force --recursive /mnt/sysroot/ishl

Если во время установки **СЗИ НСД Dallas Lock Linux** был запущен сервис ssh, то после выполнения установки **СЗИ НСД** сервис ssh необходимо остановить.

Для остановки сервиса ssh необходимо выполнить команды:

systemctl stop ssh

systemctl disable ssh

Для возможности удаленного управления **СЗИ НСД** необходимо выполнить дополнительную настройку Firewall Linux, открыв порт 13133.

Для установки **СЗИ НСД** необходимо выполнить следующие действия:

1. Скопировать с установочного диска из каталога в домашний каталог пользователя файл «*dllx-<номер сборки>.run*».

2. Проверить, является ли файл «*dllx-<номер сборки>.run»* исполняемым, с помощью команды *ls –l.*

Пример:

ls -l <enter>

rw-rw---- отображаются последовательно без пробелов флаги владельца, флаги группы, флаги всех остальных пользователей. В данном примере файл не является исполняемым ни для владельца, ни для группы, ни для всех остальных пользователей.

Если файл не является исполняемым, необходимо ввести команду *chmod a+x dllx-<номер сборки>.run;*

Пример:

chmod a+x dllx-<номер сборки>.run <enter> с помощью этой команды файл становится исполняемым для его владельца.

3. Запустить файл командой *./dllx-<номер сборки>.run*, в качестве атрибута к которой можно указать номер лицензии.

Пример:

./dllx-<номер сборки>.run 0-0000-0000

Если не указать номер лицензии при запуске скрипта, он будет запрошен во время процесса установки.

Номер лицензии указан на коробке компакт-диска с дистрибутивом **Dallas Lock Linux**.

По умолчанию временные файлы, образующиеся при установке **СЗИ**, располагаются в каталоге «/tmp». Если перед установкой системы защиты обнаруживается менее 3 Гб требуемого пространства монтируемого раздела «/tmp», то следует использовать переменную окружения TMPDIR до запуска установочного файла **СЗИ НСД**, указав в ней путь каталога с необходимым свободным пространством для временных файлов.

Пример:

TMPDIR=/root <путь к установочному файлу> <dllx-<номер сборки>.run

Важно! При использовании переменной TMPDIR всегда прописывается абсолютный путь в ФС. Также, если при указании пути к папке, которая будет использоваться вместо каталога «/tmp», имеются пробелы или другие спецсимволы, то значение TMPDIR заключается в двойные или одиночные кавычки.

В качестве атрибутов к команде *./dllx-<номер сборки>.run* можно указывать следующие:

Таблица 2

Атрибут	Описание
--help	Вывод на экран списка атрибутов с подсказками **Пример:** *./dllx-<номер сборки>.run --help <enter>*
--info	Печать встроенной информации: заголовок, целевой каталог по умолчанию, встроенный скрипт
--lsm	Данный атрибут не используется в процессе установки **СЗИ НСД**
--list	Вывод на экран списка файлов в архиве
--check	Проверка целостности архива
--verify-sig key	Проверка GPG подписи по представленному идентификатору ключа
--confirm	Спросить перед запуском встроенного скрипта
--quiet	Не печатать ничего кроме сообщений об ошибках
--accept	Принять номер лицензии
--noexec	Не запускать встроенный скрипт установки дистрибутива **СЗИ НСД**
--noexec-cleanup	Не запускать встроенный скрипт удаления временных файлов после установки дистрибутива **СЗИ НСД**
--keep	Не удалять данные о целевой директории после выполнения встроенного скрипта
--noprogress	Не показывать прогресс в процессе декомпрессии
--nox11	Данный атрибут не используется в процессе установки **СЗИ НСД**
--nochown	Не давать доступ к распакованным файлам текущему пользователю
--chown	Рекурсивно назначить доступ к распакованным файлам текущему пользователю
--nodiskspace	Не проверять доступное место на диске
--target dir	Извлечь непосредственно в целевую директорию (по абсолютной или относительной ссылке). Этот каталог может быть подвергнут рекурсивной обработке (см. *nochown*)
--tar arg1 [arg2 ...]	Доступ к содержимому архива через команду *tar*. Во встроенный скрипт будут переданы следующие аргументы
--ssl-pass-src src	Использовать указанный src в качестве источника пароля для расшифровки данных с помощью OpenSLL, см. «Аргументы парольной фразы» в руководстве OpenSLL. По умолчанию пользователю предлагается ввести пароль для расшифровки на текущем терминале

Атрибут	Описание
--cleanup-args args	Аргументы встроенного скрипта очистки. Для передачи нескольких аргументов требуется заключать их в кавычки
--arm-name=name	Указать под каким именем будет зарегистрирован АРМ в Домене безопасности **ЕЦУ**
--ucc-addr=address	Указать IP-адрес или сетевое имя компьютера Домена безопасности **ЕЦУ**
--ucc-key=key	Указать ключ Домена безопасности **ЕЦУ**
--grub-pass=password	Установить пароль GRUB для суперпользователя. По умолчанию — *dlladmin*
--just-check	Не устанавливать, а только проверить поддержку хост-системы

Для защиты от несанкционированного изменения параметров загрузки на загрузчик установлен пароль.

1. Задание пароля[7] загрузчика во время установки **СЗИ НСД**.

Чтобы задать пароль загрузчика при установке, необходимо ввести пароль в качестве аргумента команды запуска установочного скрипта:

./dllx-<номер сборки>.run -- --bootpass=<пароль загрузчика> <enter>

или

./dllx-<номер сборки>.run <номер лицензии СЗИ НСД> --bootpass=<пароль загрузчика> <enter>

Если при установке **СЗИ НСД** не ввести пароль, будет установлен пароль по умолчанию — *dlladmin*[8].

2. Смена пароля[7] загрузчика после установки **СЗИ НСД**.

Для смены пароля загрузчика GRUB необходимо:

2.1 запустить программу grub-mkpasswd-pbkdf2;

2.2 дважды ввести новый пароль загрузчика. Программа выдаст хэш нового пароля: *grub.pbkdf2.sha512.10000…*;

2.3 открыть файл */etc/grub.d/40_custom*, и добавить в него логин и сгенерированный новый пароль:
set-superusers="dlladmin"
password_pbkdf2 dlladmin grub.pbkdf2.sha512.10000…

2.4 сохранить файл;

2.5 поскольку файл */etc/grub.d/40_custom* содержит хэш пароля, то рекомендуется запретить его чтение и изменения всеми, кроме пользователя root, выполнив следующую команду:
sudo chmod 771 /etc/grub.d/40_custom

2.6 запустить программу для создания нового конфигурационного файла загрузчика, выполнив следующую команду:
sudo grub-mkconfig –o /boot/grub/grub.cfg

2.7 в результате, пароль загрузчика будет заменен на новый.

Для смены пароля загрузчика GRUB2 необходимо:

Для систем с UEFI файл конфигурации GRUB2 располагается по адресу */boot/efi/EFI/<имя системы>/grub.cfg*. Следовательно, создание нового конфигурационного файла загрузчика будет выглядеть следующим образом: *grub2-mkconfig -0 /boot/efi/EFI/<имя системы>/grub.cfg*. Также стоит учесть, что и dsb-правило для пользователя root следует создавать для каталога */boot/efi/EFI/<имя системы>*.

2.8 запустить программу grub2-setpassword;

2.9 дважды ввести новый пароль загрузчика. Программа выдаст хэш нового пароля загрузчика GRUB в файле */boot/grub2/user.cfg*, который можно посмотреть с помощью команды *cat*:
cat /boot/grub2/user.cfg

2.10 открыть файл */etc/grub.d/40_custom*, добавить в него логин и сгенерированный новый пароль:
set-superusers="dlladmin"

[7] Необходимо обладать правами суперпользователя (*root*).
[8] Также будет установлен логин по умолчанию — *dlladmin*.

password_pbkdf2 dlladmin grub.pbkdf2.sha512.10000…

2.11 сохранить файл;

2.12 поскольку файл */etc/grub.d/40_custom* содержит хэш пароля, то рекомендуется запретить его чтение и изменение всеми, кроме пользователя root, выполнив следующую команду:
sudo chmod 771 /etc/grub.d/40_custom

2.13 запустить создание нового конфигурационного файла загрузчика, выполнив следующую команду:
grub2-mkconfig –o /boot/grub2/grub.cfg

2.14 в результате, пароль загрузчика будет заменен на новый.

После завершения процедуры смены пароля загрузчика рекомендуется удалить dsb-правило для каталога */boot/grub* (или */boot/grub2*).

Пример:

ishl <enter>

resources <enter>

files <enter>

rm-rights-user root /boot/grub <enter>

Для смены логина необходимо в строке *set superusers="dlladmin"* заменить *dlladmin* на новый логин.

Информацию о ходе процесса установки можно увидеть в файле install.log, который создается при установке DLL в папке, в которой находится установочный файл install.sh.

После выполнения всех вышеуказанных действий ТС уйдет в автоматическую перезагрузку. Для отмены автоматической перезагрузки ТС после успешной установки необходимо перед запуском файла *./dllx-<номер сборки>.run* в качестве атрибута указать *--no-reboot*.

Номер лицензии может активировать модуль управления правилами межсетевого экрана, а также функциональные возможности контроля съемных накопителей.

При первой загрузке ОС, защищаемой **СЗИ НСД**, начинают функционировать защитные механизмы изделия (см. раздел Вход в защищенную ОС).

После В Таблица 3 представлена подробная информация об известных случаях сбоя установки и удаления системы и их коды возврата при аварийном завершении процесса инсталляции или деинсталляции **СЗИ НСД Dallas Lock Linux**.

Таблица 3

Код возврата ошибки	Сбой
Стартовый скрипт инсталлятора	
201	Был получен отказ принять условия лицензионного соглашения
202	Не совпадает ключ GPG подписи
203	Не удалось проверить GPG подпись
204	Архив имеет неожиданный размер[9]
205	Контрольная сумма SHA256 файлов дистрибутива **СЗИ НСД** не совпадает[9]
206	Контрольная сумма MD5 файлов дистрибутива **СЗИ НСД** не совпадает[9]

[9] Основной причиной может являться поврежденный файл инсталлятора **СЗИ НСД Dallas Lock Linux**.

Код возврата ошибки	Сбой
207	Контрольная сумма CRC файлов дистрибутива **СЗИ НСД** не совпадает[9]
208	Процессу инсталляции был отправлен сигнал: – 1 (SIGHUP) – обнаружено зависание на управляющем терминале или завершение процесса управления; – 2 (SIGINT) – пользователем отправлен сигнал прерывания (по нажатию Ctrl+C); – 3 (SIGQUIT) – пользователем отправлен сигнал выхода (по нажатию Ctrl+D); – 15 (SIGTERM) – прекращение работы программного обеспечения (по умолчанию отправляется *kill*)
209	Не удалось подтвердить извлечение файлов **СЗИ НСД** из архива
210	Невозможно извлечь файлы **СЗИ НСД** из архива. Архив поврежден или имеет неизвестный формат
Основной скрипт инсталлятора	
221	**СЗИ НСД** уже установлена (на диске присутствует директория /dllx)
222	Не найден файл /etc/os-release. По причине чего не представляется возможным проверить, поддерживается ли данный дистрибутив
223	Дистрибутив не поддерживается
224	На дисковом пространстве недостаточно места для развёртывания **СЗИ НСД**. Перед началом установки запускается проверка, которая может сгенерировать ошибку
225	В /etc/fstab обнаружена не поддерживаемая ФС
226	Не обнаружена одна из основных утилит, необходимых для установки **СЗИ НСД**: – chmod; – cut; – df; – find; – grep; – sed; – systemctl; – truncate
227	В инсталляторе отсутствует скрипт, содержащий функции, специфичные для установки на данный дистрибутив
228	По файлу /etc/os-release не удалось определить имя скрипта, содержащего функции, специфичные для установки на данный дистрибутив
229	Указан неверный номер лицензии
231	Установка **СЗИ НСД** на данную архитектуру ОС не поддерживается
232	Установка **СЗИ НСД** остановлена. На текущей ОС включен SELinux
233	Не указан логин учетной записи администратора **СЗИ НСД**. Код ошибки возвращается, если процесс обновления **СЗИ НСД** был запущен с ключом *–upgrade*
234	Не указан пароль учетной записи администратора **СЗИ НСД**. Код ошибки возвращается, если процесс обновления **СЗИ НСД** был запущен с ключом *--upgrade*

Код возврата ошибки	Сбой
235	Указано несколько форматов экспорта журналов. Код ошибки возвращается, если перед запуском процесса обновления **СЗИ НСД** было указано несколько команд формата экспорта журналов
236	Не указан формат экспорта журналов в требуемом формате. Код ошибки возвращается, если перед запуском процесса обновления **СЗИ НСД** не выбран требуемый формат экспорта журналов
Деинсталлятор	
230	Недостаточно прав для запуска процесса деинсталляции **СЗИ НСД**
Коды ошибок Linux перед процессом инсталляции СЗИ НСД	
1	Для выполнения операции недостаточно прав. Для установки **СЗИ НСД** необходимо обладать правами администратора операционной системы (*root*)
17	Невозможно создать уже существующий файл или каталог. Например, на устройстве уже присутствует каталог */tmp/tmp.xxx*, в который инсталлятор пробует распаковать файлы **СЗИ** для последующей установки
22	Недопустимый аргумент. Один (или несколько) параметр(-ов) командной строки, указанных при запуске инсталлятора, имеют некорректные значения
28	На устройстве нет свободного места. Ошибка может возникнуть после проверки достаточного количества места в рамках основного скрипта инсталляции, либо до запуска основного скрипта инсталляции

3.2.1 Установка графической оболочки администрирования

Установка графической оболочки администрирования в операционных системах на базе Linux

С установочного диска необходимо скопировать в домашний каталог пользователя файл *«dllx-gui-<номер сборки>.run»* и запустить его, выполнив команду *./dllx-gui-<номер сборки>.run*.

Пример:

./dllx-gui-<номер сборки>.run <enter>

Установка графической консоли не требует перезагрузки ТС.

Установка графической оболочки администрирования в операционных системах на базе Windows

Для установки графической оболочки администрирования в ОС на базе Windows необходимо запустить файл *«dllx-gui-<номер сборки>.exe»*.

Графическая оболочка администрирования **СЗИ НСД** в ОС на базе Windows поддерживает 64-битные версии ОС Windows:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге инсталляции предоставляется возможность отмены инсталляции с возвратом сделанных изменений с помощью кнопки «**Отмена**». Выполнение следующего шага инсталляции выполняется с помощью кнопки «**Далее**».

3.3 Удаление системы защиты

Для удаления **СЗИ НСД** необходимо обладать правами администратора операционной системы (*root*) на данном ТС.

Для отключения механизмов защиты и удаления **СЗИ НСД** необходимо запустить исполняемый файл *dllx-remove.sh*, который расположен в директории */dllx/.remove,* в качестве атрибутов указав логин и пароль учетной записи администратора **СЗИ НСД** *dlladmin* (по умолчанию пароль администратора **СЗИ НСД** — *dlladmin*).

Пример:

/dllx/.remove/dllx-remove.sh dlladmin dlladmin<enter>

В случаях, когда к **СЗИ НСД** невозможно подключиться, используя учетные данные администратора **СЗИ НСД**, необходимо запустить исполняемый файл *run-dllx-remove.sh*.

Пример:

/dllx/.remove/run-dllx-remove.sh <enter>

Логин и пароль для аутентификации использовать при вызове скрипта *run-dllx-remove.sh* не нужно.

3.3.1 Удаление системы защиты с помощью консольной оболочки администрирования

Удалить **СЗИ НСД** также можно с помощью управляющих команд консольной оболочки администрирования. Для этого необходимо выполнить следующие шаги:

1. Выполнить команду *ishl* и авторизоваться в консольной оболочке администрирования.

2. Выполнить команду *services*, после выполнения команды система перейдет в раздел встроенных сервисов *services*.

3. В разделе *services* выполнить ввод команды *uninstall,* затем последовательно ввести *login* и *password* (требуется указать логин и пароль Администратора **СЗИ НСД Dallas Lock Linux**).

Пример:

services <enter>

uninstall <enter>

login <login> <enter>

password <password> <enter>

execute <enter>

Для отслеживания процесса удаления **СЗИ НСД** по лог-файлу в режиме реального времени, необходимо выполнить команду *tail –f /dllx-remove-<дата>-<время>.log*.

3.3.2 Удаление графической оболочки администрирования

Чтобы удалить графическую оболочку **СЗИ НСД**, необходимо запустить исполняемый файл *uninstall.sh*, который расположен в директории */dllx-gui/bin*.

Пример:

/dllx-gui/bin/uninstall.sh <enter>

Также процесс деинсталляции графической оболочки **СЗИ НСД** можно запустить из информационного окна «**О программе**», вызвав его из списка дополнительных функций кнопки главного меню (см. Рисунок 1).

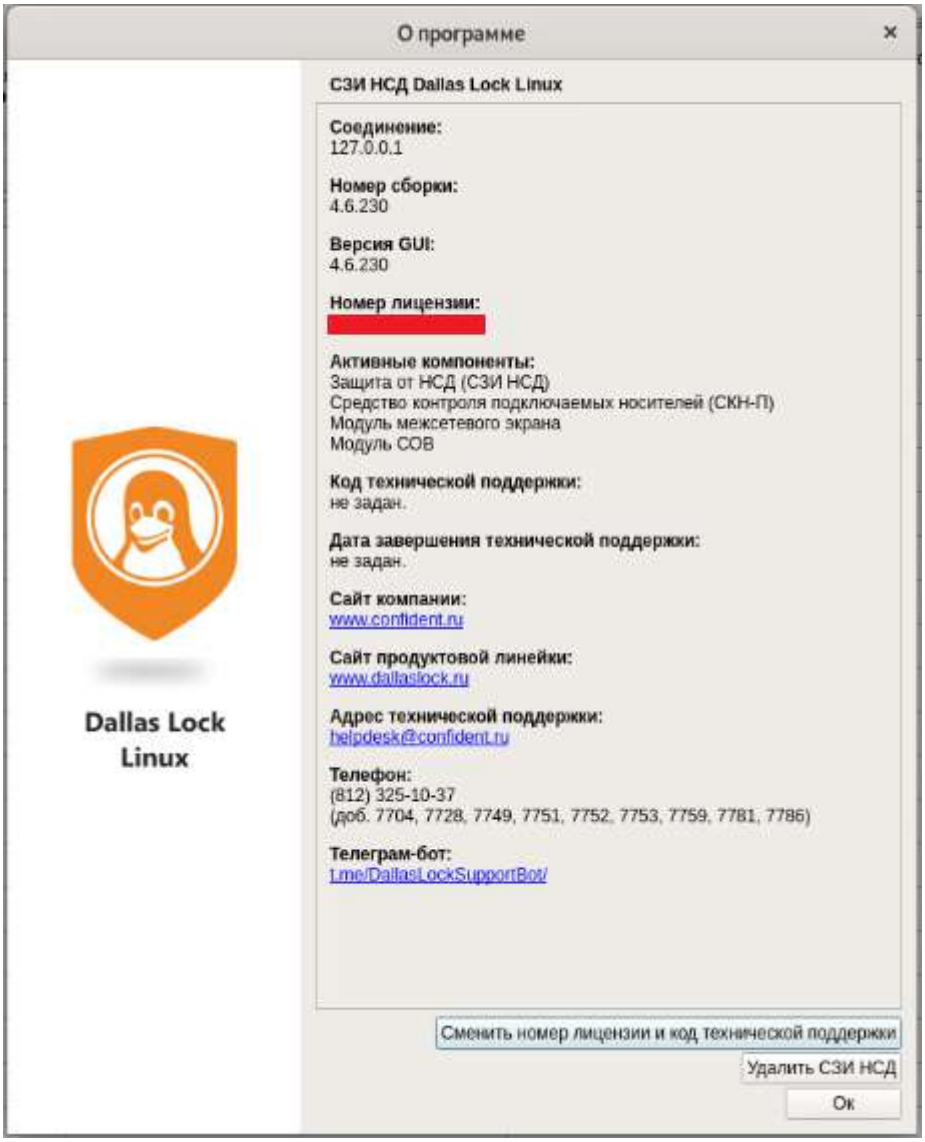


Рисунок 1. Кнопка «Удалить СЗИ НСД DLL»

3.4 Обновление системы защиты

Обновление **СЗИ НСД Dallas Lock Linux** направлено на:

- устранение уязвимостей средства защиты информации;
- добавление функции (функций) безопасности средства защиты информации, направленной (направленных) на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ;
- добавление функции (функций), не влияющей (не влияющих) на функции безопасности СЗИ (например, изменение интерфейса **СЗИ**).

Информация о появлении обновленной версии **СЗИ НСД** регистрируется на сайте www.dallaslock.ru с указанием устраненных недостатков и добавленных функциональных возможностей.

Пользователи **СЗИ НСД** информируются о выпуске обновлений **СЗИ НСД Dallas Lock Linux** (с указанием устраненных недостатков и добавленных функциональных возможностей) по электронной почте с подтверждением получения информации.

После получения информации о наличии обновлений на **СЗИ НСД Dallas Lock Linux** необходимо выполнить следующие действия:

1. С сайта компании www.dallaslock.ru скачать архив, который будет содержать обновленный дистрибутив **СЗИ НСД**.

2. Сохранить указанный архив на жесткий диск ТС, на котором требуется обновить **СЗИ НСД**.

3. Рассчитать контрольную сумму для дистрибутива по алгоритму ГОСТ Р 34.11-94 с помощью программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (сертификат соответствия ФСТЭК России № 2031 от 03.02.2010) либо по алгоритму MD5 с помощью программы «md5sum» (является встроенной в поддерживаемые операционные системы) или программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Fsum Frontend» (свободно распространяемая программа, входит в комплект поставки на компакт-диске с **СЗИ НСД**).

4. Сверить полученную контрольную сумму с соответствующими контрольными суммами, хранящимися на сайте компании www.dallaslock.ru. В случае совпадения контрольных сумм производится установка обновлений. В случае несовпадения контрольных сумм рекомендуется обратиться в службу технической поддержки **ООО** «**Конфидент**».

5. Перед установкой обновлений необходимо удалить установленную ранее версию **СЗИ НСД** (подробнее — в разделе Удаление системы защиты) и выполнить установку СЗИ НСД, используя в качестве дистрибутива скачанный архив (подробнее — в разделе Установка системы защиты).

6. После установки обновлений необходимо сделать соответствующую отметку в разделе 13 формуляра **СЗИ НСД Dallas Lock Linux** с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

Для ТС, защищенных **СЗИ НСД Dallas Lock Linux** предыдущих версий 3.25.21, 3.31.58 и 3.34.44, реализована возможность обновления системы защиты на текущую с сохранением действующих настроек и экспортом журналов аудита.

Перед выполнением процедуры обновления необходимо убедиться в том, что защищаемое ТС находится под управлением поддерживаемой ОС.

Для обновления системы защиты:

1. Скопировать с установочного диска из каталога в домашний каталог пользователя файл «*dllx-<номер сборки>.run*». Не удаляя предыдущую версию дистрибутива **СЗИ НСД Dallas Lock Linux**.

2. Проверить является ли файл «*dllx-<номер сборки>.run*» исполняемым, с помощью команды *ls –l*. Если файл не является исполняемым, необходимо ввести команду *chmod a+x dllx-<номер сборки>.run*. С помощью данной команды файл становится исполняемым для его владельца.

3. Запустить файл командой *./dllx-<номер сборки>.run*, в качестве атрибута необходимо указать параметры представленные в Таблица 4.

Пример:

./dllx-<номер сборки>.run -- --upgrade --admin-login=dlladmin --admin-pass=dlladmin X-XXX-XXXX

4. После деинсталляции системы защиты предыдущей версии 3.25.21, 3.31.58 или 3.34.44 ТС уйдет в автоматическую перезагрузку.

После выполнения деинсталляции системы защиты и перезагрузки будет проходить процедура установки новой версии. Установка новой версии происходит в фоновом режиме. Предоставлена возможность авторизации в терминальную сессию для просмотра процедуры обновления на текущую версию, для этого необходимо выполнить команду *tail –f /dllx-setup-*.log*.

По завершению успешного обновления **СЗИ**, система автоматический уйдет в перезагрузку. В случае возникновения ошибок установки, автоматической перезагрузки происходить не будет. Для определения причины возникновения ошибки обновления необходимо авторизоваться в системе и выполнить команду *tail –f /dllx-setup-*.log*.

Таблица 4

№	Параметр	Описание
1	*--upgrade*	Запуск обновления ранее установленной системы защиты Dallas Lock Linux, версия сборки 3.25.21, 3.31.58 или 3.34.44. При указании данного атрибута будет осуществлена идентификация и деинсталляция Dallas Lock Linux версии 3.25.21, 3.31.58 или 3.34.44
2	*--admin-login=<login>*	Ввод логина Администратора **СЗИ НСД** при запуске обновления ранее установленной системы защиты **Dallas Lock Linux** версии *4550.* Обязательный параметр
3	*--admin-pass=<password>*	Ввод пароля Администратора **СЗИ НСД** при запуске обновления ранее установленной системы защиты **Dallas Lock Linux** версии *4550.* Обязательный параметр
4	*X-XXXX-XXXX*	Номер лицензии при запуске обновления системы защиты **Dallas Lock Linux**. Обязательный параметр

Путь к экспортируемым журналам по умолчанию установлен */dllx/backup/ik2_journals.*

Реализована возможность обновления системы защиты с предыдущей версии 3.25.21, 3.31.58 или 3.34.44 на текущую с сохранением действующих настроек и экспортом журналов аудита с помощью Единого центра управления **Dallas Lock** (**ЕЦУ Dallas Lock**), управление которым осуществляется отдельным приложением «**Консоль ЕЦУ**».

Для этого в окне «**Мастер удаленной установки Dallas Lock Linux**» в дополнительные ключи установки необходимо ввести параметры представленные в Таблица 4. С подробным описанием **ЕЦУ Dallas Lock** можно ознакомиться в Инструкции по использованию **ЕЦУ Dallas Lock** ПФНА.501410.002 И3.

3.5 Управление сертификатами системы защиты

Необходимо вовремя обновлять корневой (*root.crt*) и пользовательский (*user.crt*) сертификаты.

В случае, если срок действия сертификата истечет — пропадет возможность подключения к **СЗИ НСД** через какую-либо оболочку администрирования (в том числе с помощью Сервера безопасности Dallas Lock и Единого центра управления Dallas Lock, возможности которых описаны в разделе Централизованное управление системой защиты). Подробнее о том, как обновить сертификат в разделе Обновление корневого и пользовательского сертификатов.

По умолчанию программа по созданию сертификатов SSL устанавливается в */dllx/bin/dll_gen_certs* и генерирует новый корневой сертификат (*root.crt*) и связанный с ним новый клиентский сертификат (*user.crt*) в текущем рабочем каталоге, оба сроком действия 365 дней. Эти сертификаты можно использовать в качестве замены текущим рабочим сертификатам **СЗИ НСД Dallas Lock Linux**.

Команда запуска *dll_gen_certs* имеет ряд параметров, которые можно использовать, чтобы изменить параметры создания сертификатов, используемые по умолчанию.

Рекомендуется при генерации новых сертификатов не указывать атрибуты путей корневому сертификату и каталогу размещения новых. Лучше использовать значения по умолчанию, указав лишь количество дней.

Пример:

/dllx/bin/dll_gen_certs --days 365

Список атрибутов приведен в Таблица 5.

Таблица 5

№	Параметр	Описание
1	*-h, --help*	Справка, помощь по программе. **Пример:** */dllx/bin/dll_gen_certs -h*
2	*-r, --rootcrt*	Указание пути к существующему корневому сертификату, при этом клиентский сертификат будет создан на его основе. Если атрибут не установлен, то создается новый корневой сертификат. **Пример:** *dll_gen_certs -r <путь_к_корневому_сертификату>*
3	*-d, --directory*	Указание каталога, в который будут размещены созданные сертификаты. Если атрибут не установлен, то созданные сертификаты будут размещены в директорию */crt* текущего рабочего каталога (например, */home/user/crt*). **Пример:** *dll_gen_certs -d <путь_к_каталогу>*
4	*--days*	Указание количества дней до истечения срока действия сертификата(-ов). Если атрибут не установлен, то созданные сертификаты будут действовать 365 дней. Если корневой сертификат не указан, то у нового корневого сертификата и нового клиентского сертификата будет установлено одинаковое заданное количество дней. Если корневой сертификат указан, то заданное количество дней будет установлено только у клиентского сертификата. **Пример:** *dll_gen_certs --days <количество_дней>*

После установки **СЗИ НСД** необходимо следить за сроком действия корневого (*root.crt*) и пользовательского (*user.crt*) сертификатов, при необходимости вовремя их обновлять.

Корневой сертификат (*root.crt*) располагается в */dllx/data/root.crt*.

Пользовательский сертификат (*user.crt*) располагается в */dllx/data/user.crt*.

3.5.1 Проверка срока действия сертификата

Для проверки срока действия сертификата необходимо выполнить команду *openssl x509 -noout -text -in <путь к сертификату>*. В результате выполнения команды будут предоставлены данные по сертификату, в том числе и срок действия.

Пример:

openssl x509 -noout -text -in /dllx/data/root.crt

Стоит учесть, что смена сертификатов на каком-либо из клиентов Сервера безопасности влечет необходимость смены сертификатов на всех узлах Домена безопасности.

3.5.2 Обновление корневого и пользовательского сертификатов

Обновление корневого и пользовательского сертификатов доступно только через консольную оболочку администрирования.

Для обновления корневого и пользовательского сертификатов необходимо выполнить команду *change-cert.* После ввода команды система перейдет в раздел *change-cert-node.*

Для данного раздела доступны следующие управляющие команды:

- *ucert* — установка пользовательского сертификата;
- *rcert* — установка корневого сертификата;
- *preview* — просмотр изменений, которые будут выполнены после команды execute;
- *list* — просмотр списка управляющих команд раздела;
- *execute* — применение внесенных изменений;
- *help* — вывод информации о встроенных командах;
- *back* — выход из подменю (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dllladmin*.

В качестве атрибута к командам ucert и rcert указывается путь к сертификатам, которые требуется установить.

Пример:

information <enter>

change-cert <enter>

rcert /home/user/crt/root.crt <enter>

ucert /home/user/crt/user.crt <enter>

execute <enter>

Для корректной смены сертификата необходимо выполнить следующие действия:

1. Проверить, что сертификаты, которые указываются в *ishl* в *меню information→change-cert*, были сгенерированы утилитой */dllx/bin/dll_gen_certs*, работа с которой описана в разделе Управление сертификатами системы защиты.

2. Вывести файлы **СЗИ НСД** из-под контроля целостности, согласно разделу Контроль целостности программных компонентов СЗИ НСД.

3. Снять правила разграничения доступа (согласно разделу Разграничение доступа к объектам файловой системы) на перечисленные ниже файлы сертификатов:
/dllx/data/root.crt;
/dllx/data/user.crt;
/dllx/backup/dllx/data/root.crt;
/dllx/backup/dllx/data/user.crt.

4. Рекомендуется удалить файлы старых сертификатов **root.crt** и **user.crt** из каталога */dllx/data*.

5. Обновить сертификаты с помощью команды change-cert консольной оболочки администрирования (на данном этапе их можно установить и вручную, скопировав новые сертификаты, сгенерированные программой *dll_gen_certs*, в каталог */dllx/data*).

6. Подписать вновь добавленные файлы сертификатов утилитой */dllx/bin/evmctl*, выполнив команду *ima_hash –s <путь к файлу>*.

7. Перезагрузить систему. Файлы **СЗИ НСД** автоматически установятся под контроль целостности после перезагрузки ОС.

Пример:

resources <enter>
software <enter>
unlock-szi-files all <enter>
back <enter>

resources <enter>
files <enter>
dsb <enter>
set-rights-other - /dllx/data/user.crt <enter>
set-rights-other - /dllx/data/root.crt <enter>
set-rights-other - /dllx/backup/dllx/data/root.crt <enter>
set-rights-other - /dllx/backup/dllx/data/user.crt <enter>
back <enter>
back <enter>
back <enter>

information <enter>
change-cert <enter>
rcert /home/user/crt/root.crt <enter>
ucert /home/user/crt/user.crt <enter>
execute <enter>
exit <enter>

/dllx/bin/evmctl ima_hash –s /dllx/data/user.crt <enter>
/dllx/bin/evmctl ima_hash –s /dllx/data/root.crt <enter>
/dllx/bin/evmctl ima_hash –s /dllx/backup/dllx/data/user.crt <enter>
/dllx/bin/evmctl ima_hash –s /dllx/backup/dllx/data/root.crt <enter>
systemctl reboot <enter>

3.6 Вход в защищенную ОС

При первой загрузке ОС, защищаемой **СЗИ НСД**, начинают функционировать защитные механизмы изделия. При этом действуют настройки и политики безопасности, установленные по умолчанию:

- Минимальная длина пароля (Minimum length of password) — 8 символов.
- Осуществление входа по паролю (Authentication by a password).
- Максимальное количество ошибок ввода пароля — 3 (Number of wrong retries).
- Максимальное количество сессий — 10 (Maximum sessions).
- Время бездействия, после которого будет заблокирован сеанс доступа — 0 (отключено), (Lock

screen timeout period).

- Включено ведение всех журналов **СЗИ НСД** (журнал входов/выходов (Login and log journal), журнал ресурсов (resources-policies), журнал доступа к устройствам (Device journal), журнал управления пользователями и группами (User and group management journal), журнал печати (Printer management and printing events journal), журнал управления политиками безопасности (Policy management journal), системный журнал (Syslog journal)).
- Период архивации журналов — 3 месяца (Journals database lifetime in months).
- Проверка целостности прогр.апп. среды при загрузке ОС — отключена.
- Генерация событий аудита аппаратной целостности — отключена.

После входа в систему администратор **СЗИ НСД** может просмотреть и изменить настройки, а также ознакомиться с журналами, в которых были зарегистрированы события, связанные со входом администратора в систему.

3.6.1 Вход в консольную оболочку ОС

При входе в ОС без использования графической оболочки ОС, если пользователю назначен аппаратный идентификатор, необходимо его предъявить. Затем, в зависимости от хранимой на идентификаторе информации, по запросу ОС нужно будет ввести:

- логин и пароль в открытой памяти идентификатора — открытая авторизация: если аппаратный идентификатор ассоциирован с пользователем, то произойдет автоматический вход в систему;
- логин и пароль в закрытой памяти идентификатора — закрытая авторизация: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации дополнительно потребуется ввести ПИН;
- только имя пользователя: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации потребуется ввести пароль;
- пустой аппаратный идентификатор: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации потребуется ввести логин, пароль.

Если подключено и назначено несколько аппаратных идентификаторов (АИ), то при входе в ОС с помощью АИ, система выберет идентификатор по возрастанию серийного номера. Например, если подключены два АИ с серийными номерами 3cb435 и 4bk456, то будет выбран АИ с серийным номером 3cb435.

Если ни одному считывателю (USB-порту или считывателю Touch Memory) не предъявлен аппаратный идентификатор, то произойдет приглашение для ввода логина.
Если с данным пользователем не ассоциирован аппаратный идентификатор, то появится соответствующее сообщение, и аутентификация будет прекращена.
Если аппаратный идентификатор ассоциирован с пользователем, но он не обнаружен ни одним считывателем, то появится сообщение, требующее предъявить аппаратный идентификатор. Если он предъявлен, то произойдет авторизация в соответствии с одним из типов, отмеченных выше. Если по истечении некоторого периода ожидания аппаратный идентификатор не предъявлен, то авторизация прекращается.

Следует обратить внимание, что в случае входа в ОС без использования графической оболочки, при вводе пароля символы пароля отображаться на экране не будут, также не будут отображаться звездочки или иные символы.

После успешной авторизации отобразится строка приглашения к вводу команд (см. Рисунок 2).

Рисунок 2. Строка приглашения к вводу команд

Более подробная информация содержится в документации к используемой операционной системе.

В зависимости от используемой ОС можно воспользоваться одним из следующих источников:

- Debian (systemd): https://www.debian.org/doc/;
- CentOS: https://wiki.centos.org/;
- Ubuntu: https://wiki.ubuntu.com;
- Astra Linux: https://astralinux.ru/information/library;
- Альт: https://docs.altlinux.org/ru-RU/index.html;

- Ред ОС: https://redos.red-soft.ru/documentation;
- РОСА: https://www.rosalinux.ru/docs/;
- Red Hat Enterprise Linux: https://docs.redhat.com/en/products.

3.6.2 Вход в консольную оболочку ОС

Для осуществления входа при помощи графической оболочки ОС в политике безопасности **СЗИ НСД** необходимо указать значение максимального допустимого количества сессий пользователей равным или большим 2 (по умолчанию установлено значение «10») или равным 0 (отключение ограничения на максимальное допустимое количество сессий). Подробнее в разделе Число разрешенных сеансов.

Если пользователю назначен аппаратный идентификатор, необходимо его предъявить. Затем, в зависимости от хранимой на идентификаторе информации, по запросу ОС нужно будет ввести:

- Логин и пароль учетной записи, если в идентификаторе не хранится информация об учетной записи.
- Пароль учетной записи, если в идентификаторе хранится информация только о логине учетной записи.
- PIN-код для аппаратного идентификатора, если в закрытой памяти идентификатора хранится пароль учетной записи.

Если в открытой памяти идентификатора хранится пароль учетной записи, при авторизации пользователю необходимо только предъявить аппаратный идентификатор, логин и пароль считаются с ключа автоматически.

Если пользователю не назначен аппаратный идентификатор, необходимо ввести логин пользователя и его пароль (см. Рисунок 3).

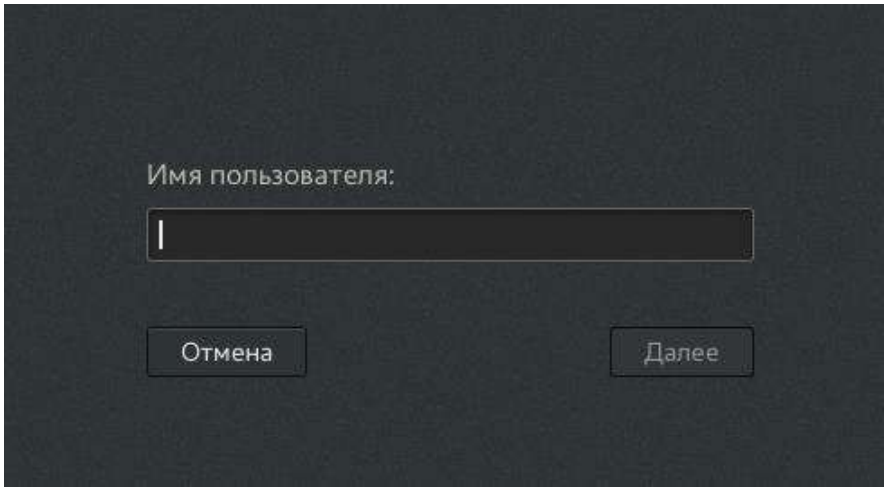


Рисунок 3. Вход в графическую оболочку ОС

Запрос PIN-кода и логина пользователя при авторизации системными средствами производится кириллицей

3.7 Запуск системы защиты

3.7.1 Консольная оболочка администрирования

Управление **СЗИ НСД** может осуществляться посредством консольной оболочки администратора **СЗИ НСД** путем ввода управляющих команд. Для запуска консольной оболочки необходимо выполнить команду *ishl*.

Для работы в консольной оболочке необходимо в ней авторизоваться.

При первом входе необходимо использовать пароль «*dlladmin*» администратора **СЗИ НСД**. По умолчанию вход осуществляется под именем «*dlladmin*» (учетная запись администратора **СЗИ НСД**) в оболочку администрирования **СЗИ НСД**, расположенную на хосте с IP-адресом 127.0.0.1

и портом 3880. После успешной авторизации строка приглашения ввода команд будет иметь следующий вид:

cli>

Далее необходимо изменить пароль администратора **СЗИ НСД** (см. Таблица 6).

Команда запуска *ishl* имеет ряд параметров, которые можно использовать, чтобы изменить параметры подключения, используемые по умолчанию. Список атрибутов приведен в Таблица 6.

Таблица 6

№	Команда	Описание
1	*-l, --login*	Имя пользователя, под учетной записью которого будет выполняться вход. После успешной авторизации строка приглашения ввода команд будет иметь следующий вид: cli> **Пример:** *ishl -l <логин_администратора_безопасности>* **Важно!** Необходимо изменить пароль администратора **СЗИ НСД**. Для этого администратор **СЗИ НСД** должен последовательно выполнить следующие команды в консольной оболочке администратора: *management <enter>* *users <enter>* *user-update <enter>* *login <логин_пользователя> <enter>* *password <пароль> <enter>* *execute <enter>*
2	*-z, --password*	Пароль пользователя, под учетной записью которого будет выполняться вход. После успешной авторизации строка приглашения ввода команд будет иметь следующий вид: cli> **Пример:** *ishl -z<пароль_администратора_безопасности>*
3	*-a, --address*	Подключение при помощи консольной оболочки администратора **СЗИ НСД** к удаленной рабочей станции, защищенной **СЗИ НСД Dallas Lock Linux**. **Пример:** *ishl -a <ip_адрес_рабочей_станции>* *-l <логин_администратора_безопасности>* или *ishl -a <имя_хоста удаленной рабочей станции>* *-l <логин_администратора_безопасности>* Необходимо ввести пароль учетной записи администратора **СЗИ НСД** удаленной рабочей станции. После успешной авторизации строка приглашения ввода команд будет иметь следующий вид: *<ip_адрес_рабочей_станции>/szi#* — в случае указания IP-адреса рабочей станции или *<имя_хоста удаленной рабочей станции>/szi#* — в случае указания сетевого идентификатора удаленного хоста
4	*-p, --port*	Ввод номера порта.

№	Команда	Описание	
		Пример: *ishl –p <порт_сервера>*	
5	*-v, --version*	Отображение версии консольной оболочки **СЗИ НСД**. **Пример:** *ishl -v* *Command line interface for Information Security System for GNU/Linux ishl: номер сборки*	
6	*-f, --cmd*	При запуске консольной оболочки **СЗИ НСД** возможно указать файл списком команд для удобства применения типовых настроек. **Пример:** *ishl -f <путь и имя_файла>*	
7	*-h, --help*	Вывести справку по использованию параметров консольной оболочки **СЗИ НСД**. **Пример:** *ishl -h* Результат выполнения команды: *Command line interface for Information Security System for GNU/Linux* *Usage: ishl [OPTION...]*	
		-l, --login	*Login to connect to the server*
		-z, --password	*Password to connect to the server*
		-a, --address	*Server's address to connect to*
		-p, --port	*Server's port to connect to*
		-v, --version	*Display version and exit*
		-f, --cmd	*Command file*
		-h, --help	*Display this help and exit*

3.7.2 Графическая оболочка администрирования

Запуск графической консоли (графической оболочки, GUI) в ОС на базе Linux осуществляется с помощью команды *dllgui*. Необходимо в терминале ОС ввести данную команду и нажать *Enter* (см. Рисунок 4).

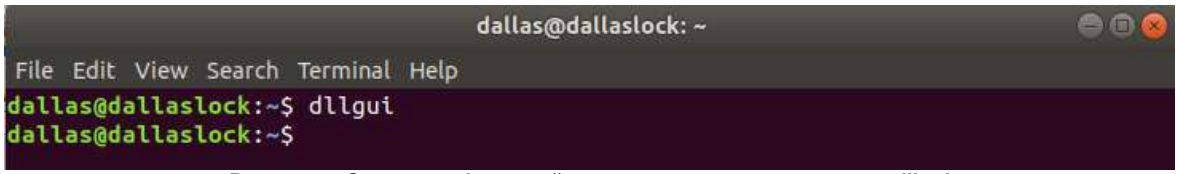


Рисунок 4. Запуск графической консоли с помощью команды dllgui

При запуске графической консоли открывается окно авторизации, где необходимо указать логин пользователя и соответствующий ему пароль (см. Рисунок 5).

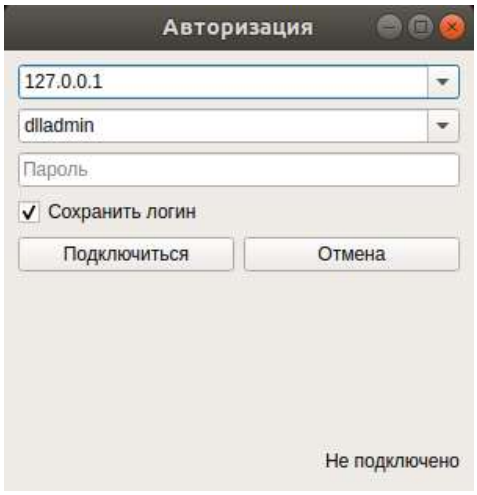


Рисунок 5. Окно авторизации

При первом входе в оболочку администрирования используется пароль администратора **СЗИ НСД** *dlladmin*. По умолчанию вход осуществляется под логином *dlladmin* (учетная запись администратора **СЗИ НСД**) в оболочку администрирования **СЗИ НСД**, расположенную на хосте с IP-адресом 127.0.0.1 и портом 3880.

Далее необходимо изменить пароль администратора **СЗИ НСД** (см. Смена пароля учетной записи пользователя).

После заполнения всех полей в окне авторизации необходимо нажать кнопку «**Подключение**».

Для отмены авторизации необходимо нажать на кнопку «**Отмена**».

После авторизации открывается графическая оболочка **СЗИ НСД** (см. Рисунок 6).

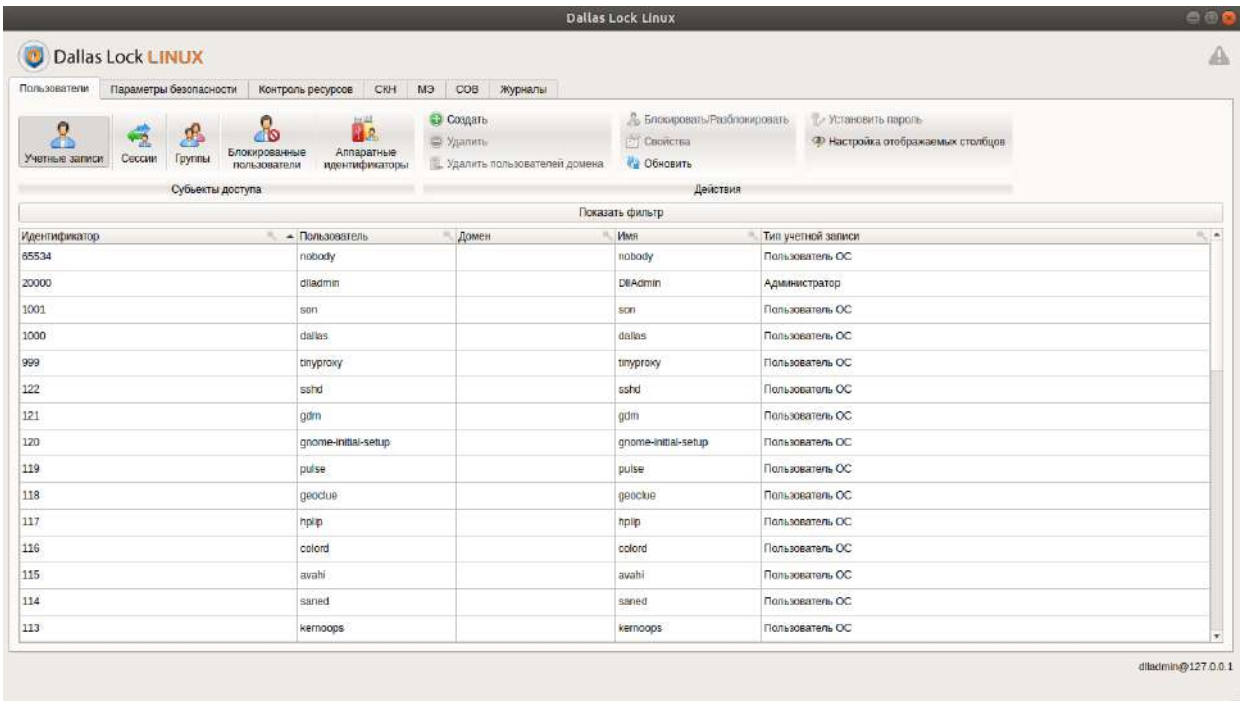


Рисунок 6. Графическая оболочка СЗИ НСД

4 УПРАВЛЕНИЕ И НАСТРОЙКА СИСТЕМЫ ЗАЩИТЫ

4.1 Описание средств администрирования

Управление и настройка **СЗИ НСД** осуществляется с помощью консольной или графической оболочки администрирования.

4.1.1 Консольная оболочка администрирования

Система меню консольной оболочки имеет многоуровневую структуру. Список команд доступных на текущем уровне можно получить при помощи команды *list*, для перехода на уровень выше следует использовать команду *back.*

Если необходимо применить внесенные изменения, выполняется команда *execute*. Для просмотра изменений, которые будут выполнены после команды *execute,* выполняется команда *preview*.

Для вызова встроенной краткой справки по командам в любом меню и подменю используется клавиша **F1**. С помощью клавиши Tab выполняется автодополнение вводимой команды.

Список основных управляющих команд:

- *audit* — переход в подменю подсистемы анализа и журналирования;
- *management* — переход в подменю управления учетными записями пользователей;
- *resources* — переход в подменю подсистемы контроля и разграничения доступа к ресурсам;
- *policies* — переход в подменю управления политиками безопасности;
- *testing* — переход в подменю тестирования системы;
- *information* — переход в подменю управления регистрационными данными **СЗИ НСД**;
- *power-management* — переход в подменю управления питанием (перезагрузка/выключение);
- *services* — переход в подменю встроенных сервисов;
- *management-dll* — переход в подменю для настройки централизованного управления с помощью Единого Центра Управления **Dallas Lock**;
- *firewall* — переход в подменю подсистемы управления межсетевым экраном;
- *list* — вывод списка доступных команд и подменю;
- *help* — вывод информации о встроенных командах;
- *back* — выход из подменю (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dlladmin*.

В *ishl* есть возможность запуска команд *list*, *exit* и *back* от имени корневого раздела меню *ishl* независимо от того, из какого конкретно раздела меню *ishl* она была вызвана.

Пример (с использованием команды *list*):

audit <enter>

list <enter>

Результат выполнения команды:

back
help
list
exit
get-journal
archivate
get-watch
get-watch-all
set-watch
remove-watch
export-ods
export-pdf
export-xml

Таким образом, с помощью команды *list* отображается список доступных команд для раздела *audit*.

Пример (с использованием команды *exit*):

audit <enter>

exit <enter>

Результат выполнения команды: выход из *ishl*.

С помощью команды *exit* происходит выход из консольной оболочки администрирования независимо от того, из какого конкретно раздела меню *ishl* она была вызвана.

Пример (с использования команды *back*):

audit <enter>

get-journal <enter>

back <enter>

Результат выполнения команды: выход из текущего подменю (*get-journal*) на уровень выше (*audit*).

При удаленном доступе к ТС с помощью консольной оболочки администрирования **СЗИ НСД** можно выполнять команды выключения и перезапуска ТС.

Для удаленного выключения ТС в *ishl* необходимо перейти в раздел *power-management* и выполнить команду *mode,* указав в качестве его атрибута значение «0».

Пример:

power-management <enter>

mode 0 <enter>

execute <enter>

Для выполнения удаленной перезагрузки ТС необходимо для атрибута *mode* установить значение «1».

Пример:

power-management <enter>

mode 1 <enter>

execute <enter>

Справочник команд консольной оболочки администрирования

audit — подсистема управления аудитом и просмотра журналов

- get-journal — подсистема журналирования
  - *archive-path* — путь к архивной копии журналов событий информационной безопасности
  - *journal* — наименование журнала, записи которого необходимо экспортировать
  - *event-type* — наименование типа события
  - *from-time* — фильтр по времени появления события, указание нижней границы
  - *till-time* — фильтр по времени появления события, указание верхней границы
  - *user-name* — фильтр по наименованию учетной записи пользователя
  - *result* — фильтр по результату выполнения события
  - *object* — фильтр по объекту доступа
  - *printer* — фильтрация по имени принтера, на который выводится объект для печати
- archivate — команда создания архивных копий журналов
- get-watch — команда с параметром *path* для просмотра прав доступа, на которые назначен аудит на этот объект ФС
- get-watch-all — команда для просмотра списка объектов ФС, находящихся под аудитом
- set-watch — команда с параметрами *path* и *mode* для назначения аудита доступа по выбранным правам доступа на выбранный объект ФС
- remove-watch — команда с параметром *path* для удаления аудита доступа с выбранного объекта ФС
- export-ods — меню экспорта журналов аудита в формат *.ods*
- export-pdf — меню экспорта журналов аудита в формат *.pdf*
- export-xml — меню экспорта журналов аудита в формат *.xml*

management — подсистема управления учетными записями пользователей

- users — управление учетными записями пользователей
  - *user-list* — команда вывода списка учетных записей пользователей
  - *group-list* — команда вывода списка групп учетных записей пользователей
  - *show-domain-users* — команда просмотра списка учетных записей в домене
  - *domain-user-del* — команда удаления учетных записей пользователей домена из базы данных системы защиты **Dallas Lock Linux**
  - *user-add* — команда создания локальной учетной записи
  - *user-update* — команда редактирования атрибутов существующей учетной записи пользователей
  - *user-remove* — команда удаления учетной записи пользователя
  - *user-change-password* — команда смены пароля учетной записи пользователя
  - *user-lock* — команда блокировки учетной записи пользователя
  - *user-unlock* — команда разблокировки учетной записи пользователя
  - *user-show* — команда просмотра атрибутов учетной записи пользователя
  - *user-show-groups* — команда просмотра списка дополнительных групп, в которые входит учетная запись пользователя
  - *user-set-schedule* — команда перехода в раздел для работы расписанием пользователей
  - *user-show-schedule* — команда просмотра и экспорта расписания работы пользователей
  - *user-get-ticket* — команда перехода в раздел получения Kerberos-билета для доступа к доменной информации учетной записи пользователя
- groups — управление группами учетных записей пользователей
  - *user-list* — команда вывода списка учетных записей пользователей
  - *group-list* — команда вывода списка групп учетных записей пользователей
  - *group-add* — команда перехода в раздел добавления группы учетных записей
  - *group-remove* — команда удаления группы учетных записей пользователей
  - *group-add-user* — команда перехода в раздел добавления учетной записи пользователя в группу
  - *group-remove-user* — команда перехода в раздел удаления учетной записи из группы
  - *group-show* — команда просмотра параметров группы пользователей
  - *group-show-users* — команда просмотра списка учетных записей пользователей, входящих в группу
- sessions — управление сессиями учетных записей пользователей
  - *show-all* — команда вывода списка открытых сессий
  - *lock-session* — команда блокировки сессии пользователя
  - *term-session* — команда завершения сессии пользователя
  - *term-user-sessions* — команда завершения сессии пользователя с указанием логина учетной записи пользователя
- tokens — управление аппаратной идентификацией пользователя
  - *tokens-info* — команда вывода информации об аппаратном идентификаторе, который на данный момент подключен к компьютеру
  - *assigned-tokens-info* — команда вывода списка всех назначенных аппаратных идентификаторов
  - *unassign-token* — команда отмены принадлежности аппаратного идентификатора учетной записи пользователя
  - *assign-token* — команда назначения аппаратного идентификатора учетной записи пользователя
  - *change-pin* — команда изменения PIN-кода для аппаратного идентификатора
  - *format* — команда выполнения форматирования аппаратного идентификатора

resources — подсистема контроля и разграничения доступа к объектам файловой системы

- files — подсистема управления файлами
  - dsb — команда перехода в раздел управления доступом
    - *rights-all* — команда вывода списка прав доступа к объекту ФС с указанием полного пути объекта ФС
    - *set-rights-user* — команда настройки прав доступа учетной записи пользователя к объекту ФС
    - *rm-rights-user* — команда удаления прав доступа для выбранной учетной записи

    - *set-rights-group* — команда настройки прав доступа группы пользователей к объекту ФС
    - *rm-rights-group* — команда удаления прав доступа для выбранной группы учетной записи
    - *set-rights-other* — команда настройки прав доступа к объекту ФС для категории «прочие пользователи и группы»
    - *rm-rights-other* — команда удаления прав доступа к объекту ФС для категории учетных записей «Остальные»
    - *get-owner* — команда запроса логина владельца объекта ФС
    - *set-owner* — команда настройки владельца объекта ФС
- erase-file — команда с параметрами «путь» и «количество циклов перезаписи» для гарантированного удаления объекта ФС
- integrity — команда для перехода в раздел контроля целостности объектов файловой системы
    - *show-all* — команда вывода списка объектов ФС с установленным контролем целостности
    - *calc-file* — команда подсчета контрольной суммы файла с указанием параметра «путь» к объекту ФС
    - *unlock-file* — команда удаления объекта ФС из списка подконтрольных объектов с указанием параметра «путь»
    - *restore-file* — команда восстановления файла из резервной копии
    - *verify-file* — команда серки контрольной суммы файла с эталонным значением
    - *lockup-file* — команда установки контроля целостности для объекта ФС
    - *update-file* — команда пересчета и установки новой контрольной суммы для объекта ФС

hardware — подсистема контроля доступа к устройствам

- *show-devices* — команда вывода списка подключенных устройств и устройств, для которых были определены правила разграничения доступа
- *show-usb-ports* — отображение всех портов (USB, COM, LPT), доступных для подключения устройств
- *show-device-info* — отображение таблицы устройств с описаниями
- *show-rules* — команда вывода списка правил разграничения доступа, назначенных на устройство
- *remove-devices* — команда удаления устройства с назначенными правилами разграничения доступа и не подключенное в данный момент, из списка устройств ТС
- *show-mtp-ptp-state* — команда вывода состояния доступа устройств по протоколу MTP/PTP
- *set-mtp-ptp-state* — команда установки правил разграничения доступа на подключение устройств по протоколу MTP/PTP
- set-usb-port-status — команда блокировки/разблокировки порта для всех учетных записей пользователей
- *set-device-info* — команда вывода описания сменного накопителя позволяет заменить установленным названием идентификатор накопителя для работы с накопителем в **СЗИ**
- *set-user-rules* — команда установки правил разграничения доступа к устройству для учетных записей
- *remove-user-rules* — команда удаления правил разграничения доступа к устройству для пользователя
- *set-group-rules* — команда установки правил разграничения доступа к устройству для группы пользователей
- *remove-group-rules* — команда удаления правил разграничения доступа к устройству для группы пользователей
- *set-other-rules* — команда установки правил разграничения доступа к устройству для учетных записей категории «*Остальные*»
- *remove-other-rules* — команда удаления правил разграничения доступа к устройству для учетных записей категории «*Остальные*»
- *remove-device-audit* — команда удаления правил аудита с устройства (типа устройств)
- printers — подсистема разграничения доступа к печатающим устройствам
    - *show-printers-rules* — команда вывода списка правил, назначенных на принтер
    - *set-user-printer-rules* — команда установки правил разграничения доступа на принтер для учетной записи пользователя

- *set-group-printer-rules* — команда установки правил разграничения доступа на принтер для группы пользователей
- *set-other-printer-rules* — команда установки правил разграничения доступа на принтер для категории учетных записей «*Остальные*»
- *remove-user-printer-rules* — команда удаления правил разграничения доступа на принтер для учетной записи пользователя
- *remove-group-printer-rules* — команда удаления правил разграничения доступа на принтер для группы пользователей

- radio-interfaces — подсистема управления беспроводными устройствами
  - *show-status* — команда вывода информации о состоянии беспроводных устройств
  - *block* — команда блокировки всех беспроводных устройств
  - *unblock* — команда разблокировки всех беспроводных устройств
- software — подсистема контроля целостности программных компонентов системы защиты
  - *show-szi-files* — команда вывода списка программных компонентов системы защиты
  - *check-szi-integrity* — команда принудительной проверки целостности программных компонентов системы защиты
  - *lock-szi-files* — команда активации контроля целостности программных компонентов системы защиты
  - *unlock-szi-files* — команда деактивации контроля целостности программных компонентов системы защиты

policies — подсистема управления политиками безопасности

- show-all — команда просмотра текущих значений политик безопасности
- user-get-ticket — команда перехода в раздел аутентификации пользователя домена
- password-policies-set — команда перехода в раздел настройки политик сложности пароля
  - *min-len* — команда определяет минимальную длину пароля
  - *has-spec-sym* — политика определяет необходимость использования в пароле специальных символов
  - *has-digit-sym* — ввод команды определяет необходимость наличия в парольной строчке цифровых символов
  - *has-upperlower-sym* — политика определяет необходимость совместного наличия в парольной строчке строчных и прописных букв
  - *retries* — политика определяет число попыток ввода неверного пароля, после которого произойдет блокировка возможности авторизации под данной учетной записью на определенный промежуток времени
  - *pswd-min-days* — команда задает минимальный срок действия пароля, который необходимо ждать пользователю, чтобы сменить пароль
  - *pswd-max-days* — команда задает максимальный срок действия пароля
  - *pswd-warn-days* — команда задает значение (в днях) после которого пользователю будут выдаваться уведомления о необходимости смены пароля, с указанием количества дней до истечения срока действия пароля
- session-policies-set — команда перехода в раздел настройки политик сессий пользователей
  - *max-sessions* — команда задает максимальное допустимое значение сессий, создаваемое от имени учетной записи пользователя
  - *lock-timeout* — политика задает максимальное время (в минутах) бездействия пользователя, по истечению которого сессия такого пользователя будет заблокирована
  - *schedule-force-shutdown* — политика позволяет выбрать принудительное завершение в качестве действия, применяемого к пользовательским сессиям по наступлению запрещенного интервала времени
- journal-policies-set — команда перехода в раздел настройки периода создания архивных копий журналов информационной безопасности системы защиты
  - *lifetime* — команда определяет срок хранения журналов в месяцах
  - *size* — команда определяет ограничение объемов журналов
  - *archive-path* — путь к архивной копии журналов событий информационной безопасности
- audit-policies-set — команда перехода в раздел настройки политик аудита
  - *entries-policies* — политика определяет, будет ли выполняться сбор событий, связанных с событиями входа в ОС, и запись таких событий в журнал входов
  - *resources-policies* — политика определяет, будет ли выполняться сбор событий, связанных с событиями доступа к защищаемым объектам, и запись таких событий в журнале ресурсов

- *users-policies* — политика определяет, будет ли выполняться сбор событий, связанных с событиями управления пользователями (группами пользователей), и запись таких событий в журнал управления пользователями
- *printing-policies* — политика определяет, будет ли выполняться сбор событий, связанных с событиями печати, и запись таких событий в журнал печати
- *devices-policies* — политика определяет, будет ли выполняться сбор событий, связанных с событиями доступа к устройствам, и запись таких событий в журнал печати
- *syslog-policies* — политика определяет, будут ли регистрироваться системные события в журнале системных событий системы защиты
- *firewall-security-events* — политика определяет, будут ли выполняться сбор событий, связанных с событиями безопасности МЭ
- *firewall-management* — политика определяет, будут ли выполняться сбор событий, связанных с управлением МЭ

- hardware-policies-set **—** установка политик проверки целостности аппаратной среды
  - *check-on-boot* — команда активации/деактивации проверки целостности при загрузке системы
  - *generate-audit* — команда активации/деактивации отслеживания событий нарушения целостности
- firewall-policies-set **—** команда перехода в подменю управления политиками межсетевого экрана
  - *firewall-is-active* — команда активации/деактивации межсетевого экрана
  - *ssl-analyze* — команда активации/деактивации шифрованного трафика
  - *audit* — команда активации/деактивации аудита событий межсетевого экрана
  - *black-white-lists* — команда активации/деактивации белого списка команд
  - *auto-block-interval* — команда определяет максимальный интервал журналирования события типа «Срабатывание правил»
  - *auto-block-burst* — команда определяет максимальное количество журналируемых событий типа «Срабатывание правил»

testing — подсистема тестирования системы защиты

- start-self-test — команда запуска самотестирования системы
- stop-self-test — команда завершения самотестирования системы
- get-self-test-result — команда вывода результата теста самотестирования системы

information — **управление регистрационными данными системы защиты**

- support-serial — команда перехода в раздел управления ключом технической поддержки
  - *set-support-serial* — команда установки ключа технической поддержки
  - *get-support-serial* — команда просмотра номера ключа технической поддержки
  - *get-serial-date* — команда просмотра срока действия ключа технической поддержки
- show-license — команда просмотра номера лицензии **СЗИ НСД**
- show-version — команда просмотра номера текущей версии и сборки **СЗИ НСД**
- set-license — смена номера лицензии **СЗИ НСД**
- change-cert — обновление корневого и пользовательского сертификатов
- show-os-version — просмотр версии операционной системы семейства Linux и версии ядра

power-management — подсистема управления питанием ТС (перезагрузка/выключение)

- mode — команда удаленной перезагрузки ТС/удаленного выключения ТС

services — подсистема удаления системы защиты Dallas Lock Linux

- uninstall — команда для запуска деинсталляции

management-dll — подсистема настройки централизованного управления с помощью Единого Центра Управления Dallas Lock

- disconnect-domain — команда вывода из домена безопасности
- disconnect-sb — команда отключения от сервера безопасности в одностороннем порядке
- synchronize — команда синхронизации системы защиты с **ЕЦУ**
- journals-synchronize — команда синхронизации журналов с **ЕЦУ**
- info — команда отображения информации о домене безопасности
- connect-domain — команда перехода в подменю подключения к домену безопасности
  - *net-name* **—** команда задает сетевое имя или IP-адрес сетевого узла, на котором установлена Служба **ЕЦУ**
  - *name* **—** команда задает сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели **ЕЦУ** в списке управляемых объектов
  - *key* **—** команда задает ключ доступа к **ДБ ЕЦУ**

firewall — подсистема управления межсетевым экраном

- show-netstat — команда вывода статистики сетевых соединений
- remove-blacklist-command — команда удаления приложений из чёрного списка
- show-commands-blacklist — команда вывода из чёрного списка приложений
- remove-whitelist-command — команда удаления приложения из белого списка
- show-commands-whitelist — команда вывода из белого списка приложений
- remove-rule — команда удаления существующего правила межсетевого экрана
- show-rule — команда вывода существующего правила межсетевого экрана
- list-rules — команда вывода всех правил межсетевого экрана
- test-firewall — активация тестирования межсетевого экрана
- show-ifconfig — команда вывода конфигурации адресов и интерфейсов хоста
- import-rules — команда импорта правил в формате JSON из указанного файла в базу данных правил МЭ
- export-rules — команда экспорта правил из базы данных МЭ в указанный файл в формате JSON
- unblock-address — команда разблокировки адреса
- list-profiles — команда вывода всех профилей правил в консоль
- remove-profile — команда удаления существующего профиля правил межсетевого экрана
- set-whitelist-command — команда добавления приложений в белый список
- change-whitelist-command — команда изменения параметров приложений из белого списка
- set-blacklist-command — команда добавления приложения в черный список
- change-blacklist-command — команда изменения параметров приложений черного списка
- set-profile — команда добавления нового профиля правил межсетевого экрана
- change-profile — команда изменения профиля правил межсетевого экрана
- set-rule — команда добавления нового правила межсетевого экрана
- change-rule — команда изменения существующего правила межсетевого экрана

hids — подсистема управления системой обнаружения вторжений

- hids-policies-set — команда перехода в меню установки политик (параметров) безопасности СОВ;
- hids-policies-get — команда просмотра установленных политик (параметров) безопасности СОВ;
- profiles — команда управления профилем СОВ;
- update-sources — команда управления источником обновления набора сигнатур трафика;
- hids-control — команда управления режимом работы СОВ;
- signatures — команда перехода в подраздел управления журнальными сигнатурами, сигнатурами трафика, эвристикой;
- list-blocked-addresses — команда просмотра заблокированных IP-адресов;
- unblock-addresses — команда разблокировки IP-адреса.

4.1.2 Графическая оболочка администрирования

Графическая оболочка администратора **СЗИ НСД** позволяет настраивать систему защиты в соответствии с необходимыми требованиями, управлять работой пользователей, управлять параметрами аудита событий, просматривать журналы событий.

На Рисунок 7 представлено деление главного окна графической консоли на рабочие области.

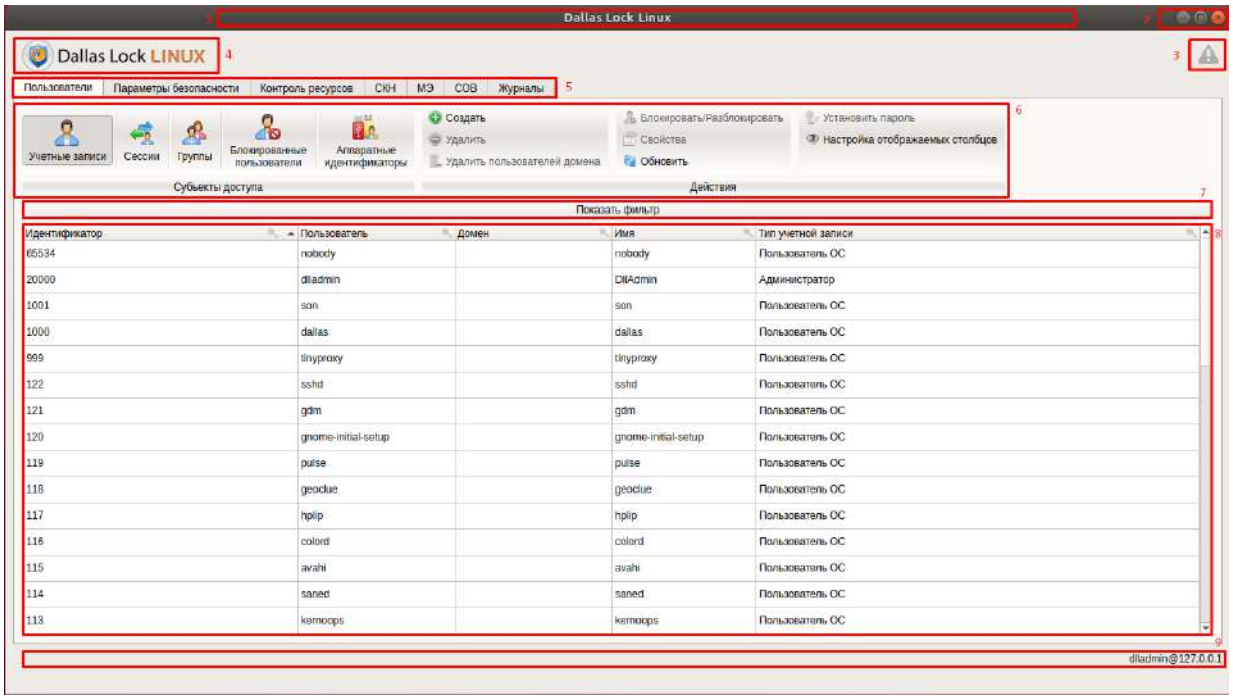


Рисунок 7. Деление окна графической консоли на рабочие области

Принято выделять следующие рабочие области:

1. Заголовок окна, содержащий наименование системы защиты.
2. Кнопка «**Свернуть**», кнопка «**Развернуть**», кнопка «**Закрыть окно**».
3. Кнопка вызова окна «**События НСД**», при нажатии на которую отобразится информация о событиях НСД с указанием времени возникновения события, имени пользователя, типа события и дополнительной информацией о событии НСД (см. Рисунок 8). При регистрации события у кнопки будет отображаться числовой индикатор.

Перечень событий СОВ в окне регистрации «**События НСД**»:

- Адрес заблокирован;
- Обнаружено вторжение.

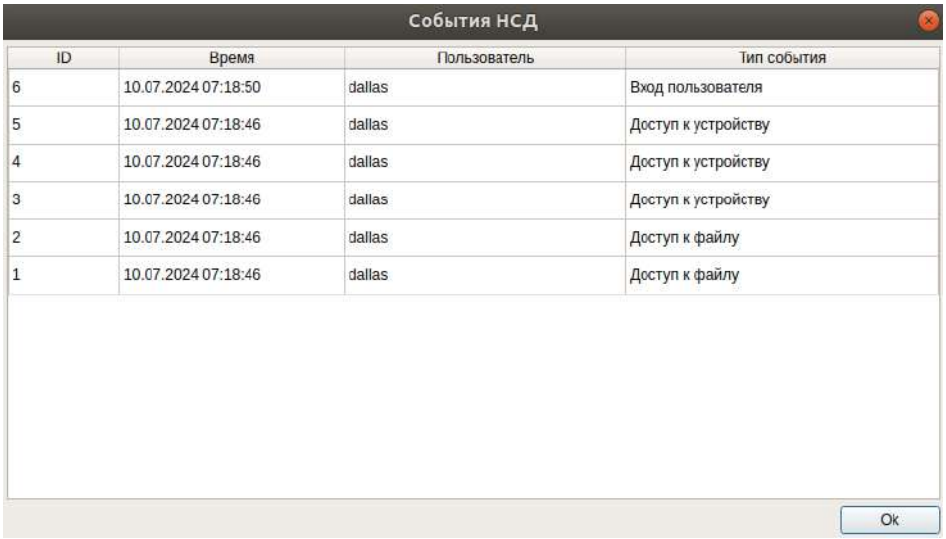


Рисунок 8. События НСД

4. Со следующими сведениями о системе защиты **Dallas Lock Linux** можно ознакомиться в информационном окне «**О программе**» (см. Рисунок 9), вызвав его из списка дополнительных функций кнопки главного меню :

- Соединение;

- Номер сборки;
- Версия GUI;
- Номер лицензии;
- Активные компоненты (модули, на которые приобретена лицензия);
- Код технической поддержки;
- Дата завершения технической поддержки;
- Адрес сайта компании разработчика;
- Адрес сайта продуктовой линейки;
- Адрес технической поддержки;
- Телефон;
- Телеграм-бот.

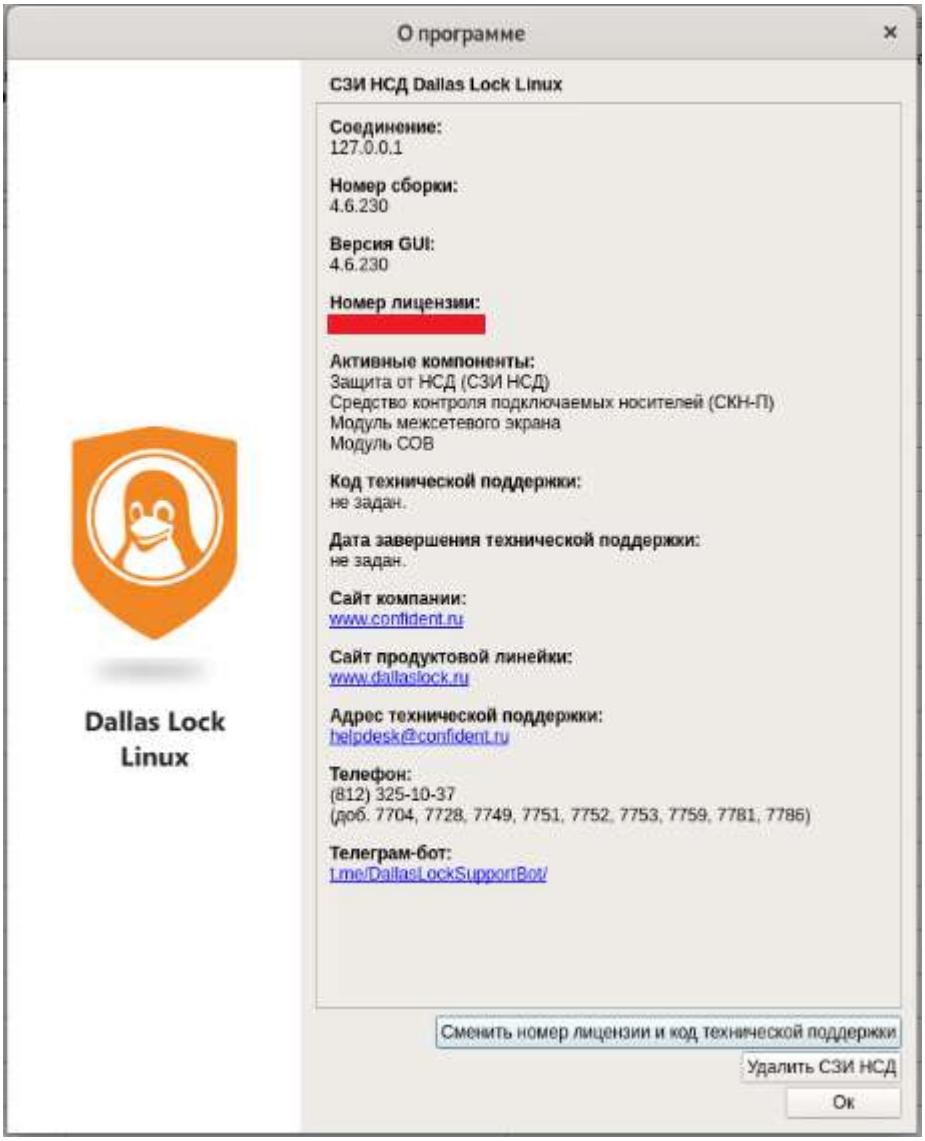


Рисунок 9. О программе

5. Лента с набором вкладок: «Пользователи», «Параметры безопасности», «Контроль ресурсов», «СКН», «МЭ», «СОВ», «Журналы».

6. Панель категорий текущей вкладки и панель инструментов.

7. Кнопка «**Показать фильтр**» — позволяет управлять настройками фильтрации.

8. Рабочая область, содержащая списки параметров или объектов текущей категории.

9. Строка состояния. На левой стороне строки состояния отображается информационное сообщение с указанием выполняемых/выполненных действий (см. Рисунок 59). На правой стороне строки состояния располагается информация, содержащая наименование хоста, имя учетной записи пользователя, запустившего оболочку администратора, адрес хоста.

Вкладка «**Пользователи**» позволяет:

- Управлять учетными записями пользователей, в том числе определять принадлежность аппаратных идентификаторов.
- Создавать локальные группы и включать в них учетные записи пользователей.
- Просматривать список активных сессий (сеансов) учетных записей на данном ТС.
- Контролировать сессии пользователей (закрыть, заблокировать).
- Управлять списком заблокированных учетных записей пользователей.

Вкладка «**Параметры безопасности**» позволяет осуществлять настройку системы защиты в соответствии с политиками безопасности. Вкладка содержит следующие категории:

- «Основные настройки». Содержит список всех параметров безопасности.
- «Настройки сессий». Позволяет регулировать настройки безопасности для сессий учетных записей пользователей (максимальное количество сессий, Время бездействия, после которого будет заблокирован сеанс доступа (в мин.), принудительное завершение работы по расписанию).
- «Политики аудита». Позволяет регулировать ведение журналов и определять срок хранения данных аудита.
- «Политики пароля». Позволяет регулировать настройки безопасности для паролей учетных записей пользователей.
- «Политики контроля целостности». Позволяет регулировать проверку аппаратной целостности и ведения событий аудита аппаратной целостности.
- «Домен безопасности». Позволяет регулировать настройки централизованного управления **СЗИ НСД** с помощью Сервера безопасности **Dallas Lock** и Единого центра управления **Dallas Lock**.

Вкладка «**Контроль ресурсов**». Позволяет настраивать параметры разграничения доступа, аудита и целостности для объектов файловой системы, и устройств.

Вкладка «**СКН**». Позволяет управлять использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) вычислительной техники, типов, подключаемых внешних аппаратных устройств, конкретных съемных машинных носителей информации.

Вкладка «**МЭ**». Позволяет настраивать правила фильтрации сетевого трафика, отображает текущие сетевые соединения. Вкладка содержит следующие категории:

- «Адреса». Просмотр списка активных сетевых соединений АРМ.
- «Заблокированные адреса». Просмотр списка заблокированных адресов АРМ.
- «Соединения». Регистрирует текущие соединения приложений АРМ.
- «Приложения». Позволяет регулировать настройки черного и белого списков приложений для фильтрации трафика по приложениям.
- «Правила МЭ». Позволяет регулировать настройки списка правил межсетевого экрана.
- «Профили МЭ». Позволяет управлять списком профилей правил межсетевого экрана.
- «Параметры». Позволяет управлять политиками межсетевого экрана.
- «Журналы МЭ». В журналах фиксируются события безопасности межсетевого экрана и управление межсетевым экраном.

Вкладка «**СОВ**». Позволяет настраивать, управлять, регистрировать, обнаруживать и блокировать основные угрозы безопасности информации, относящихся к вторжениям (атакам). Вкладка содержит следующие категории:

- «Информация о СОВ». Позволяет просмотреть статистику и обновления.
- «Параметры СОВ». Позволяет управлять параметрами СОВ.
- «Сигнатуры». Категория является инструментом управления сигнатурами СОВ. По умолчанию содержит готовые шаблоны наиболее типовых сигнатур.
- «Блокировки». Позволяет управлять заблокированными адресами.
- «Журналы СОВ». В журналах фиксируются события безопасности СОВ и управление СОВ.

Вкладка «**Журналы**» предназначена для просмотра зарегистрированных событий в журналах информационной безопасности и для предоставления администратору **СЗИ НСД** инструментальных средств для работы с журналами. Вкладка содержит следующие категории журналов:

- «Общие». Просмотр всех зарегистрированных событий.

- «Входы». Журнал входов содержит события аутентификации пользователей в операционной системе.
- «Учетные записи». Журнал управления пользователями содержит события, связанные с созданием учетных записей пользователей, групп учетных записей и их редактированием.
- «Ресурсы». Журнал ресурсов содержит события, связанные с настройками правил разграничения доступа и обращением к защищаемым объектам доступа.
- «Печать». В журнал заносятся все события, связанные с распечаткой документов на локальных и удаленных принтерах.
- «Управление политиками». Журнал управления параметрами содержит события изменения параметров политик безопасности.
- «События ОС». Журнал системных событий содержит события системного журнала ОС (syslog).
- «Устройства». В журнале фиксируются события, связанные с настройкой правил разграничения доступа и получением доступа к подключаемым устройствам.

4.2 Полномочия пользователей на администрирование системы защиты

В системе защиты **Dallas Lock Linux** полномочия на администрирование системы защиты определяются ролью пользователя. Порядок предоставления полномочий подробнее описан в разделе Создание локальной учетной записи пользователя.

В зависимости от предоставленных полномочий, каждый пользователь может быть отнесен к одной из трех категорий:

- **Администратор** — обладает всеми привилегиями на администрирование и аудит системы защиты.
- **Аудитор** — обладает почти всеми привилегиями в части аудита.
- **Пользователь** — все привилегии на администрирование и аудит **Dallas Lock Linux** отключены.

Полномочия **Администратора** по администрированию системы защиты, следующие:

- возможность назначения ролей учетным записям;
- возможность создания и удаления учетных записей и групп, редактирования их свойств;
- возможность настройки политик безопасности;
- возможность назначения прав пользователей;
- возможность регистрации устройств, назначения, изменения и удаления прав доступа для устройств;
- возможность сбора журналов, экспорта, удаления, настройки параметров фильтра журналов;
- возможность архивации (очистки) содержимого журналов аудита;
- возможность изменения номера лицензии и ключа технической поддержки;
- возможность изменения настроек межсетевого экрана, управления правилами МЭ, профилями, соединениями и правилами исключения;
- запуск автоматического тестирования основных функциональных возможностей;
- доступ к настройкам централизованного управления;
- управление параметрами безопасности;
- все возможности роли «Аудитор».

Учетная запись с ролью «*Администратор*» не имеет возможности сменить собственную роль администрирования. Ее может сменить только администратор **СЗИ НСД** *dlladmin*.

Роль **«***Аудитор***»** обладает всеми привилегиями на просмотр информации, в том числе:

- возможность просмотра назначений ролей;
- просмотр списка учетных записей и групп, а также просмотр свойств учетных записей и групп;
- просмотр политик безопасности;
- просмотр прав пользователей и их назначений;
- просмотр списка зарегистрированных устройств, назначенных на них прав доступа;
- возможность сбора и просмотра журналов, настройки параметров фильтра журналов;
- просмотр номера лицензии и ключа технической поддержки;
- просмотр настроек МЭ, правил МЭ, правил исключений, профилей и соединений;
- запуск автоматического тестирования основных функциональных возможностей;
- просмотр настроек централизованного управления.

Роль **«***Пользователь ОС***»** не имеет полномочий на администрирование **СЗИ НСД Dallas Lock Linux**.

4.3 Управление учетными записями пользователей

Подсистема осуществляет управление средствами защиты входа в операционную систему и систему защиты информации, использующих механизмы идентификации и аутентификации пользователей, и предоставляющих аутентифицированную сессию для работы в ОС.

Подсистема базируется на использовании подключаемых аутентификационных модулей (PAM).

Подсистема управления пользователями:

- Реализует хранение идентификационной и аутентификационной информации пользователей, информации о сроках действия, статусах и типах учетных записей пользователей.
- Контролирует сессии работы пользователей, проводит процедуры проверки подлинности.
- Осуществляет управление учетными записями пользователей, группами пользователей — добавление, удаление, блокирование, смена паролей.
- Содержит механизмы работы с аппаратными идентификаторами.

Идентификация и аутентификация пользователя осуществляются при каждом входе в операционную систему и в консольное приложение управления **СЗИ**, проверяется имя пользователя и пароль. Подсистема содержит механизмы проверки качества (надежности) задаваемого пароля при его изменении пользователем.

События об успешных и неуспешных попытках прохождения идентификации и аутентификации пользователя в ОС регистрируются в журналах информационной безопасности **СЗИ**.

В **СЗИ НСД** для усиления процедур идентификации и аутентификации возможно применение аппаратных идентификаторов. В идентификаторе может храниться ключ (сертификат) для усиленной аутентификации пользователя.

4.3.1 Управление учетными записями пользователей в консольной оболочке администрирования

Для перехода в подменю управления учетными записями пользователей в консольной оболочке администрирования необходимо выполнить команду *management*. После выполнения команды система перейдет в соответствующий раздел *management.*

Для данного раздела доступны следующие управляющие команды:

- *users* — переход в подменю управления учетными записями пользователей;
- *groups* — переход в подменю управления группами учетных записей;
- *sessions* — переход в подменю управления сессиями учетных записей пользователей;
- *tokens* — переход в подменю управления аппаратной идентификацией пользователя;
- *list* — просмотр списка управляющих команд раздела;
- *back* — выход из раздела;
- *exit* — выход из консольной оболочки администрирования.

В разделе *management* необходимо выполнить команду *users.* После ввода команды система перейдет в раздел *users (*подменю управления учетными записями пользователей). Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 7.

Информация, приведенная в данном Руководстве по эксплуатации, относится как к локальным, так и к доменным учетным записям, если не указано иное.

Таблица 7

№	Команда	Описание
1	*user-list*	Вывод на экран списка учетных записей пользователей. После ввода команды будет выведен список учетных записей с полями: – идентификатор (*uid*) учетной записи; – логин (*login*) учетной записи пользователя; – имя (*first-name*) пользователя; – идентификатор основной группы (*gid*) группы;

№	Команда	Описание
		– имя домена[10] (*domain*); – название основной группы (*main-group*), в которую входит учетная запись. **Пример:** *management <enter>* *users <enter>* *user-list <enter>* *q <enter>*
2	*group-list*	Вывод на экран списка групп учетных записей пользователей. После ввода команды будет выведен список групп с полями: – идентификатор (*gid*) группы; – наименование группы (*name*); – системная группа (*system*). Атрибут, показывающий, является ли данная группа системной. Принимает значения: *yes* или *no*. В таблице выводятся первые 50 групп, для дальнейшего вывода списка необходимо нажать *Enter*. Команду *Enter* необходимо будет вводить до тех пор, пока система не выдаст весь список групп. По завершению вывода всего списка, снова станут доступны команды из раздела *users.* Для выхода из списка в том случае, когда вывод списка еще не окончен, необходимо набрать команду *q*. **Пример:** *management <enter>* *users <enter>* *group-list <enter>* *q <enter>*
3	*user-add*	Переход в раздел добавления учетной записи пользователя, подробнее — в разделе Создание локальной учетной записи пользователя
4	*user-update*	Команда изменения атрибутов существующей учетной записи пользователя, подробнее — в разделе Просмотр и изменение атрибутов учетной записи пользователей
5	*user-change-password*	Команда смены пароля учетной записи пользователя, подробнее — в разделе Смена пароля учетной записи пользователя
6	*user-lock*	Команда блокировки учетной записи пользователя, подробнее — в разделе Блокировка и разблокировка учетной записи пользователя
7	*user-unlock*	Команда разблокировки учетной записи пользователя, подробнее — в разделе Блокировка и разблокировка учетной записи пользователя
8	*user-remove*	Команда удаления учетной записи пользователя, подробнее — в разделе Удаление учетной записи пользователя
9	*user-show*	Команда просмотра атрибутов учетной записи пользователя, подробнее — в разделе Просмотр и изменение атрибутов учетной записи пользователей
10	*user-show-groups*	Команда просмотра списка дополнительных групп, в которые входит учетная запись пользователя, подробнее — в разделе Просмотр информации о группе пользователей
11	*user-set-schedule*	Переход в раздел управления расписанием работы пользователей, подробнее — в разделе Управление расписанием работы пользователей

[10] Только для доменных учетных записей. Для локальных учетных записей значение этого атрибута — пустое.

№	Команда	Описание
12	*user-show-schedule*	Команда просмотра и экспорта расписания работы пользователей, подробнее — в разделе 4.3.6.2 Просмотр и экспорт расписания работы пользователей
13	*user-get-ticket*	Переход в раздел получения Kerberos-тикета для доступа к доменной информации учетной записи пользователя, подробнее — в разделе Регистрация учетных записей доменных пользователей
14	*show-domain-users <значение>*	Вывод на экран списка учетных записей пользователей домена. При выполнении команды необходимо указать имя домена. **Пример:** *management <enter>* *users <enter>* *show-domain-users DLL.LOCAL <enter>* После ввода команды будет выведен список учетных записей домена с полями: – идентификатор (*uid*) учетной записи; – логин (*login*) учетной записи пользователя; – описание учетной записи
15	*domain-user-del <значение>*	Команда удаления учетных записей пользователей домена из базы данных системы защиты **Dallas Lock Linux**. **Пример:** *management <enter>* *users <enter>* *domain-user-del DLL.LOCAL <enter>*

4.3.2 Управление учетными записями пользователей в графической оболочке администрирования

Для просмотра списка учетных записей пользователей, а также идентификационной и аутентификационной информации таких учетных записей, в графической оболочке **СЗИ НСД** следует выбрать вкладку «**Пользователи**» (см. Рисунок 10).

Рисунок 10. Вкладка «Пользователи»

Панель категорий вкладки «**Пользователи**» содержит разделы «**Субъекты доступа**» и «**Действия**». В рабочей области вкладки отображаются списки объектов выбранной категории раздела «**Субъекты доступа**».

Раздел «**Субъекты доступа**» содержит категории:

– «Учетные записи» — список всех зарегистрированных учетных записей пользователей;

После установки **СЗИ НСД Dallas Lock Linux** в данной категории, кроме зарезервированной учетной записи *dlladmin*[11], отображаются учетные записи пользователей ОС Linux. В данную категорию пользователей входят «демоны»/системные пользователи (пользователи без возможности авторизации) и пользователи, с возможностью авторизации (например, *root*). Удалять пользователей из этого списка не рекомендуется.

- «Сессии» — список всех активных сессий учетных записей на данном ТС;
- «Группы» — список всех групп учетных записей на данном ТС;

После установки **СЗИ НСД Dallas Lock Linux** в данной категории выводится список групп учетных записей ОС Linux. В данную категорию входят группы системных пользователей и группы пользователей, с возможностью авторизации. Удалять группы из этого списка не рекомендуется.

- «Блокированные пользователи» — список заблокированных учетных записей пользователей;
- «Аппаратные идентификаторы» — список зарегистрированных аппаратных идентификаторов.

4.3.3 Создание локальной учетной записи пользователя

Консольная оболочка администрирования

Для создания локальной учетной записи пользователя в консольной оболочке администратора, в подсистеме управления пользователями необходимо выполнить команду *user-add.* После ввода команды система перейдет в раздел *user-add.*

На одну рабочую станцию можно создать не более 10 000 учетных записей пользователей.

Далее консольное приложение будет ожидать последовательного ввода атрибутов создаваемого пользователя, список атрибутов приведен в Таблица 8.

Следует обратить внимание, что все сервисы, которые требуют создания пользователей в системе, рекомендуется устанавливать до установки **СЗИ НСД**. В случае если после установки **СЗИ НСД** возникла необходимость установить какой-либо сервис, который требует создания в системе специального пользователя, можно создать его средствами **СЗИ НСД** (с флагом «системный») до установки сервиса. Необходимо учитывать, что этот способ может не привести к тому, что сервис установится и установится корректно.

У учетной записи администратора[12] должны быть права на запись и выполнение в соответствующем каталоге, где будет создаваться домашняя директория нового пользователя (см. Задание и изменение прав доступа к защищаемым объектам).

Таблица 8

№	Атрибут	Описание
1	*uid <число>*	Системный идентификатор пользователя. **Принимает значения:** от 0 до 65534. По умолчанию — следующее доступное значение. Необязательный атрибут. Если атрибут не указывается, будет использован первый свободный идентификатор в системе
2	*login <значение>*	Наименование учетной записи. Обязательный атрибут. Имена пользователей должны начинаться со строчной буквы или символа подчеркивания и должны состоять только

[11] Зарезервированную учетную запись *dlladmin* нельзя добавлять в дополнительные группы и (или) менять его основную группу *dlladmin*.

[12] Системный администратор *root*, от имени которого будет создаваться домашняя директория.

№	Атрибут	Описание
		из строчных латинских[13] букв, цифр, символов «_» и «-». Могут заканчиваться символом «$»
3	*main-group <значение>*	Наименование основной группы пользователя. При добавлении пользователя группа уже должна быть создана. Обязательный атрибут
4	*password <значение>*	Пароль пользователя. Обязательный атрибут. Устанавливаемое значение должно соответствовать текущим политикам сложности пароля
5	*home <значение>*	Домашняя директория пользователя. Обязательный атрибут. /<полный путь к домашнему каталогу пользователя> **Пример:** *home* "*/home/значение*"
6	*first-name <значение>*	Имя пользователя. Необязательный атрибут. Устанавливаемое значение должно быть заключено в двойные кавычки, например: "Дмитрий"
7	*second-name <значение>*	Фамилия пользователя. Необязательный атрибут. Устанавливаемое значение должно быть заключено в двойные кавычки, например: "Петров". Значение может быть пустым (но обязательно в двойных кавычках)
8	*middle-name <значение>*	Отчество пользователя. Необязательный атрибут. Устанавливаемое значение должно быть заключено в двойные кавычки, например: "Александрович". Значение может быть пустым (но обязательно в двойных кавычках).
9	*shell <значение>*	Интерпретатор командной строки. Необязательный атрибут. /<полный путь к файлу интерпретатору командной строки> **Пример:** /bin/bash На запускаемый файл должны быть установлены права на чтение и запуск для всех пользователей
10	*max-sessions <число>*	Максимальное допустимое значение сессий, создаваемое от имени учетной записи пользователя. Необязательный атрибут. Не распространяется на суперпользователя *root*. **Принимает значения:** -1, от 1 до 20. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на максимальное допустимое значение сессий накладываться не будет
11	*inactive-days <число>*	Допустимый период неиспользования учетной записи. Если период, в который под учетной записью не производился вход в систему, превышает выбранный допустимый период — учетная запись блокируется. Необязательный атрибут. **Принимает значения:** -1, от 0 до 180. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на период ее неиспользования накладываться не будет

[13] С помощью Консоли Единого центра управления **Dallas Lock** (см. раздел Централизованное управление системой защиты) можно создать учетные записи, наименования которых могут содержать символы кириллицы. В результате синхронизации эти учетные записи будут созданы в **СЗИ НСД Dallas Lock Linux**.

№	Атрибут	Описание
12	*blocked <yes/no>*	Статус учетной записи пользователя (активен/заблокирован). Необязательный атрибут. **Принимает значения:** *yes* — пользователь заблокирован, *no* — пользователь не заблокирован. По умолчанию установлено значение *no*
13	*require-password <yes/no>*	Требовать смену пароля при следующем входе в ОС. Необязательный атрибут. **Принимает значения:** *yes* — при входе в ОС, пользователю необходимо сменить пароль, *no* — требования сменить пароль отображено не будет. По умолчанию установлено значение *no*
14	*create-home-directory <yes/no>*	Создание домашней директории для учетной записи пользователя. Обязательный атрибут. Если при создании учетной записи пользователя не будет создана домашняя директория, то вход в графическую оболочку ОС для этого пользователя будет невозможен. Но возможен вход в терминальную оболочку ОС. **Принимает значения:** *yes* — создавать, *no* — не создавать. По умолчанию установлено значение *no*
15	*system <yes/no>*	Указание на то, что учетная запись пользователя является системной. Необязательный атрибут. **Принимает значения:** *yes* — системный пользователь, *no* — не является системным пользователем. По умолчанию установлено значение *no*
16	*no-sync <yes/no>*	Указание на то, что доменная учетная запись будет синхронизирована с Единым Центром Управления **Dallas Lock** или Сервером безопасности **Dallas Lock**. УЗ с установленным значением *no* «не синхронизируемая УЗ» не передаются на **ЕЦУ**/**СБ** (при вводе в **ДБ**). **Принимает значения:** *yes* — учетная запись будет синхронизирована с Единым Центром Управления **Dallas Lock** или Сервером безопасности **Dallas Lock**, *no* — учетная запись не будет синхронизирована
17	*domain <значение>*	Наименование домена, подробнее — в разделе Регистрация учетных записей доменных пользователей
18	*role <значение>*	Роль пользователя. Позволяет предоставить порядок полномочий учетной записи на администрирование системы защиты. **Принимает значения:** *not-admin — роль «Пользователь»*, *master-admin — роль «Администратор»*, *auditor-admin — роль «Аудитор»*. По умолчанию установлено значение *not-admin*
19	*clear*	Команда очистки всех введенных атрибутов при создании учетной записи пользователя

Пример:

management <enter>
users <enter>
user-add <enter>
login pol <enter>
main-group user <enter>

password 87456321 <enter>
home “/home/user“ <enter>
role not-admin <enter>
first-name “Иван” <enter>
second-name “Петров” <enter>
middle-name “ ” <enter>
shell /bin/bash <enter>
max-sessions 1 <enter>
inactive-days -1 <enter>
create-home-directory yes <enter>
system yes <enter>
execute <enter>

Если в процессе определения атрибутов учетной записи было задано неверное значение параметра, то после ввода команды *execute* система выдаст соответствующие предупреждение и учетная запись не будет создана. Например, если при определении атрибутов было указано имя несуществующей группы, система после ввода команды *execute* выдаст сообщение «*Unknown main group*» («*Неизвестная основная группа*»).

Если все атрибуты были определены верно, то после ввода команды *execute* учетная запись будет создана, и система выдаст сообщение «*Command ‘user-add’ executed successfully*» (команда *‘user-add’* успешно выполнена).

Для создания «демона» — системного пользователя Linux, без возможности авторизации по паролю, необходимо задать параметру *system* значение «*yes*», а параметру *password* значение «!!».

Графическая оболочка администрирования

Для создания учетной записи пользователя с помощью графической оболочки **СЗИ НСД** на вкладке «Пользователи» необходимо выбрать категорию «**Учетные записи**» и нажать на кнопку  «**Создать**» на панели действий (см. Рисунок 6).

Все сервисы, которые требуют создания пользователей в системе, рекомендуется устанавливать до первоначальной установки **СЗИ НСД**. В случае если после установки **СЗИ НСД** возникла необходимость в установке какого-либо сервиса, который требует создания в системе специального пользователя, можно создать его средствами **СЗИ НСД** (с флагом системный) до установки сервиса. Необходимо обратить внимание, что этот способ может не привести к желаемому результату.

После нажатия на кнопку «**Создать**» открывается окно выбора размещения учетной записи (см. Рисунок 11).

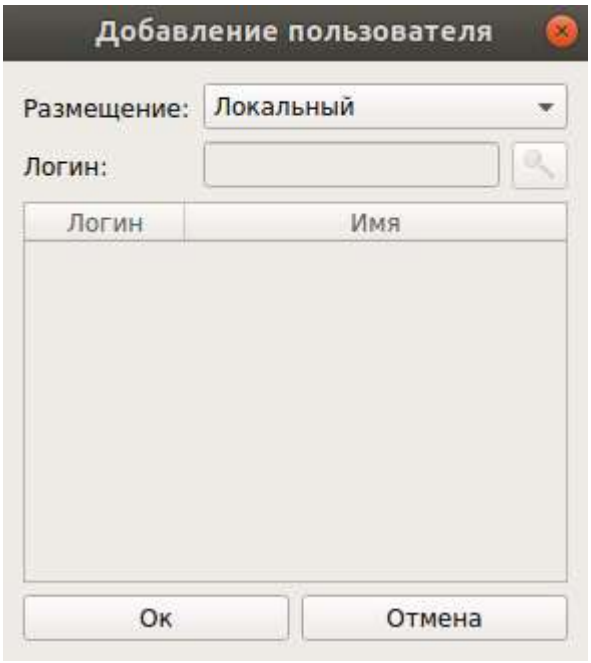


Рисунок 11. Выбор размещения учетной записи

Для создания локальной учетной записи необходимо выбрать в выпадающем списке поля «*Размещение*» значение «*Локальный*». Нажать на кнопку «**Ок**», далее откроется форма «**Добавить пользователя**» (см. Рисунок 12).

На одну рабочую станцию можно создать не более 10 000 учетных записей пользователей.

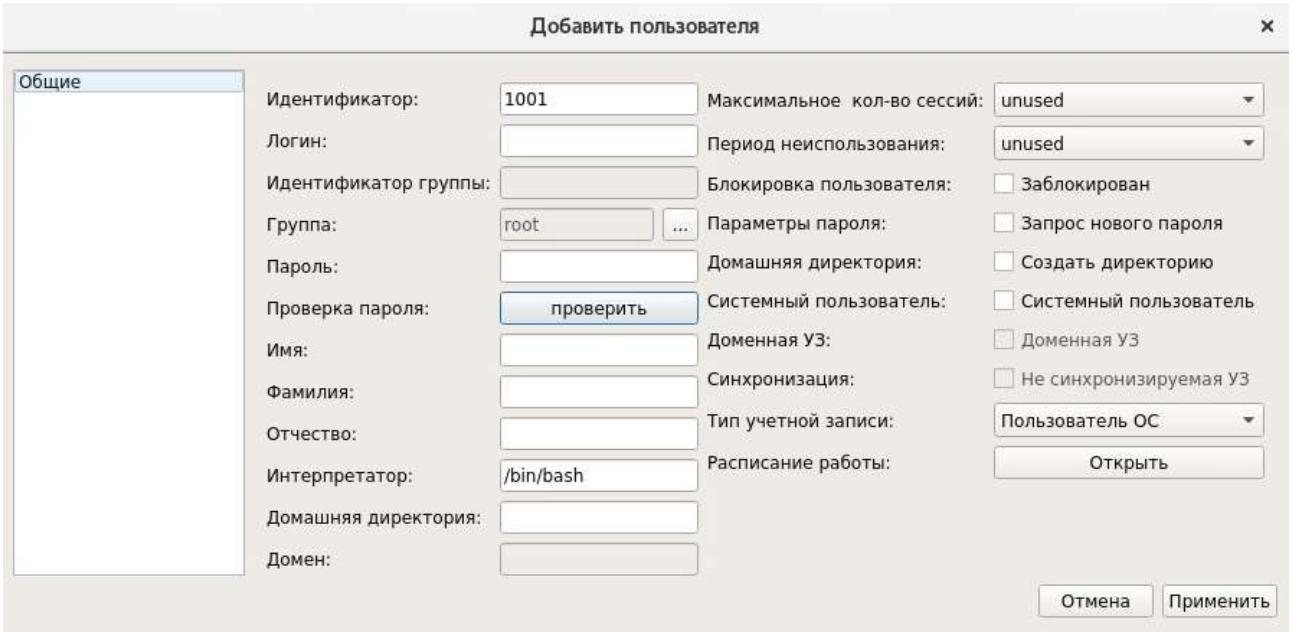


Рисунок 12. Параметры учетной записи пользователя

Раздел «*Общие*» содержит следующий список доступных атрибутов:

– «Идентификатор» — системный идентификатор учетной записи пользователя. Принимает значения: от 0 до 65534. По умолчанию устанавливается и используется следующий доступный идентификатор в системе. Необязательный атрибут;

- «Логин» — наименование учетной записи. Обязательный атрибут. Имена пользователей должны начинаться со строчной буквы или символа подчеркивания и должны состоять только из строчных латинских[14] букв, цифр, символов «_» и «-». Могут заканчиваться символом «$»;
- «Группа» — наименование основной группы пользователя. При добавлении учетной записи группа должна быть уже создана. По умолчанию в поле указана основная группа пользователя, под учетной записью которого выполняется создание новой учетной записи. Обязательный атрибут;
- «Пароль» — пароль пользователя. Устанавливаемое значение должно соответствовать политикам сложности пароля. Обязательный атрибут;
- «Проверка пароля» — кнопка проверки соответствия назначенного пароля установленным политикам сложности паролей. Если пароль соответствует/не соответствует политикам безопасности, то при проверке система выдаст информационное сообщение (см. Рисунок 13 и Рисунок 14). Текст информационного сообщения о несоответствии пароля зависит от того, по каким параметрам не прошел проверку пароль (например, «Отсутствуют цифры в пароле» или «Отсутствуют спецсимволы в пароле»);

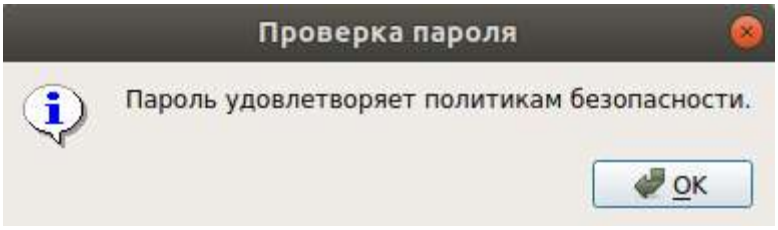


Рисунок 13. Информационное сообщение

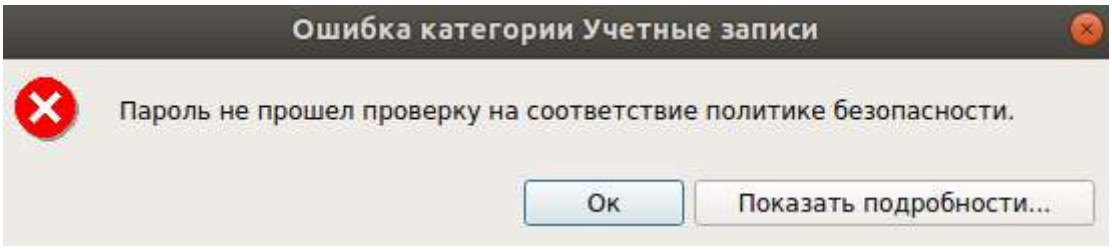


Рисунок 14. Информационное сообщение

- «Имя» — Имя пользователя. Является обязательным атрибутом, значение может быть пустым. По умолчанию в поле отображается логин учетной записи;
- «Фамилия» — Фамилия пользователя. Значение может быть пустым. Необязательный атрибут;
- «Отчество» — Отчество пользователя. Значение может быть пустым. Необязательный атрибут;
- «Интерпретатор» — интерпретатор командной строки. В данном поле указывается полный путь к файлу интерпретатору командной строки. На указанный файл должны быть установлены права на чтение и запуск для всех пользователей. По умолчанию в поле указан путь /bin/bash. Обязательный атрибут;

Интерпретатор — программа, принимающая и выполняющая команды.

- «Домашняя директория» — домашняя директория пользователя, поле заполняется автоматически (есть возможность редактировать вручную). Формат заполнения: */home/логин*. По умолчанию при создании учетной записи в поле «Домашняя директория» указывается путь */home/наименование учетной записи*. Обязательный атрибут (если установлен флаг «Создавать домашнюю директорию»);

[14] С помощью Консоли Единого Центра Управления **Dallas Lock** (см. раздел Централизованное управление системой защиты) можно создать учетные записи, наименования которых могут содержать символы кириллицы. В результате синхронизации эти учетные записи будут созданы в **СЗИ НСД Dallas Lock Linux**.

- «Максимальное кол-во сессий» — максимально допустимое значение сессий[15], создаваемое от имени учетной записи пользователя. Принимает значения: от 0 до 10. По умолчанию установлено значение «Не используется». Обязательный атрибут;
- «Период неиспользования» — допустимый период неиспользования учетной записи. Принимает значения: от 0 до 180. Если период, в течение которого под учетной записью не производился вход в систему, превышает выбранный допустимый период — учетная запись блокируется;
- «Блокировка пользователя» (флаг) — при установленном флаге учетная запись блокируется (становится неактивной), вход в ОС на защищенном АРМ запрещен. Для пользователей, в данный момент работающих в системе, в момент блокировки учетной записи сеанс не блокируется, блокируется следующий вход в систему. По умолчанию флаг не установлен;
- «Параметры пароля. Запрос нового пароля» (флаг) — требовать смену пароля при следующем входе в ОС. По умолчанию флаг не установлен. Если флаг установлен, то при входе в ОС, пользователю необходимо сменить пароль. Необязательный атрибут;
- «Домашняя директория. Создать директорию» (флаг) — если при создании учетной записи пользователя не будет создана домашняя директория, то вход в систему для этой учетной записи будет невозможен. По умолчанию флаг не установлен. Необязательный атрибут;

У учетной записи администратора[16] должны быть права на запись и выполнение в соответствующем каталоге, где будет создаваться домашняя директория нового пользователя (см. раздел Разграничение доступа к объектам файловой системы).

- «Системный пользователь» (флаг) — указание на то, что пользователь является системным пользователем. По умолчанию флаг не установлен. Необязательный атрибут;
- «Тип учетной записи» — роль пользователя. Позволяет предоставить порядок полномочий учетной записи на администрирование системы защиты, подробнее — в разделе Полномочия пользователей на администрирование системы защиты.
- «Расписание работы» — управление расписанием работы и период действия учетной записи пользователя, подробнее — в разделе Управление расписанием работы пользователей.

Учетная запись пользователя может быть включена в дополнительные группы. Для добавления учетной записи в дополнительные группы необходимо в окне параметров учетной записи выбрать раздел «Группы» (см. Рисунок 15).

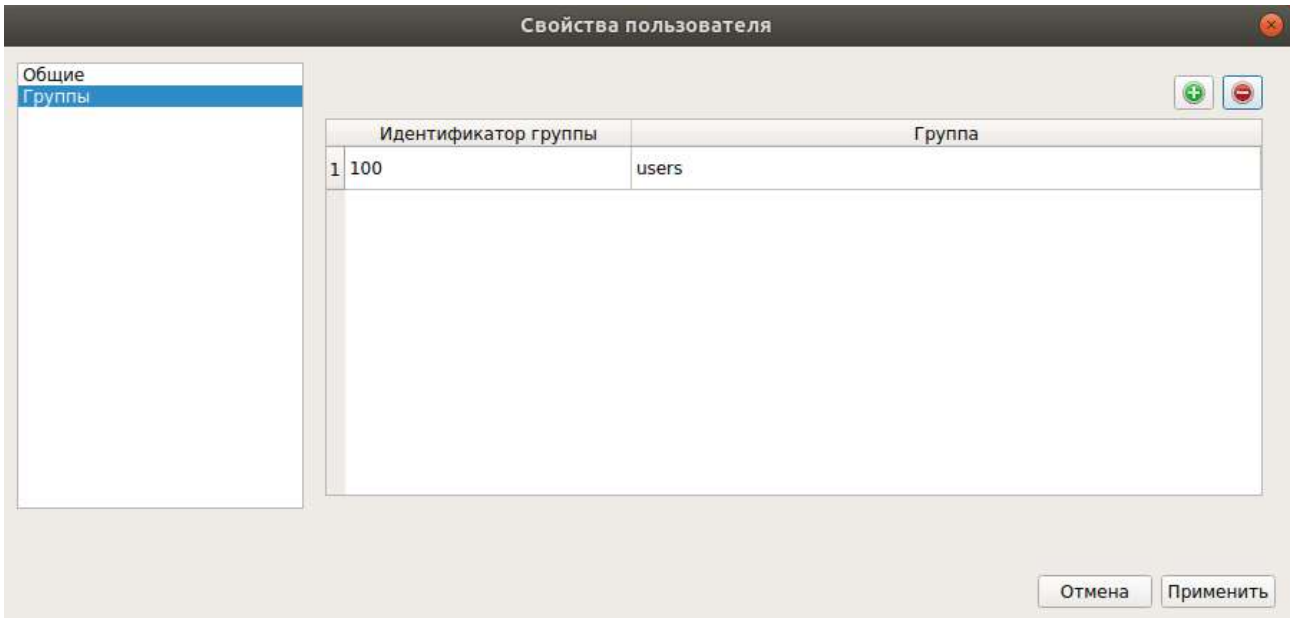


Рисунок 15. Раздел «Группы»

[15] Не распространяется на суперпользователя root.

[16] Системный администратор *root*, от имени которого будет создаваться домашняя директория.

Добавить дополнительные группы можно только в режиме редактирования параметров учетной записи пользователя.

Для добавления учетной записи в группу необходимо нажать на кнопку «**Добавить в группу**», далее откроется форма выбора группы (см. Рисунок 16).

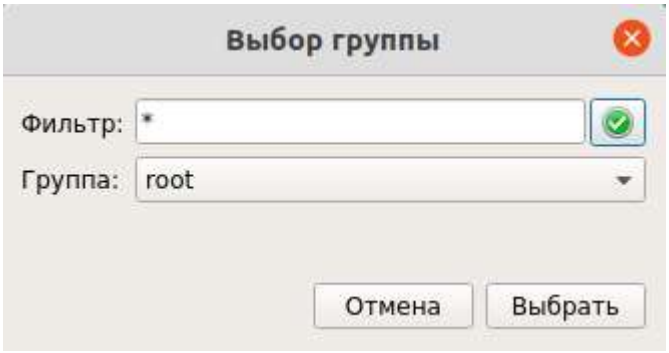


Рисунок 16. Форма выбора группы

Из выпадающего списка необходимо выбрать наименование группы и нажать на кнопку «**Выбрать**», после чего имя группы отобразится в списке дополнительных групп учетной записи пользователя.

Для удаления учетной записи из группы необходимо выделить наименование группы в списке и нажать на кнопку «**Удалить из группы**».

При создании учетной записи пользователя есть возможность изменить основную группу пользователя. Для этого в окне «Добавить пользователя» (см. Рисунок 12) необходимо напротив атрибута «*Группы*» нажать на кнопку ... . Далее откроется окно редактирования основной группы ученой записи пользователя.

4.3.4 Регистрация учетных записей доменных пользователей

СЗИ НСД предоставляет возможность работы на защищенных АРМ не только для локальных, но и для доменных учетных записей пользователей. Стоит отметить, что для корректного взаимодействия доменных пользователей и **СЗИ НСД** обязательно, чтобы АРМ было введено в домен.

Для работы с доменными учетными записями (регистрация, авторизация и т.д.) необходимо убедиться в том, что настройки сети корректны и имя домена доступно по сети (необходимо проверить доступность имени домена с указанием имени АРМ, являющегося контроллером домена, — *<hostname>.<domain>* и без указания имени этого АРМ — *<domain>*). Контроллер домена должен быть доступен по сети как по ip-адресу, так и по FQDN. Если в сети несколько контроллеров домена, их FQDN должны быть указаны в разделе URL файла */etc/ldap/ldap.conf*.

Непосредственно на клиентских рабочих станциях выполняется только регистрация доменных учетных записей пользователей, уже существующих в домене. Управление доменными УЗ (создание, удаление, блокировка) выполняется непосредственно на контроллере домена.

При регистрации доменных учетных записей по маске Сервер безопасности **Dallas Lock/ЕЦУ Dallas Lock** и рабочая станция Linux, на которой установлен **СЗИ НСД**, должны быть участниками одного контроллера домена.

Консольная оболочка администрирования

Для регистрации учетной записи пользователя в **СЗИ НСД** конкретного домена необходимо получить разрешение на получение информации в домене. Для этого необходимо в консольной оболочке администратора в подсистеме управления пользователями (*users*) выполнить команду *user-get-ticket.* После ввода команды система перейдет в раздел *user-get-ticket.* Система будет ожидать ввод логина, имя домена и пароль регистрируемой учетной записи (см. Таблица 9).

Необходимо в конфигурационном файле Kerberos — *krb5.conf* указать, что kerberos-тикеты пользователей должны храниться в ядре ОС:

1. Открыть */etc/krb.5.conf* с правами суперпользователя (root).
2. В файле */etc/krb.5.conf* в разделе [*libdefalts*] прописать *default_ccache_name = KEYRING:persistent:%{uid}.*

Для просмотра информации полученного Kerberos-тикета необходимо выполнить в терминале ОС команду *klist -A* (см. Рисунок 17).

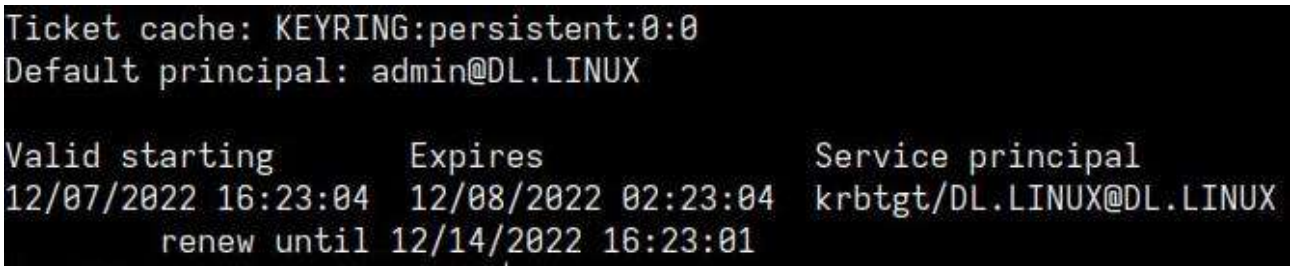


Рисунок 17. Информации Kerberos-тикета

Для дальнейшей регистрации доменной учетной записи пользователя в консольной оболочке администратора в подсистеме управления пользователями (*users*) доступны атрибуты, приведенные в таблице ниже.

Таблица 9

№	Атрибут	Описание
1	*user-get-ticket*	Переход в раздел получения Kerberos-билета для доступа к доменной информации учетной записи пользователя. **Пример:** *management <enter>* *users <enter>* *user-get-ticket <enter>* *login user@DLL.LOCAL <enter>* *password ***** <enter>* *execute <enter>* При успешном выполнении команды система выдаст следующее сообщение: *Success getting user credentials* (*Успешное получение учетных данных пользователя)*
2	*show-domain-users <domain-name>*	Вывод на экран списка учетных записей пользователей домена. При выполнении команды необходимо указать имя домена. **Пример:** *management <enter>* *users <enter>* *show-domain-users DLL.LOCAL <enter>* После ввода команды будет выведен список учетных записей домена с полями: – идентификатор (*uid*) учетной записи; – логин (*login*) учетной записи пользователя; – описание учетной записи
3	*user-add*	Регистрация доменной учетной записи пользователя. **Пример:** *management <enter>* *users <enter>*

№	Атрибут	Описание
		user-add <enter> *login user <enter>* *domain DLL.LOCAL <enter>* *execute <enter>* При успешном выполнении регистрации доменной учетной записи пользователя, система выдаст следующее сообщение: *Success registering domain user "DLL.LOCAL\user" (Успешная регистрация пользователя домена "DLL.LOCAL\user")*
4	*domain-user-del <all/domain-name>*	Команда удаления учетных записей пользователей домена из базы данных системы защиты **Dallas Lock Linux**. **Принимает значения:** *all* — удаление всех учетных записей пользователей из базы данных системы защиты, *<domain-name>* — удаление учетных записей пользователей из базы данных системы защиты определённого домена. **Пример:** *management <enter>* *users <enter>* *domain-user-del DLL.LOCAL <enter>*
5	*user-remove*	Команда удаления одной учетной записи пользователя домена из базы данных системы защиты **Dallas Lock Linux**. **Пример:** *management <enter>* *users <enter>* *user-remove <enter>* *login user <enter>* *domain DLL.LOCAL <enter>* *execute <enter>* При успешном удалении учетной записи пользователя домена система выдаст следующее сообщение: *Success removing user "DLL.LOCAL\user" (Успешное удаление пользователя "DLL.LOCAL\user")*

Графическая оболочка администрирования

Для проверки статуса домена с помощью графической оболочки необходимо открыть окно «**Статус домена**», вызвав его из списка дополнительных функций кнопки главного меню  . Может потребоваться ввод авторизационных данных уполномоченного пользователя для подтверждения Kerberos-тикета (см. Рисунок 18).

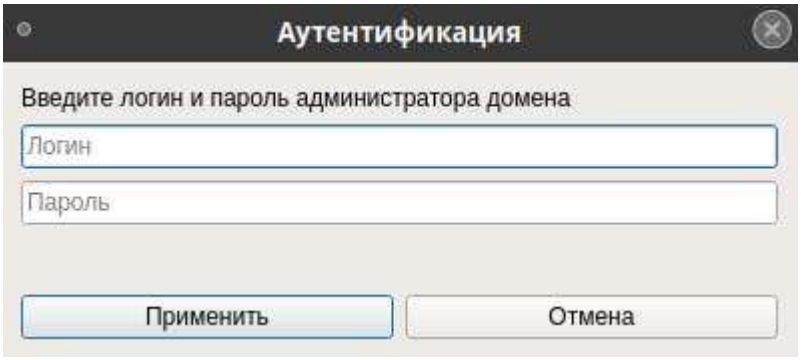


Рисунок 18. Аутентификация уполномоченного пользователя

При успешном подтверждении данных уполномоченного пользователя появится информационное сообщение в строке состояния (см. Рисунок 19), далее — окно «**Статус**» (см. Рисунок 20).

Рисунок 19. Успешное получение Kerberos-тикета пользователя домена

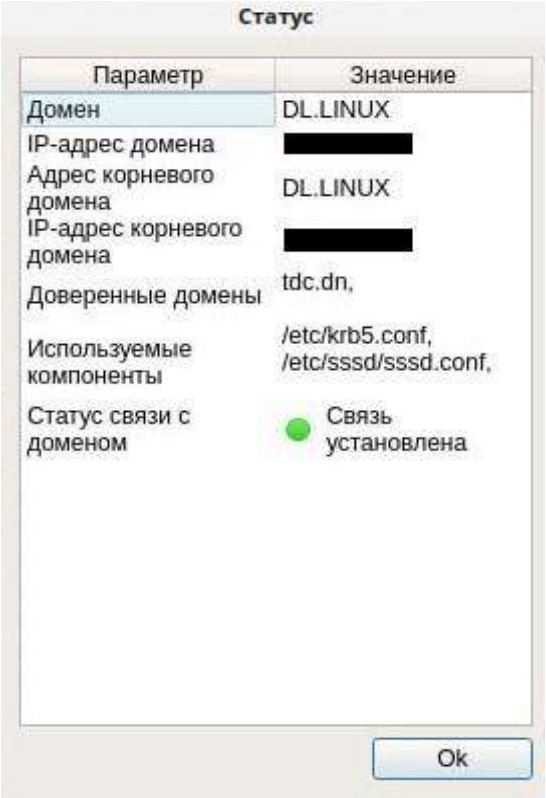


Рисунок 20. Статус

4.3.4.1 Регистрация доменных пользователей по маске

В системе защиты **Dallas Lock Linux** реализован механизм регистрации доменных учетных записей пользователей системы с использованием масок, по символу «*». В этом контексте символ «*» имеет значение «все». Учетная запись «Имя_домена*» указывает на всех пользователей данного домена. Учетная запись «**» указывает на всех доменных пользователей (в том числе доверенных доменов). Учетная запись «Имя_домена\логин_УЗ» указывает на пользователя «логин_УЗ» домена «Имя_домена».

Если для существующей учетной записи вида «**» запретить вход в систему (заблокировать УЗ), и одновременно разрешить вход для учетных записей типа «ZCB*», то на АРМ смогут входить только пользователи домена ZCB, пользователи всех остальных доменов входить не смогут.
Если запретить вход в систему для записи «ZCB*» (заблокировать УЗ), и разрешить для «ZCB\user1», «ZCB\user2», то это будет означать, что из домена ZCB на АРМ смогут входить только пользователи user1 и user2.

Таким образом, систему проверки пользователей можно легко привести к «строгой» системе, достаточно отключить учетную запись «**», и далее в явном виде регистрировать учетные записи необходимых доменных пользователей.

Консольная оболочка администрирования

Для регистрации доменной учетной записи пользователя в **СЗИ НСД** в консольной оболочке администратора в подсистеме управления пользователями (*users*) необходимо выполнить команду *user-add*. Система перейдет в раздел user-add. Ниже представлены примеры регистрации доменных пользователей по маске.

Регистрация всех пользователей домена по маске.

Пример:

management <enter>

users <enter>

user-add <enter>

login DLL.LINUX <enter>*

execute <enter>

*Success creating user '**' (Успешная создание пользователей '**')*

Регистрация пользователя домена по маске

Пример:

management <enter>

users <enter>

user-add <enter>

login DLL.LINUX\\user <enter>

execute <enter>

Success registering domain user 'DLL.LINUX\user' (Успешная регистрация пользователя домена DLL.LINUX\user')

Регистрация всех доменных пользователей (в том числе доверенных доменов)

Пример:

management <enter>

users <enter>

user-add <enter>

*login ** <enter>*

execute <enter>

*Success creating user '**' (Успешная создание пользователей '**')*

Графическая оболочка администрирования

Для регистрации учетной записи пользователя с помощью графической оболочки **СЗИ НСД** на вкладке «**Пользователи**» необходимо выбрать категорию «**Учетные записи**» и нажать на кнопку «**Создать**» на панели действий (см. Рисунок 10).

> **!** Все сервисы, которые требуют создания пользователей в системе, рекомендуется устанавливать до первоначальной установки **СЗИ НСД**. В случае если после установки **СЗИ НСД** возникла необходимость в установке какого-либо сервиса, который требует создания в системе специального пользователя, можно создать его средствами **СЗИ НСД** (с флагом системный) до установки сервиса. Необходимо обратить внимание, что этот способ может не привести к желаемому результату.

Для регистрации доменной учетной записи необходимо выбрать в выпадающем списке поля «*Размещение*» значение «<Имя домена>»[17]. При выборе имени домена может потребоваться ввод авторизационных данных уполномоченного пользователя[18] (администратора контроллера домена). Затем открывается форма «*Добавление пользователя*» (см. Рисунок 21, Рисунок 22).

[17] В данном выпадающем списке будет имя домена, для работы с которым настроено **СЗИ НСД** из раздела Регистрация учетных записей доменных пользователей. В выпадающем списке отобразятся также имена доверенных доменов, они тоже будут доступны для выбора.

[18] Уполномоченный пользователь обладает правами доступа к списку УЗ домена и к их необходимым атрибутам.

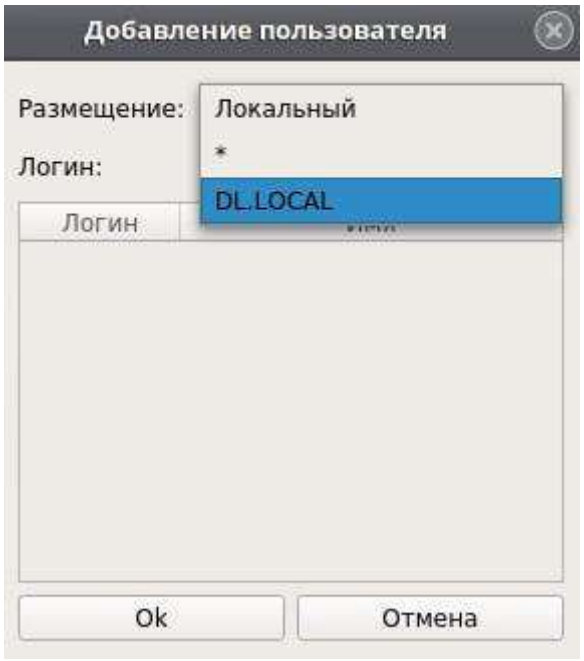


Рисунок 21. Выбор размещения УЗ

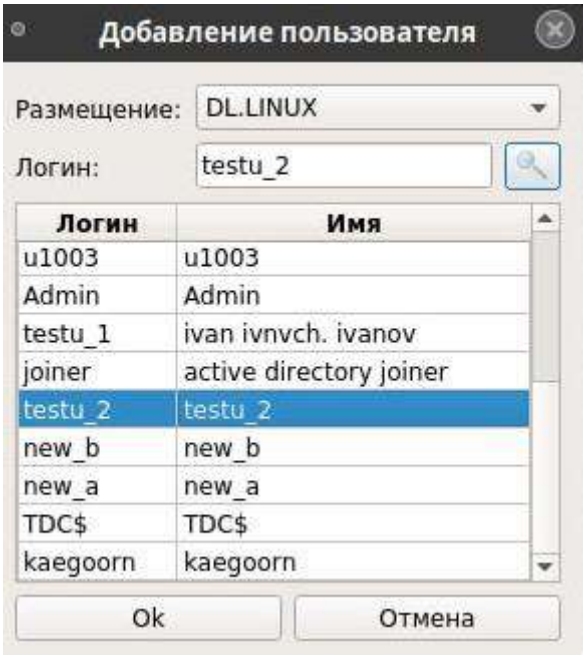


Рисунок 22. Выбор пользователя домена для регистрации в СЗИ НСД

Форма по добавлению доменной учетной записи отличается от формы по добавлению локальной учетной записи тем, что для доменной учетной записи заполнено поле «*Домен*». Раздел «*Общие*» содержит список атрибутов, аналогичный списку атрибутов для локальной учетной записи.

В режиме редактирования доступны следующие атрибуты:

- «Максимальное кол-во сессий» — максимально допустимое значение сессий, создаваемое от имени учетной записи пользователя. Принимает значения: от 0 до 10. По умолчанию установлено значение «Не используется». Обязательный атрибут;
- «Интерпретатор» — интерпретатор командной строки. В данном поле указывается полный путь к файлу интерпретатору командной строки. На указанный файл должны быть установлены права на чтение и запуск для всех пользователей. По умолчанию в поле указан путь /bin/bash. Обязательный атрибут;
- «Блокировка пользователя» (флаг) — при установленном флаге учетная запись блокируется (становится неактивной), вход в ОС на защищенном АРМ запрещен. Для пользователей, в данный момент работающих в системе, в момент блокировки учетной записи сеанс не блокируется, блокируется следующий вход в систему. По умолчанию флаг не установлен;

- «Параметры пароля. Запрос нового пароля» (флаг) — требовать смену пароля при следующем входе в ОС. По умолчанию флаг не установлен. Если флаг установлен, то при входе в ОС, пользователю необходимо сменить пароль. Необязательный атрибут.
- «Расписание работы» — настройка расписания работы и период действия учетной записи, подробнее — в разделе Управление расписанием работы пользователей.
- «Синхронизация» — указание на то, что учетная запись будет синхронизирована с Единым центром управления **Dallas Lock** или Сервером безопасности **Dallas Lock**. УЗ с установленным чекбоксом «не синхронизируемая УЗ» не передаются на **ЕЦУ/СБ** (при вводе в **ДБ**).

Значения остальных атрибутов редактировать нельзя.

Доменные учетные записи могут быть добавлены в дополнительные группы таким же способом, что и локальные учетные записи.

4.3.5 Просмотр и изменение атрибутов учетной записи пользователя

Консольная оболочка администрирования

Для просмотра атрибутов учетной записи пользователя в консольной оболочке администрирования, в подсистеме управления пользователями *users* необходимо выполнить команду *user-show*, далее — указать логин учетной записи пользователя и имя домена (если учетная запись принадлежит домену).

Пример:

management <enter>

users <enter>

user-show <enter>

login <имя_пользователя> <enter>

domain <имя_домена> <enter>

execute <enter>

Для изменения атрибутов существующей учетной записи пользователя необходимо воспользоваться командой *user-update.* После ввода управляющей команды необходимо указать наименование учетной записи, затем атрибуты учетной записи и их новые значения. Допускается изменение атрибутов в произвольном порядке и необходимом количестве.

Список атрибутов пользователя доступных для обновления:

- *password* — пароль пользователя;
- *login* — наименование учетной записи;
- *main-group* — группа учетной записи;
- *role* — роль администрирования пользователя;
- *first-name* — имя пользователя;
- *second-name* — фамилия пользователя;
- *middle-name* — отчество пользователя;
- *shell* — наименование оболочки командной строки;
- *max-sessions* — максимальное допустимое значение сессий, создаваемое от имени учетной записи пользователя;
- *inactive-days* — допустимый период неиспользования учетной записи;
- *require-password* — требовать смену пароля при следующем входе в ОС;
- *no-sync* — синхронизировать учетную запись пользователя с Единым Центром Управления **Dallas Lock** или Сервером безопасности **Dallas Lock**.

Полное описание атрибутов приведено в Таблица 10.

Пример:

management <enter>

users <enter>

user-update <enter>

login dlladmin <enter>

second-name “Петров” <enter>

execute <enter>

После успешного выполнения команды система выдаст сообщение «*Command 'user-update' executed successfully*» (команда *'user-update'* успешно выполнена).

Для доменных учетных записей, зарегистрированных в **СЗИ НСД**, для обновления доступны атрибуты, приведенные в таблице ниже.

На запускаемый файл должны быть установлены права на чтение и запуск для всех пользователей.

Таблица 10

№	Атрибут	Описание
1	*shell <значение>*	Интерпретатор командной строки. Обязательный атрибут. /<полный путь к файлу интерпретатору командной строки> **Пример:** /bin/bash
2	*max-sessions <число>*	Максимальное допустимое значение сессий, создаваемое от имени учетной записи пользователя. Обязательный атрибут. **Принимает значения:** -1, от 1 до 20. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на максимальное допустимое значение сессий накладываться не будет
3	*user-lock*	Команда блокировки учетной записи пользователя, подробнее — в разделе Блокировка и разблокировка учетной записи пользователя
4	*user-set-schedule*	Переход в раздел управления расписанием работы пользователей, подробнее — в разделе Управление расписанием работы пользователей
5	*no-sync <yes/no>*	Указание на то, что учетная запись будет синхронизирована с Единым Центром Управления **Dallas Lock** или Сервером безопасности **Dallas Lock**. УЗ с установленным значением *no* «не синхронизируемая УЗ» не передаются на **ЕЦУ/СБ** (при вводе в **ДБ**). **Принимает значения:** *yes* — учетная запись будет синхронизирована с Единым Центром Управления **Dallas Lock** или Сервером безопасности **Dallas Lock**, *no* — учетная запись не будет синхронизирована

Графическая оболочка администрирования

Для просмотра параметров учетной записи пользователя в графической оболочке администрирования необходимо на вкладке «**Пользователи**» в категории «**Учетные записи**» в общем списке учетных записей выбрать запись и открыть окно редактирования с помощью кнопки «**Свойства**» на панели действий. В режиме просмотра откроется окно «**Свойства пользователя**».

Для изменения атрибутов учетной записи пользователя в графической оболочке администрирования необходимо открыть окно редактирования параметров учетной записи двойным кликом левой кнопки мышки на необходимой записи. Откроется окно «**Свойства пользователя**» в режиме редактирования. Для редактирования доступны следующие атрибуты учетной записи:

- Пароль пользователя.
- Фамилия, Имя, Отчество.
- Наименование оболочки командной строки (интерпретатор).
- Максимальное кол-во сессий.
- Период неиспользования.
- Блокировка пользователя.
- Параметры пароля.

- Изменение типа учетной записи.
- Расписание работы пользователя.

В режиме редактирования параметров учетной записи возможно добавление/удаление дополнительных групп.

4.3.6 Управление расписанием работы пользователей

4.3.6.1 Настройка расписания работы пользователей

Консольная оболочка администрирования

Для того, чтобы задать расписание работы пользователей, необходимо в разделе управления учетными записями пользователей *management* зайти в подраздел *users* и выполнить команду *user-set-schedule*. Система перейдет в конструктор установки расписания работы пользователей. Команды и настраиваемые параметры для расписания работы пользователей представлены в Таблица 11.

Задание расписания работы пользователей возможно исключительно для пользователей с ролью «Пользователь ОС» и для пользователей, не являющихся базовыми субъектами доступа[19].

Таблица 11

№	Атрибут	Описание
1	*login <значение>*	Логин пользователя, для которого устанавливается расписание работы
2	*mon <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Понедельник». При вводе несколько временных интервалов необходимо разделять их символом «,». **Пример:** 1. mon 00:00-23:00 – выделяет временной период с 00:00 до 23:00. 2. mon 00:00-8:30,17:30-00:00 – выделяет временные периоды с 00:00 до 08:30 и с 17:30 до 00:00
3	*tue <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Вторник». При вводе несколько временных интервалов необходимо разделять их символом «,»
4	*wed <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Среда». При вводе несколько временных интервалов необходимо разделять их символом «,»
5	*thu <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Четверг». При вводе несколько временных интервалов необходимо разделять их символом «,»
6	*fri <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Пятница». При вводе несколько временных интервалов необходимо разделять их символом «,»

[19] Под базовыми субъектами доступа подразумеваются пользователи, идентификатор (uid) которых меньше значения параметра UID_MIN в файле /etc/login.defs.

№	Атрибут	Описание
7	*sat <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Суббота». При вводе несколько временных интервалов необходимо разделять их символом «,»
8	*sun <значение>*	Позволяет задать разрешенный временной интервал (временные интервалы) для дня недели «Воскресенье». При вводе несколько временных интервалов необходимо разделять их символом «,»
9	*mon, tue, wed, thu, fri, sat, sun <remove>*	Для атрибутов mon — sun, при использовании значения remove, будут удалены все разрешенные временные интервалы для указанного дня
10	*set-worktime <значение>*	Позволяет установить (перезаписать) для каждого из дней рабочей недели (пн-пт) разрешенный временной интервал, указанный в качестве значения параметра «*set-worktime*», а для выходных дней (сб-вс) позволяет удалить все разрешенные временные интервалы. **Пример:** «*set-worktime 9:00-18:00*» заменит 7 команд: «mon 9:00-18:00», «tue 9:00-18:00», «wed 9:00-18:00», «thu 9:00-18:00», «fri 9:00-18:00», «sat remove», «sun remove»
11	*schedule-import-file <значение>*	Позволяет установить расписание работы пользователя, заданное в JSON-файле. /<полный путь к JSON-файлу>. **Пример:** */home/user/demouser.json*
12	*start-date <значение>*	Дата начала действия учетной записи. Значение года в дате может принимать значение от 0 до 9999 включительно. Если значение в пределах от 0 до 99, используется значение 20xx, где xx – вводимое обозначение года. Необязательный атрибут. При установке только даты *start-date* устанавливаемая дата должна быть равной или дальше от текущей даты. **Принимает значения**: дата в формате ДД/ММ/ГГГГ (или -1, для отключения проверки)
13	*expiration-date <значение>*	Дата истечения срока действия учетной записи. Значение года в дате может принимать значение от 0 до 9999 включительно. Если значение в пределах от 0 до 99, используется значение 20xx, где xx – вводимое обозначение года. При установке значения expiration-date, превышающего количество дней в месяце, лишние дни будут прибавлены к следующему месяцу. Необязательный атрибут. Например, 31 апреля будет соответствовать 1 мая. Количество дней не должно превышать 31, номер месяца не должен превышать значение 12. При установке только даты *expiration-date* устанавливаемая дата должна быть дальше от текущей даты минимум на один день. **Принимает значения**: дата в формате ДД/ММ/ГГГГ (или -1, для отключения проверки).

Пример:

management <enter>

users <enter>

user-set-schedule <enter>

login user <enter>

mon 9:00-17:00 <enter>

tue 9:00-17:00 <enter>

wed 9:00-17:00 <enter>

thu 9:00-17:00 <enter>

fri 9:00-16:00 <enter>

sat remove <enter>

sun remove <enter>

execute <enter>

Successfully applied schedule (Расписание успешно применено).

При установке временного интервала, возможны следующие значения временных границ: 00:00, 00:30, 01:00, 01:30, 02:00 , 2:30, 03:00, 3:30, 04:00, 4:30, 05:00, 05:30, 06:00, 06:30, 07:00, 07:30, 08:00, 08:30, 09:00, 09:30, 10:00, 10:30, 11:00, 11:30, 12:00, 12:30, 13:00, 13:30, 14:00, 14:30, 15:00, 15:30, 16:00, 16:30, 17:00, 17:30, 18:00, 18:30, 19:00, 19:30, 20:00, 20:30, 21:00, 21:30, 22:00, 22:30, 23:00, 23:30, 00:00.

В расписании работы пользователя исключена возможность устанавливать временные интервалы с точностью до 1 минуты.

Для редактирования, существующего расписания работы пользователя необходимо в подразделе *users* раздела *management* выполнить команду *user-set-schedule.* Система перейдет в *user-set-schedule* для изменения существующего расписания работы пользователя. Команды и настраиваемые параметры для редактирования расписания работы пользователя подробно представлены в Таблица 11.

Пример:

management <enter>

users <enter>

user-set-schedule <enter>

login user <enter>

t

u

e

e

Для пользователя user был успешно добавлен запрещающий временной интервал для работы с 13:00 до 15:00 во вторник.

При повторной установке временного интервала для какого-либо дня, старый временной интервал для выбранного дня будет полностью перезаписан.

e

Графическая оболочка администрирования

t

e

Для того, чтобы настроить расписание работы пользователей с помощью графической оболочки **СЗИ НСД** необходимо на вкладке «**Пользователи**» перейти в раздел «**Учетные записи**». Выделить пользователя, для которого будет настраиваться расписание работы, и запустить окно «**Свойства**». Далее в рабочем окне «**Свойства пользователя**» открыть поле «*Расписание работы*» кликнув на кнопку «**Открыть**» (см. Рисунок 23).

Задать расписание работы пользователей возможно исключительно для пользователей с ролью «*Пользователь ОС*» и для пользователей, не являющихся базовыми субъектами доступа[20].

[20] Под базовыми субъектами доступа подразумеваются пользователи, идентификатор (uid) которых меньше значения параметра UID_MIN в файле /etc/login.defs.

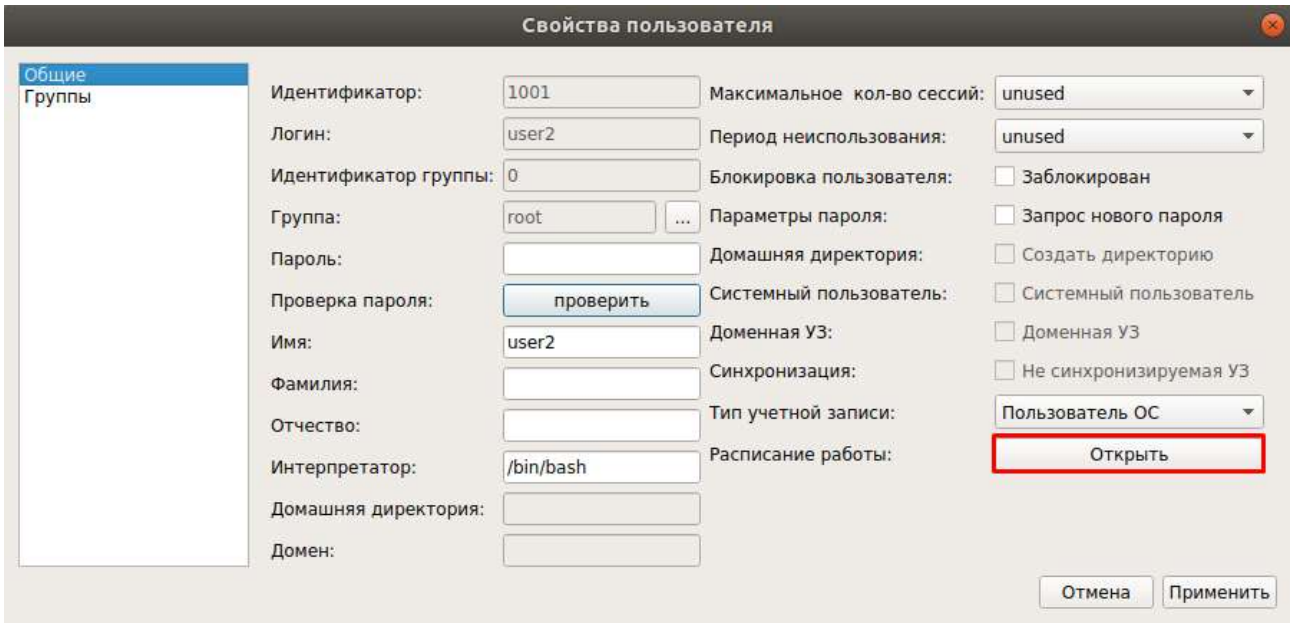


Рисунок 23. Поле «Расписание работы»

После выполнения действия «**Открыть**» запустится окно «**Расписание работы и период действия**» (см. Рисунок 24).

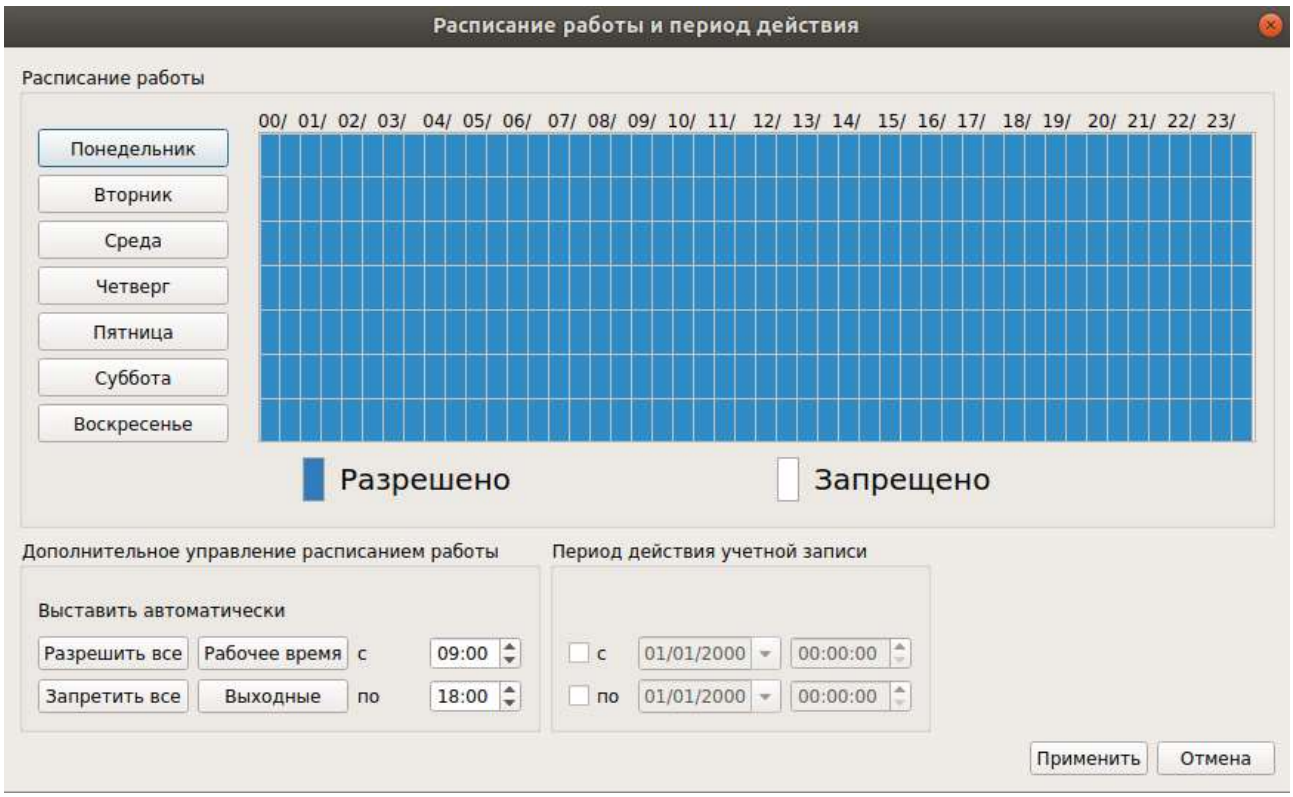


Рисунок 24. Окно «Расписание работы и период действия»

В рабочем окне «**Расписание работы пользователей и период действия**» представлен следующий блок настроек:

- «Расписание работы» — блок реализует возможность выделять временные отрезки для каждого дня недели с целью разрешить/запретить работу пользователя;
- «Дополнительное управление расписанием работы» — блок реализует возможность:
  - разрешить работу пользователя в любое время (кнопка «**Разрешить все**»);
  - запретить работу пользователя в любое время (кнопка «**Запретить все**»);
  - установить рабочее время (два текстовых поля с возможностью указать границы временного интервала рабочего дня и кнопка «**Рабочее время**»);

–разрешить/запретить работу пользователя в выходные (сб и вс).

- «Период действия учетной записи» — блок реализует возможность включить/отключить даты начала действия и истечения срока действия учетной записи пользователя, а также указать непосредственно дату и время.

4.3.6.2 Просмотр и экспорт расписания работы пользователей

Консольная оболочка администрирования

Для просмотра и экспорта расписания работы пользователей необходимо в разделе *users* подсистемы управления *management* выполнить команду *user-show-schedule*. Система перейдет в подменю просмотра и экспорта расписания пользователей, где доступны управляющие команды, представленные в Таблица 12.

Таблица 12

№	Атрибут	Описание
1	*login <значение>*	Логин пользователя, для которого необходимо просмотреть и (или) экспортировать расписание работы
2	*schedule-export-file <путь>*	Команда позволяет установить путь к директории, в которой файл, содержащий расписание работы пользователя, будет сохранен в формате JSON. /<полный путь к директории, где JSON-файл будет сохранен>. Экспорт расписания работы пользователей возможен только с помощью консольной оболочки администрирования. При экспорте файла расписания работы пользователя файл автоматически именуется в формате «логин_текущая дата.json»

Пример:

management <enter>

users <enter>

user-set-schedule <enter>

login user <enter>

e

x

При успешном завершении запроса в консольной оболочке администрирования будет выведено *e*расписание работы пользователя.

c

4.3.7 Блокировка и разблокировка учетной записи пользователя

t

Механизм блокировки предназначен для предотвращения несанкционированного входа *e*в операционную систему учетной записи пользователя. Предусмотрена принудительная блокировка *n*администратором и автоматическая блокировка учетной записи пользователя в случае истечения *t*срока действия пароля.

К*r*

Консольная оболочка администрирования

Для принудительной блокировки существующей учетной записи пользователя необходимо воспользоваться командой *user-lock,* далее — указать логин учетной записи пользователя и имя домена (если учетная запись принадлежит домену).

Пример:

management <enter>

users <enter>

user-lock <enter>

login <имя_пользователя> <enter>

domain <имя_домена> <enter>

execute <enter>

Для разблокирования учетной записи пользователя необходимо воспользоваться командой *user-unlock* аналогичным образом, как и для осуществления блокировки.

Графическая оболочка администрирования

Для принудительной блокировки необходимо на вкладке «**Пользователи**» в категории «**Учетные записи**» выделить учетную запись и выбрать команду  «**Блокировать/Разблокировать**» на панели действий.

После блокировки учетной записи пользователя в свойствах данного аккаунта напротив параметра «**Блокировка пользователя**» будет выставлен флаг «*Заблокирован*» (см. Рисунок 25).

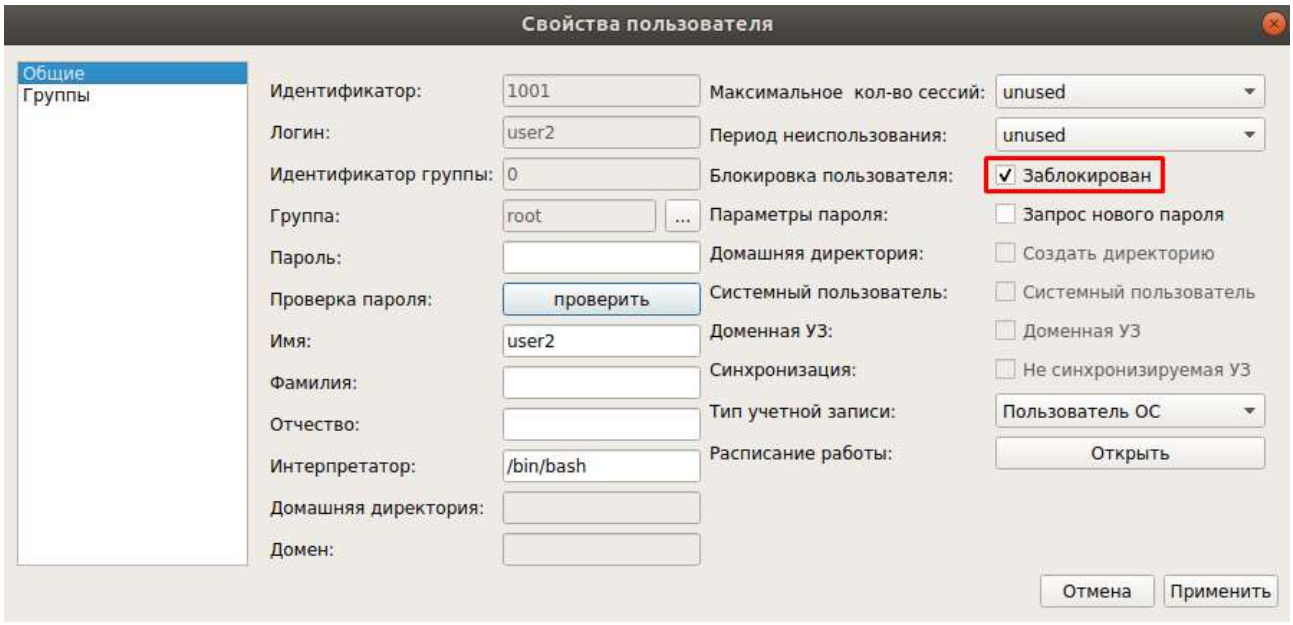


Рисунок 25. Заблокированная учетная запись пользователя

Для разблокировки учетной записи пользователя необходимо в свойствах учетной записи снять флаг «Заблокирован» или воспользоваться командой  «**Разблокировать**» на панели действий в разделе «**Блокированные пользователи**».

Список всех заблокированных учетных записей отображается на вкладке «**Пользователи**» в разделе «**Блокированные пользователи**» (см. Рисунок 26).

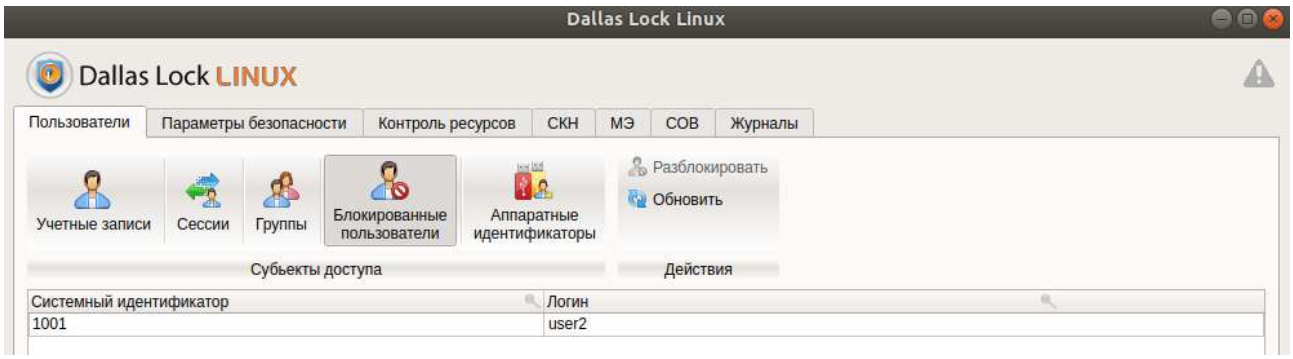


Рисунок 26. Список заблокированных учетных записей

4.3.8 Смена пароля учетной записи пользователя

Консольная оболочка администрирования

Для смены пароля учетной записи пользователя, администратор должен воспользоваться командой *user-change-password,* указав в качестве параметров логин и новый пароль учетной записи (Рисунок 27).

```
dallas@dallaslock:~$ ishl
Connection to localhost:3880
enter password for dlladmin:
cli> management
management> users
users> user-change-password
user-change-password> login user2
user-change-password> password *********
user-change-password> execute
Success updating password of user '"user2"'
users>
```

Рисунок 27. Смена пароля

Пример:

management <enter>

users <enter>

user-change-password <enter>

login user3 <enter>

password qwerty <enter>

execute <enter>

Пользователь также имеет возможность сменить пароль через консольную оболочку ОС. Для смены пароля пользователь должен запустить эмулятор терминала или перейти в терминальный сеанс (одновременно нажать клавиши «**Ctrl**», «**Alt**» и одну из функциональных клавиш «**F2**» — «**F6**») и ввести команду *passwd*.

При необходимости сменить пароль, следует обратиться к администратору.

Также поддерживается смена пароля с использованием графической оболочки ОС. За более подробной информацией следует обратиться к документации на используемую ОС.

Графическая оболочка администрирования

Для смены пароля учетной записи пользователя необходимо в категории «**Учетные записи**» в общем списке учетных записей выделить пользователя и на панели действий выбрать команду  «**Установить пароль**». После выбора команды откроется окно смены пароля (см. Рисунок 28).

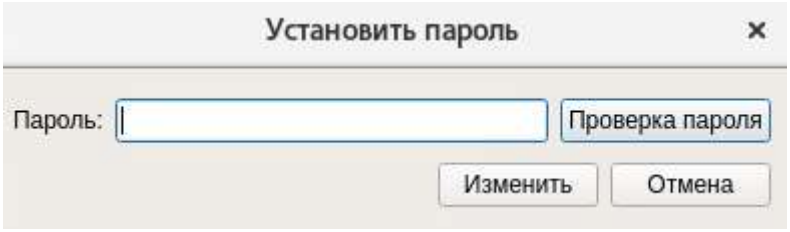


Рисунок 28. Окно смены пароля

В поле «Пароль» вводится новый пароль, при необходимости можно его проверить — кнопка «**Проверка пароля**». Для принятия изменений — кнопка «**Изменить**», для отмены действий — кнопка «**Отмена**».

Также пароль можно изменить в форме редактирования параметров учетной записи, необходимо открыть свойства учетной записи и в поле «*Пароль*» ввести новое значение пароля.

4.3.9 Удаление учетной записи пользователя

Консольная оболочка администрирования

Для удаления учетной записи пользователя необходимо воспользоваться командой *user-remove,* далее — указать логин учетной записи пользователя и наименование домена (если учетная запись принадлежит домену).

Пример:

management <enter>
users <enter>
user-remove <enter>
login <имя_пользователя> <enter>
domain <имя_домена> <enter>
execute <enter>

> При удалении системы защиты с ТС учетные записи системных пользователей, созданные средствами **СЗИ НСД**, остаются в операционной системе.

Графическая оболочка администрирования

Для удаления учетной записи пользователя необходимо в категории «**Учетные записи**» выделить учетную запись и выбрать команду «**Удалить**». При удалении система запросит подтверждение операции (см. Рисунок 29).

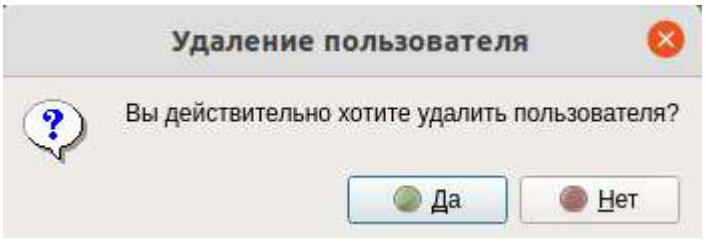


Рисунок 29. Запрос на удаление

Для подтверждения операции — кнопка «**Да**», для отмены действий — «**Нет**».

4.3.10 Управление группами учетных записей

Для перехода в подменю управления группами учетных записей в консольной оболочке администрирования в разделе *management* необходимо выполнить команду *groups*. После ввода команды система перейдет в раздел *groups.* Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 13.

Таблица 13

№	Команда	Описание
1	*user-list*	Вывод на экран списка пользователей. После ввода команды будет выведен список учетных записей с полями: – идентификатор (*uid*) учетной записи; – логин (*login*) учетной записи пользователя; – имя (*first-name*) пользователя; – идентификатор основной группы (*main-group*), в которую входит учетная запись; – домен (domain). **Пример:** *management <enter>* *groups <enter>* *user-list <enter>* *q <enter>*
2	*group-list*	Вывод на экран списка групп пользователей. После ввода команды будет выведен список групп с полями: – идентификатор (*gid*) группы; – наименование группы (*name*). В таблице выводятся первые 50 групп, для дальнейшего вывода списка необходимо нажать *Enter*. Команду *Enter* необходимо будет вводить

№	Команда	Описание
		до тех пор, пока система не выдаст весь список групп. По завершению вывода всего списка система выдаст сообщение «*Command ‘group-list’ executed successfully*» (команда ‘*group-list*’ выполнена успешно), и снова станут доступны команды из раздела *groups*. Для выхода из списка в том случае, когда вывод списка еще не окончен, необходимо ввести команду *q*. **Пример:** *management <enter>* *groups <enter>* *group-list <enter>* *q <enter>*
3	*group-add*	Переход в раздел добавления группы учетных записей, подробнее — в разделе Создание группы учетных записей пользователей
4	*group-add-user*	Переход в раздел добавления учетной записи в группу, подробнее — в разделе Редактирование данных о группе
5	*group-remove-user*	Переход в раздел удаления учетной записи из группы, подробнее — в разделе Редактирование данных о группе
6	*group-remove*	Команда удаления группы пользователей, более подробнее — в разделе Удаление группы пользователей
7	*group-show*	Команда просмотра параметров группы пользователей, подробнее — в разделе Просмотр информации о группе пользователя
8	*group-show-users*	Команда просмотра списка учетных записей пользователей, входящих в группу, подробнее — в разделе Просмотр информации о группе пользователя

Просмотреть список всех групп можно на вкладке «**Пользователи**» в разделе «**Группы**» (см. Рисунок 30).

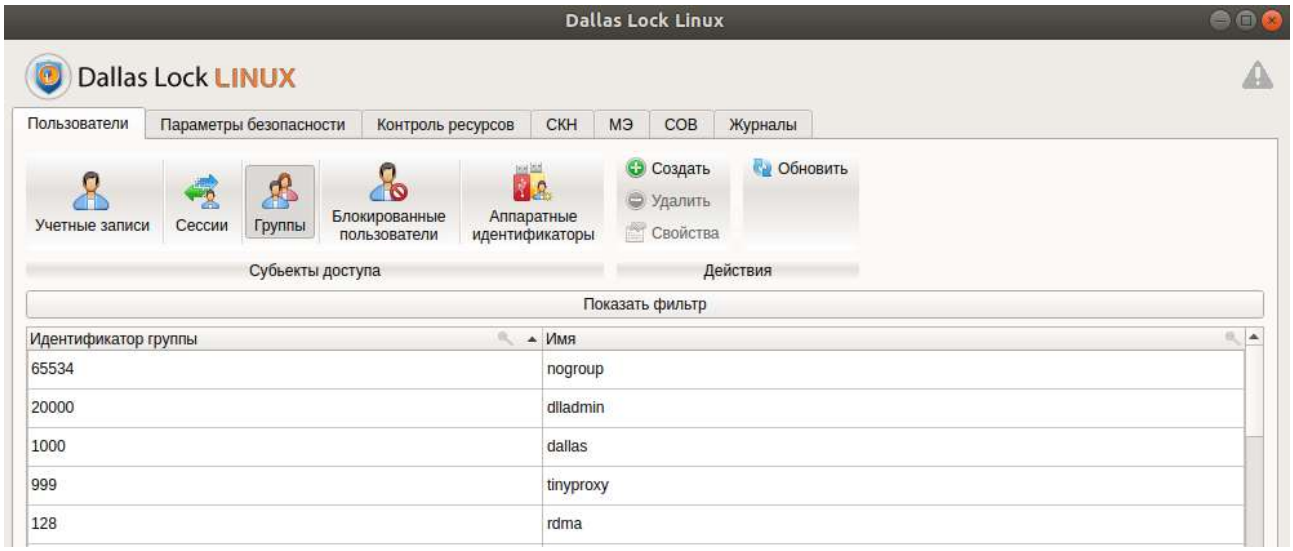


Рисунок 30. Категория «Группы»

4.3.10.1 Создание группы учетных записей пользователей

Консольная оболочка администрирования

Для создания группы пользователей необходимо выполнить команду *group-add,* список атрибутов команды представлен в Таблица 14.

Таблица 14

№	Атрибут	Описание
1	*gid*	Системный идентификатор группы. **Принимает значения:** от 0 до 65534. По умолчанию — следующее доступное значение. Необязательный атрибут. Если атрибут не указывается, будет использован первый свободный идентификатор в системе
2	*group-name <значение>*	Наименование группы пользователей
3	*system <yes/no>*	Указание на то, что группа пользователей является системной. **Принимает значения:** *yes* — системная группа, *no* — не является системной группой пользователей. Необязательный атрибут. По умолчанию установлено значение *no*

Пример:

management <enter>
groups <enter>
group-add <enter>
group-name group1 <enter>
system no <enter>
execute <enter>

Графическая оболочка администрирования

Для создания группы учетных записей необходимо в разделе «**Группы**» на панели действий выбрать команду «**Создать**». После выбора откроется форма «**Создание группы**» (см. Рисунок 31).

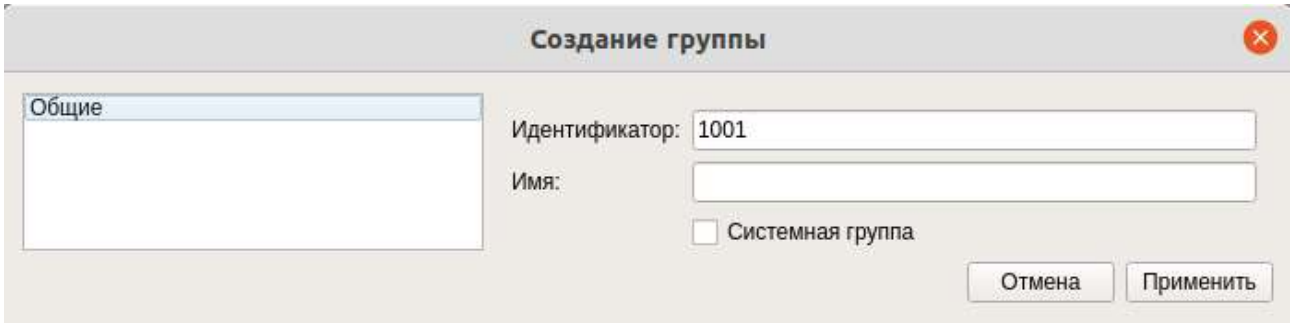


Рисунок 31. Форма «Создание группы»

Форма по добавлению группы содержит раздел «**Общие**».

В разделе «**Общие**» необходимо указать:

- «Идентификатор» — системный идентификатор группы. По умолчанию — следующее доступное значение;
- «Имя» — наименование группы пользователей;
- «Системная группа» (флаг) — указание на то, что группа пользователей является системной. Если флаг установлен, то группа является системной. По умолчанию флаг не установлен. Необязательный атрибут.

Для добавления учетной записи пользователя в группу необходимо в общем списке раздела «Группы» двойным кликом левой кнопки мыши по идентификатору группы открыть окно редактирования параметров группы. В разделе «**Пользователи**» нажать на кнопку «**Добавить в группу**» (см. Рисунок 32).

Добавление учетных записей в группу возможно только после регистрации этой группы в системе.

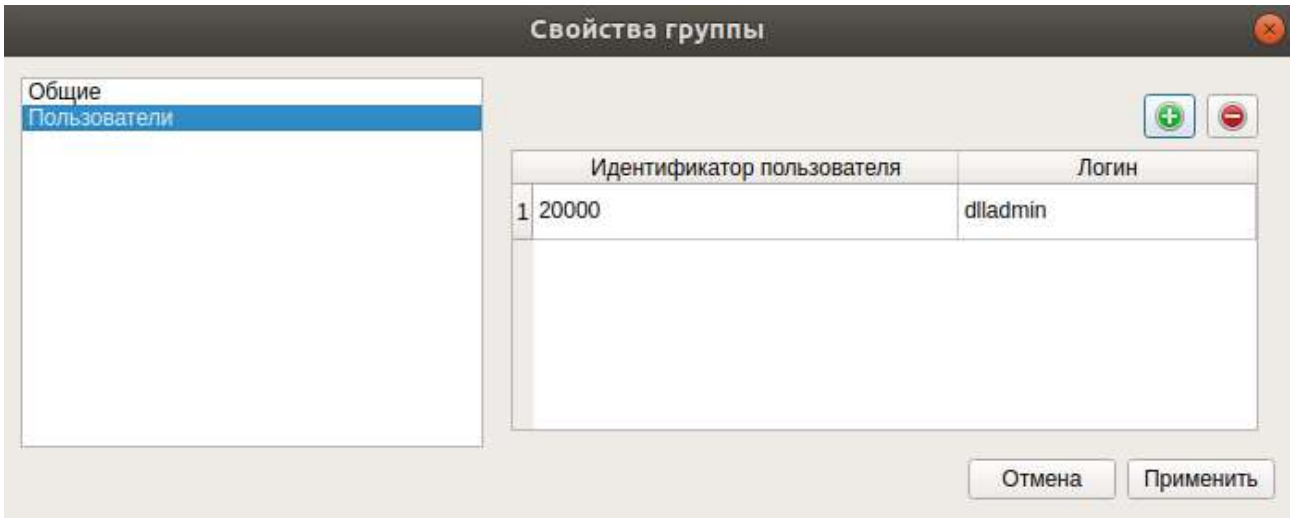


Рисунок 32. Добавление учетной записи

После нажатия на кнопку откроется форма по выбору учетной записи пользователя (см. Рисунок 33).

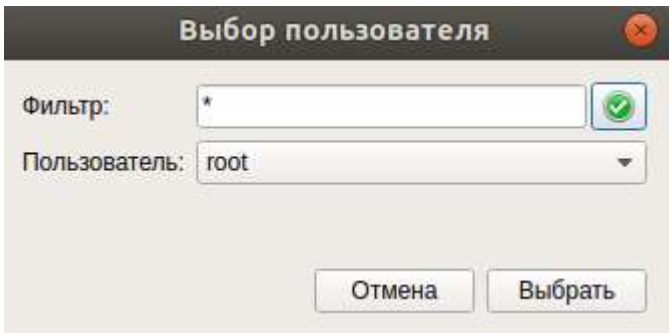


Рисунок 33. Выбор учетной записи пользователя

Из выпадающего списка необходимо выбрать логин учетной записи. Для включения выбранной учетной записи в группу следует нажать на кнопку «**Выбрать**», для отмены операции — кнопку «**Отмена**».

Для удаления учетной записи пользователя из группы необходимо в общем списке раздела «**Группы**» двойным кликом левой кнопки мыши по идентификатору группы открыть окно редактирования параметров группы. В окне «**Свойства группы**» перейти в раздел «**Пользователи**», в списке выделить имя учетной записи и нажать на кнопку «**Удалить пользователя**» , после этого учетная запись пользователя будет удалена из группы.

4.3.10.2 Просмотр данных о группе

Консольная оболочка администрирования

Для просмотра параметров группы пользователя необходимо воспользоваться командой *group-show,* указав в качестве параметра наименование группы.

Пример:

management <enter>

groups <enter>

group-show <наименование_группы> <enter>

Для просмотра списка учетных записей пользователей, входящих в группу, необходимо воспользоваться командой *group-show-users,* указав в качестве параметра наименование группы. Будет отображен список пользователей, для которых указанная группа является дополнительной.

Пример:

management <enter>

groups <enter>

group-show-users <наименование_группы> <enter>

Если группа не является дополнительной для каких-либо учетных записей пользователей, система выдаст сообщение «*Group is empty*» («Группа пустая»).

Для просмотра списка дополнительных групп, в которые входит пользователь, необходимо воспользоваться командой *user-show-groups,* далее — указать логин учетной записи пользователя и наименование домена (если учетная запись принадлежит домену).

Пример:

management <enter>

users <enter>

user-show-groups <enter>

login <имя_пользователя> <enter>

domain <имя_домена> <enter>

execute <enter>

Если учетная запись пользователя не включена в состав дополнительных групп, система выдаст сообщение «*No additional groups*» («*Нет дополнительных групп*»).

Для возможности просмотра списка групп учетных записей без выхода из раздела *users* необходимо выполнить команду *group-list*.

Графическая оболочка администрирования

Для просмотра информации о группе необходимо выделить наименование группы в общем списке и выбрать команду «**Свойства**» на панели действий (см. Рисунок 34).

Откроется форма «**Свойства группы**» в режиме просмотра.

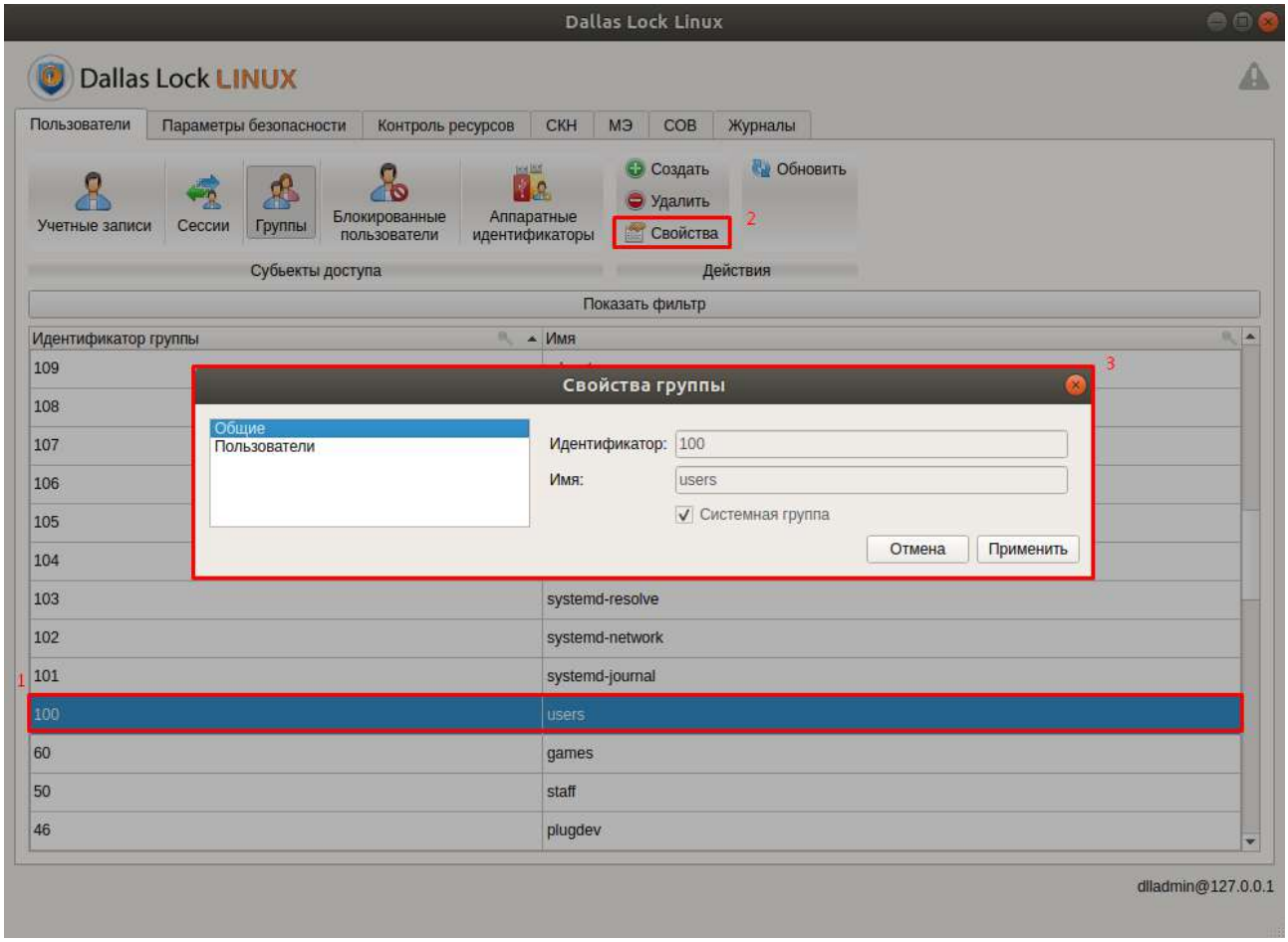


Рисунок 34. Выбор команды «Свойства»

4.3.10.3 Редактирование данных о группе

Консольная оболочка администрирования

Для добавления учетной записи пользователя в группу необходимо воспользоваться управляющей командой *group-add-user,* с указанием атрибутов, приведенных в Таблица 15.

Таблица 15

№	Атрибут	Описание
1	*login <значение>*	Наименование добавляемой учетной записи пользователя
2	*domain <значение>*	Наименование домена (если учетная запись принадлежит домену)
3	*group-name <значение>*	Наименование группы пользователей

Пример:

management <enter>

groups <enter>

group-add-user <enter>

login <имя_пользователя> <enter>

domain <имя_домена> <enter>

group-name <наименование_группы> <enter>

execute <enter>

Для удаления учетной записи пользователя из группы необходимо воспользоваться командой *group-remove-user,* используя аналогичные атрибуты, как и для команды добавления пользователя в группу.

Графическая оболочка администрирования

Для изменения атрибутов группы учетных записей пользователей необходимо открыть окно редактирования параметров группы двойным кликом левой кнопки мыши откроется окно «**Свойства группы**» (см. Рисунок 35), далее необходимо перейти на вкладку «**Пользователи**». Для редактирования доступно только:

- Добавить в группу.
- Удалить из группы.

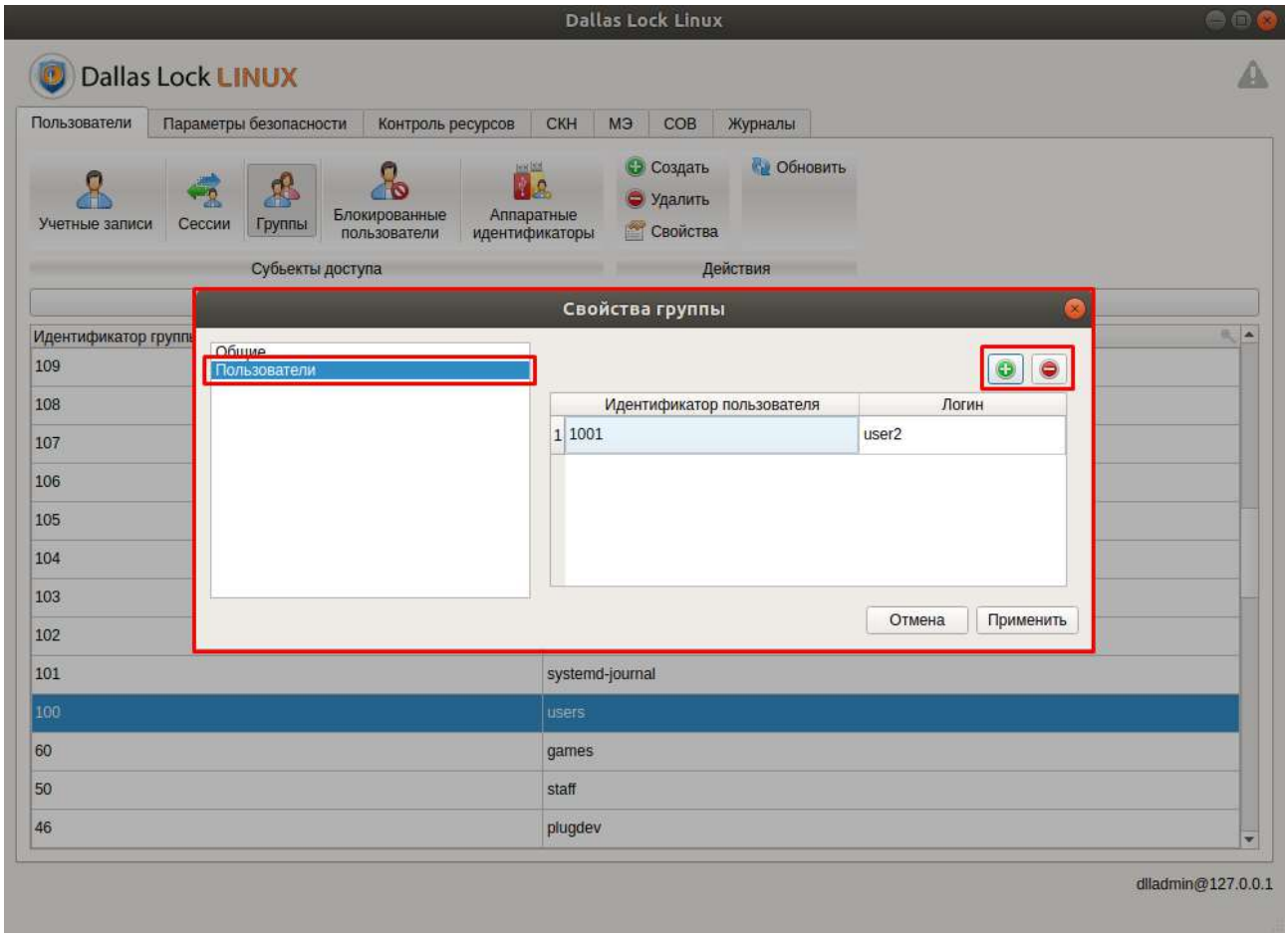


Рисунок 35. Редактировать группу

4.3.10.4 Удаление группы пользователей

Консольная оболочка администрирования

Для удаления группы пользователей необходимо воспользоваться управляющей командой *group-remove,* указав в качестве параметра наименование группы.

> Группа пользователей не должна быть основной для какой-либо учетной записи пользователя.

Пример:

management <enter>

groups <enter>

group-remove <наименование_группы> <enter>

После успешного выполнения команды система выдаст сообщение «*Command 'group-remove' executed successfully*» (команда *'group-remove'* выполнена успешно).

Графическая оболочка администрирования

Для удаления группы учетных записей пользователей необходимо выделить группу в категории «**Группы**» и воспользоваться командой  «**Удалить**» на панели действий.

4.3.11 Управление сессиями учетных записей пользователей

Консольная оболочка администрирования

Для перехода в подменю управления сессиями учетных записей пользователей в консольной оболочке администрирования в разделе *management* необходимо выполнить команду *sessions*. После ввода команды система перейдет в раздел *sessions*.

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 16.

Таблица 16

№	Команда	Описание
1	*show-all*	Отображение списка открытых локальных сессий. В результате выполнения команды будет отображен список сессий, состоящий из 4 колонок: – *id* — идентификатор сессии; – *user* — наименование учетной записи пользователя; – *service* — наименование сервиса открытой сессии; – *opened* — дата и время момента открытия сессии
2	*lock-session<значение>*	Блокировка сессии пользователя. **Принимает значение:** идентификатор сессии. Идентификатор сессии можно посмотреть в таблице открытых локальных сессий в поле *id*
3	*term-session <значение>*	Завершение сессии пользователя. **Принимает значение:** идентификатор сессии. Идентификатор сессии можно посмотреть в таблице терминальных сессий в поле *id*
4	*term-user-sessions <значение>*	Завершение терминальной сессии пользователя с указанием логина учетной записи пользователя **Принимает значение:** логин учетной записи пользователя

Пример:

management <enter>

sessions <enter>

lock-session <enter>

show-all <enter>

Для блокировки терминальной сессии пользователем необходимо запустить исполняемый файл *vlock*, выполнив в терминале ОС команду */dllx/bin/vlock*.

В случае ввода неверного пароля пользователем при разблокировки терминальной сессии, появится приглашение ввода пароля *root*. Необходимо нажать *Enter* и повторить попытку ввода пароля пользователя.

Графическая оболочка администрирования

Для просмотра списка активных сессий учетных записей необходимо на вкладке «**Пользователи**» перейти в раздел «**Сессии**» (см. Рисунок 36).

Рисунок 36. Список активных сессий

В рабочем поле раздела отображается список, состоящий из 4 колонок:

- «Номер» — идентификатор сессии;
- «Пользователь» — наименование учетной записи пользователя;
- «Сервис» — наименование сервиса открытой сессии;
- «Дата открытия» — дата и время момента открытия сессии.

Для завершения сессии учетной записи пользователя необходимо в общем списке выделить строку с требуемой активной или заблокированной сессией и на панели действий выбрать команду «**Закрыть сессию**». После завершения сессии в левом нижнем углу графической оболочки отобразится сообщение «*Сессия успешно закрыта*» (см. Рисунок 37).

Рисунок 37. Информационное сообщение

Для блокировки сессии учетной записи пользователя необходимо в общем списке выделить строку с требуемой активной сессией и на панели действий выбрать команду «**Заблокировать сессию**». После блокировки сессии в левом нижнем углу графической оболочки появится сообщение «*Сессия успешно заблокирована*» (см. Рисунок 38). После блокировки сессии пользователю (владельцу сессии) отобразится экран входа в операционную систему. Записи заблокированных сессий в общем списке будут отображаться серым цветом.

Рисунок 38. Информационное сообщение

4.3.12 Управление аппаратной идентификацией пользователя

4.3.12.1 Предварительная подготовка ОС для работы с аппаратной идентификацией пользователя

СЗИ НСД Dallas Lock Linux позволяет в качестве усиления механизма аутентификации пользователя использовать электронные идентификаторы:

- USB-ключи Aladdin eToken Pro/Java, 72K;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи и смарт-карты Рутокен (Rutoken): Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite, Рутокен ЭЦП PKI;
- электронные ключи Touch Memory (iButton): DS-1990, DS-1992, DS-1993, DS-1994, DS-1995, DS-1996;
- USB-ключи и смарт-карты JaCarta: JaCarta SF/ГОСТ, JaCarta ГОСТ, JaCarta PKI, JaCarta PKI/Flash, JaCarta LT, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta PRO;
- USB-ключи и смарт-карты ESMART: ESMART Token, ESMART Token ГОСТ, ESMART 64k.

Для работы с электронными ключами Touch Memory (iButton) администратор **СЗИ** (либо пользователи, запускающие клиенты) должны состоять в группе *dialout*, либо иметь права суперпользователя (root).

При настройке аппаратного идентификатора рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификатором, или скачивать их с сайта производителя.

Перед настройкой идентификации с помощью аппаратных средств необходимо:

1. Обновить кэш пакетов ПО в ОС. Для ОС с менеджером пакетов YUM в терминале выполнить команду: *yum makecache*, для ОС с менеджером пакетов APT выполнить команду: *apt-get update*.
2. Установить необходимые пакеты для работы с USB-устройствами — *libusb*.
3. Установить демон *pcscd*.
4. Установить соответствующие драйверы.

Установка драйверов возможна как перед установкой на ТС системы защиты **Dallas Lock Linux**, так и после. Рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификаторами, или скачать их с сайта производителя.

4.1 В зависимости от используемой системы, загрузить драйверы АИ: файл с расширением .deb для ОС на основе deb-пакетов, файл с расширением .rpm для ОС на основе rpm-пакетов;
4.2 Установить драйверы:
- для ОС на основе deb-пакетов в терминале выполнить команду: *apt-get install <driver_name>.deb*;
- для ОС на основе rpm-пакетов в терминале выполнить команду *yum install <driver_name>.rpm*;
- для Альт Рабочая станция, Альт Сервер в терминале выполнить команду: *apt-get install <driver_name>.rpm*.

5. После обновления системных пакетов и установки утилит ОС необходимо перезагрузить.

Если установка соответствующих драйверов была выполнена после установки системы защиты, то для последующей корректной работы **СЗИ** с аппаратными идентификаторами, для которых установлены драйверы, ОС необходимо перезагрузить.

При использовании ПО SafeNetAuthentication Client для корректной работы ОС и **СЗИ НСД Dallas Lock Linux** необходимо создать символическую ссылку на библиотеку *libcrypto.so.<версия>.*

Для этого в терминале, нужно выполнить команду: *sudo ln -sf /usr/lib/x86_64-linux-gnu/libcrypto.so.<версия> /usr/lib/libcrypto.so.6*

Таблица 17

Особенности работы с аппаратной идентификацией пользователя	
USB-ключи Aladdin eToken Pro/Java, 72K	Для USB-ключа eToken 32Кб обеспечивается только возможность усиления механизма аутентификации. Запись учетных данных пользователя на такой идентификатор не производится в силу ограниченного объема доступной памяти аппаратного идентификатора. Для корректной работы аппаратных идентификаторов eToken необходимо использовать драйверы SafeNet. Версию драйвера SafeNet для работы с аппаратными идентификаторами eToken в операционных системах семейства GNU Linux рекомендуется использовать – 10.0.37
Электронные ключи Touch Memory (iButton)	Для работы электронных ключей Touch Memory (iButton) необходимы драйверы «Prolific USB-to-Serial Common Port» (данные драйверы уже могут быть в составе ОС, или их можно скачать с сайта производителя драйверов Prolific).

Особенности работы с аппаратной идентификацией пользователя	
	Электронный ключ iButton поддерживается только для чтения, то есть можно только назначить пользователю. Запись учетных данных пользователя на такой идентификатор не производится
USB-ключи и смарт-карты JaCarta	В связи с особенностью устройства JaCarta-2 ГОСТ, операция форматирования аппаратных идентификаторов данного типа должна выполняться только с использованием ПО «Единый Клиент JaCarta»

4.3.12.2 Администрирование аппаратной идентификации пользователя

Аппаратная идентификация в **СЗИ НСД Dallas Lock Linux** не является обязательной и может применяться дополнительно к основному способу аутентификации пользователя с помощью пароля.

Запрос аппаратного идентификатора осуществляется при каждом входе пользователя в ОС, если идентификатор был назначен учетной записи пользователя. При отключении аппаратного идентификатора все сессии учетной записи пользователя, за которой был зарегистрирован извлекаемый идентификатор, будут автоматически заблокированы.

Для каждой учетной записи пользователя может быть назначен только один аппаратный идентификатор. Регистрация одного и того же аппаратного идентификатора для разных учетных записей не допускается.

Следует обратить внимание, что аппаратные идентификаторы модели JaCarta-2 PKI/ГОСТ и JaCarta SF/ГОСТ являются комбинированными устройствами JaCarta, т.е. содержат несколько апплетов, что позволяет назначить данные апплеты как аппаратные идентификаторы нескольким учетным записям.

Пользователям, которым был назначен аппаратный идентификатор, авторизация по SSH запрещена.

Для перехода в подсистему управления аппаратными идентификаторами учетных записей пользователей в консольной оболочке администрирования в разделе *management* необходимо выполнить команду *tokens*. После ввода команды система перейдет в раздел *tokens*.

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 18.

Таблица 18

№	Команда	Описание
1	*tokens-info*	Отображение аппаратного идентификатора, который на данный момент времени подключен к компьютеру. После ввода команды будет выведен список с полями: – Идентификатор (*TokenID*). – Логин пользователя (*User*). Если идентификатор не ассоциирован с учетной записью пользователя, в данном поле будет указано «*Do not assign*» («Не назначен»). – Наименование идентификатора (*Token*). Если у идентификатора нет имени, в данном поле указано «*no_label*». – Серийный номер идентификатора (*Serial*). – Тип хранимой на идентификаторе информации (*LoginType*)
2	*assigned-tokens-info*	Отображение списка всех назначенных аппаратных идентификаторов. После ввода команды будет выведен список с полями: – Идентификатор (*TokenID*). – Логин пользователя (*User*).

№	Команда	Описание
		– Наименование идентификатора (*Token*). – Серийный номер идентификатора (*Serial*). – Тип хранимой на идентификаторе информации (*LoginType*)
3	*assign-token*	Команда назначения аппаратного идентификатора учетной записи пользователя, подробнее — в разделе Назначение аппаратного идентификатора
4	*unassign-token*	Команда отмены принадлежности аппаратного идентификатора учетной записи пользователя, подробнее — в разделе Отключение аппаратной идентификации
5	*change-pin*	Команда изменения PIN-кода для аппаратного идентификатора, подробнее — в разделе Смена PIN-кода аппаратного идентификатора
6	*format*	Команда выполнения форматирования аппаратного идентификатора, подробнее — в разделе Форматирование аппаратного идентификатора
7	*user-list*	Команда позволяет просмотреть список учетных записей пользователей, не выходя из подменю управления аппаратными идентификаторами *tokens*

4.3.12.3 Назначение аппаратного идентификатора

При назначении аппаратного идентификатора требуется ввод пользовательского PIN-кода аппаратного идентификатора для следующих типов хранимой информации:

- Открытая аутентификационная информация.
- Закрытая аутентификационная информация.
- Только имя пользователя.

В связи с ограниченными возможностями ввода пользовательских данных менеджера рабочего стола FlyDM в Astra Linux, при входе пользователю с назначенным ему аппаратным идентификатором с закрытой аутентификационной информацией, необходимо вводить PIN-код в поле «*Пароль*».

При назначении аппаратного идентификатора учетной записи пользователя с помощью консольной оболочки администрирования или графической оболочки администрирования необходимо использовать атрибуты или параметры представленные в Таблица 18.

При изменении параметров доступа АИ и синхронизации через **ЕЦУ** на **СЗИ НСД Dallas Lock Linux** выполняется сброс «типа доступа» АИ до значения **ЕЦУ**: «SET FROM UCC» для консольной оболочки администрирования, «UCC» для графической оболочки администрирования.

При последующей авторизации пользователя в Linux, в **СЗИ НСД Dallas Lock Linux** присваивается соответствующий тип доступа, что и на **ЕЦУ**.

Таблица 19

№	Атрибут	Описание
1	*ishl: login-type <значение [1,4]>* *GUI: тип доступа*	Выбор вида хранимой на аппаратном идентификаторе информации. Атрибуту может быть назначено одно из значений: – «1» / «Открытая аутентификационная информация» В открытой памяти идентификатора хранится пароль учетной записи. При авторизации пользователю необходимо только предъявить аппаратный идентификатор, логин и пароль считываются с ключа автоматически (*Full public*); – «2» / «Закрытая аутентификационная информация» В закрытой памяти идентификатора хранится пароль учетной записи. При авторизации пользователю необходимо предъявить аппаратный идентификатор и ввести его PIN-код (*Full private*); – «3» / «Только имя пользователя» В идентификаторе хранится информация только о логине учетной записи. При авторизации пользователь должен предъявить идентификатор и самостоятельно ввести пароль учетной записи (*Only username*); – «4» / «Пустой идентификатор» В идентификаторе не хранится информация об учетной записи. При авторизации пользователь должен предъявить идентификатор и самостоятельно ввести логин и пароль учетной записи (*Empty token*)
2	*ishl: token-uid <значение>* *GUI: идентификатор*	Наименование аппаратного идентификатора в HEX-формате В поле автоматически отображается имя предъявленного в данный момент времени аппаратного идентификатора
3	*ishl: user <значение>* *GUI: пользователь*	Указывается логин учетной записи пользователя
4	*ishl: password <значение>* *GUI: пароль*	Указывается текущий пароль учетной записи пользователя
5	*ishl: pin <значение>* *GUI: PIN*	Указывается текущий пользовательский PIN-код аппаратного идентификатора

Консольная оболочка администрирования

Для перехода в подменю управления аппаратными идентификаторами в консольной оболочке администрирования в разделе *management* необходимо выполнить команду *tokens*. В разделе *tokens* выполнить команду *assign-token*, с указанием атрибутов, представленных в Таблица 19. Ниже представлены примеры назначения аппаратных идентификаторов учетной записи пользователя.

Если для атрибута *login-type* было выбрано значение «1», необходимо заполнить поля *user* и *password.*

Пример:

management <enter>
tokens <enter>
assign-token <enter>
token-uid <значение> <enter>
login-type 1 <enter>
user pol <enter>
password 12345678 <enter>
pin 00000000 <enter>
execute <enter>

Если для атрибута *login-type* было выбрано значение «2», необходимо заполнить поля *user, password, pin.*

Пример:

management <enter>
tokens <enter>
assign-token <enter>
token-uid <значение> <enter>
login-type 2 <enter>
user pol <enter>
password 12345678 <enter>
pin 00000000 <enter>
execute <enter>

Если для атрибута *login-type* было выбрано значение «3», необходимо заполнить поле *user.*

Пример:

management <enter>
tokens <enter>
assign-token <enter>
token-uid <значение> <enter>
login-type 3 <enter>
user pol <enter>
pin 00000000 <enter>
execute <enter>

Если для атрибута *login-type* было выбрано значение «4», необходимо заполнить поле *user.*

Пример:

management <enter>
tokens <enter>
assign-token <enter>
token-uid <значение> <enter>
login-type 4 <enter>
user pol <enter>
execute <enter

Графическая оболочка администрирования

Для назначения аппаратного идентификатора учетной записи пользователя в графической оболочке администрирования необходимо выполнить следующие шаги:

1. На вкладке «**Пользователи**» перейти в категорию «**Аппаратные идентификаторы**».

2. Предъявить аппаратный идентификатор, вставив его в соответствующий USB-порт или прикоснувшись к считывателю (в зависимости от типа).

3. В категории «**Аппаратные идентификаторы**» на панели «**Действия**» выбрать команду «**Назначить**» .

4. В открывшемся диалоговом окне необходимо.

4.1 Выбрать аппаратный идентификатор в выпадающем списке (в списке отображаются все подключенные аппаратные идентификаторы).

4.2 Указать необходимые параметры (см. Рисунок 39).

В связи с ограниченными возможностями ввода пользовательских данных менеджера рабочего стола FlyDM в Astra Linux, при входе пользователю с назначенным ему аппаратным идентификатором с закрытой аутентификационной информацией, необходимо вводить PIN-код в поле «*Пароль*».

4.3При назначении аппаратного идентификатора учетной записи пользователя с помощью консольной оболочки администрирования или графической оболочки администрирования необходимо использовать атрибуты или параметры представленные в Таблица 18.

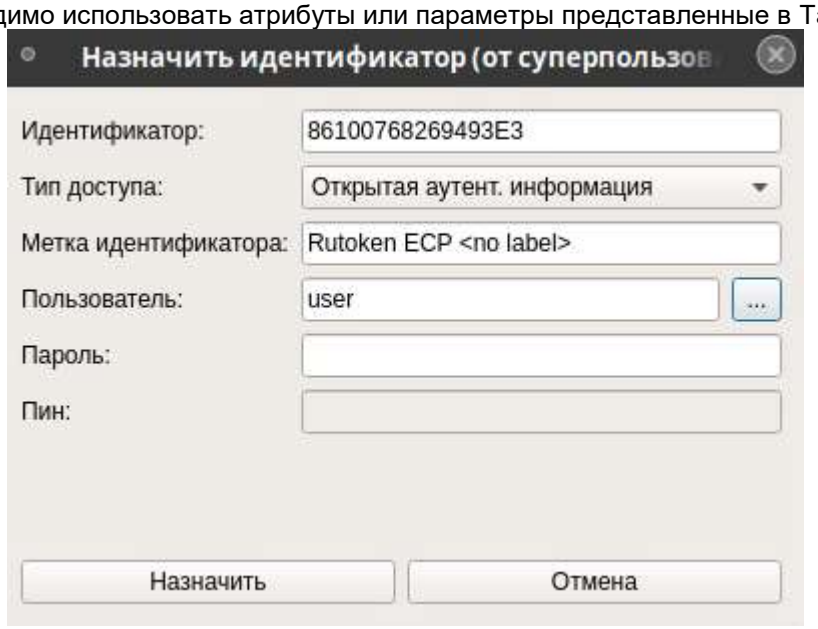


Рисунок 39. Форма «Назначить идентификатор»

После установки всех параметров необходимо нажать кнопку «**Назначить**». После назначения идентификатора для учетной записи данные ключа добавляются в общую таблицу зарегистрированных ключей (см. Рисунок 40).

Пользователь	Метка	Идентификатор	Тип доступа	Модель
user.al	UccToken	5FF7C73544ED3699	UCC	JaCartaGOST
	pin 9-10	EF225E0E571E6C79	Не назначен	JaCartaGOST
	11111111	EFCF6050CFF3573D	Не назначен	JaCartaPKI

Рисунок 40. Общая таблица зарегистрированных аппаратных идентификаторов

Для каждой учетной записи пользователя может быть назначен только один аппаратный идентификатор. Регистрация одного и того же идентификатора для разных учетных записей не допускается, при попытке повторной регистрации отображается предупреждение (см. Рисунок 41).

Следует обратить внимание, что аппаратные идентификаторы модели JaCarta-2 PKI/ГОСТ и JaCarta SF/ГОСТ являются комбинированными устройствами JaCarta, т.е. содержат несколько апплетов, что позволяет назначить данные апплеты как аппаратные идентификаторы нескольким учетным записям.

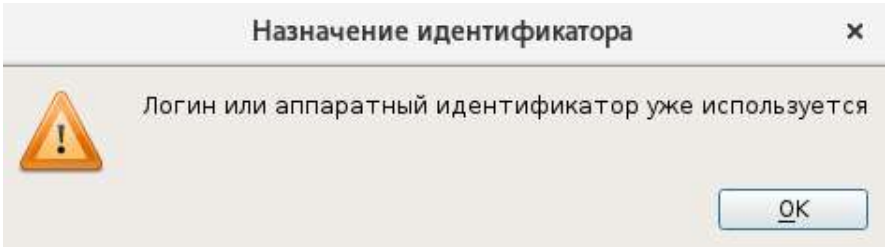


Рисунок 41. Информационное сообщение

Для определения принадлежности предъявленного аппаратного идентификатора необходимо на панели действий выбрать команду «**Информация об идентификаторе**». После выбора команды откроется информационное окно, в котором будет указано имя предъявленного аппаратного идентификатора и логин пользователя, которому назначен данный идентификатор.

4.3.12.4 Отключение аппаратной идентификации

Консольная оболочка администрирования

Для отключения аппаратной идентификации для учетной записи пользователя необходимо в разделе *tokens* выполнить команду *unassign-token, с* указанием логина *(user*).

Пример:

management <enter>

tokens <enter>

unassign-token pol <enter>

Графическая оболочка администрирования

Для того чтобы снять назначение аппаратного идентификатора для учетной записи, необходимо в общей таблице выделить строку с параметрами ключа и на панели «**Действия**» выбрать команду «**Отмена**» .

4.3.12.5 Смена PIN-кода аппаратного идентификатора

Для работы с аппаратными идентификаторами необходимы их авторизационные PIN-коды. PIN-коды аппаратных идентификаторов установлены в памяти идентификаторов по умолчанию.

Параметры символов PIN-кода для идентификатора (наличие цифр, букв и т.п.) определяются настройкой параметров в утилите соответствующего идентификатора. Прежде чем изменить PIN-код, администратор ИБ настраивает данные параметры именно в утилите. Если введенный в графической оболочке **СЗИ НСД** новый PIN-код не соответствует политикам, которые установлены в утилите, то выдается соответствующее сообщение и новый PIN-код не применяется. Если политики сложности пароля выключены в утилите, то ввод нового PIN-кода в **СЗИ НСД** не ограничивается.

Консольная оболочка администрирования

Для смены PIN-кода администратора аппаратного идентификатора необходимо в разделе *tokens* выполнить команду *change-pin*, с указанием атрибутов, приведенных в Таблица 20.

Таблица 20

№	Атрибут	Описание
1	*token-uid <значение>*	Уникальный идентификатор аппаратного идентификатора
2	*account <значение>*	Логин администратора аппаратного идентификатора или пользователя для смены PIN-кода
3	*old-pin <значение>*	Ввод старого PIN-кода, соответствующего указанному логину администратора или пользователя идентификатора
4	*new-pin <значение>*	Ввод нового PIN-кода

Пример:

management <enter>

tokens <enter>

change-pin <enter>

account admin <enter>

old-pin 123 <enter>

new-pin 321 <enter>

execute <enter>

Графическая оболочка администрирования

Для смены PIN-кода необходимо:

1. Предъявить аппаратный идентификатор.
2. На панели действий выбрать команду «**Сменить PIN-код**» .
3. В открывшемся окне выбрать идентификатор и заполнить поля (см. Рисунок 42).

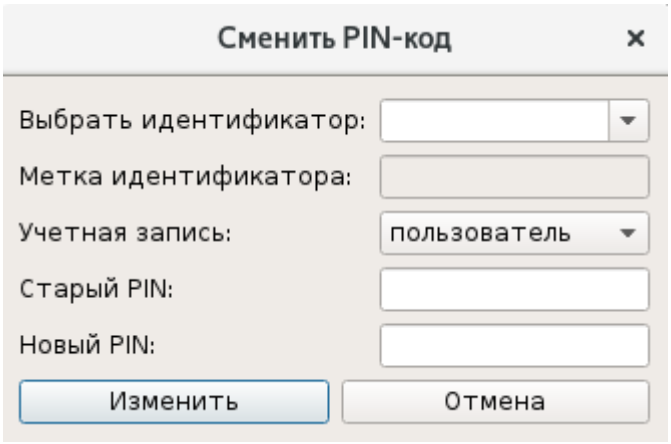


Рисунок 42. Смена PIN-кода для аппаратного идентификатора

- «Выбрать идентификатор»;
- «Метка идентификатора»;
- «Учетная запись» — аккаунт администратора или пользователя идентификатора;
- «Старый PIN» — ввод старого PIN-кода идентификатора;
- «Новый PIN» — ввод нового PIN-кода идентификатора;

4. После ввода параметров для выполнения операции смены PIN-кода необходимо нажать кнопку «**Изменить**».

4.3.12.6 Форматирование аппаратного идентификатора

Консольная оболочка администрирования

Для форматирования аппаратного идентификатора необходимо в разделе *tokens* выполнить команду *format*, с указанием атрибутов, приведенных в Таблица 21.

Таблица 21

№	Атрибут	Описание
1	*admin-pin <значение>*	Ввод текущего PIN-кода администратора аппаратного идентификатора
2	*token-uid <значение>*	Уникальный идентификатор аппаратного идентификатора
3	*new-user-pin <значение>*	Ввод нового пароля пользователя аппаратного идентификатора
4	*label <значение>*	Наименование аппаратного идентификатора

Пример:

management <enter>
tokens <enter>
format <enter>
token-uid <значение> <enter>
admin-pin 321 <enter>
new-user-pin 951 <enter>
label token <enter>
execute <enter>

Графическая оболочка администрирования

Для форматирования аппаратного идентификатора необходимо:

1. Предъявить аппаратный идентификатор.
2. На панели действий выбрать команду «**Форматировать**»  .

3. В открывшейся форме выбрать идентификатор и заполнить поля (см. Рисунок 43).

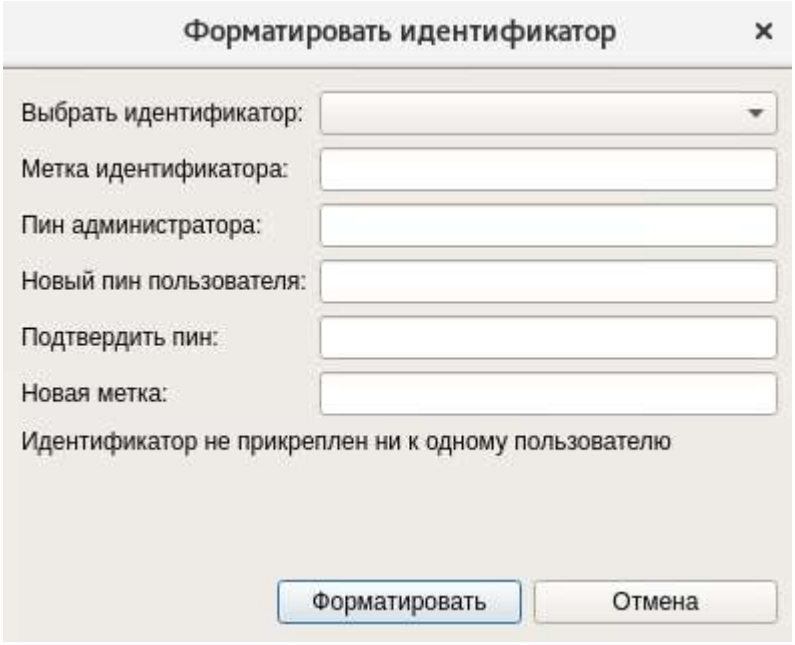


Рисунок 43. Форматирование аппаратного идентификатора

Для выполнения форматирования требуется указать действующий PIN-код администратора идентификатора, новый PIN-код пользователя идентификатора, новое имя идентификатора. Для завершения операции форматирования требуется нажать кнопку «**Форматировать**».

4.4 Настройка политик безопасности

Политики безопасности или параметры безопасности — совокупность правил по обеспечению безопасности информации, выраженные настраиваемыми категориями системы защиты.

Политики безопасности определяют принципы функционирования защитных механизмов **СЗИ НСД** и ОС:

- Параметры, связанные с входом пользователей в систему.
- Сложность пароля учетных записей пользователей.
- Число разрешенных сеансов.
- Работа **СЗИ НСД** с учетными записями домена.
- Политики аудита.
- Периоды создания архивных копий журналов информационной безопасности.
- Политики проверки целостности аппаратной среды.

Консольная оболочка администрирования

Для удобства администрирования параметры безопасности объединены в следующие категории:

- Политики входа.
- Политики аудита.
- Политики целостности аппаратной среды.

Для перехода в подменю управления политиками безопасности в консольном приложении управления средством защиты информации необходимо набрать команду *policies.* Для выхода из раздела необходимо набрать команду *back*.

Доступные команды раздела *policies:*

- *show-all* — просмотр текущих значений политик безопасности;
- *user-get-ticket* — переход в раздел получения Kerberos-билета для доступа к доменной информации учетной записи пользователя;
- *password-policies-set* — переход в раздел настройки политик сложности пароля;
- *session-policies-set* — переход в раздел настройки политик сессий пользователей;

- *journal-policies-set* — переход в раздел настройки периода создания архивных копий журналов информационной безопасности **СЗИ НСД**;
- *audit-policies-set* — переход в раздел настройки политик аудита;
- *hardware-policies-set* — переход в раздел настройки политик проверки целостности аппаратной среды;
- *firewall-policies-set* — переход в раздел настройки политик работы межсетевого экрана;
- *list* — просмотр списка доступных команд и подменю;
- *help* — вывод информации о встроенных командах;
- *back* — выход из подменю (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dlladmin*.

Для просмотра текущих значений политик безопасности необходимо набрать управляющую команду *show-all.*

Результат успешного выполнения (возвращается список политик, состоящий из разделов):

- наименование политики безопасности;
- текущее значение атрибутов политики безопасности.

Результат ошибочного выполнения:

- *"send_zmq_cmd()# timeout response"* — не удалось передать запрос на получение списка политики безопасности;
- *"Error 13: Authorization is needed"* — не удалось получить политики безопасности, так как нарушена связь с **СЗИ НСД**.

Графическая оболочка администрирования

Для настройки политик безопасности **СЗИ НСД** в графической оболочке администрирования необходимо выбрать вкладку «**Параметры безопасности**» (см. Рисунок 44). На данной вкладке представлены следующие категории настраиваемых параметров системы защиты:

- «Основные настройки»;
- «Настройки сессий»;
- «Политики аудита»;
- «Политики паролей»;
- «Политики контроля целостности»;
- «Домен безопасности».

Для каждой категории в рабочей области отображается таблица с полями «*Имя*» и «*Значение*». Настройка параметров выполняется непосредственно в таблице, путем редактирования установленного значения (установка курсора в ячейке «Значение» напротив соответствующего названия параметра). После настройки параметров на панели действий необходимо выбрать команду «**Сохранить**» (см. Рисунок 44).

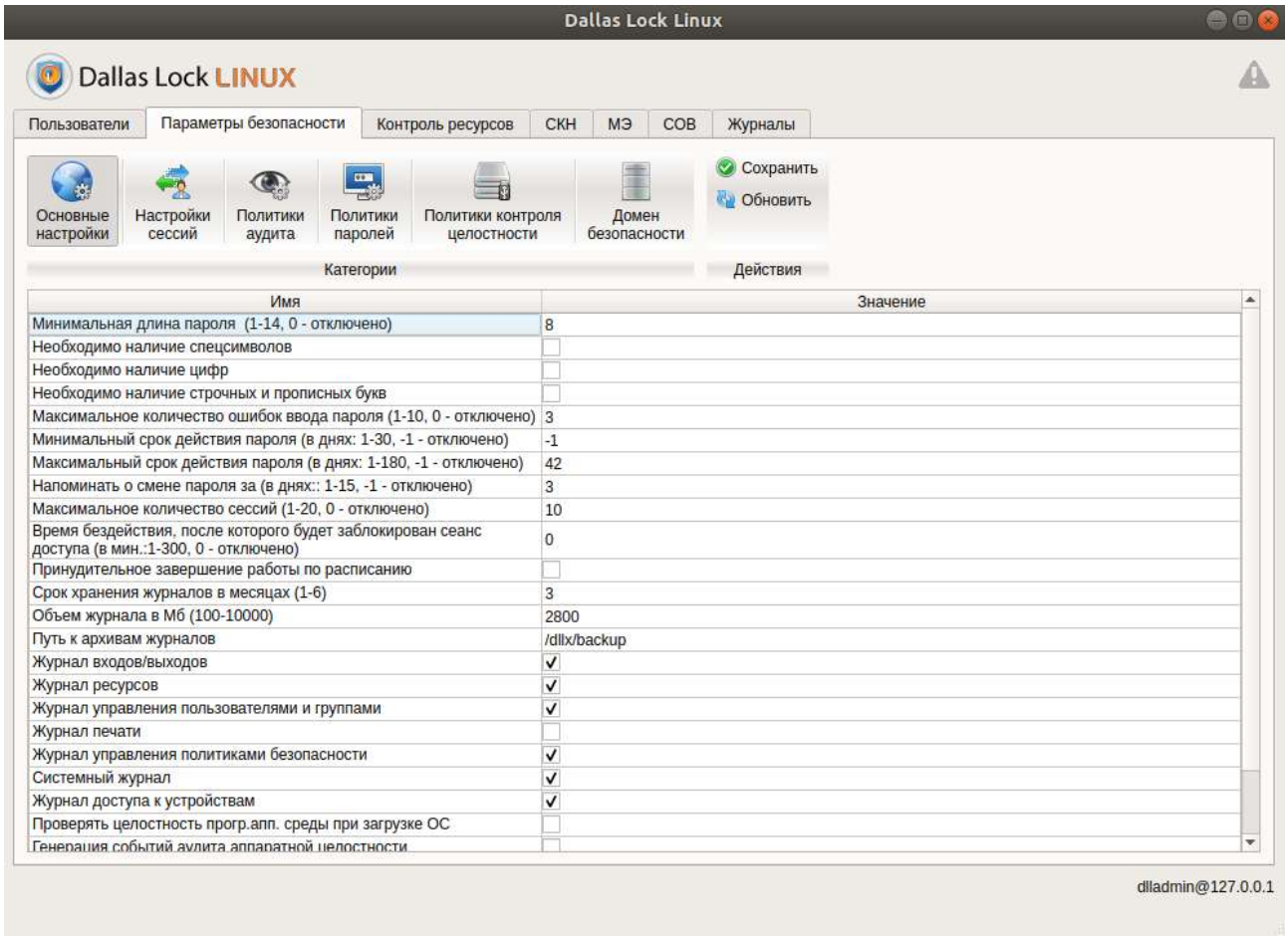


Рисунок 44. Вкладка «Параметры безопасности»

4.4.1 Настройка пароля

Консольная оболочка администрирования

Для определения (установки) политик, связанных со сложностью пароля, необходимо ввести команду *password-policies-set* в разделе управления политиками безопасности консольной оболочки администрирования. После ввода команды система перейдет в раздел *password-policies-set,* где необходимо установить параметры сложности пароля, используя команды, указанные в Таблица 22.

Следует обратить внимание, что политики сложности пароля не работают для администратора безопасности в сеансе *ishl*.

> По истечении установленного срока действия пароля во время блокировки экрана **СЗИ** автоматически предложит сменить пароль только при входе в ОС.

Таблица 22

№	Команда	Описание
1	*min-len <число>*	Определяет минимальную длину пароля, допустимое значение атрибута в пределах от 0 до 14 символов в пароле. Установленное значение «0» означает, что параметр не используется
2	*has-spec-sym <yes/no>*	Политика определяет необходимость использования в пароле специальных символов: “!”, “«”, “#”, “$”, “%”, “&”, “‘”, “(”, “)”, “*”, “+”, “,”, “-”, “.”, “/”, “:”, “<”, “=”, “>”, “?”, “@”, “[”, “\”, “]”, “^”, “_”, “`”, “{”, “}”, “~”. Установка значения *yes* обозначает, что специальные символы в пароле должны присутствовать обязательно.

№	Команда	Описание
		Пример. Если у пользователя имеется пароль «password1» и если политика включена, то при смене пароля на «password**2**» выведется сообщение об ошибке. Правильной будет смена пароля, например, с «password1» на «password#»
3	*has-digit-sym <yes/no>*	Ввод команды определяет необходимость наличия в парольной строчке цифровых символов. Установка значения *yes* обозначает, что цифровые символы в пароле должны присутствовать обязательно. **Пример.** У пользователя имеется пароль «password», если описанная выше политика включена, то при смене пароля на «password**d**» выведется сообщение об ошибке. Правильной будет смена пароля, например, с «password» на «password**12**»
4	*has-upperlower-sym <yes/no>*	Политика определяет необходимость совместного наличия в парольной строчке строчных и прописных букв. Установка значения *yes* обозначает, что буквенные символы в нижнем и верхнем регистре в пароле должны присутствовать обязательно. **Пример.** Если у пользователя имеется пароль «password1», и если политика включена, то при смене пароля на «pa**c**sword1» будет выведено сообщение об ошибке. Если пользователь сменит пароль «password1» на «pa**S**sword1», то операция завершится успешно
5	*retries <число>*	Политика определяет максимальное число попыток ввода неверного пароля, после которого произойдет блокировка возможности авторизации под данной учетной записью на определенный промежуток времени. Принимает числовое значение от 0 до 10. Значение «0» обозначает, что данная политика отключена. Длительность блокировки по умолчанию — пять минут (или иное время в зависимости от настроек системы)
6	*pswd-min-days <число>*	Минимальный срок действия пароля, который необходимо задать пользователю, чтобы сменить пароль. Указывается в днях. Необязательный атрибут. **Принимает значения:** -1, от 1 до 30. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на минимальный срок действия пароля накладываться не будет
7	*pswd-max-days <число>*	Максимальный срок действия пароля. После истечения срока действия пароля система будет требовать смену пароля учетной записи пользователя. Необязательный атрибут. **Принимает значения:** -1, от 1 до 180. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на максимальный срок действия пароля накладываться не будет
8	*pswd-wrn-days <число>*	Значение (в днях), после которого пользователю будут выдаваться уведомления о необходимости смены пароля, с указанием количества дней до истечения срока действия пароля. Необязательный атрибут. **Принимает значения:** -1, от 1 до 15. Установка значения -1 обозначает, что уведомлений выдаваться не будет

Пример:

policies <enter>

password-policies-set <enter>

has-spec-sym yes <enter>

min-len 9 <enter>

execute <enter>

Результат успешного выполнения:

– *"Success setting password policies"*— политики сложности пароля установлены успешно.

Результат ошибочного выполнения:

– *"send_zmq_cmd()# timeout responses"* — не удалось передать запрос на изменение политик сложности пароля;

– *"Error 13: Authorization is needed"* — не удалось получить политики безопасности, так как нарушена связь с **СЗИ НСД**.

> **!** На некоторых дистрибутивах GNU/Linux, для активации политики «**Срок действия пароля**», необходимо принудительно изменить пароль пользователям, созданным до установки **СЗИ**.

Графическая оболочка администрирования

К категории «**Политики паролей**» относятся следующие параметры (см. Рисунок 45):

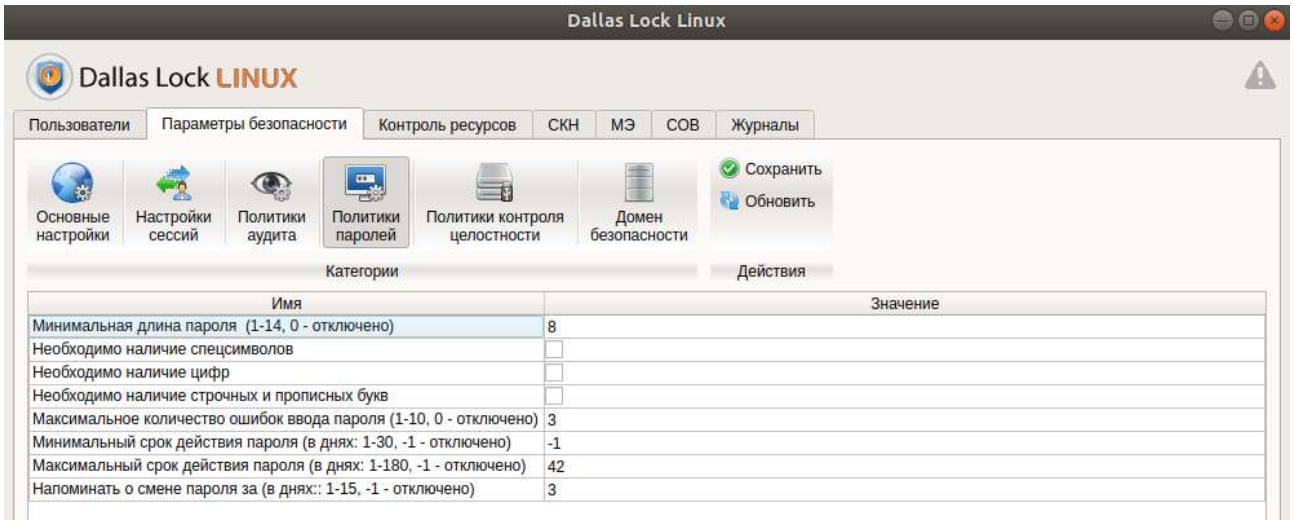


Рисунок 45. Категория «Политики паролей»

> **!** По истечении установленного срока действия пароля во время блокировки экрана **СЗИ** автоматически предложит сменить пароль только при входе в ОС.

– Минимальная длина пароля. Данным параметром устанавливается ограничение на минимальную длину пароля. Длина пароля может быть от 0 до 14 символов. Установленное значение «0» означает, что параметр не используется. Если число символов в пароле меньше установленного значения, то при проверке пароля будет выходить сообщение «*Неверная длина пароля*». По умолчанию установлено значение *8*.

– Необходимо наличие спецсимволов. Если флаг для данного параметра установлен, то при создании пароля в нем должны присутствовать специальные символы: «!», «@», «#», «$», «%», «&», «‘», «“», «)», «(», «*», «+», «,», «-», «.», «/», «;», «:», «<», «>», «?», «[», «]», «\», «^», «_», «{», «}», «~», «|». Если в пароле нет спецсимволов, то при проверке пароля будет выходить сообщение «*Пароль должен содержать специальные символы*». По умолчанию флаг не установлен.

– Необходимо наличие цифр. Если флаг для данного параметра установлен, то при создании пароля в нем должны присутствовать цифры. Если в пароле нет цифр, то при проверке пароля будет выходить сообщение «*Пароль должен содержать цифры*». По умолчанию флаг не установлен.

– Необходимо наличие строчных и прописных букв. Если флаг для данного параметра установлен, то при создании пароля в нем должны присутствовать строчные и прописные

буквы. Если в пароле нет символов верхнего и нижнего регистра, то при проверке пароля будет выходить сообщение «Парол*ь должен содержать символы верхнего и нижнего регистров*». По умолчанию флаг не установлен.

- Максимальное количество ошибок ввода пароля. Установленное значение регламентирует, сколько раз пользователь может ошибиться при вводе пароля. Если при авторизации на ТС пользователь ввел неверный пароль, то появится предупреждение «Указан неверный логин и/или пароль». Если число ошибок достигнет установленного допустимого значения, то учетная запись будет заблокирована, и пользователь не сможет войти в систему. Учетная запись будет заблокирована в течение 5 минут, после чего пользователь может попытаться ввести пароль еще раз. По умолчанию установлено значение *3*.
- Минимальный срок действия пароля. Минимальный срок действия пароля, который необходимо задать пользователю, чтобы сменить пароль. Указывается в днях. Необязательный атрибут. Принимает значения: -1, от 1 до 30. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на минимальный срок действия пароля накладываться не будет. По умолчанию установлено значение *-1*.
- Максимальный срок действия пароля. После истечения срока действия пароля учетной записи система будет требовать смену пароля учетной записи пользователя. Принимает значения: -1, от 1 до 180. Установка значения -1 обозначает, что для данной учетной записи пользователя ограничений на максимальный срок действия пароля в днях накладываться не будет. По умолчанию установлено значение *42*.
- Напомнить о смене пароля за. Значение (в днях) после которого пользователю будут выдаваться уведомления о необходимости смены пароля, с указанием количества дней до истечения срока действия пароля. Необязательный атрибут. Принимает значения: -1, от 1 до 15. Установка значения -1 обозначает, что уведомлений выдаваться не будет. По умолчанию установлено значение *3*.

На некоторых дистрибутивах GNU/Linux, для активации политики «**Срок действия пароля**», необходимо принудительно изменить пароль пользователям, созданным до установки **СЗИ**.

4.4.2 Число разрешенных сеансов

Консольная оболочка администрирования

Для определения (установки) политик, связанных с ограничением числа допустимых сессий пользователей, необходимо ввести команду *session-policies-set* в разделе управления политиками безопасности консольной оболочки администрирования. После ввода команды система перейдет в раздел управления политиками сессий *session-policies-set*, где необходимо задать правила, используя атрибуты, указанные в Таблица 23.

Таблица 23

№	Атрибуты	Описание
1	*max-sessions <число>*	**Политика не распространяется на суперпользователя *root*.** Политика задает максимальное допустимое количество сессий пользователей на данном ТС. Принимает числовое значение от 0 до 20. Если значение равно нулю — данная политика отключена. Следует обратить внимание, что для осуществления входа при помощи графической оболочки ОС в политике безопасности СЗИ НСД необходимо указать значение максимального допустимого количества сессий пользователей равным или большим 2. При превышении максимального количества сессий пользователю при авторизации будет выводиться предупреждение (например, «Не удалось создать/удалить запись...», «Cannot make/remove an entry for the specifed session», «Достигнут лимит подключений пользователя»)
2	*lock-timeout <число>*	**Политика не применяется на ОС Astra Linux Special Edition 2.12.**

		Политика задает максимальное время (в минутах) бездействия пользователя, по истечению которого сессия такого пользователя будет заблокирована. Принимает числовое значение от 1 до 300, установленное значение равное нулю — данная политика отключена. Политика вступает в силу для всех новых графических и терминальных сессий
3	*schedule-force-shutdown <значение>*	Политика позволяет выбрать принудительное завершение в качестве действия, применяемого к пользовательским сессиям по наступлению запрещенного интервала времени. **Принимает значения**: *no* — для всех пользовательских сессий применяется блокировка, *yes* — для пользовательских сессий будет применяться принудительное завершение. По умолчанию в качестве значения политики установлено «no»

Настройка блокировки графической сессии также доступна к изменению с помощью стандартных утилит настройки ОС. Такое изменение не отобразится в оболочке администрирования **СЗИ НСД**.

Пример:

policies <enter>

session-policies-set <enter>

lock-timeout 0 <enter>

execute <enter>

Результат успешного выполнения:

- "*Session settings session policies*" — политики пользовательских сессий успешно установлены.

Результат ошибочного выполнения:

- *"send_zmq_cmd()# timeout responses"* — не удалось передать запрос на изменение политик пользовательских сессий;
- *"Error 13: Authorization is needed"* — не удалось получить политики безопасности, так как нарушена связь с СЗИ НСД;
- *"Invalid input: <наименование атрибута> should be in range <[граничные значения указанного атрибута]>"* — введено недопустимое значение.

Графическая оболочка администрирования

Количество разрешенных сеансов задается в категории «**Настройки сессий**». Категория содержит параметры настройки сессий учетных записей пользователей (см. Рисунок 46). К данным параметрам относятся:

- Максимальное количество сессий[21]. Максимальное количество активных сессий на данном ТС. Возможные значения 0 и от 1 до 20. Установка значения «0» означает, что параметр будет отключен. По умолчанию установлено значение *10*.
- Время бездействия, после которого будет заблокирован сеанс доступа (в минутах). Автоматическое закрытие сессии пользователя через определенное время неактивности учетной записи пользователя. Возможные значения 0 и от 1 до 300 Установка значения «0» означает, что параметр будет отключен. По умолчанию установлено значение *0*.
- Принудительное завершение работы по расписанию (флаг). Установка данного параметра позволяет принудительно завершить работу пользовательских сессий, а не блокировать при наступлении запрещенного временного интервала. По умолчанию флаг не установлен.

[21] Не распространяется на суперпользователя root.

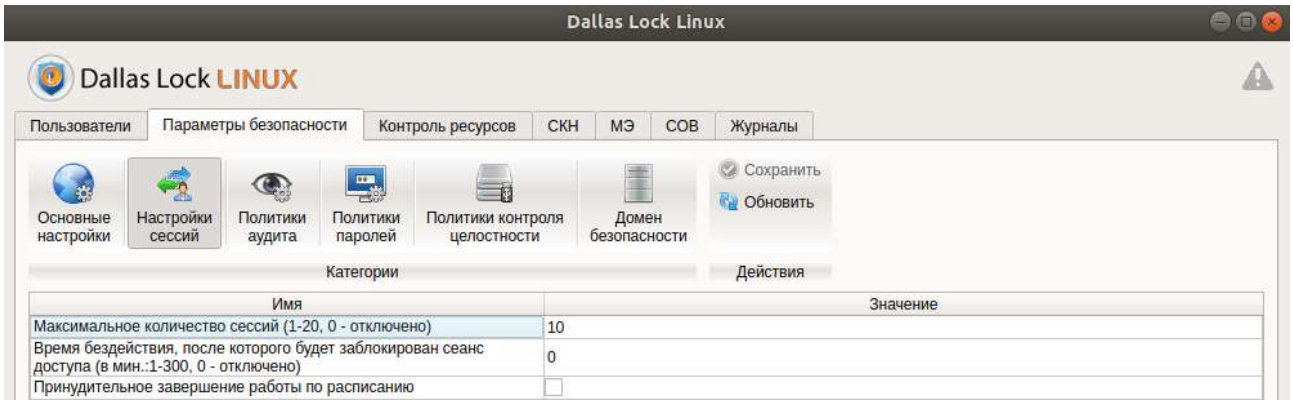


Рисунок 46. Категория «Настройки сессий»

Настройка блокировки графической сессии также доступна к изменению с помощью стандартных утилит настройки ОС. Такое изменение не отобразится в оболочке администрирования **СЗИ НСД**.

4.4.3 Политики аудита

Консольная оболочка администрирования

Для установки политик, связанных с правилами аудита, необходимо в консольной оболочке администрирования в разделе управления политиками безопасности *policies* набрать команду *audit-policies-set.* После ввода команды система перейдет в раздел управления политиками аудита *audit-policies-set*, где необходимо задать правила, используя атрибуты, приведенные в Таблица 24.

Таблица 24

№	Атрибуты	Описание
1	*entries-policies <yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с событиями входа в ОС, и запись таких событий в журнал входов. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
2	*resources-policies<yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с событиями доступа к защищаемым объектам, и запись таких событий в журнал ресурсов. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
3	*users-policies <yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с событиями управления пользователями (группами пользователей), и запись таких событий в журнал управления пользователями. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
5	*printing-policies <yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с событиями печати, и запись таких событий в журнал печати. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
6	*policies-policies <yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с управлением политиками безопасности, и запись таких событий в журнал управления политиками. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
7	*devices-policies <yes/no>*	Политика определяет, будет ли выполняться сбор событий, связанных с событиями доступа к устройствам, и запись таких событий в журнал печати. **Принимает значения:** *yes* — собирать, *no* — сбор не производится

8	*syslog-policies <yes/no>*	Политика определяет, будут ли регистрироваться системные события в журнале системных событий **СЗИ**. **Принимает значения:** *yes* — собирать, *no* — запись не производится
9	*firewall-security-events <yes/no>*	Политика определяет, будут ли выполняться сбор событий, связанных с событиями безопасности МЭ, и запись таких событий в журнал события безопасности МЭ. **Принимает значения:** *yes* — собирать, *no* — сбор не производится
10	*firewall-management <yes/no>*	Политика определяет, будут ли выполняться сбор событий, связанных с событиями управления МЭ, и запись таких событий в журнал управления МЭ **Принимает значения:** *yes* — собирать, *no* — сбор не производится

Пример:

policies <enter>

audit-policies-set <enter>

syslog-policies yes <enter>

execute <enter>

Результат успешного выполнения:

- *"Success setting audit policies"* — политики аудита успешно установлены.
- *"Nothing to change"* — ничего не изменить. Сообщение выводится в случае, если в политиках аудита нечего менять.

Результат ошибочного выполнения:

- *"send_zmq_cmd()# timeout responses"* — не удалось передать запрос на изменение политик аудита;
- *“Error 13: Authorization is needed"* — не удалось получить политики безопасности, так как нарушена связь с **СЗИ НСД**.

Графическая оболочка администрирования

Чтобы установить политики аудита, необходимо перейти в категорию «**Политики аудита**» (см. Рисунок 47), затем с помощью установки флага отметить необходимые для протоколирования журналы. Категория «**Политики аудита**» включает следующие параметры:

- Срок хранения журналов в месяцах. Данным параметром устанавливается срок хранения журналов в месяцах. Принимает значения от 1 до 6. По умолчанию установлено значение 3.
- Объем журнала в Мб. Параметр устанавливает ограничения объема журналов в диапазоне от 100 Мб до 10000 Мб для архивации. По умолчанию установлено значение 2800 Мб.
- Путь к архивам журналов. Установка пути архивации журналов в системе. По умолчанию указан путь: */dllx/backup*.
- Журнал входов/выходов. Установка флага позволяет протоколировать в журнале события аутентификации пользователей в операционной системе.
- Журнал ресурсов. Установка флага позволяет протоколировать в журнале события, связанные с настройкой правил разграничения доступа и обращением к защищаемым объектам доступа.
- Журнал управления пользователями и группами. Установка флага позволяет протоколировать в журнале события, связанные с созданием, редактированием, удалением учетных записей пользователей и групп пользователей.
- Журнал печати. Установка флага позволяет протоколировать в журнале события печати на печатающих устройствах. Принимает значения – Да и нет. По умолчанию установлено значение Нет.
- Журнал управления политиками безопасности. Установка флага позволяет протоколировать в журнале события по изменению политик безопасности.
- Системный журнал. Установка флага позволяет протоколировать в журнале события системного журнала операционной системы (syslog).

– Журнал доступа к устройствам. Установка флага позволяет протоколировать в журнале события, связанные с настройками правил разграничения доступа и обращения к подключаемым устройствам.

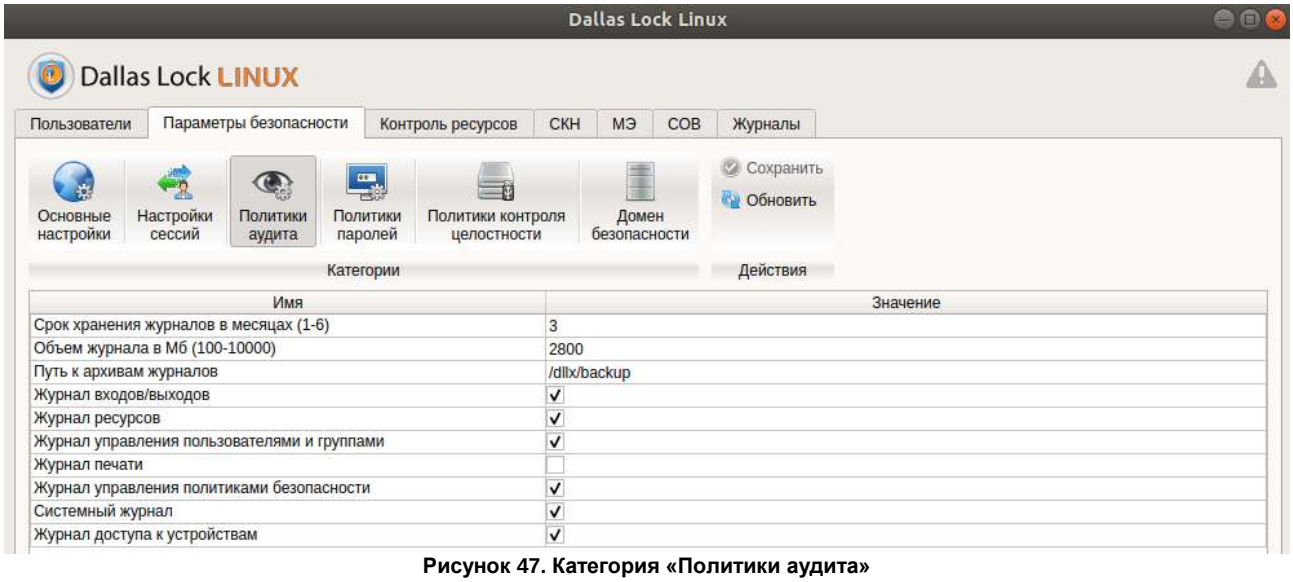


Рисунок 47. Категория «Политики аудита»

4.4.4 Срок хранения журналов в месяцах

Консольная оболочка администрирования

Для установки срока хранения журналов информационной безопасности **СЗИ НСД** необходимо в консольной оболочке администрирования в разделе управления политиками безопасности *audit* набрать команду *journal-policies-set*. После ввода команды система перейдет в раздел *journal-policies-set*, где необходимо задать срок хранения журналов в месяцах с помощью команды *lifetime.* В качестве передаваемого значения указывается целое число месяцев в диапазоне от 1 до 6 включительно.

Пример:

policies <enter>

journal-policies-set <enter>

lifetime 5 <enter>

execute <enter>

Результат успешного выполнения:

– *"Success setting journal policies"* — политики настройки периода хранения архивных копий журнала установлены.

Результат ошибочного выполнения:

– *"send_zmq_cmd()# timeout responses"* — не удалось передать запрос на изменение политик аудита;

– *"Error 13: Authorization is needed"* — не удалось получить политики безопасности, так как нарушена связь с **СЗИ НСД**;

– *"Invalid input: journal lifetime should be in range [1, 6]"* — введено неверное значение.

Графическая оболочка администрирования

Срок хранения журналов можно задать в категории «**Политики аудита**» (см. Рисунок 47). Установка срока хранения журналов осуществляется в месяцах (от 1 до 6 включительно). После окончания указанного срока формируется архив, и журналы начинают заполняться новыми данными. По умолчанию установлено значение 3.

4.4.5 Ограничение объема журналов

При превышении заданного объема журнала, происходит создание архивной копии журнала.

Консольная оболочка администрирования

Для установки объема журналов, необходимого для создания архивных копий журналов информационной безопасности **СЗИ НСД**, необходимо в консольной оболочке администрирования в разделе управления политиками безопасности *policies* набрать команду *journal-policies-set*. После ввода команды система перейдет в раздел *journal-policies-set*, где необходимо задать ограничения объема журналов в диапазоне «от 100 Мб до 10000 Мб».

Пример:

policies <enter>

journal-policies-set <enter>

size 500 <enter>

execute <enter>

Для принудительного создания архивных копий журналов необходимо перейти в раздел *audit* и выбрать команду *archivate* без параметров.

Пример:

audit <enter>

archivate <enter>

Графическая оболочка администрирования

Для установки объема журналов, необходимого для создания архивной копии, нужно перейти в категорию «**Политики аудита**» (см. Рисунок 47), затем в строке «*Объем журнала в Мб (100-10000)*» необходимо задать объем, при достижении которого будет создана архивная копия журнала.

4.4.6 Настройка политик проверки целостности аппаратной среды

Консольная оболочка администрирования

Для установки политик проверки целостности аппаратной среды необходимо в консольной оболочке администрирования в разделе управления политиками безопасности *policies* выполнить команду *hardware-policies-set*. После ввода команды система перейдет в раздел *hardware-policies-set*, где необходимо задать правила, используя атрибуты, приведенные в Таблица 25.

Таблица 25

№	Атрибуты	Описание
1	*check-on-boot <yes/no>*	Включение/отключение проверки целостности прогр.апп. среды при загрузке системы. По умолчанию параметр отключен. **Принимает значения:** *yes* — включить, *no* — отключить
2	*generate-audit <yes/no>*	Включение/отключение отслеживания событий нарушения целостности. По умолчанию параметр отключен. **Принимает значения:** *yes* — включить, *no* — отключить
3	*umount-unsupported-usb <yes/no>*	Включение/отключение автоматического размонтирования неподдерживаемых USB-устройств. Установка данного параметра позволяет СЗИ НСД автоматически размонтировать внешние накопители с неподдерживаемой ФС. **Принимает значения:** *yes* — включить, *no* — отключить

Пример:

policies<enter>

hardware-policies-set<enter>

check-on-boot yes<enter>

generate-audit yes<enter>

execute<enter>

Результат успешного выполнения:

- *"Success setting hardware integrity policy"* — политика проверки целостности включена;
- *“Success updating policies"* — политика аудита включена.

Результат ошибочного выполнения:

- *"Invalid input: ‘yes’ or ‘no’ expected"* — логическое значение не является допустимым. Доступные значения «yes» или «no».

Графическая оболочка администрирования

Для установки политик проверки целостности программно-аппаратной среды необходимо перейти в категорию «**Политики контроля целостности**» (см. Рисунок 48). Категория содержит следующие параметры:

- Проверять целостность программно-аппаратной среды при загрузке ОС. Установка данного параметра позволяет осуществлять автоматическую проверку целостности аппаратной среды при загрузке системы. По умолчанию флаг не установлен.
- Генерация событий аудита аппаратной целостности. Установка данного параметра позволяет отслеживать события нарушения аппаратной целостности. По умолчанию флаг не установлен.
- Автоматическое размонтирование неподдерживаемых USB-устройств. Установка данного параметра позволяет **СЗИ НСД** автоматически размонтировать внешние накопители с неподдерживаемой ФС. По умолчанию флаг установлен.

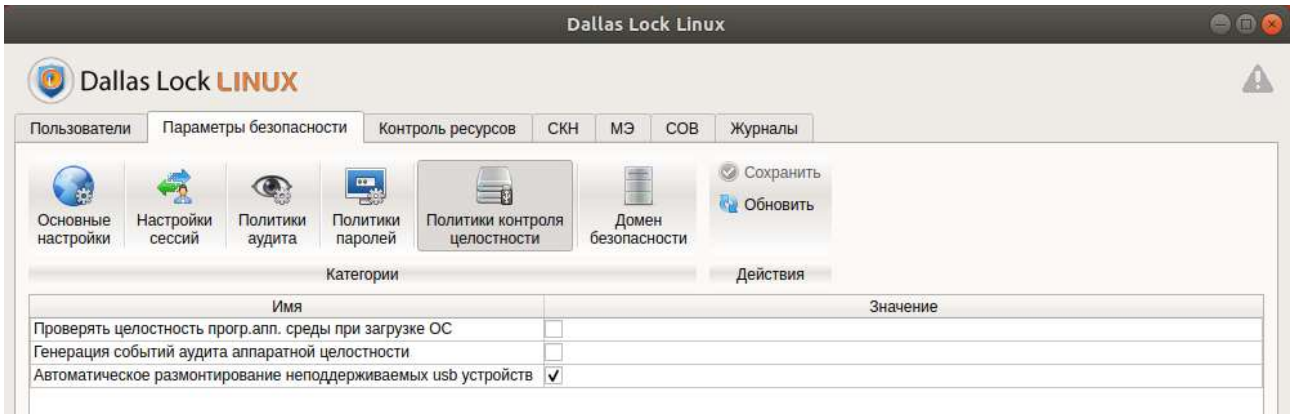


Рисунок 48. Категория «Политики контроля целостности»

4.4.7 Настройка политик работы межсетевого экрана

Консольная оболочка администрирования

Для перехода в подменю управления политиками непосредственно межсетевого экрана необходимо в подменю управления политиками *policies* выполнить команду *firewall-policies-set.* После ввода команды система перейдет в раздел *firewall-policies-set*, где необходимо задать политики МЭ, используя атрибуты, представленные в Таблица 26.

Таблица 26

№	Атрибуты	Описание
1	*firewall-is-active <yes/no>*	Запуск работы межсетевого экрана. **Принимает значения:** *yes* — включить; *no* — отключить
2	*ssl-analyze <yes/no>*	Запуск проверки шифрованного трафика. **Принимает значения:** *yes* — включить; *no* — отключить

№	Атрибуты	Описание
3	*audit <значение>*	Включение анализа и журналирования событий межсетевого экрана. **Принимает значения:** *yes* — включить; *no* — отключить. Доступен аудит следующих событий межсетевого экрана: *–address-blocking;* *–kill-connection;* *–policies-change;* *–testing;* *–set-rule;* *–change-rule;* *–remove-rule;* *–firewall-state;* *–set-profile;* *–change-profile;* *–remove-profile;* *–set-blacklist-command;* *–change-blacklist-command;* *–remove-blacklist-command;* *–set-whitelist-command;* *–change-whitelist-command;* *–remove-whitelist-command* **Пример:** *policies <enter>* *firewall-policies-set <enter>* *audit remove-rule yes <enter>* *execute <enter>*
4	*black-white-lists <значение>*	Включение/отключение белого и черного списков команд. **Принимает значения:** *whitelis*t — включение белого списка команд, *blacklist* — включение черного списка команд, *none* — выключение белого и черного списков команд. Одновременно включить черный и белый списки команд невозможно. **Пример:** *policies <enter>* *firewall-policies-set <enter>* *black-white-lists blacklist <enter>* *execute <enter>*
5	*auto-block-interval <значение>l*	Изменение максимального интервала журналирования события типа «Срабатывание правил» (в минутах). Политика определяет интервал срабатывания правил для автоматической блокировки адресов. **Принимает значения:** от 1 до 60
6	*auto-block-burst <значение>*	Изменение максимального количества журналируемых событий типа «Срабатывание правил». Политика определяет количество срабатывания правил для автоматической блокировки адресов. **Принимает значения:** от 1 до 10

Пример:

policies <enter>
firewall-policies-set <enter>
firewall-is-active yes <enter>
execute <enter>

Графическая оболочка администрирования

Чтобы установить политики аудита межсетевого экрана с помощью графической оболочки **СЗИ НСД**, необходимо во вкладке «**МЭ**» перейти в категорию «**Параметры**» (см. Рисунок 49).

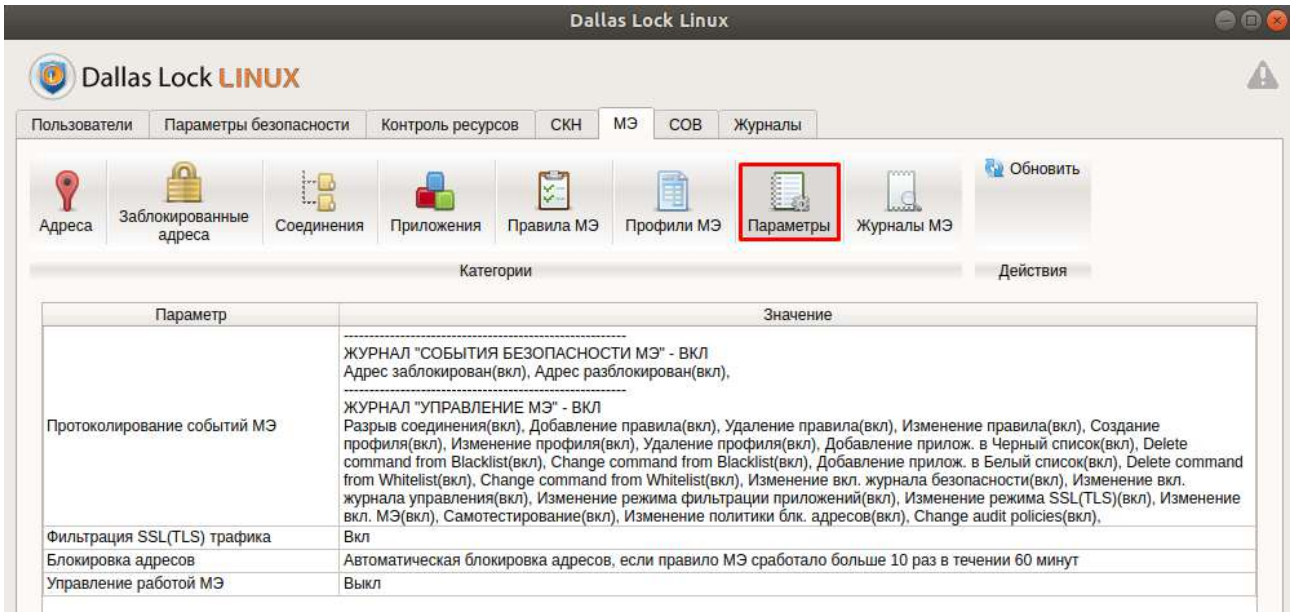


Рисунок 49. Категория «Параметры»

Категория «**Параметры**» включает в себя следующие параметры:

- Протоколирование событий МЭ. Политика позволяет определить тип регистрируемых событий межсетевого экрана, а также включение и отключение введения журналов МЭ. При выключении журналов события МЭ удаляются. Доступны следующе типы регистрируемых событий:
  - разрыв соединения;
  - адрес заблокирован;
  - адрес разблокирован;
  - добавление правил МЭ;
  - удаление правил МЭ;
  - изменение правил МЭ;
  - создание профиля;
  - изменение свойств профиля;
  - удаление профиля;
  - изменение режима фильтрации SSL(TLS) трафика;
  - изменение политики блокировки адресов;
  - изменение режима фильтрации приложений;
  - изменение режима работы МЭ;
  - самотестирование МЭ;
  - добавление приложения в *Blacklist*;
  - удаление приложения из *Blacklist*;
  - изменение свойств приложения в *Blacklist*;
  - добавление приложения в *Whitelist*;
  - удаление приложения из *Whitelist*;
  - изменение свойств приложения в *Whitelist*;
  - изменение событий протоколирования конфигурации;
  - изменение режима работы журнала «События безопасности МЭ»
  - изменение режима работы журнала «Управление МЭ».

Для регистрации требуемых событий для протоколирования событий МЭ необходимо двойным кликом мыши запустить «Значение» параметра «**Протоколирование событий МЭ**». Далее — откроется окно «**Протоколирование событий МЭ**» (см. Рисунок 50).

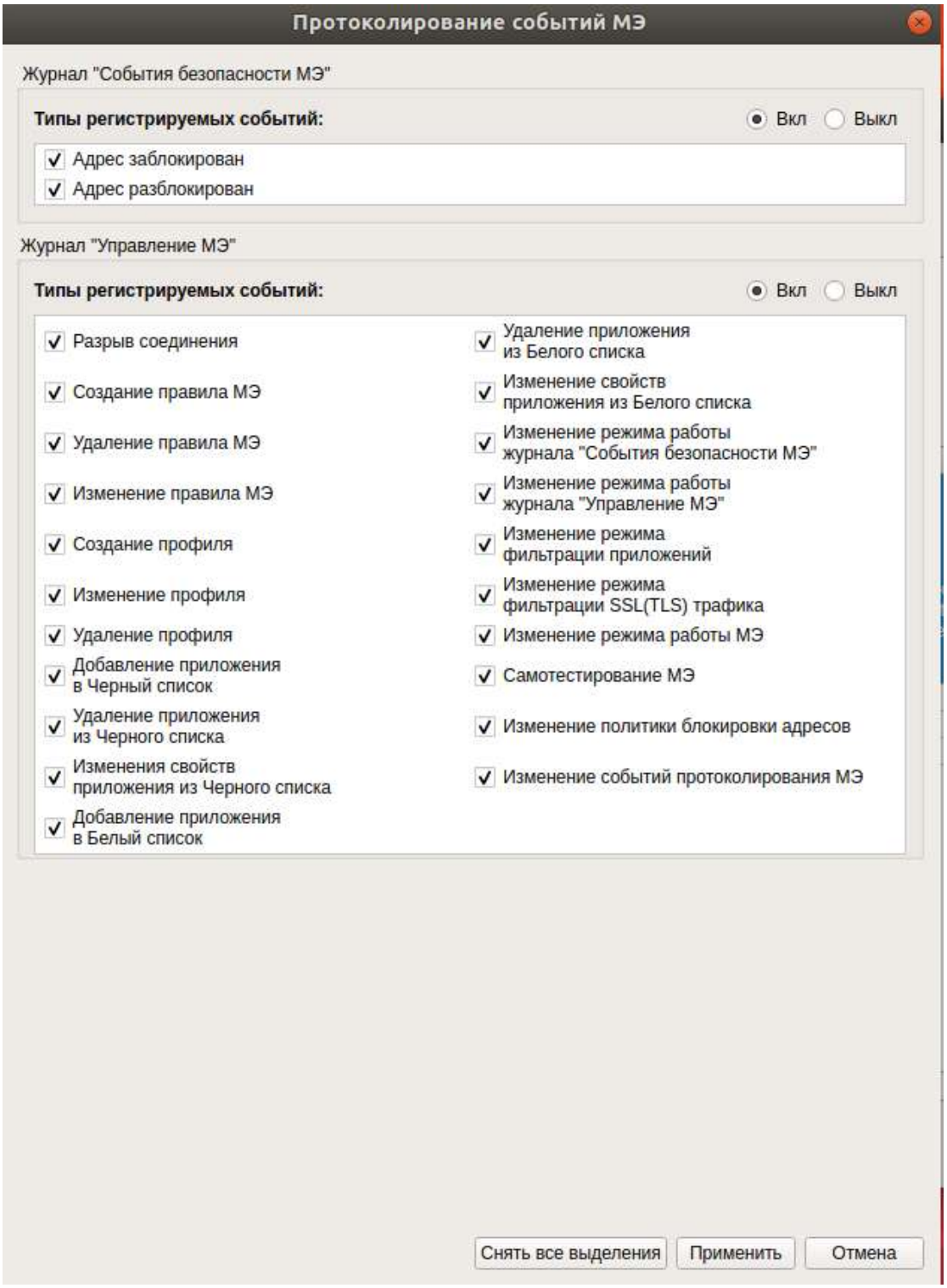


Рисунок 50. Протоколирование событий МЭ

- Фильтрация SSL (TLS) трафика. Параметр позволяет включить режим фильтрации SSL (TLS) трафика. Принимает значения: «вкл», «выкл». По умолчанию установлено значение *Вкл.*
- Блокировка адресов. Политика позволяет осуществить блокировку адресов при установленном количестве срабатываний правил межсетевого экрана в течении установленного периода времени. Принимает значение количества срабатываний: от 2 до 10; принимает значение срабатываний правил МЭ: от 5 до 60 минут. По умолчанию политика осуществляет блокировку адресов при 10 срабатываниях правил МЭ в течение 60 минут (см. Рисунок 51).

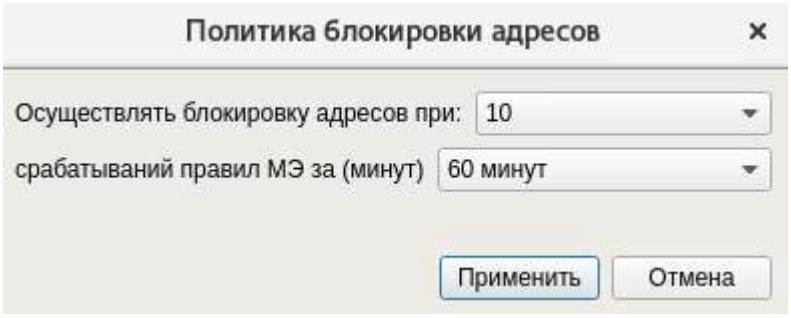


Рисунок 51. Политика блокировки адресов

– Управление работой МЭ. Политика позволяет включить или выключить работу межсетевого экрана. По умолчанию установлено значение «*Выкл*» При выключенном МЭ отключается только фильтрация согласно установленным правилам МЭ и списки команд *Blacklist* и *Whitelist.*

4.5 Разграничение доступа к объектам файловой системы

С помощью **СЗИ НСД Dallas Lock Linux** можно разграничить доступ к объектам файловой системы. **СЗИ НСД** позволяет гибко задавать пользователям права на доступ к объектам ФС. После задания прав пользователи могут работать только с теми объектами, доступ к которым им разрешен, и совершать над ними только санкционированные операции.

Дискреционные права доступа и контроль целостности принудительно назначены системой защиты на каталог /boot. В случае необходимости взаимодействия с объектами файловой системы из вышеупомянутого каталога, есть возможность их отключить. По завершению работы рекомендуется дискреционные права доступа и контроль целостности восстановить. На случай, если рекомендация будет не выполнена, то после перезагрузки ТС права доступа и контроль целостности **СЗИ НСД** на /boot восстановятся.

Для корректной работы разграничения доступа к объектам файловой системы, расположенных на съемных накопителях, смонтированный раздел съемного накопителя должен иметь какую-либо из файловых систем: ext2, ext3, ext4, JFS, ReiserFS. На ReiserFS под управлением CentOS 7[2] не поддерживается управление дискретным доступом.

СЗИ НСД Dallas Lock Linux не поддерживает имена файлов и каталогов, содержащих в своем имени специальные символы.

В **СЗИ НСД Dallas Lock Linux** реализовано управление механизмом разграничения прав доступа к объектам ФС на базе POSIX ACL[22]. Этот механизм предоставляет возможность установки прав доступа конкретным пользователям и группам, тем самым расширяя стандартные права.

Применительно к правам доступа, всех пользователей (субъекты доступа), зарегистрированных в системе защиты, можно разделить на три категории.

1. Учетные записи. Это индивидуальные учетные записи пользователей, для которых установлены индивидуальные (отличные от других пользователей и групп пользователей) права доступа.
2. Группа учетных записей. Всем учетным записям, входящим в одну группу, автоматически назначаются права на доступ, установленные для группы.
3. Остальные. Остальные учетные записи, для которых не назначены ни индивидуальные права доступа, ни групповые.

В **СЗИ НСД Dallas Lock Linux** каждому объекту может быть сопоставлен список, элементами которого могут являться индивидуальные учетные записи, группы пользователей и категория «**Остальные**».

Каждый объект системы защиты характеризуется набором параметров безопасности. Каждый параметр безопасности контролирует определенную операцию (чтение, выполнение, запись,

[22] POSIX ACL — система контроля для работы с ФС в ОС семейства Linux, посредством которой осуществляется установка прав доступа к файлам.

неуспешные попытки доступа), которая может быть произведена с объектом. Любая операция с объектом может быть разрешена, запрещена или не установлена пользователю.

Операции, которые можно производить с объектами в системе защиты, зависят от типа объекта.

Администратор ИБ имеет возможность назначать следующие права доступа к объекту системы защиты для выбранного субъекта доступа:

- каталоги, подкаталоги и файлы (могут находиться на локальных дисках, на сменных носителях, на сетевых ресурсах), символические ссылки:
  - «Чтение» — просмотр содержимого файла любого типа; обозначение — «*r*».
  - «Запись» — запись на диск измененного файла (изменение содержимого); обозначение — «*w*».
  - «Выполнение» — возможность загрузки файла в память и попытки запустить его на выполнение как исполняемую программу (только для программ); обозначение — «*x*».

При назначении прав доступа на системные директории необходимо учитывать зависящие от содержания этих директорий программы и сервисы. В случае высокой активности в целевой директории, операция назначения прав доступа может занять длительное время.

При запрете записи в папку переименование вложенных объектов 1-го уровня вложенности не выполняется.

Изменение прав доступа жесткой ссылки вызовет соответствующие изменения и в самом файле (объекте ссылки). Удаление ссылки, если она не последняя, не повлечет удаление файла, он остается существовать с назначенными правами.

При создании символической ссылки владельцы назначаются в соответствии с конфигурацией ОС (учетная запись пользователя и основная группа).

Если объект является вложенным и ему не сопоставлен список учетных записей с правами, то права доступа учетной записи к данному объекту определяются параметрами корневого объекта.

Если учетная запись находится в сопоставленном объекту списке и одновременно входит в состав группы учетных записей, находящихся в сопоставленном объекту списке, то действуют параметры доступа, установленные для этой учетной записи.

Если учетная запись входит в состав нескольких групп, находящихся в сопоставленном объекту списке, и, хотя бы для одной из этих групп установлен запрет на совершение данной операции, а также отсутствует индивидуальное сопоставление данной учетной записи объекту (нет явно назначенных прав), то учетной записи эта операция запрещается.

Следует учесть, что установленные права доступа для групп действительны только для сессий пользователей, запущенных после добавления пользователей в эти группы.

Если учетная запись не находится в сопоставленном объекту списке и не входит ни в одну из сопоставленных объекту (или корневому объекту) групп учетных записей, то для нее действуют параметры, установленные для категории учетных записей «*Остальные*» (пользователи, для которых не назначены индивидуальные права).

При назначении полных запрещающих прав доступа к объекту файловой системы, в общий список необходимо добавить категорию «*Остальные*».

Если для какого-то объекта назначаются права доступа, потом этот объект переименовывается/перемещается, то права доступа сохраняются, в данном случае права доступа «привязаны» к объекту.

Для перехода в подменю разграничения доступа к объектам файловой системы необходимо в консольной оболочке администрирования **СЗИ НСД** (*ishl*), в разделе *resources* выполнить команду *files*.

После ввода команды система перейдет в раздел *files,* где необходимо выполнить команду *dsb*, система перейдет в раздел управления доступом. Консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 27.

Пример:

resources <enter>

files <enter>

dsb <enter>

Таблица 27

№	Команда	Описание
1	*get-rights*	Получить список прав доступа к объекту ФС. Необходимо указать полный путь к объекту. **Пример:** *get-rights "/home/user/test.odt"* Если на объект ФС не были назначены права средствами **СЗИ НСД**, система выдаст сообщение *"Missing dsb rules" ("Права dsb отсутствуют").* Если на объект ФС были назначены права средствами **СЗИ НСД**, система выдаст сообщение, с указанием логина учетной записи и набором назначенных прав
2	*set-rights-user*	Установить права доступа учетной записи пользователя к объекту ФС, подробнее — в разделе Права доступа к объекту ФС
3	*user-list*	Команда просмотра списка учетных записей
4	*set-rights-group*	Установить права доступа группы пользователей к объекту ФС, подробнее — в разделе Права доступа к объекту ФС
5	*group-list*	Команда просмотра списка групп учетных записей
6	*set-rights-other*	Установить права доступа к объекту ФС для категории «прочие пользователи и группы», подробнее — в разделе Права доступа к объекту ФС
7	*get-owner*	Команда запроса логина владельца объекта ФС, подробнее — в разделе Смена владельца объекта файловой системы
8	*set-owner*	Установить владельца объекта ФС, подробнее — в разделе Смена владельца объекта файловой системы
9	*rm-rights-user*	Команда удаления прав доступа для выбранной учетной записи, подробнее — в разделе Удаление прав/правил доступа для субъекта доступа
10	*rm-rights-group*	Команда удаления прав доступа для выбранной группы учетной записи, подробнее — в разделе Удаление прав/правил доступа для субъекта доступа

4.5.1 Права доступа к объекту ФС

Консольная оболочка администрирования

Для задания прав доступа к объекту ФС для учетной записи пользователя в разделе управления доступом (*dsb*) необходимо выполнить команду *set-rights-user,* с указанием атрибутов, приведенных в Таблица 28.

Таблица 28

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*rights <значение>*	Задаваемые права на объект файловой системы. **Принимает значения:** строка в формате 'rwx', состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ "-".

№	Атрибут	Описание
		– *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Следует обратить внимание, что привилегия «*x*» для директорий имеет свойство разрешения вхождения в нее для субъектов доступа. Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой
3	*login <значение>*	Наименование учетной записи пользователя

Пример: назначение прав на чтение и запись на файл /home/user/test.odt для учетной записи user.

resources <enter>
files <enter>
dsb <enter>
set-rights-user /home/user/test.odt rw user<enter>

Для задания прав доступа к объекту ФС для группы пользователей в разделе управления доступом (*dsb*) необходимо выполнить команду *set-rights-group,* с указанием атрибутов, приведенных в Таблица 29.

Таблица 29

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*rights <значение>*	Задаваемые права на объект файловой системы. **Принимает значения:** строка в формате ‘rwx’, состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ “-”. – *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Следует обратить внимание, что привилегия «*x*» для директорий имеет свойство разрешения вхождения в нее для субъектов доступа. Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой
3	*group <значение>*	Наименование группы пользователей

Пример: назначение прав на чтение и запись на файл /home/user/test.odt для группы пользователей user.

resources <enter>

files <enter>

dsb <enter>

set-rights-group /home/user/test.odt rx user <enter>

Для задания прав на доступ для учетных записей категории «*Остальные*» (пользователи, для которых не назначены индивидуальные права), необходимо воспользоваться управляющей командой *set-rights-other,* указав в качестве атрибутов параметры, указанные в Таблица 30.

Таблица 30

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*rights <значение>*	Задаваемые права на объект файловой системы.

№	Атрибут	Описание
		Принимает значения: строка в формате 'rwx', состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ “-”. – *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Следует обратить внимание, что привилегия «*x*» для директорий имеет свойство разрешения вхождения в нее для субъектов доступа. Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой

Пример: назначение прав на чтение и запись на файл /home/user/test.odt для учетных записей категории «Остальные».

resources <enter>

files <enter>

dsb <enter>

set-rights-other /home/user/test.odt rw <enter>

Для корректной работы разграничения доступа к объектам файловой системы, расположенным на съемных накопителях, смонтированный раздел съемного накопителя должен иметь какую-либо из файловых систем: ext2, ext3, ext4, JFS, ReiserFS.

Графическая оболочка администрирования

Для того чтобы назначить дискреционный доступ для объекта ФС, необходимо выполнить следующие шаги:

1. В графической оболочке открыть вкладку «**Контроль ресурсов**» и перейти в категорию «**Файлы**» (см. Рисунок 52).

Рисунок 52. Выбор категории «Файлы»

2. В дереве объектов выбрать файл, на панели действий нажать на кнопку  «**Контроль над файлом**». (см. Рисунок 53).

Рисунок 53. Выбор объекта ФС

3. Далее в открытом окне «**Контроль над объектом: *file_name***» перейти в раздел «Дискреционный доступ». Задать набор разрешений, который будет определять права к данному объекту, можно с помощью команд панели действий «**Свойства**» для «**Пользователи**», «**Группы**» или «**Остальные**».

Панель действий «**Свойства**» позволяет определить права доступа к объекту для учетной записи пользователя. При выборе команды открывается форма, в которой из выпадающего списка необходимо выбрать наименование учетной записи. После добавления в общий список для данной учетной записи необходимо назначить набор прав (установка флага в поле соответствующего разрешения) (см. Рисунок 54).

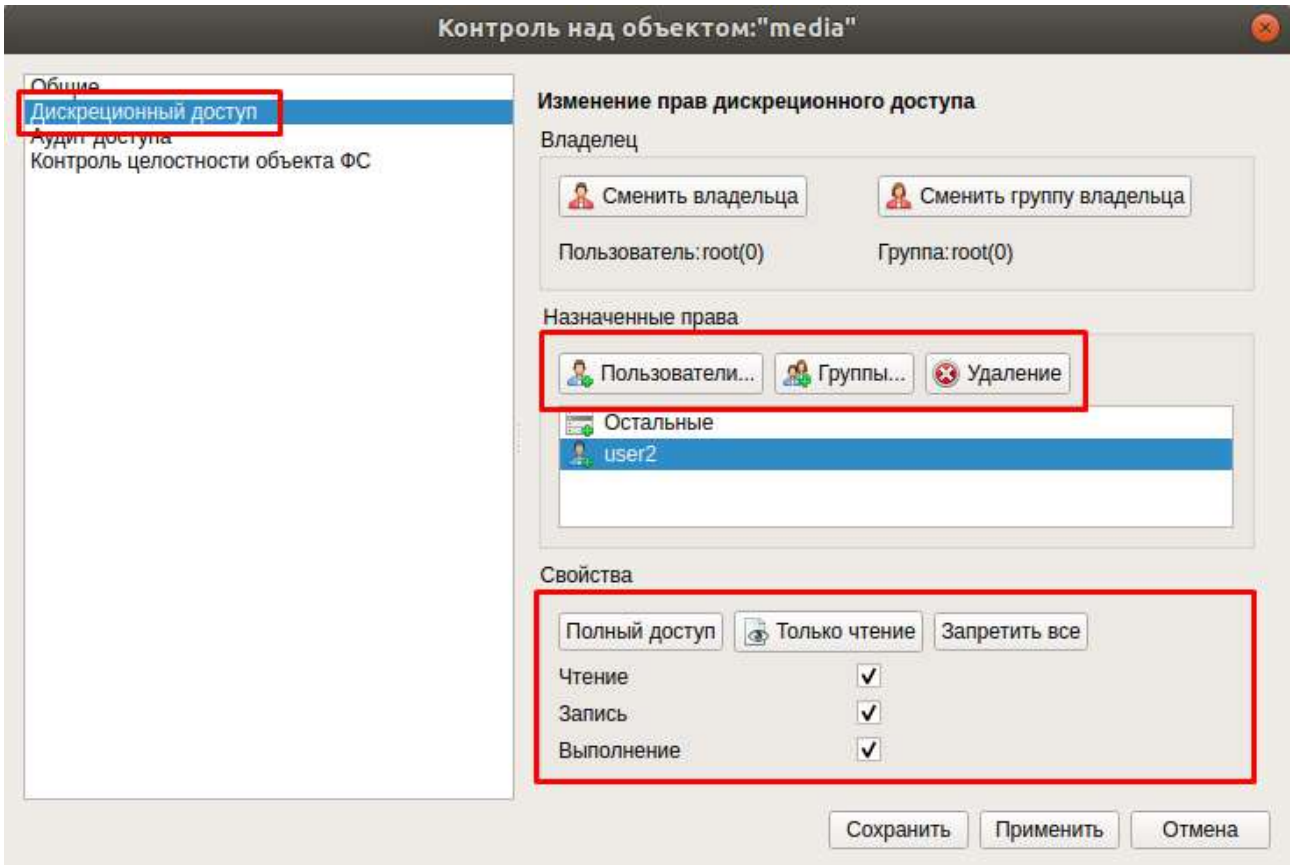


Рисунок 54. Создание нового пользовательского правила

Команда «Группы» позволяет определить права доступа к объекту для группы учетных записей пользователей. При выборе команды открывается форма, в которой из ниспадающего меню необходимо выбрать наименование группы. После добавления в общий список, для данной группы необходимо назначить набор прав.

Команда «*Остальные*» позволяет определить права доступа к категории учетных записей «*Остальные*». По умолчанию в **СЗИ НСД** права доступа для «*Остальные*» назначены «*Чтение*» и «*Выполнение*».

Для объекта ФС можно назначить следующие типы разрешений:

- Чтение — право на чтение.
- Запись — право на запись.
- Выполнение — право на выполнение (только для файлов).

Следует обратить внимание, что разрешение «*Выполнение*» для директорий означает право вхождения в нее для субъектов доступа.

4. После установки разрешений их следует сохранить, нажав кнопку «**Сохранить**», далее — «**Применить**».

4.5.2 Смена владельца объекта файловой системы

Каждый объект файловой системы в ОС семейства Linux имеет владельца. Тот, кто создал этот объект, считается его владельцем.

Консольная оболочка администрирования

Для просмотра логина владельца объекта необходимо выполнить команду *get-owner*, указав полный путь к объекту ФС.

Пример:

resources <enter>

files <enter>

dsb <enter>

get-owner /home/user/test.odt <enter>

В результате успешного выполнения команды система выдаст сообщение, в котором будет указан логин учетной записи-владельца и наименование группы-владельца.

Для смены владельца объекта необходимо выполнить команду *set-owner*, далее указать в качестве атрибутов параметры, указанные в Таблица 31.

Таблица 31

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*user <значение>*	Логин учетной записи-владельца
3	*group <значение>*	Наименование группы владельца

Пример:

resources <enter>

files <enter>

dsb <enter>

set-owner <enter>

path /home/user/test.odt <enter>

user user <enter>

group user <enter>

execute <enter>

Графическая оболочка администрирования

Для смены владельца необходимо:

1. На панели действий выбрать команду «**Контроль над файлом**» (см. Рисунок 53).
2. В открывшемся окне перейти в раздел «Дискреционный доступ» (см. Рисунок 54).
3. В панели действий «**Владелец**» нажать на кнопку «**Сменить владельца**» (см. Рисунок 55)

Смена группы владельца выполняется аналогичным способом, что и смена владельца файла.

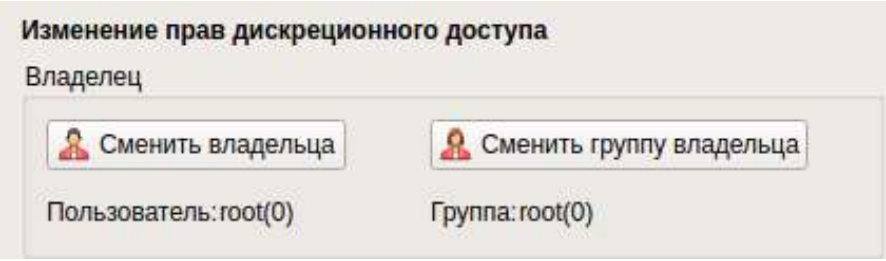


Рисунок 55. Команды «Сменить владельца»/«Сменить группу владельца»

4.5.3 Удаление прав/правил доступа для субъекта доступа

Консольная оболочка администрирования

Для удаления прав доступа учетной записи пользователя к выбранному объекту доступа в разделе управления доступом (*dsb*) необходимо выполнить команду *rm-rights-user* с указанием атрибутов, представленных в Таблица 32.

Таблица 32

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*login <значение>*	Логин учетной записи пользователя

Пример:

resources <enter>

files <enter>

dsb <enter>

rm-rights-user /home/user/test user <enter>

Для удаления прав доступа группы учетных записей к выбранному объекту доступа в разделе управления доступом (*dsb*) необходимо выполнить команду *rm-rights-group* с указанием атрибутов, представленных в Таблица 33.

Таблица 33

№	Атрибут	Описание
1	*path <значение>*	Путь к объекту файловой системы
2	*group <значение>*	Наименование группы учетных записей

Графическая оболочка администрирования

Удалить правила дискреционного доступа можно с помощью команды  «**Удаление**» (см. Рисунок 56).

По умолчанию с **СЗИ НСД** права доступа для «*Остальные*» назначены «*Чтение*» и «*Выполнение*», их можно только сменить, но не удалить.

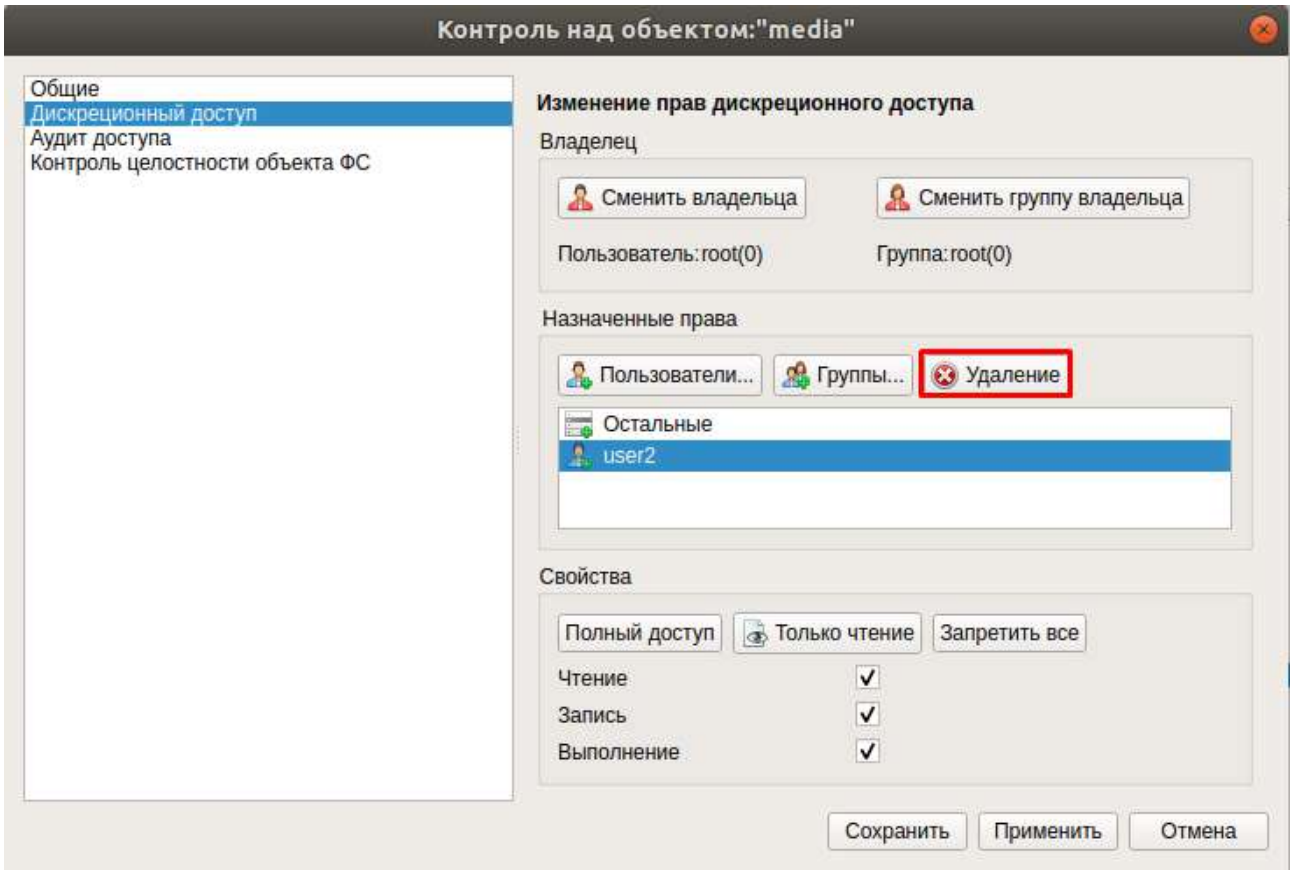


Рисунок 56. Удаление правила дискреционного доступа

4.6 Контроль устройств

Подсистема применяется для разграничения доступа пользователей и групп пользователей к блочным устройствам, ограничения доступа к беспроводным устройствам передачи информации, устройствам вывода на печать в целях предотвращения несанкционированной утечки информации с защищаемого ТС.

При первом подключении устройства к ТС устройство регистрируется в **СЗИ НСД** с назначенными правами доступа для категории учетных записей «Остальные», аналогичными правами доступа для данной категории пользователей для класса блочных устройств.

СЗИ НСД осуществляет контроль устройств после монтирования их ФС. Таким образом, если ФС подключенного устройства не смонтировалась, правила разграничения доступа действовать не будут. Также стоит отметить, что не все устройства могут автоматически монтироваться к системе в процессе ее функционирования. Поэтому необходимо проверить возможность автоматического монтирования устройств в процессе работы **СЗИ НСД**.

В том случае если ФС подключенного устройства не смонтировалась автоматически (такое возможно при работе без графической оболочки), пользователю необходимо будет смонтировать устройство вручную или обратиться к АИБ.

Количество правил, назначаемых на устройство ограничено:

- для пользовательских — не более 32 правил;
- для групповых — не более 32 правил;
- для категории «*Остальные*» — не более 1 правила.

4.6.1 Разграничение доступа к блочным устройствам

СЗИ НСД предоставляет возможность разграничения доступа к классу блочных устройств. Разграничение доступа возможно на уровне учетных записей, групп учетных записей, категории учетных записей «Остальные».

Разграничение доступа осуществляется на основе матрицы доступа, описывающей права доступа учетных записей пользователей и групп, к зарегистрированным в системе блочным устройствам.

Осуществляется разграничение доступа к следующим типам устройств:

- USB-накопители ;
- накопители на жестких дисках[23] ;
- другие устройства .

Контролируется доступ к следующим интерфейсам ввода (вывода):

- порты (USB, COM, LPT);
- контроллеры шины IEEE-1394.

Структура контролируемых устройств, типов устройств отображается в виде дерева. Контроль интерфейсов ввода (вывода) осуществляется в отдельной категории «Порты» вкладки «СКН» графической оболочки администрирования **СЗИ НСД**.

Разграничение доступа к устройствам, прописанным в файле */etc/fstab*, не производится. Рекомендуется обеспечить защиту данного файла с помощью механизмов **СЗИ НСД**.

LVM добавляет уровень абстракции при взаимодействии с физическими носителями LVM, поэтому контроль таких устройств осуществляется на логическом уровне, внутри файловой системы.

[23] Устройства, подключаемые посредством использования интерфейсов SATA, IDE, шины PCI Express.

В **СЗИ НСД** подключаемые блочные устройства отождествляются с точками монтирования — каталогами, в которые монтируются ФС устройства. Таким образом, маска прав доступа к устройству и значение атрибутов маски прав доступа аналогичны атрибутам прав доступа к каталогам и подкаталогам.

Если пользователь состоит в группе, которой запрещен доступ к устройствам, то запрет распространяется и на пользователя.
Если пользователь состоит в группе, которой разрешен доступ к устройствам, то пользователю так же будет разрешен доступ к устройствам.
Если пользователь входит в нескольких группах, то для каждой из таких групп с помощью логического умножения вычисляются эффективные права доступа к устройству:

Группа 1	Группа 2	Доступ
–	–	–
+	–	–
–	+	–
+	+	+

«+» — доступ разрешен
«–» — доступ запрещен

В случае если конкретному пользователю назначены явные разрешающие права — групповые права анализироваться не будут. В этом случае, разрешающее право будет иметь приоритет над запрещающим.

Если учетной записи не назначены индивидуальные права, и она не входит ни в одну из групп учетных записей, то для нее действуют параметры, установленные для категории «*Остальные*».

Процедура назначения прав для каждой из оболочек администрирования описана ниже, в подразделах консольная оболочка администрирования и графическая оболочка администрирования текущего раздела.

Отсутствие разрешения на чтение (параметр *r* в маске прав доступа) ведет к полному запрету доступа к устройству/типу устройств/классу блочных устройств.

Консольная оболочка администрирования

Для перехода к подсистеме контроля доступа к устройствам необходимо в консольной оболочке администрирования **СЗИ НСД** (*ishl*) в разделе *resources* выполнить команду *hardware.* После ввода команды система перейдет в раздел *hardware*. Далее консольное приложение будет ожидать ввода управляющих команд подсистемы, список команд приведен в Таблица 34.

Таблица 34

№	Команда	Описание
1	*show-devices*	Вывод списка подключенных устройств и устройств, для которых были определены правила разграничения доступа. **Пример:** *hardware <enter>* *show-devices <enter>* В результате выполнения команды будет выведена таблица с полями: – *device ID* — идентификатор устройства; – *name* — имя устройства; – *label* — метка устройства; – *status* — статус устройства.

№	Команда	Описание
2	*show-rules <значение>*	Вывод списка правил разграничения доступа, назначенных на устройство. В качестве параметра к команде необходимо указать имя устройства. **Пример:** вывести список правил для устройства с именем *sdb*. *hardware <enter>* *show-rules /dev/sdb <enter>* Если для устройства не были назначены правила разграничения доступа, система выдаст сообщение «*Warning! no rules for this device. Nothing to display» («Предупреждение! нет правил для этого устройства. Нечего показать»)*
3	*remove-device <значение>*	Команда удаляет устройство с назначенными правилами разграничения доступа и не подключенное в данный момент из списка устройств ТС. В качестве параметра к команде необходимо указать имя устройства. **Пример:** *hardware <enter>* *remove-device /dev/sdb <enter>*
4	*remove-user-rules*	Удаление правил разграничения доступа к устройству для пользователя. В качестве атрибутов необходимо указать следующие параметры: – *device* — идентификатор устройства; – *login* — логин учетной записи пользователя. **Пример:** *hardware <enter>* *remove-user-rules <enter>* *device /dev/sdb <enter>* *login user <enter>* *execute <enter>*
5	*remove-group-rules*	Удаление правил разграничения доступа к устройству для группы пользователей. В качестве атрибутов необходимо указать следующие параметры: – *device* — идентификатор устройства; – *group* — наименование группы пользователей. Синтаксис команды аналогичен синтаксису команды *remove-user-rules*
6	*set-user-rules*	Установка правил разграничения доступа к устройству для учетных записей. В качестве атрибутов необходимо указать следующие параметры: – *device* — идентификатор устройства; – *login* — логин учетной записи пользователя; – *rules* — матрица прав доступа, в формате «rwx». **Принимает значения:** строка в формате ‘rwx’, состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ “-”. – *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой.

№	Команда	Описание
		Пример: *hardware <enter>* *set-user-rules <enter>* *device /dev/sdb <enter>* *login user <enter>* *rules rwx <enter>* *execute <enter>*
7	*user-list*	Вывод списка учетных записей в разделе *hardware*
8	*set-group-rules*	Установка правил разграничения доступа к устройству для группы пользователей. В качестве атрибутов необходимо указать следующие параметры: – *device* — идентификатор устройства; – *group* — наименование группы пользователей; – *rules* — маска прав доступа, в формате «rwx». **Принимает значения:** строка в формате ‘rwx’, состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ “-”. – *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой. Синтаксис команды аналогичен синтаксису команды *set-user-rules*
9	*group-list*	Вывод списка групп пользователей в разделе *hardware*
10	*set-other-rules*	Установка правил разграничения доступа к устройству для учетных записей категории «Остальные» (пользователи, для которых не назначены индивидуальные права). В качестве атрибутов необходимо указать следующие параметры: – *device* — идентификатор устройства; – *rules* — маска прав доступа, в формате «rwx». **Принимает значения:** строка в формате ‘rwx’, состоящая из 3 буквенных символов, обозначающих права доступа. При отсутствии определенных прав, буквенное значение привилегии может быть заменено на символ “-”. – *r* — право на чтение; – *w* — право на запись; – *x* — право на выполнение (для файлов и каталогов); Порядок указания символов, обозначающих права доступа или их отсутствие, может быть любой. **Пример:** *hardware <enter>* *set-other-rules <enter>* *device /dev/sdb <enter>* *rules r <enter>* *execute <enter>*
11	*remove-other-rules*	Удаление правил разграничения доступа к устройству для учетных записей категории «Остальные» (пользователи, для которых не назначены индивидуальные права). В качестве атрибутов необходимо указать следующий параметр:

№	Команда	Описание
		– *device* — идентификатор устройства
12	*show-usb-ports*	Отображение всех портов (USB, COM, LPT), доступных для подключения устройств, в формате таблицы со столбцами *port* (наименование порта) и *status* (текущий статус порта)
13	*set-usb-port-status*	Блокировка/разблокировка порта для всех учетных записей пользователей. В качестве атрибутов необходимо указать следующие параметры: – *port* — наименование порта; – *status* — статус порта. **Принимает значение:** – *0* – заблокировать порт; – 1 – разблокировать порт. **Пример:** *hardware <enter>* *set-usb-port-status <enter>* *port <значение> <enter>* *status 0 <enter>* *execute <enter>*
14	*set-device-info*[24]	Описание сменного накопителя позволяет заменить установленным названием идентификатор накопителя для работы с накопителем в СЗИ. В качестве атрибутов необходимо указать следующие параметры: *device* — идентификатор устройства; *info* — описание для сменного накопителя. **Пример:** *hardware <enter>* *set-device-info <enter>* *device <значение> <enter>* *info <значение> <enter>* *execute <enter>*
15	*show-device-info*[24]	Отображение таблицы устройств с описаниями, установленными с помощью команды *set-device-info*

Графическая оболочка администрирования

Настройка параметров доступа осуществляется на вкладке «**Контроль ресурсов**» в категории «**Блочные устройства**».

Для назначения прав доступа на устройство/тип устройств необходимо выполнить следующие шаги:

1. В общем списке выделить идентификатор устройства/типа устройств/класса блочных устройств и на панели действий нажать на кнопку  «**Контроль над устройством**» (см. Рисунок 57).

[24] Команда доступна только при наличии соответствующей лицензии.

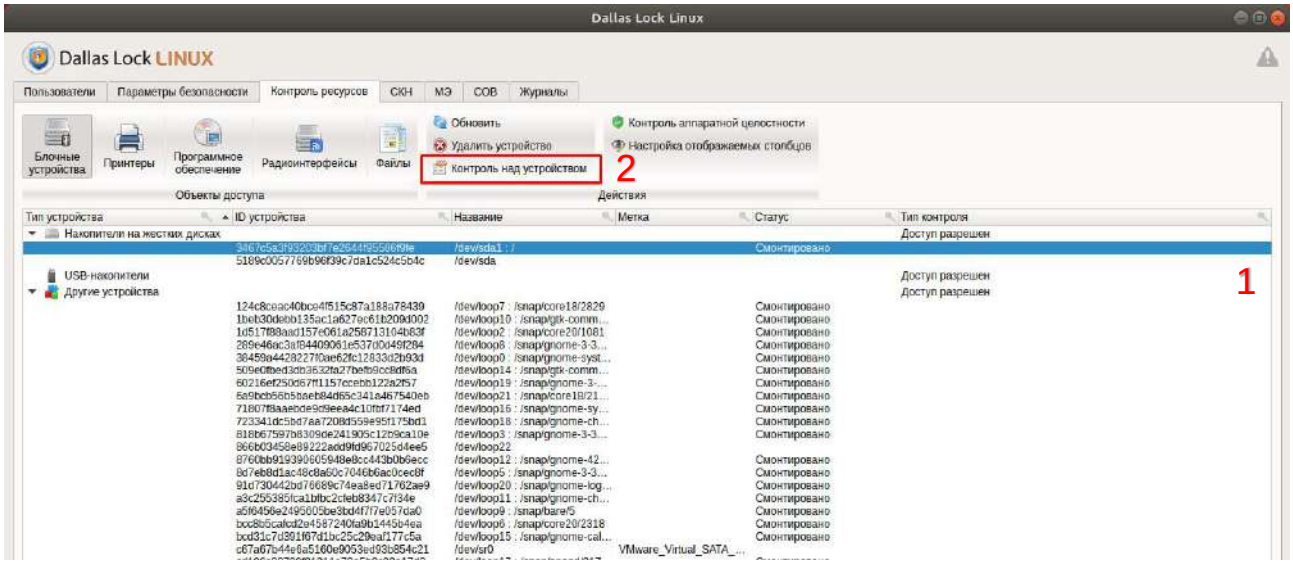


Рисунок 57. Выбор идентификатора устройства

2. Далее в открытом окне «Контроль над устройством: *file_name*» система автоматически перейдет в раздел «**Общие**». Здесь, на панели свойств, задается «Имя», «Полный путь», «Доступ» и чекбокс «Аудит». По умолчанию **СЗИ НСД** в разделе «Доступ» назначает в комбо-боксе «Не установлено». В выпадающем списке раздела «**Доступ**» выбрать «*Разрешен*».

> **!** Если на конкретное устройство не установлены права, то напротив устройства будет отображаться «Не установлен».

3. В открытом окне «Контроль над устройством: *file_name*» перейти в раздел «Аудит доступа». Здесь задается набор разрешений, который будет определять права к данному объекту.

На панели свойств назначается аудит к объекту. Для выбора нужного аудита необходимо назначить набор прав (установка флага в поле соответствующего разрешения) (см. Рисунок 58).

4. После назначения нужных флагов и настроек, требуется нажать на кнопку «**Применить**», затем «**Сохранить**».

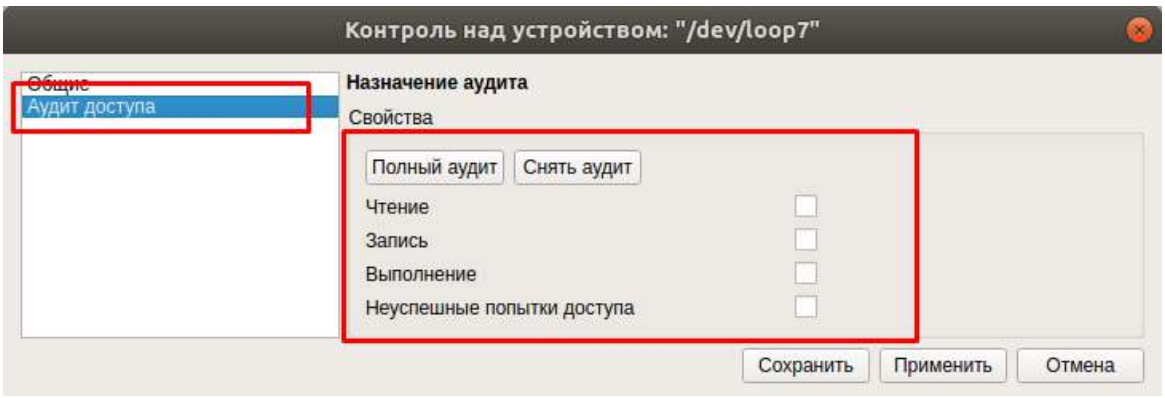


Рисунок 58. Создание нового правила для контроля

Команда  «**Удалить устройство**» позволяет удалить устройство из списка «Блочные устройства» для выбранного устройства. После удаления в левом нижнем углу графической консоли **СЗИ НСД** появится информационное сообщение «*Настройки устройства успешно изменены*» (см. Рисунок 59).

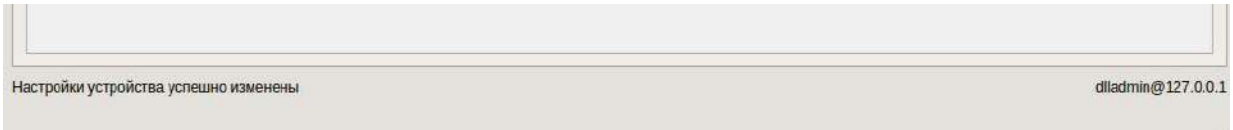


Рисунок 59. Информационное сообщение

Управление контролем интерфейсов ввода (вывода) в **СЗИ НСД Dallas Lock Linux** сводится к возможности блокировки или разблокировки устройства.

Управление контролем интерфейсов ввода (вывода) в **СЗИ НСД Dallas Lock Linux** осуществляется в категории «Порты» вкладки «**СКН**» графической оболочки администрирования (см. Рисунок 60). Для блокировки интерфейса ввода (вывода) необходимо выделить его в общем списке и на панели действий выбрать команду «**Блокировать**». Интерфейс ввода (вывода) будет заблокирован и в столбце «Статус» для него будет отображаться состояние «Заблокировано».

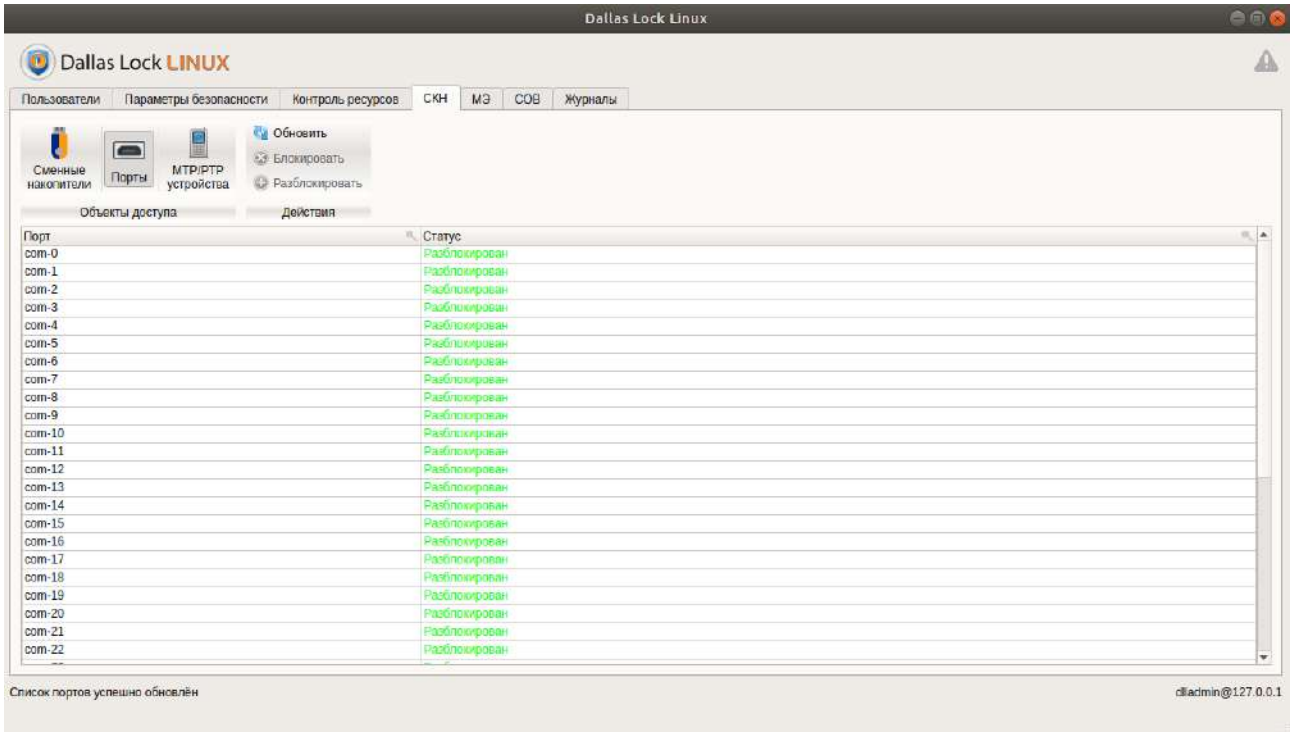


Рисунок 60. Категория «Порты» вкладки «СКН»

Для разблокировки интерфейса ввода (вывода) необходимо выделить в общем списке интерфейс ввода (вывода) и на панели действий выбрать команду «**Разблокировать**». Интерфейс ввода (вывода) будет разблокирован.

При наличии лицензии становится доступным раздел «**Сменные накопители**» вкладки «**СКН**» графической оболочки администрирования (см. Рисунок 61).

Рисунок 61. Категория «Сменные накопители» вкладки «СКН»

Для добавления (изменения) описания подключенного к АРМ устройства нужно нажать кнопку «Изменить описание», добавить необходимое описание, нажать кнопку «**Применить**» для сохранения или кнопку «**Отмена**» для отмены добавления описания (см. Рисунок 62).

Для удаления описания устройства из списка нужно нажать на кнопку «**Удалить описание**».

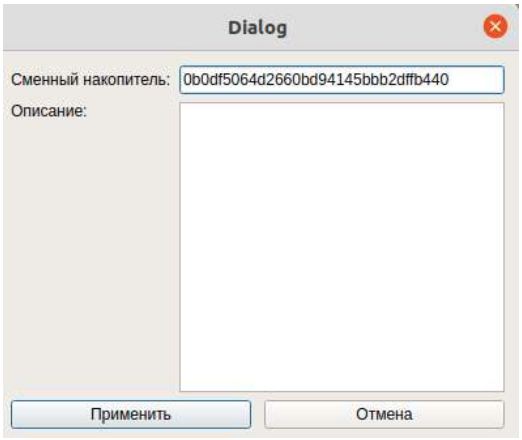


Рисунок 62. Добавление (изменение) описания сменного накопителя

Для удобства пользователя чтобы увидеть все устройства, для которых добавлены описания, необходимо отсортировать список устройств, нажав на столбец «Описание».

Наличие соответствующей лицензии обеспечивает возможность **СЗИ НСД** сигнализировать администратору информационной безопасности о событиях возможного нарушения безопасности, связанных с доступом к устройствам. Подробнее — в разделе Подсистема аудита устройств.

4.6.2 Разграничение доступа к печатающим устройствам

С помощью подсистемы разграничения доступа можно гибко настроить список учетных записей пользователей, для которых будет разрешен доступ к установленным в системе печатающим устройствам, и как следствие, ограничить возможность печати информации для таких учетных записей.

Принцип разграничения доступа к печатающим устройствам аналогичен принципу разграничения доступа к блочным устройствам (см. Разграничение доступа к блочным устройствам).

По умолчанию для принтеров, настроенных в ОС до установки **СЗИ НСД**, отсутствует разрешение на доступ.

Консольная оболочка администрирования

Для управления доступом к принтерам в консольной оболочке администрирования (*ishl*) в разделе *resources* необходимо выполнить команду *printers*. После выполнения команды система перейдет в раздел *printers*.

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 35.

Таблица 35

№	Команда	Описание
1	*show-printers*	Вывод списка доступных принтеров. В результате выполнения команды отображается список “*Printer List*”, состоящий из 2-х колонок: – *model* — модель принтера; – *driver* — имя принтера. **Пример:** *resources <enter>* *printers <enter>* *show-printers <enter>*

№	Команда	Описание
2	*show-printer-rules <значение>*	Отображение списка правил, назначенных на принтер, производится при помощи управляющей команды с указанием в качестве атрибута наименования принтера. **Пример:** *resources <enter>* *printers <enter>* *show-printer-rules laser <enter>* В результате выполнения команды отображается список *“Printer rules”,* состоящий из 3-х колонок: – *subject type* — тип субъекта доступа; – *subject name* — имя субъекта доступа; – *value* — право доступа, принимает значения: *yes* — печать разрешена, *no* — печать запрещена
3	*set-user-printer-rules*	Установка правил разграничения доступа на принтер для учетной записи пользователя. В качестве атрибутов необходимо указать следующие параметры: – *printer* — наименование принтера; – *login* — учетная запись пользователя; – *access* — право доступа, принимает значения: *yes* — печать разрешена, *no* — печать запрещена. **Пример:** *resources <enter>* *printers <enter>* *set-user-printer-rules <enter>* *printer laser <enter>* *login user <enter>* *access yes <enter>* *execute <enter>*
4	*set-group-printer-rules*	Установка правил разграничения доступа на принтер для группы пользователей. В качестве атрибутов необходимо указать следующие параметры: – *printer* — наименование принтера; – *group* — наименование группы пользователей; – *access* — право доступа, принимает значения: *yes* — печать разрешена, *no* — печать запрещена. **Пример:** *resources <enter>* *printers <enter>* *set-group-printer-rules <enter>* *printer laser <enter>* *group user <enter>* *access yes <enter>* *execute <enter>*
5	*remove-user-printer-rules*	Удаление правил разграничения доступа на принтер для учетной записи пользователя. В качестве атрибутов необходимо указать следующие параметры: – *printer* — наименование принтера; – *login* — учетная запись пользователя. **Пример:**

№	Команда	Описание
		resources <enter> *printers <enter>* *remove-user-printer-rules <enter>* *printer laser <enter>* *login user <enter>* *execute <enter>*
6	*remove-group-printer-rules*	Удаление правил разграничения доступа на принтер для группы пользователей. В качестве атрибутов необходимо указать следующие параметры: – *printer* — наименование принтера; – *group* — учетная запись пользователя. **Пример:** *resources <enter>* *printers <enter>* *remove-group-printer-rules <enter>* *printer laser <enter>* *group user <enter>* *execute <enter>*
7	*set-other-printer-rules*	Установка правил разграничения доступа на принтер для категории учетных записей «Остальные» (пользователи, для которых не назначены индивидуальные права). В качестве атрибутов необходимо указать следующие параметры: – *printer* — наименование принтера; – *access* — право доступа, принимает значения: *yes* — печать разрешена, *no* — печать запрещена. **Пример:** *resources <enter>* *printers <enter>* *set-other-printer-rules <enter>* *printer laser <enter>* *access no <enter>* *execute <enter>*

Графическая оболочка администрирования

Настройка прав доступа выполняется на вкладке «**Контроль ресурсов**» в категории «Принтеры» (см. Рисунок 63).

В категории «Принтеры» в списке устройств будут отображаться все подключенные к данному ТС печатающие устройства, «Права доступа» — список субъектов доступа (учетная запись пользователя, группа учетных записей) с назначенными правами отображаются в окне настройки «**Контроль над принтером**».

Рисунок 63. Категория «Принтеры» вкладки «Контроль ресурсов»

Принцип выбора учетной записи пользователя/группы учетных записей аналогичен процедуре, описанной для блочных устройств. Для выбора субъекта доступа необходимо выполнить шаги 1–5 подраздела Графическая оболочка администрирования раздела Разграничение доступа к блочным устройствам.

После выбора соответствующего субъекта доступа устанавливаются права на возможность выполнения печати с данного принтера. Если флаг «Печать» установлен, то для субъекта доступа разрешено выполнение печати, если флаг не установлен, то пользователю/группе запрещается выполнение печати.

При печати в файл не фиксируются соответствующие события о распечатывании документа.

4.6.3 Разграничение доступа к мобильным устройствам

Сотовые телефоны в зависимости от комплектации самого устройства могут определяться как беспроводное устройство, как USB-Flash-накопитель или как устройство, работающее по протоколу MTP/PTP.

Управление MTP/PTP-устройствами в **СЗИ НСД Dallas Lock Linux** сводится к возможности блокировки или разблокировки устройства.

Установленный в ходе работы по протоколу запрет подключения MTP/PTP-устройств сработает только при повторном подключении устройства.

Установленное разрешение подключения MTP/PTP-устройств сработает только при повторном подключении устройства.

Консольная оболочка администрирования

Для запрета подключения устройств по протоколу MTP/PTP в консольной оболочке администрирования **СЗИ НСД** (*ishl*) в разделе *resources* необходимо выполнить команду *hardware.* После ввода команды система перейдет в раздел *hardware*. Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 36.

Таблица 36

№	Команда	Описание
1	*show-mtp-ptp-state*	Показать состояние доступа устройств по протоколу MTP/PTP. Если доступ «Разрешен» — система выдаст сообщение «*Access is allowed*» («Доступ разрешен»). Если доступ «Запрещен» — система выдаст сообщение «*Access is denied*» («Доступ запрещен»)
2	*set-mtp-ptp-state*	Установка правил разграничения доступа на подключение устройств по протоколу MTP/PTP. В качестве атрибутов необходимо указать следующие параметры: *off* — доступ запрещен; *on* — доступ разрешен

Графическая оболочка администрирования

MTP/PTP-устройства вынесены в отдельную категорию «MTP/PTP-устройства» вкладки «СКН» графической оболочки администрирования **СЗИ НСД** (см. Рисунок 64).

Для того чтобы запретить работу с устройствами, работающими по протоколу MTP/PTP, необходимо перейти в категорию «MTP/PTP-устройства» вкладки «СКН» и в выпадающем списке выбрать значение «Отключить». Далее нужно нажать кнопку «**Сохранить**» в панели действий.

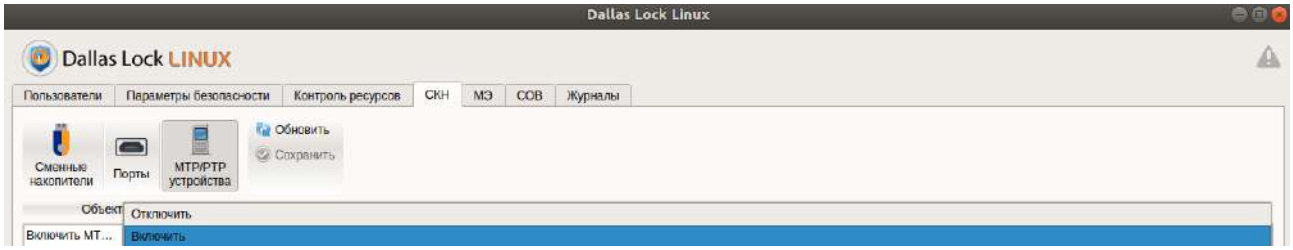


Рисунок 64. Категория «MTP/PTP-устройства» вкладки «СКН»

4.6.4 Управление беспроводными устройствами

Консольная оболочка администрирования

Для перехода к подсистеме контроля доступа к беспроводным устройствам необходимо в консольной оболочке администрирования (*ishl*) в разделе *resources* выполнить команду *radio-interfaces.*

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 37.

Таблица 37

№	Команда	Описание
1	*show-status*	Отображение информации о состоянии беспроводных устройств. В результате выполнения команды, отображается список устройств, состоящий из 4-х колонок: – *index* — идентификатор устройства; – *name* — имя сетевого интерфейса устройства; – *type* — тип устройства; – *status* — состояние. **Пример:** *resources <enter>* *radio-interfaces <enter>* *show-status <enter>*
2	*block*	Заблокировать все беспроводные устройства. **Пример:** *resources <enter>* *radio-interfaces <enter>* *block <enter>* В результате выполнения команды система выдаст сообщение *“RIF blocked successfully”* (“*Радиоинтерфейсы заблокированы успешно*”)
3	*unblock*	Разблокировать все беспроводные устройства. **Пример:** *resources <enter>* *radio-interfaces <enter>* *unblock <enter>* В результате выполнения команды система выдаст сообщение *“RIF unblocked successfully”* (“*Радиоинтерфейсы разблокированы успешно*”)

Графическая оболочка администрирования

Просмотреть список беспроводных устройств можно на вкладке «**Контроль ресурсов**» в категории «**Радиоинтерфейсы**».

В рабочей области категории «**Радиоинтерфейсы**» регистрируются беспроводные устройства, распознаваемые данным ТС (см. Рисунок 65). Список устройств выводится в виде таблицы со следующими полями:

- «Идентификатор» — идентификатор устройства;
- «Интерфейс» — имя сетевого интерфейса устройства;
- «Тип» — тип устройства;
- «Статус» — состояние устройства.

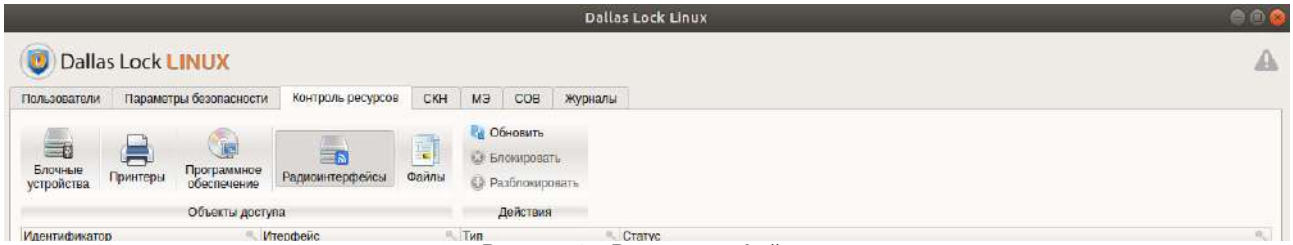


Рисунок 65. Радиоинтерфейсы

Управление беспроводными устройствами в **СЗИ НСД Dallas Lock Linux** сводится к возможности блокировки или разблокировки устройства.

Для блокировки устройства необходимо выделить в общем списке устройство и на панели действий выбрать команду «**Блокировать**». Устройство будет заблокировано и в столбце «Статус» для него будет отображаться состояние «Заблокировано». В левом нижнем углу графической оболочки появится информационное сообщение «*Радиоинтерфейсы были успешно заблокированы*».

Для разблокировки устройства необходимо выделить в общем списке устройство и на панели действий выбрать команду «**Разблокировать**». Устройство будет разблокировано и в левом нижнем углу появится информационное сообщение «*Радиоинтерфейсы были успешно разблокированы*».

4.7 Контроль целостности

СЗИ НСД Dallas Lock Linux включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность аппаратной среды ТС, целостность объектов файловой системы[25] и целостность программных компонентов **СЗИ**, а также восстанавливать целостность для программных компонентов средства защиты информации.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы, рассчитанные по алгоритму SHA1.

Факт нарушения целостности для каждого объекта фиксируется индивидуально. Объект признается целостным, когда фиксируемый параметр контрольной суммы соответствует значениям из базы данных контроля целостности.

4.7.1 Контроль целостности объектов файловой системы

Консольная оболочка администрирования

Для перехода к подсистеме контроля целостности объектов ФС необходимо в консольной оболочке администрирования (*ishl*) в разделе *resources* перейти в подраздел *files*, и выполнить команду *integrity*.

СЗИ НСД осуществляет периодическую проверку целостности объектов файловой системы — один раз в пять минут.

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 38.

[25] **СЗИ НСД Dallas Lock Linux** не контролирует целостность объектов файловых систем съемных накопителей.

Таблица 38

№	Команда	Описание
1	*show-all*	Вывод списка объектов ФС с установленным контролем целостности. **Пример:** *resources <enter>* *files <enter>* *integrity <enter>* *show-all <enter>*
2	*calc-file <значение>*	Команда подсчета контрольной суммы файла. При вводе команды указывается путь к объекту ФС в двойных кавычках. **Пример:** *resources <enter>* *files <enter>* *Integrity <enter>* *calc-file "/home/user/Текстовый документ.odt" <enter>* В результате выполнения команды будет отображена таблица с контрольной и эталонной суммой объекта
3	*lockup-file*	Команда установки контроля целостности для объекта ФС. При вводе команды необходимо задать атрибуты: – *path <значение>* — путь к объекту ФС (в двойных кавычках); – *backup <значение>* — флаг создания резервной копии объекта ФС, на который устанавливается контроль целостности. **Принимает значение:** *yes/no.* **Пример:** *resources <enter>* *files <enter>* *integrity <enter>* *lockup-file <enter>* *path "/home/user/Текстовый документ.odt" <enter>* *backup yes <enter>* *execute <enter>* В результате успешного выполнения команды системой будет выведено сообщение "*Success setting file under integrity control*"
4	*unlock-file <значение>*	Команда удаления объекта ФС из списка подконтрольных объектов. При вводе команды необходимо указать полный путь к объекту ФС в двойных кавычках. **Пример:** *resources <enter>* *files <enter>* *integrity <enter>* *unlock-file "/home/user/Текстовый документ.odt" <enter>* В результате успешного выполнения команды системой будет выведено сообщение "*Success removing file from integrity control*"
5	*restore-file <значение>*	Команда восстановления файла из резервной копии. При вводе команды необходимо указать полный путь к объекту ФС в двойных кавычках. **Пример:** *resources<enter>*

№	Команда	Описание
		files<enter> *integrity<enter>* *restore-file “/home/user/Текстовый документ.odt” <enter>* В результате успешного выполнения команды системой будет выведено сообщение “ *Success setting file under integrity control*”. ! Если на данный файл был назначен аудит (см. Подсистема аудита объектов файловой системы), то после восстановления из резервной копии по контролю целостности аудит будет снят автоматически
6	*verify-file <значение>*	Команда сверки контрольной суммы файла с эталонным значением. При вводе команды необходимо указать полный путь к объекту ФС в двойных кавычках. **Пример:** *resources <enter>* *files <enter>* *integrity <enter>* *verify-file “/home/user/Текстовый документ.odt” <enter>* Если значения контрольной и эталонной суммы совпадают, системой будет выведено сообщение “*File integrity is correct*”. Если значения контрольной и эталонной суммы не совпадают, системой будет выведено сообщение “*The result of the file verification---ERROR*”
7	*update-file*	Команда пересчета и установки новой контрольной суммы для объекта ФС. При вводе команды необходимо задать атрибуты: – *path <значение>* — путь к объекту ФС (в двойных кавычках); – *backup <значение>* — флаг создания резервной копии объекта ФС. **Принимает значения:** yes/no. **Пример:** *resources <enter>* *files <enter>* *integrity <enter>* *update-file <enter>* *path “/home/user/Текстовый документ.odt” <enter>* *backup yes <enter>* *execute <enter>* В результате успешного выполнения команды системой будет выведено сообщение “*Success: file integrity was updated*”

Графическая оболочка администрирования

Для назначения контроля целостности на объект ФС необходимо выполнить следующие шаги:

1. Выбрать вкладку «**Контроль ресурсов**» и перейти в раздел «**Файлы**».

2. В дереве объектов выбрать файл, на панели действий нажать кнопку «**Контроль над файлом**». Далее в открывшемся окне «**Контроль над объектом**» перейти в раздел «**Контроль целостности объекта ФС**» (см. Рисунок 66).

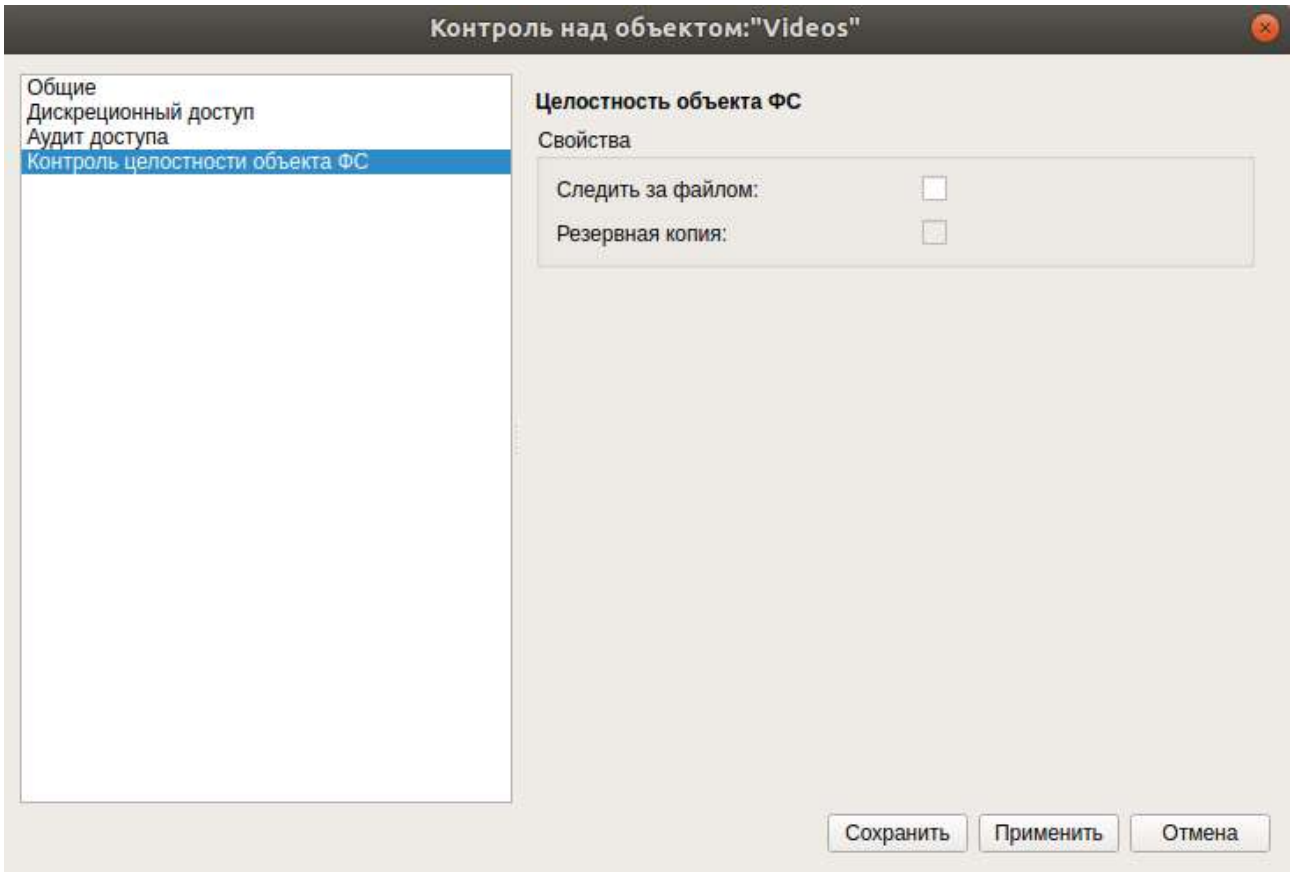


Рисунок 66. Раздел «Контроль целостности объекта ФС»

3. В разделе «**Контроль целостности объекта ФС**» на панели действий поставить флаг «Следить за файлом». Подтвердить (или отменить) создание копии объекта ФС в открывшемся диалоговом окне (см. Рисунок 67).

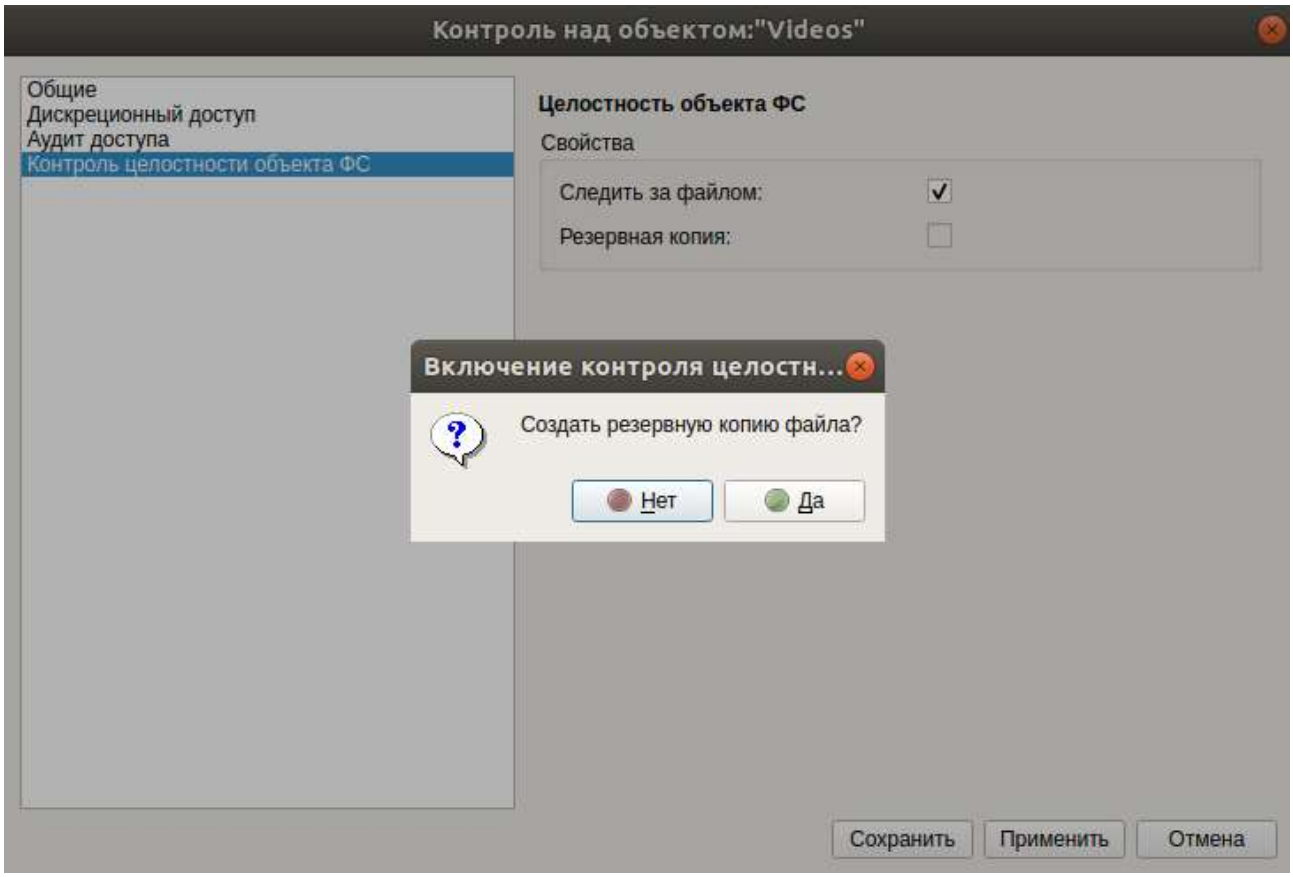


Рисунок 67. Назначение контроля целостности для объекта ФС

4. После подтверждения (или отмены) создания копии файл будет добавлен в общий список объектов ФС под контролем целостности в окне «**Контроль целостности файлов**». Общий список объектов, находящихся под контролем целостности, доступен по нажатию кнопки «Контроль целостности файлов» из основного окна графической оболочки администрирования в категории «Файлы» на вкладке «Контроль ресурсов». Система будет отслеживать целость объектов ФС, находящихся в данном списке.
В случае нарушения целостности и при условии формирования копии файла, система сможет его восстановить с помощью данной копии. Если копия не была сделана, то система будет только отслеживать целостность данного файла без возможности его восстановления. Информация о наличии копии указана в столбце «Копия» на вкладке «**Контроль целостности файлов**» (см. Рисунок 68).

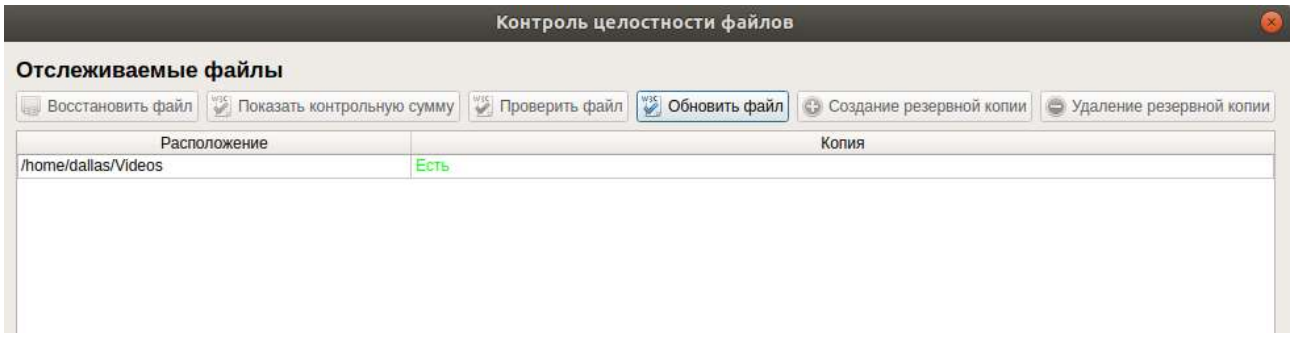


Рисунок 68. Информация о копии объекта ФС

Для проверки целостности объекта необходимо на панели инструментов нажать на кнопку «Контроль целостности файлов». На вкладке «**Контроль целостности файлов**» выделить контролируемый файл и нажать на кнопку «**Проверить файл**». В случае нарушения целостности система выдаст сообщение «*Целостность файла была нарушена*» (см. Рисунок 69).

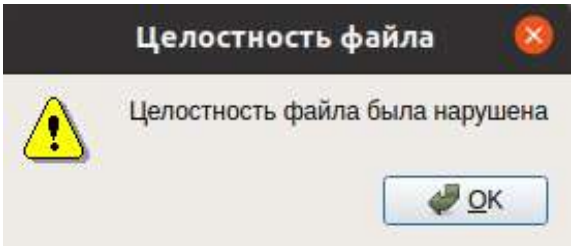


Рисунок 69. Информационное сообщение

Если целостность файла не нарушена, то при проверке система выдаст сообщение «*Целостность файла не была нарушена*» (см. Рисунок 70).

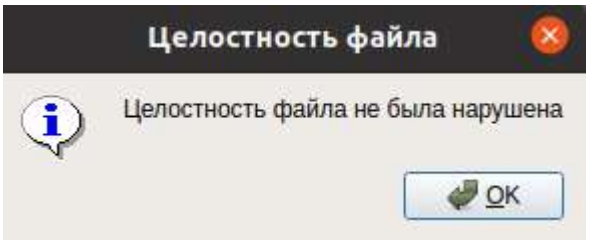


Рисунок 70. Информационное сообщение

В случае нарушения целостности можно либо обновить файл, если нарушение целостности было санкционированным, либо восстановить файл.

Для обновления файла необходимо на панели инструментов нажать на кнопку «**Обновить файл**» . Система выдаст запрос на формирование новой копии объекта.

Для восстановления объекта необходимо на панели инструментов нажать на кнопку «**Восстановить файл**» . Файл будет восстановлен в соответствие с его действующей копией.

Если на данный файл был назначен аудит, аудит будет снят автоматически.

Для просмотра текущего состояния (значения контрольных сумм, состояние целостности) контролируемого объекта необходимо на панели инструментов нажать на кнопку «**Показать контрольную сумму**» , после чего система выдаст информационное сообщение (см. Рисунок 71).

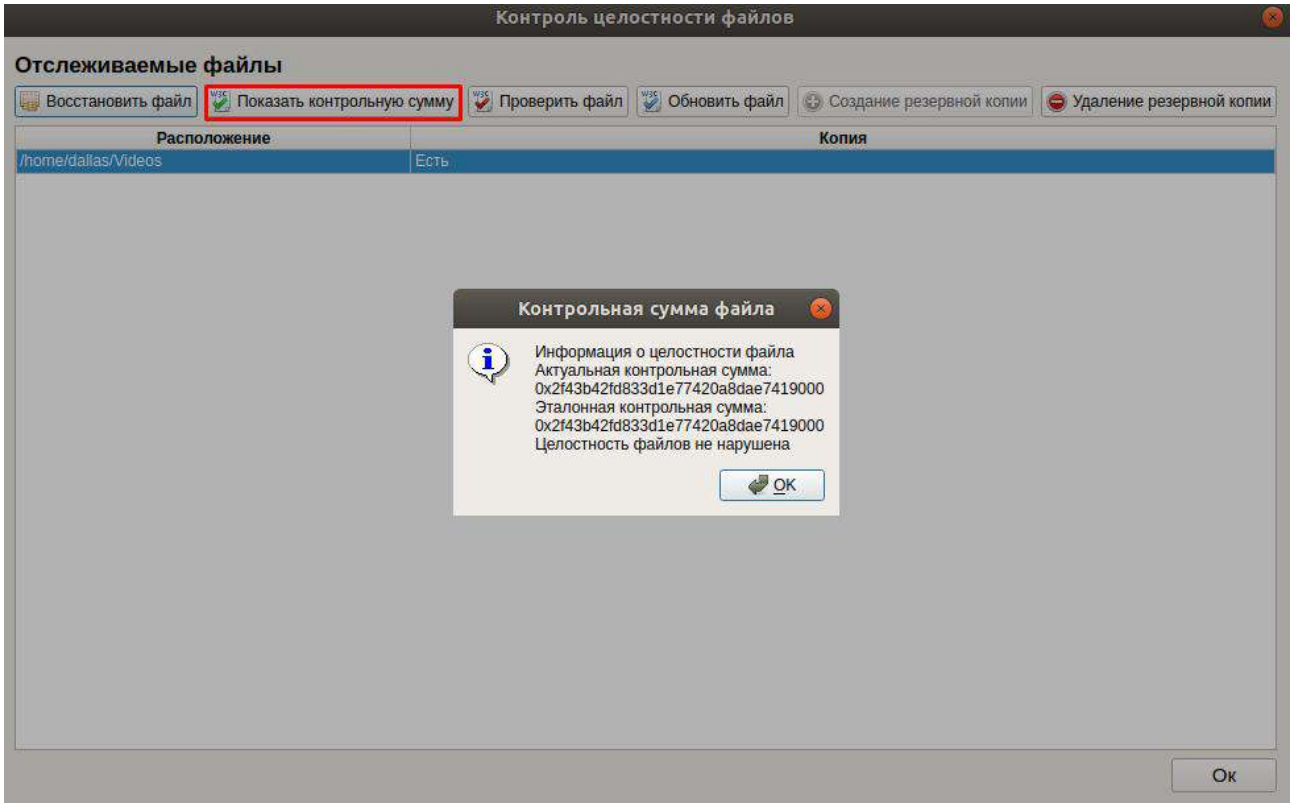


Рисунок 71. Информационное сообщение

Для отмены выполнения контроля целостности необходимо в окне «Контроль над объектом ФС» выбрать в левой части окна элемент списка «Контроль целостности объекта ФС» и снять флаг напротив «Следить за файлом» и сохранить данные изменения. После выполнения этих действий данные объекта ФС будут удалены из общей таблицы «Контроль целостности файлов».

4.7.2 Контроль целостности аппаратной среды

Консольная оболочка администрирования

Для перехода к подсистеме контроля целостности аппаратной среды необходимо в консольной оболочке администрирования (*ishl*) в разделе *resources* перейти в подраздел *hardware* и выполнить команду *integrity.*

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 39.

Таблица 39

№	Команда	Описание
1	*check-integrity*	Команда проверки целостности аппаратной среды. После выполнения команды будут выведены сообщения о состоянии аппаратной целостности. Если эталонная сумма не посчитана, будет выведено предупреждение. **Пример:** *resources <enter>*

		hardware <enter> *integrity <enter>* *check-integrity <enter>*
2	*recalculate-checksum*	Команда вычисления/пересчета контрольной суммы. **Пример:** *resources <enter>* *hardware <enter>* *integrity <enter>* *recalculate-checksum <enter>*
3	*get-checksum*	Команда проверки контрольной суммы. **Пример:** *resources <enter>* *hardware <enter>* *integrity <enter>* *get-checksum <enter>* В результате успешного выполнения команды системой будет выведено сообщение *“Integrity is not broken”*

Следует обратить внимание, что сразу после установки **СЗИ НСД** контрольная сумма аппаратной среды отсутствует и ее необходимо вычислить командой *recalculate-checksum*.

Графическая оболочка администрирования

С помощью политик контроля целостности на вкладке «**Параметры безопасности**» → «**Политики контроля целостности**» устанавливаются параметры контроля целостности, см. Настройка политик безопасности.

Для настройки контроля целостности аппаратной среды необходимо выполнить следующие шаги:

1. В графической оболочке **СЗИ НСД** перейти на вкладку «**Контроль ресурсов**» → «**Устройства**».
2. В списке объектов выделить строку с идентификатором объекта.
3. Нажать на кнопку  «**Контроль аппаратной целостности**».

Далее в окне «Контроль аппаратной целостности» отобразятся значения актуальной и контрольной суммы и статус проверки целостности (см. Рисунок 72).

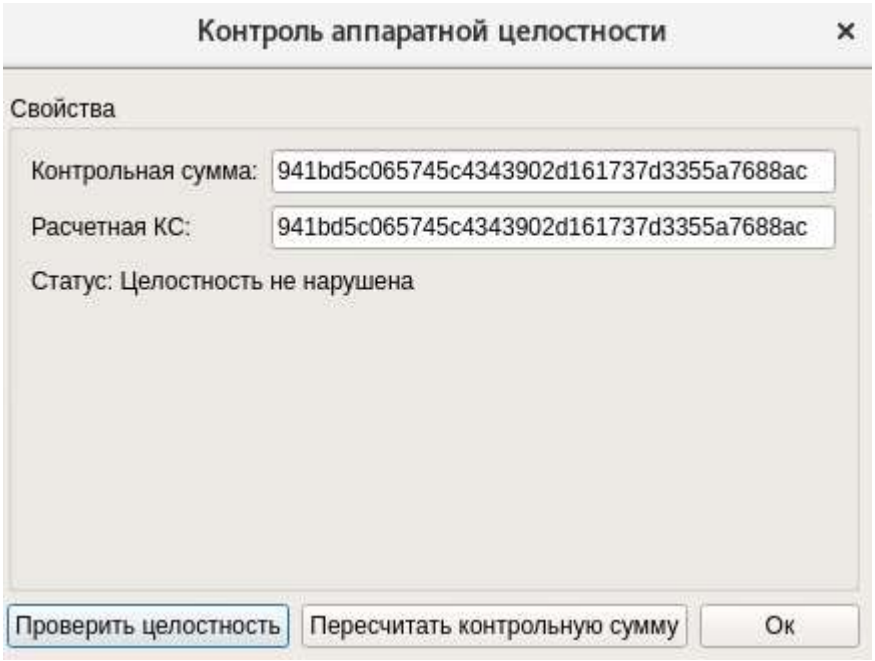


Рисунок 72. Настройка контроля целостности

После установки **СЗИ НСД Dallas Lock Linux** эталонная сумма для устройств аппаратной среды отсутствует, ее необходимо вычислить. Для этого в окне «Контроль аппаратной целостности» необходимо нажать на кнопку «**Пересчитать контрольную сумму**». После нажатия эталонная сумма будет рассчитана.

Если значение актуальной и эталонной суммы не совпадают, то статус проверки будет «Целостность нарушена».

Если вычислена эталонная сумма, включена проверка аппаратной целостности во время загрузки и была нарушена аппаратная целостность, то последует запрет авторизации в системе (для всех кроме *root*) (см. Рисунок 73). В таком случае администратору безопасности необходимо восстановить целостность или подключиться к ТС удаленно при помощи консольной оболочки либо графической оболочки администрирования **СЗИ НСД** и пересчитать контрольную сумму, так как при загрузке ОС с нарушенной аппаратной целостностью она доступна только удаленно (через **СБ Dallas Lock** либо оболочку администрирования).

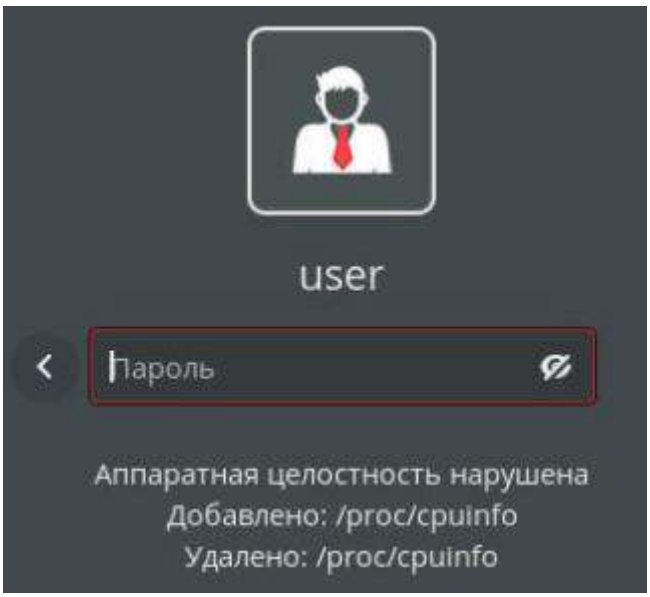


Рисунок 73. Запрет авторизации в системе

Если значения актуальной и контрольной суммы совпадают, то статус проверки будет «Целостность не нарушена».

4.7.3 Контроль целостности программных компонентов СЗИ НСД

Постановка компонентов **СЗИ НСД** на контроль и сам контроль осуществляются автоматически без участия администратора **СЗИ НСД**. При этом вся настройка механизма контроля целостности программных компонентов **СЗИ НСД** выполняется в процессе установки **СЗИ НСД** на ТС.

Консольная оболочка администрирования

Для перехода к подсистеме контроля целостности программных компонентов **СЗИ НСД** необходимо в консольной оболочке администрирования (*ishl*) перейти в раздел *resources*. В разделе *resources* выполнить команду *software*.

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 40.

Таблица 40

№	Команда	Описание
1	*show-szi-files*	Команда выводит список программных компонентов **СЗИ НСД**. В результате выполнения команды будет выведена таблица с полями: – *location* – путь программного компонента **СЗИ НСД**;

		– *backup* – флаг создания резервной копии программного компонента **СЗИ НСД**
2	*check-szi-integrity*	Принудительная проверка целостности программных компонентов **СЗИ**. В результате проверки система выдаст сообщение, что целостность программных компонентов **СЗИ** не нарушена/нарушена. **Пример:** *resources <enter>* *software <enter>* *check-szi-integrity <enter>*
3	*lock-szi-files*	Команда включает контроль целостности программных компонентов **СЗИ НСД**
4	*unlock-szi-files <all/szi>*	Выключить контроль целостности файлов **СЗИ НСД**. **Принимает значения:** *all* и *szi* — все файлы **СЗИ НСД**

В случае загрузки ОС в режиме «Emergency mode» необходимо запустить программу проверки и восстановления целостности СЗИ /usr/sbin/int-check.

Графическая оболочка администрирования

Если для программных компонентов **СЗИ НСД Dallas Lock Linux** будет нарушена целостность, то на вкладке «**Контроль ресурсов**» в категории «**Программное обеспечение**» в рабочей области будет выведен список компонентов с нарушенной целостностью (см. Рисунок 74).

Рисунок 74. Список компонентов с нарушенной целостностью

4.8 Гарантированная очистка остаточной информации

Большинство операционных систем при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории файловой системы (так сделано для ускорения работы системы).

Реальное содержимое файла остается на запоминающем устройстве и его можно просмотреть до тех пор, пока операционная система заново не использует это пространство для хранения новых данных. Такая остаточная информация может привести к непреднамеренному распространению конфиденциальной информации.

СЗИ НСД включает подсистему гарантированной очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Консольная оболочка администрирования

Для гарантированной очистки остаточной информации освобождаемых областей памяти внешних накопителей и объектов ФС с помощью консольной оболочки администрирования СЗИ НСД необходимо в *ishl* перейти в раздел *resources*, далее перейти в раздел *files* и выполнить команду *erase-file.* После выполнения команды система перейдет в раздел *erase-file.*

Далее в оболочку администрирования следует ввести атрибуты данной команды, список атрибутов представлен в Таблица 41.

Таблица 41

№	Атрибут	Описание

1	*path <значение>*	Путь к объекту файловой системы
2	*passed <значение>*	Количество циклов перезаписи. Параметр может принимать значения от 1 до 75

Пример:

resources <enter>
files <enter>
erase-file <enter>
path /home/user/test.odt <enter>
passed 10 <enter>
execute <enter>

Графическая оболочка администрирования

Для гарантированной очистки остаточной информации освобождаемых областей памяти внешних накопителей и объектов ФС в графической оболочке администрирования необходимо:

1. Перейти на вкладку «Контроль ресурсов» в раздел «**Файлы**».
2. В дереве объектов выбрать файл и открыть вкладку «**Удалить файл**».
3. Далее в открытом окне «**Удаление файла**» указать количество циклов перезаписи в поле «Количество циклов перезаписи» и нажать кнопку «**Удалить**» (см. Рисунок 75). Параметр «**Количество циклов перезаписи**» может принимать значения от 1 до 75.

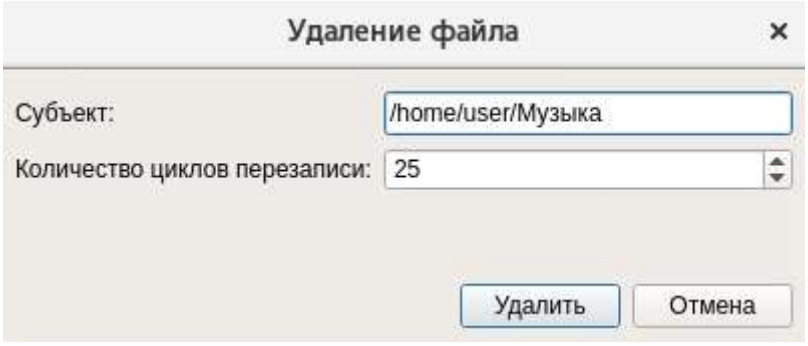


Рисунок 75. Удаление объекта ФС

4.9 Регистрация и учет событий

Подсистема регистрации и учета **СЗИ НСД Dallas Lock Linux** реализует возможность аудита событий, производимых пользователями над защищаемыми объектами, аудита событий входов (выходов) в информационную систему, в т.ч. сетевых, аудита системных событий, отчуждения информации на накопители или твердую копию, а также фиксацию таких событий в журналах информационной безопасности.

Для перехода в подсистему регистрации и учета необходимо в консольной оболочке администрирования (*ishl*) выполнить команду *audit.* После выполнения команды система перейдет в раздел *audit.*

Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд представлен в Таблица 42.

Таблица 42

№	Команда	Описание
1	*get-journal*	Переход в подменю подсистемы журналирования, подробнее — в разделе Подсистема журналирования
2	*archivate*	Команда принудительного создания архивных копий журналов, подробнее — в разделе Ограничение объема журналов
3	*get-watch*	Команда для просмотра правил аудита объекта ФС, подробнее — в разделе Подсистема аудита объектов файловой системы

№	Команда	Описание
4	*get-watch-all*	Команда для просмотра списка объектов ФС, находящихся под аудитом, подробнее — в разделе Подсистема аудита объектов файловой системы
5	*set-watch*	Команда настройки аудита объектов ФС, подробнее — в разделе Подсистема аудита объектов файловой системы
6	*remove-watch*	Команда отмены аудита объектов ФС, подробнее — в разделе Подсистема аудита объектов файловой системы
7	*export-ods*	Команда экспорта журнала в формат ODS, подробнее — в разделе Экспорт журналов информационной безопасности
8	*export-pdf*	Команда экспорта журнала в формат PDF, подробнее — в разделе Экспорт журналов информационной безопасности
9	*export-xml*	Команда экспорта журнала в формат XML, подробнее — в разделе Экспорт журналов информационной безопасности

Настройка параметров аудита графической оболочки администрирования выполняется в политиках безопасности, см. Настройка политик безопасности.

4.9.1 Подсистема журналирования

Подсистема журналирования предназначена для регистрации событий в журналах информационной безопасности и предоставления администратору **СЗИ НСД** инструментальных средств для работы с такими журналами.

Важно заметить, если пароль суперпользователя (*root*) не был задан до установки **СЗИ НСД**, то в журналах регистрации событий в связи с блокировкой *root* со временем будет увеличиваться неограниченное количество записей об ошибках по любым действиям, которым в процессе обращения к системным вызовам требуются привилегии уровня «root».

Интервал времени между событием и внесением записи в журнал информационной безопасности составляет не менее 20 секунд.

Администратор безопасности может определить правила вывода информации о событиях, установив правила фильтрации для такого журнала.

Консольная оболочка администрирования

Для просмотра журналов регистрации событий необходимо в консольной оболочке администрирования (*ishl*) перейти в раздел *audit.* В разделе *audit* выполнить команду *get-journal*. После ввода команды система перейдет в раздел *get-journal.*

Для вывода информации из журналов на экран необходимо использовать следующую последовательность команд:

journal <имя журнала> <enter>

execute <enter>

В **СЗИ НСД Dallas Lock Linux** предусмотрены следующие параметры для просмотра журналов.

Таблица 43

№	Наименование журнала	Параметры
1	Общий журнал	*overall*
2	Журнал входов	*entries*
3	Журнал ресурсов	*resources*
4	Журнал доступа к устройствам	*devices*
5	Журнал управления пользователями и группами	*users*

6	Журнал печати	*printing*
7	Журнал управления политиками безопасности	*policies*
8	Журнал системных событий	*syslog*
9	Журнал событий безопасности МЭ	*fw-sec-events*
10	Журнал управления МЭ	*fw-management*
11	Журнал событий безопасности СОВ	hids-sec-events
12	Журнал управление СОВ	hids-management

1. Общий журнал *(overall)*. В журнале фиксируются события всех журналов, кроме событий системного журнала *(syslog).*
2. Журнал входов (*entries*) содержит события аутентификации пользователей в операционной системе.
3. Журнал ресурсов (*resources*) содержит события, связанные с настройками правил разграничения доступа и обращениями к защищаемым объектам доступа.
4. Журнал доступа к устройствам (*devices*) содержит события, связанные с настройками правил разграничения доступа и обращениями к подключаемым устройствам.
5. Журнал управления пользователями и группами (*users*) содержит события, связанные с настройками и созданием учетных записей пользователей, групп учетных записей.
6. Журнал печати (*printing*) содержит события печати, выполненные с печатающих устройств.
7. Журнал управления политиками безопасности (*policies*) содержит события изменения политик безопасности.
8. Журнал системных событий (*syslog*) содержит события системного журнала ОС.
9. Журнал событий безопасности МЭ (*fw-sec-events*) содержит события о действиях, предпринимаемых в ответ на возможные нарушения безопасности.
10.Журнал управления МЭ (*fw-management*) содержит события о модификации правил МЭ, данных МЭ, результатах управления профилями проверок МЭ, результатах самотестирования МЭ, модификации значений атрибутов безопасности, о действиях, предпринимаемых в ответ на возможные нарушения безопасности.
11.Журнал событий безопасности СОВ (*hids-sec-events)* содержит события сигнатур трафика, журнальных сигнатур, эвристик и адрес источника.
12. Журнал управление СОВ (*hids-management*) содержит события, связанные с изменениями СОВ.

Для определения правил вывода информации о событиях в журналах используется фильтр. При установке фильтрации для такого журнала необходимо использовать атрибуты, указанные в Таблица 44.

Таблица 44

№	Атрибуты	Описание
1	*event-type <значение>*	Наименование типа события **Принимает значения:** **Для журнала входов (Entries):** – *userLogin* — вход пользователя; – *userLogout* — выход пользователя; – *systemStartUp* — старт системы; – *systemShutDown* — завершение работы; – *selfTest* — самотестирование; – *journalArchived* — архивация журнала; – *sessionsExcess* — превышено количество разрешенных сессий; – *sessionStart* — запущенные сессии на ТС; – *timeChange* — изменение системного времени. **Для журнала доступа к ресурсам (Resources):** – *auditSet* — назначение аудита на объект ФС; – *auditRemove* — снятие аудита с объекта ФС;

№	Атрибуты	Описание
		– *sziFsRightsSet* — установка прав доступа к объектам ФС; – *sziFsRightsRemoved* — удаление прав доступа к объектам ФС; – *fileIntegrity* — внесение объекта ФС под контроль целостности; – *fileCalc* — расчет файловой целостности; – *hwIntegrityRecalc* — пересчет аппаратной целостности; – *objectMovedTo* — объект перемещен в <*файл размещения*>; – *UccSetTime* — синхронизация времени с ЕЦУ; – *fileRightsChanged* — изменение прав доступа к объекту ФС; – *hwIntegrityErr* — аппаратная целостность нарушена; – *fileRestored* — объект ФС восстановлен; – *fileIntegrityErr* — нарушена целостность объекта ФС; – *sziRestored* — компонент СЗИ восстановлен; – *sziIntegrityErr* — целостность СЗИ нарушена; – *writeFail* — нарушение целостности журнала; – *formatToken* — форматирование аппаратного идентификатора; – *changeTokenPin* — изменение PIN-кода для аппаратного идентификатора; – *unassignToken* — отключение аппаратного идентификатора; – *assignToken* — подключение аппаратного идентификатора; – *dirOpen* — открытие директории; – *fileAccess* — доступ к объекту ФС; – *sfileAccess* — доступ к специальному объекту ФС; – *fileRead* — чтение объекта ФС; – *sfileRead* — чтение специального объекта ФС; – *fileWrite* — запись объекта ФС; – *sfileWrite* — запись в специальный объект ФС; – *fileExecute* — выполнение объекта ФС; – *sfileExecute* — выполнение специального объекта ФС; – *fileOpen* — открытие объекта ФС; – *dirRead* — чтение директории; – *dirCreate* — создание директории; – *fileCreate* — создание объекта ФС; – *sfileCreate* — создание специального объекта ФС; – *dirRemoved* — удаление директории; – *fileRemoved* — удаление объекта ФС; – *sfileRemoved* — удаление специального объекта ФС; – *fileAttrChanged* — изменение атрибутов объекта ФС; – *objectMoved* — перемещение объекта ФС; – *linked* — создание жесткой ссылки. **Для журнала доступа к устройствам (Devices):**

№	Атрибуты	Описание
		– *deviceMount* — монтирование устройства; – *deviceUnmount* — размонтирование устройства; – *mtpDevAccess* — доступ к MTP/PTP-устройству; – *deviceAccess* — доступ к устройству после монтирования; – *deviceInfoChanged* — изменение описания устройства[26]; – *deviceRightsChanged* — изменение прав доступа к устройству; – *portStatusChange* — изменение состояния порта; – *deviceAuditSet* — установка аудита на устройство; – *deviceAuditRemove* — удаление аудита, назначенного на устройство; – *cupsJobCheck* — проверка прав доступа для печати; – *devicePlugIn* — подключение устройства через порт. **Для журнала управления пользователями (Users):** – *userCreate* — создание пользователя; – *userUpdate* — изменение пользователя; – *groupCreate* — создание группы; – *userAddToGroup* — добавление пользователя в группу; – *userRemoveFromGroup* — удаление пользователя из группы; – *userChangePassword* — изменение пароля пользователя; – *userLock* — блокировка пользователя; – *userUnlock* — разблокировка пользователя; – *groupRemove* — удаление группы; – *userRemove* — удаление пользователя; – *domainEnter* — ввод в домен; – *domainExit* — вывод из домена; – *domainUserRemove* — удаление учетной записи доменного пользователя. **Для журнала печати (printing):** – *cupsJobCreated* — старт печати; – *cupsJobCompleted* — завершение печати; – *cupsPrinterAdded* — добавление принтера; – *cupsPrinterDeleted* — удаление принтера. **Для журнала управления политиками (Policies):** – *setPolicy* — изменение политики; – *journalPolicyStatus* — запуск аудита; – *auditRead* — чтение журналов[27]; – *connectToUcc* — подключение к **ЕЦУ**; – *disconnectToUcc* — отключение от **ЕЦУ**; – *supportKeyChange* — изменение ключа технической поддержки; – *synchroUcc* — синхронизация с **ЕЦУ**; – *licenseChange* — изменение лицензии.

[26] Событие фиксируется при наличии соответствующей лицензии.

[27] Регистрируется событие для пользователей с ролью Администратор и Аудитор.

№	Атрибуты	Описание
		Для журнала системных событий (Syslog): – *syslog* — событие системного журнала; – *processKill* — прерывание процесса; – *processStart* — запуск процесса; – *processStop* — остановка процесса. **Для журнала событий безопасности МЭ (fw-sec-events):** – *firewallBlockAddress* — адрес заблокирован; – *firewallPassPacket* — пакет пропущен; – *firewallRejectPacket* — пакет отклонен. **Для журнала управление МЭ (fw-management):** – *firewallSetRule* — правило установлено; – *firewallTesting* — самотестирование МЭ; – *firewallChangeRule* — правило изменено; – *firewallRemoveRule* — правило удалено; – *firewallSetProfile* — профиль установлен; – *firewallChangeProfile* — профиль изменен; – *firewallRemoveProfile* — профиль удален; – *firewallSetBlacklistCmd* — установлен черный список приложений; – *firewallChangeBlacklistCmd* — изменен черный список приложений; – *firewallRemoveBlacklistCmd* — удален черный список приложений; – *firewallSetWhitelistCmd* — установлен белый список приложений; – *firewallChangeWhitelistCmd* — изменен белый список приложений; – *firewallRemoveWhitelistCmd* — удален белый список приложений; – *firewallChangeState* — изменено состояние МЭ; – *firewallKillConnection* — соединение разорвано; – *firewallPoliciesChange* — изменение политик безопасности; – *firewallUnblockAddress* — адрес разблокирован. **Для журнала событий безопасности СОВ (hids-sec-events):** – *hidsNetSign* — сработала сигнатура трафика; – *hidsSyslogSign* — сработала журнальная сигнатура; – *hidsScenario* — сработала эвристика; – *intrusionDetected* — обнаружено вторжение; – *hidsIpBlocked* — IP-адрес заблокирован; – *hidsIpUnblocked* — IP-адрес разблокирован. **Для журнала управление СОВ (hids-management):** – *hidsPoliciesChange* — изменение политики СОВ; – *enableNetSign* — включение сигнатуры трафика; – *disableNetSign* — выключение сигнатуры трафика; – *updateNetSign* — сигнатура трафика изменена; – *enableSyslogSign* — включение журнальной сигнатуры;

№	Атрибуты	Описание
		– *disabledSyslogSign* — выключение журнальной сигнатуры; – *updateSyslogSign* — журнальная сигнатура изменена; – *enableScenario* — включение эвристики; – *disabledScenario* — выключение эвристики; – *updateScenario* — эвристика изменена; – *importNetSign* — импорт сигнатур трафика; – *saveHidsProfile* — сохранение профиля СОВ; – *loadHidsProfile* — загрузка профиля СОВ.
2	*from-time <значение>*	Фильтр по времени появления события, указание нижней границы. **Принимает значения:** дата и время в формате дд-мм-гггг@чч:мм:сс
3	*till-time <значение>*	Фильтр по времени появления события, указание верхней границы. **Принимает значения:** дата и время в формате дд-мм-гггг@чч:мм:сс
4	*user-name <значение>*	Фильтр по наименованию учетной записи пользователя
5	*result <значение>*	Фильтр по результату выполнения события. **Принимает значения:** – *ok* — успешный результат; – *fail* — неуспешный
6	*object <значение>*	Фильтр по объекту доступа
7	*printer <значение>*	Фильтрация по имени принтера, на который выводится объект для печати[28]
8	*archive-path <значение>*	Путь к архивной копии журналов событий информационной безопасности

Пример последовательности команд для вывода данных журнала входов, с применением правил фильтрации:

audit <enter>

get-journal <enter>

journal entries <enter>

event-type userLogin <enter>

execute <enter>

Пример последовательности команд для вывода данных журнала «Управление СОВ»:

cli> audit <enter>

audit> get-journal <enter>

get-journal> journal hids-management <enter>

get-journal> execute <enter>

Графическая оболочка администрирования

В системе защиты **Dallas Lock Linux** регистрация и запись ведется в различных типах журналов. На вкладке «Аудит» выделено 8 категорий, соответствующих основным журналам:

1. Журнал «**Общие**». В журнале фиксируются события всех журналов, кроме событий системного журнала (syslog).

[28] Фильтрация по данному параметру применяется только к журналу печати (printing).

2. Журнал «**Входы**». В журнале фиксируются события аутентификации пользователей в операционной системе.

3. Журнал «**Учетные записи**». В журнале фиксируются события, связанные с созданием, редактированием, удалением учетных записей пользователей и групп пользователей.

4. Журнал «**Ресурсы**». В журнале фиксируются события, связанные с настройкой правил разграничения доступа и с обращением к защищаемым объектам доступа.

5. Журнал «**Печать**». В журнале фиксируются все события, связанные с распечаткой документов на печатающих устройствах.

6. Журнал «**Управление политиками**». В журнале фиксируются события по изменению политик безопасности.

7. Журнал «**События ОС**». В журнале фиксируются события системного журнала операционной системы (syslog).

8. Журнал «**Устройства**». В журнале фиксируются события, связанные с настройкой правил разграничения доступа и получением доступа к подключаемым устройствам.

9. Журнал «**События безопасности МЭ**». В журнале фиксируются события, связанные с действиями предпринимаемых в ответ нарушений безопасности (см. Рисунок 76).

10. Журнал «**Управление МЭ**». В журнале фиксируются события, связанные с модификацией, правил МЭ, данными МЭ, результатах управления профилями проверок МЭ, результатах самотестирования МЭ, модификации значений атрибутов безопасности, о действиях, предпринимаемых в ответ на возможные нарушения безопасности (см. Рисунок 76).

11. Журнал «**События безопасности СОВ**». В журнале фиксируются события сигнатур трафика, журнальных сигнатур, эвристик и адреса источников (см. Рисунок 77).

12. Журнал «**Управление СОВ**». В журнале фиксируются события, связанные с изменениями СОВ (см. Рисунок 77).

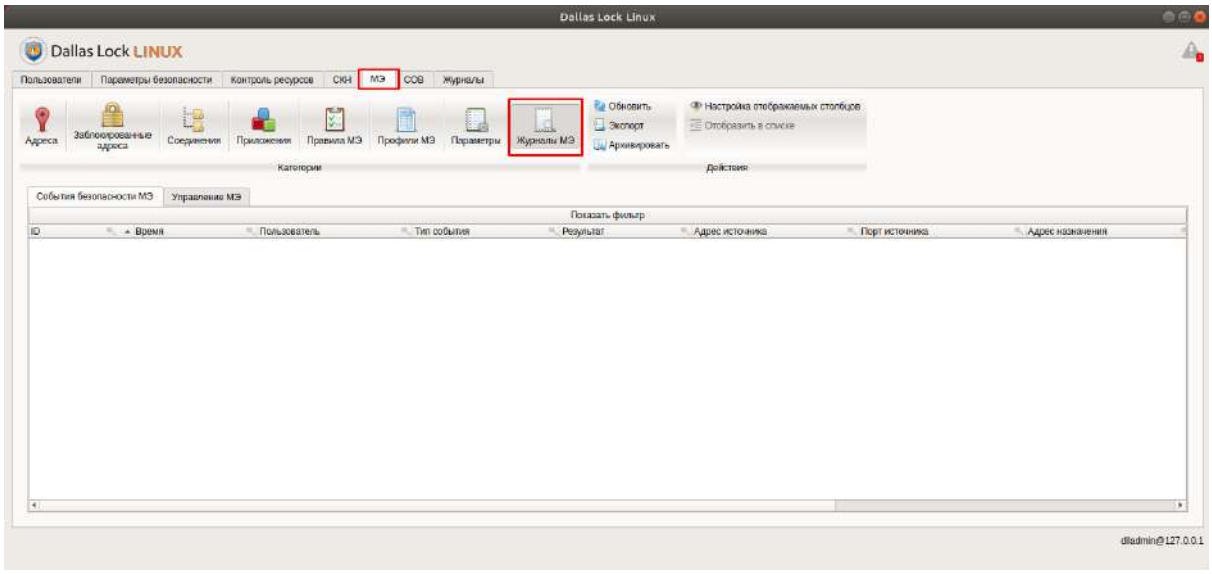


Рисунок 76. Расположение журналов МЭ

При переходе в категорию «**Журналы СОВ**» в графической оболочке администрирования **СЗИ НСД** по умолчанию отображен журнал «**События безопасности СОВ**» (см. Рисунок 77).

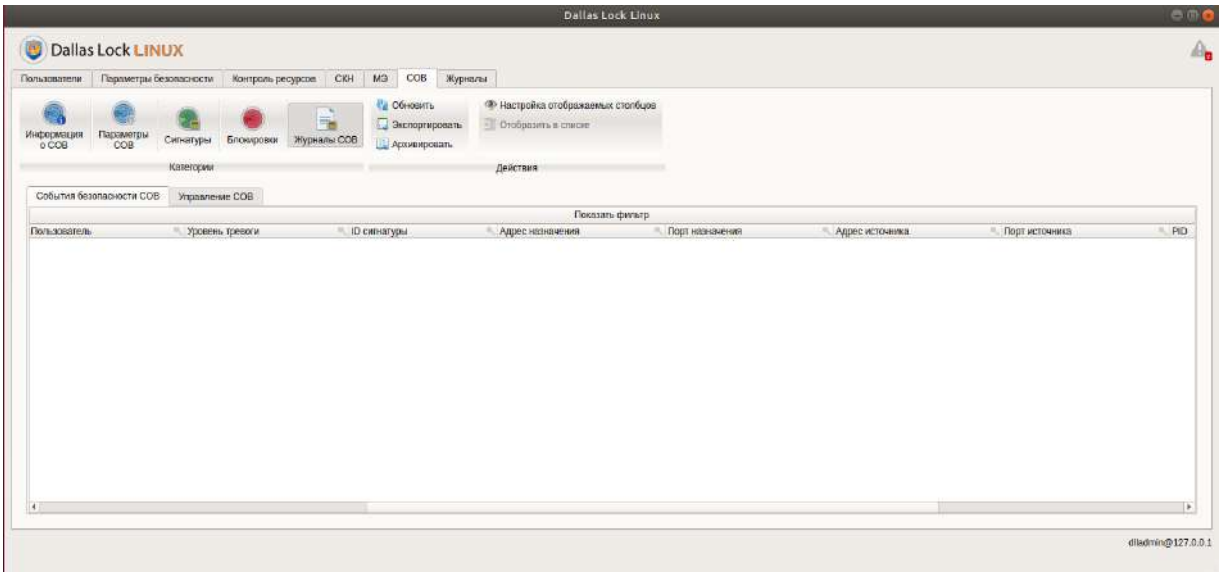


Рисунок 77. Расположение журналов СОВ

Для установки правил фильтрации необходимо на вкладке «**Журналы**» нажать на кнопку «**Параметры**», после чего откроется дополнительная панель (см. Рисунок 78 и Рисунок 79).

Рисунок 78. Открытие дополнительной панели инструментов

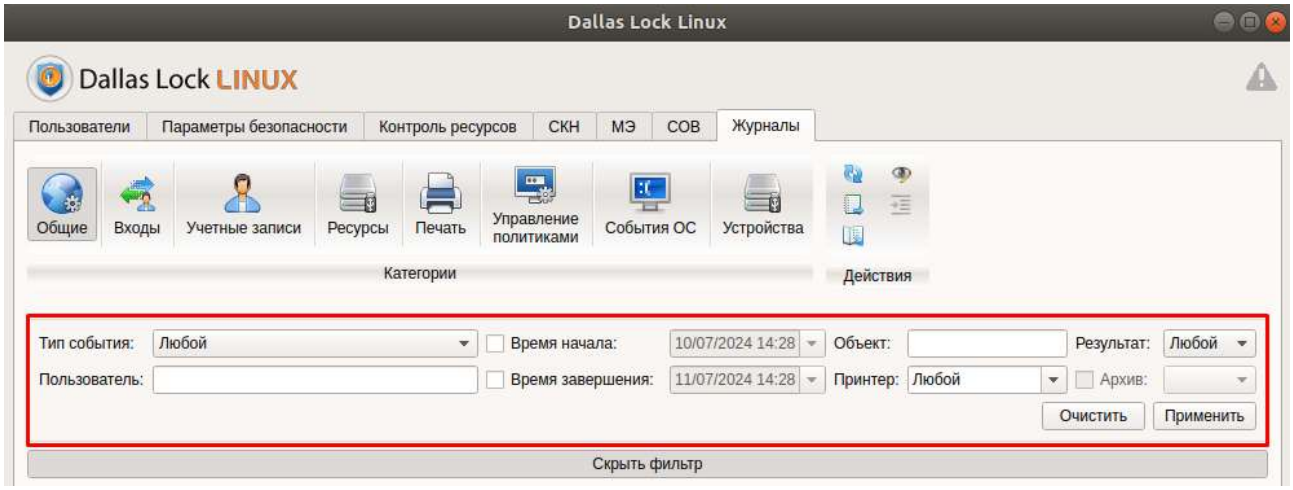


Рисунок 79. Панель настройки параметров фильтрации

Использование фильтров дает возможность отсеять ненужные данные в журнале так, что они становятся невидимы для просмотра, в то же время информация при использовании фильтров из журналов не удаляется.

Чтобы выполнить настройки, необходимо установить соответствующие атрибуты и нажать на кнопку «**Применить**», после чего к записям журнала будут применены параметры фильтрации.

Каждый фильтр имеет параметры настройки, которые соответствуют основным элементам списка открытого журнала. Также записи в каждом журнале можно отсортировать по определенному типу события, которое соответствует только выбранному журналу.

4.9.2 Подсистема аудита объектов файловой системы

Подсистема аудита объектов ФС предназначена для учета действий субъектов доступа над защищаемыми объектами. Такой учет основан на определении правил аудита для защищаемых объектов. Под правилами аудита подразумевается регистрация набора операций, выполняемых субъектами над объектами доступа (чтение параметров файла или каталога, изменение атрибутов доступа, удаление, создание или переименование файла (каталога) и иные действия субъектов доступа над защищаемым объектом).

Установка аудита на каталог «/» запрещена. В этом случае будет возвращена ошибка.

Подсистема аудита объектов ФС предоставляет администратору **СЗИ НСД** возможность добавлять, удалять и редактировать правила аудита в системе.

Для корректной работы аудита объектов файловой системы, расположенных на съемных накопителях, смонтированный раздел съемного накопителя должен иметь какую-либо из файловых систем: ext2, ext3, ext4, JFS, ReiserFS.

При восстановлении объекта ФС из резервной копии, аудит будет снят автоматически.

Консольная оболочка администрирования

Для установки аудита на объект ФС необходимо в консольной оболочке администрирования (*ishl*) перейти к подсистеме аудита, набрав команду *audit*, а затем определить параметры аудита объекта ФС командой *set-watch*, используя атрибуты, указанные в Таблица 45.

Таблица 45

№	Атрибуты	Описание
1	*path <значение>*	Путь к объекту файловой системы, на который устанавливается аудит
2	*mode <значение>*	Маска правил аудита, в формате «rwx», где параметр: *r* — отслеживает события чтения; *w* — отслеживает события записи; *x* — отслеживает события выполнения (только для файлов). При установке данного параметра для файла-скрипта (sh, python и т. д.) событие «processStop» регистрироваться не будет, т.к. источником процесса в ОС будет интерпретатор (bash, python и т. д.); e — отслеживает события неуспешных попыток доступа. Если какое-то правило аудита не назначается, то вместо соответствующего параметра устанавливается «-». Порядок указания символов, обозначающих правила аудита или их отсутствие, может быть любой

Пример: необходимо включить аудит чтения и изменения атрибутов для файла /etc/fstab.

audit <enter>

set-watch /etc/fstab wr <enter>

Удалить правила аудита с объекта файловой системы возможно при помощи команды *remove-watch*, указав в качестве его значения *path* (описание атрибута приведено в Таблица 45).

Пример: необходимо отключить аудит для объекта ФС.

audit <enter>

remove-watch /etc/fstab <enter>

Для просмотра списка объектов ФС, находящихся под аудитом, необходимо выполнить команду *get-watch-all*.

Пример:

audit <enter>

get-watch-all <enter>

Просмотреть правила аудита объекта файловой системы возможно при помощи команды *get-watch*, указав в качестве его значения *path* (описание атрибута приведено в Таблица 45).

Пример:

audit <enter>

get-watch /etc/fstab <enter>

Графическая оболочка администрирования

Для установки аудита на объект файловой системы необходимо выполнить следующие шаги:

1. В графической оболочке **СЗИ НСД** выбрать вкладку «**Контроль ресурсов**» и перейти в категорию «**Файлы**».

2. В дереве объектов выбрать файл и нажать на кнопку  «**Контроль над файлом**», либо 2 раза кликнуть левой кнопкой мыши на выбранный объект ФС. Появится окно «**Контроль над объектом: «наименование выбранного объекта ФС**» (см. Рисунок 80).

3. В окне «**Контроль над объектом: «наименование выбранного объекта ФС**» в левой части окна выбрать из списка категорий элемент «Аудит доступа».

4. Установить правила аудита для выбранного объекта ФС. Назначение правил выполняется путем установки флага напротив соответствующего параметра. На объект ФС можно назначить следующие правила:

- Чтение — отслеживать события чтения.
- Запись — отслеживать события записи.
- Выполнение — отслеживать события запуска, выполнения.
- Неуспешные попытки доступа — отслеживать события неуспешных попыток доступа.

С помощью кнопок «**Полный аудит**» и «**Снять аудит**», соответственно, можно выставить или убрать все флаги аудита.

5. После установки флага на панели инструментов «Контроль над объектом» необходимо сохранить правило – нажать на кнопку «**Сохранить**». Нажатие кнопки «**Применить**» ведет к сохранению изменений и закрытию окна «**Контроль над объектом: «наименование выбранного объекта ФС**».

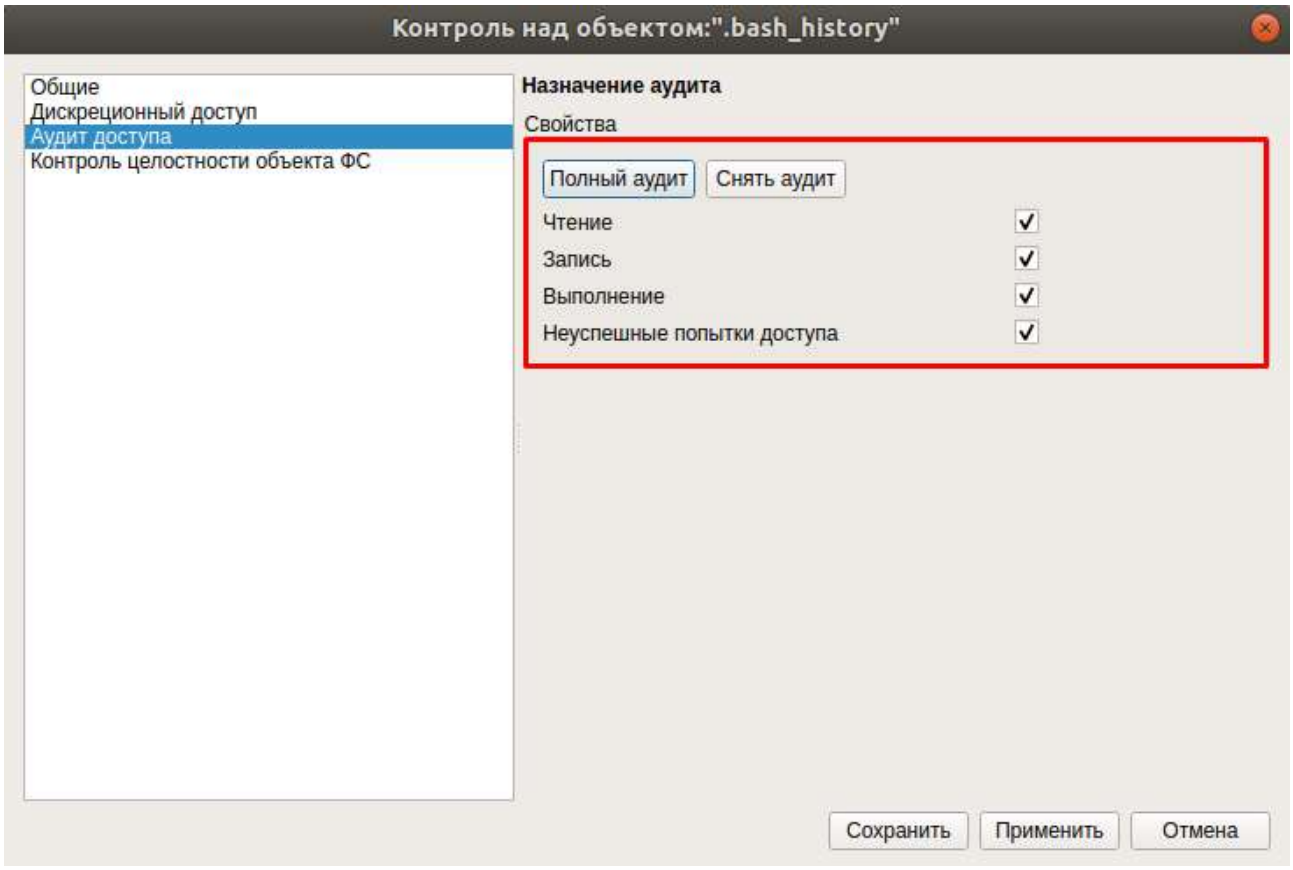


Рисунок 80. Окно «Контроль над объектом: «Наименование выбранного объекта ФС»

Информация об объектах, находящихся под аудитом, отображается в общей таблице в панели «**Контроль аудита файлов**» (см. Рисунок 81). В таблице указывается полный путь к объекту ФС и флаг правил аудита, в формате «rwxe», где параметр:

- *r* — правило чтения;
- *w* — правило записи;
- *x* — правило выполнения;
- *e* — правило неуспшных попыток доступа.

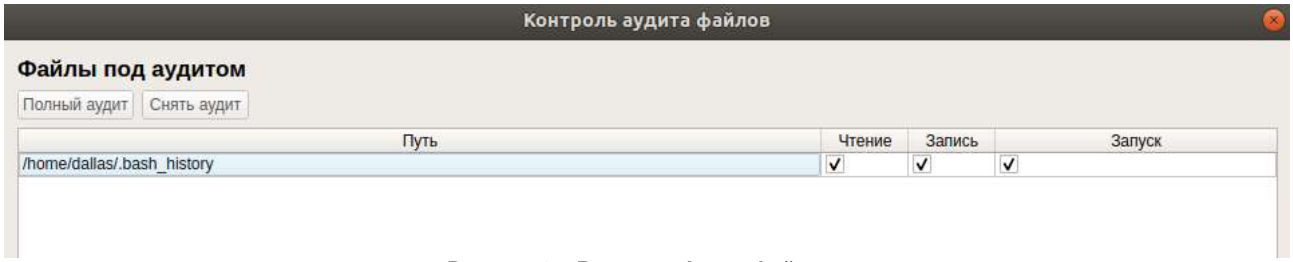


Рисунок 81. Вкладка «Аудит файлов»

Для редактирования набора правил необходимо:

1. В общей таблице выделить строку с объектом ФС.
2. Установить флаг напротив соответствующего правила (или убрать).
3. Нажать на кнопку «**Применить**». Новое правило добавится, и маска правил в общей таблице будет обновлена.

Для отмены выполнения аудита необходимо в общей таблице выделить объект и нажать на кнопку «**Снять аудит**». После отмены аудита в левом нижнем углу графической оболочки появится сообщение, что с объекта был снят аудит, и информация по данному объекту будет удалена из таблицы.

4.9.3 Подсистема аудита устройств

4.9.3.1 Аудит устройств

Подсистема аудита устройств предназначена для учета действий субъектов доступа над защищаемыми объектами. Такой учет основан на определении правил аудита для защищаемых объектов.

Под правилами аудита подразумевается регистрация набора операций, выполняемых субъектами над объектами доступа (чтение, запись, исполнение, доступ к атрибутам, перемещение, удаление, специальные права).

Подсистема аудита устройств предоставляет администратору **СЗИ НСД** возможность добавлять, удалять и редактировать правила аудита в системе. **СЗИ НСД** позволяет назначить аудит не только на конкретное устройство, но и на тип устройств.

СЗИ НСД фиксирует события подключения устройств к интерфейсам ввода/вывода в «Журнал доступа к устройствам» (см. Подсистема журналирования).

Для корректной работы аудита устройств, смонтированный раздел съемного накопителя должен иметь какую-либо из файловых систем: ext2, ext3, ext4, JFS, ReiserFS, VFAT. Корректная работа с другими типами ФС не гарантируется.

Консольная оболочка администрирования

Для установки аудита на устройство (тип устройств) необходимо в консольной оболочке администрирования (*ishl*) перейти к разделу *resources*, далее перейти к подсистеме управления оборудованием *hardware*, затем — определить параметры аудита объекта ФС командой *set-device-audit*, используя атрибуты:

device <имя устройства (типа устройств)>;
audit <режим аудита> — режим аудита в формате «rwx». Порядок указания прав доступа к устройству может быть любой.

Пример:

resources <enter>

hardware <enter>

set-device-audit <enter>

device /dev/sdb <enter>

audit rwx <enter>

execute <enter>

Удаление правил аудита с устройства (типа устройств) осуществляется при помощи команды *remove-device-audit <название устройства>.*

Пример:

resources <enter>

hardware <enter>

remove-device-audit /dev/sdb <enter>

execute <enter>

Для просмотра списка устройств, на которые назначен аудит, необходимо выполнить команду *show-audit*.

Пример:

resources <enter>

hardware <enter>

show-audit <enter>

Графическая оболочка администрирования

Для установки аудита устройств необходимо выполнить следующие шаги:

1. В графической оболочке **СЗИ НСД** перейти на вкладку «**Контроль ресурсов**», выбрать категорию «**Устройства**».

2. В дереве объектов выбрать устройство (или тип устройства) и нажать на кнопку  «Контроль над устройством». Появится окно «**Контроль над устройством: <имя устройства>**».

3. В окне «**Контроль над устройством: <имя устройства>**» в левой части окна выбрать из списка категорий элемент «Аудит доступа».

4. Установить правила аудита для выбранного устройства. Назначение правил выполняется путем установки флага напротив соответствующего параметра. На устройство (тип устройства) можно назначить следующие правила:

- Чтение — отслеживать события чтения.
- Запись — отслеживать события записи.
- Выполнение — отслеживать события запуска, выполнения.
- Неуспешные попытки доступа — отслеживать события неуспешных попыток доступа.

С помощью кнопок «**Полный аудит**» и «**Снять аудит**», соответственно, можно выставить или убрать все флаги аудита.

5. После установки флага на панели инструментов окна «**Контроль над устройством: <имя устройства>**» необходимо сохранить правило – нажать на кнопку «**Сохранить**».

Нажатие кнопки «**Применить**» приведет к сохранению изменений и закрытию окна «**Контроль над устройством: <имя устройства>**».

4.9.3.2 Аудит устройств, работающих по протоколам MTP/PTP

СЗИ НСД обеспечивает фиксацию событий, связанных с осуществлением доступа к устройствам, работающим по протоколам MTP/PTP. Подобные события фиксируются в «Журнале доступа к устройствам» (см. Подсистема журналирования).

В случае возникновения события попытки получения доступа к устройствам, работающих по протоколам MTP/PTP, фиксируются наименование производителя устройства и логин пользователя, в графической сессии которого подключено устройство.

4.9.3.3 Автоматическая реакция подсистемы аудита на событие возможного нарушения безопасности

Консольная оболочка администрирования

В **СЗИ НСД Dallas Lock Linux** предусмотрена автоматическая реакция аудита безопасности на событие возможного нарушения безопасности. Событие возможного нарушения безопасности — это событие «Получение доступа к устройству после монтирования» с результатом «*Fail*».

При обнаружении возможного нарушения безопасности **СЗИ НСД** будет выводиться информация о соответствующем событии с указанием времени возникновения события, имени пользователя и полного пути к объекту, к которому была осуществлена попытка получения доступа.

Графическая оболочка администрирования

При возникновении события возможного нарушения безопасности значок  (см. Рисунок 82), расположенный в правом верхнем углу графической оболочки администрирования **СЗИ НСД**, будет отображаться с числовым индикатором.

Рисунок 82. Графическая оболочка администрирования СЗИ НСД при условии наличие событий возможного нарушения безопасности

Для отображения информации о подобных событиях необходимо нажать на значок  . При нажатии отобразится информация об инцидентах безопасности с указанием времени возникновения события, имени пользователя и полного пути к объекту, к которому была осуществлена попытка получения доступа.

4.9.4 Архивация журналов информационной безопасности

В **СЗИ НСД** возможна архивация журналов информационной безопасности администратором.

Архивация журналов информационной безопасности **СЗИ НСД** производится автоматически, согласно заданному интервалу или установленному объему, указанным в соответствующих политиках безопасности. По наступлению срока архивации или по достижению заданного размера архивации, события, хранящиеся в журналах информационной безопасности, сохраняются в архив, а в журнал входов добавляется запись о том, что была произведена архивация. Архивы журналов информационной безопасности при создании автоматически ставятся под контроль целостности.

По умолчанию, архивы журналов информационной безопасности хранятся в директории */dllx/backup/* с именем, включающим дату и время создания архива. Каталог для хранения журналов информационной безопасности можно задать в политике безопасности «Путь к архивам журналов / *archive-path*» (в графической и консольной оболочках, соответственно).

Консольная оболочка администрирования

Для выполнения архивации журналов информационной безопасности необходимо в консольной оболочке администрирования (ishl) в разделе *audit* выполнить команду *archivate*.

Для просмотра событий из архивных копий журналов информационной безопасности необходимо воспользоваться командой *archive-path* из подсистемы *audit* с указанием полного пути к архивной копии.

Пример:

audit <enter>

get-journal <enter>

archive-path “/var/log/dll_archive/journal_archive_2015-04-15-19:53:40.sql” <enter>

execute <enter>

Графическая оболочка администрирования

Для выполнения архивации журналов информационной безопасности необходимо под администратором в графической оболочке открыть вкладку «**Журналы**» и на панели «**Действия**» нажать кнопку  «**Архивировать**» (см. Рисунок 83).

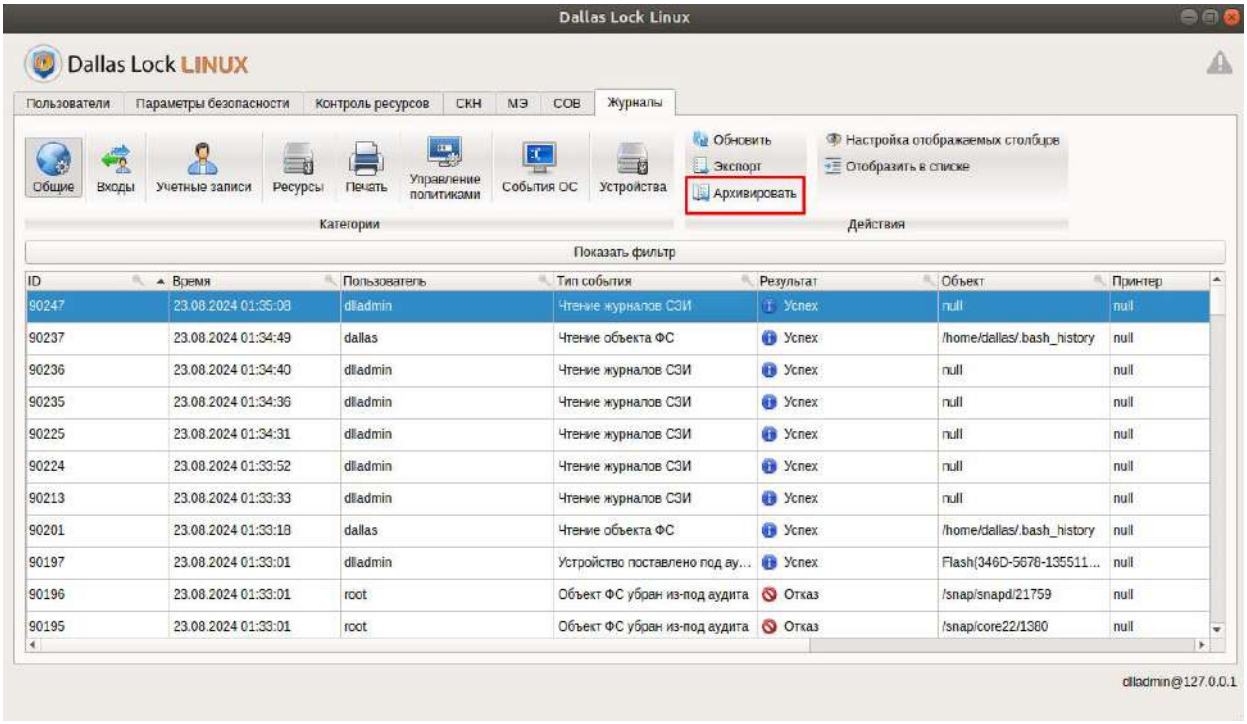


Рисунок 83. Архивация журналов информационной безопасности

Для загрузки архива журнала необходимо в параметрах журнала указать путь к каталогу (по умолчанию прописан путь к */dllx/backup/journals_archive_xxx-xx-xx:xx:xx.db/*) и нажать кнопку «**Применить**» (см. Рисунок 84).

Рисунок 84. Настройка загрузки архива журнала

4.9.5 Экспорт журналов информационной безопасности

В **СЗИ НСД** возможен экспорт записей журнала или отфильтрованных записей журнала в следующие форматы: PDF, ODS, XML.

Консольная оболочка администрирования

Для выполнения экспорта данных в формат PDF необходимо в консольной оболочке администрирования (ishl) в разделе *audit* выполнить команду *export-pdf.* После выполнения команды система перейдет в раздел *export-pdf.* Далее необходимо определить параметры экспорта данных, используя атрибуты, указанные в Таблица 46.

Таблица 46

№	Команда	Описание
1	*export-path <значение>*	Путь к каталогу, куда будут экспортированы данные
2	*archive-path <значение>*	Путь к архивной копии журнала, записи которой необходимо экспортировать
3	*journal <значение>*	Наименование журнала, записи которого необходимо экспортировать
4	*event-type <значение>*	Настройка фильтра по типу события, подробнее — см. Таблица 44
5	*from-time <значение>*	Фильтр по времени появления события, указание нижней границы. **Принимает значения:** дата и время в формате дд-мм-гггг@чч:мм:сс
6	*till-time <значение>*	Фильтр по времени появления события, указание верхней границы. **Принимает значения:** дата и время в формате дд-мм-гггг@чч:мм:сс
7	*user-name <значение>*	Фильтр по наименованию учетной записи пользователя
8	*result <значение>*	Фильтр по результату выполнения события. **Принимает значения:** – *ok* — успешный результат; – *fail* — неуспешный
9	*object <значение>*	Фильтр по объекту или субъекту доступа
10	*printer <значение>*	Фильтрация по имени принтера, на который выводится объект для печати

Пример: необходимо экспортировать записи журнала *entries*, с фильтром по полю *event-type.*

audit <enter>

export-pdf <enter>

export-path /home/user/doc <enter>

journal entries <enter>

event-type userLogin <enter>

execute <enter>

Для выполнения экспорта данных в формат ODS необходимо воспользоваться командой *export-ods* и установить требуемые атрибуты (см. Таблица 46).

Для выполнения экспорта данных в формат XML необходимо воспользоваться командой *export-xml* и установить требуемые атрибуты (см. Таблица 46).

Графическая оболочка администрирования

Для выполнения экспорта данных журнала необходимо:

1. На вкладке «**Журналы**» открыть категорию с соответствующим журналом.
2. На панели «**Действия**» выбрать команду  «**Экспорт**».
3. В открывшейся форме указать параметры экспорта данных (см. Рисунок 85):
   - «Каталог». С помощью кнопки выбора  указывается полный путь к каталогу, в котором будут сохранены данные журнала;
   - «Имя». Указывается наименование файла с данными;
   - «Формат». Из ниспадающего списка выбирается формат выгрузки данных.

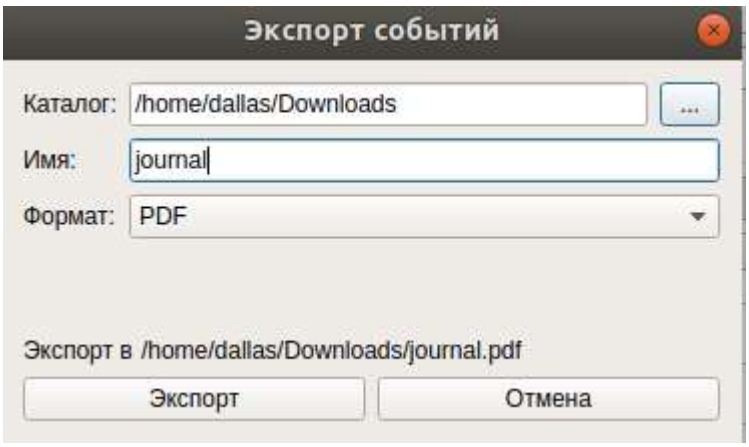


Рисунок 85. Диалоговое окно параметров экспорта данных журнала

4.Для выполнения экспорта данных нажать на кнопку «**Экспорт**», для отмены операции — кнопка «**Отмена**».

4.10 Управление регистрационными данными системы защиты

Подсистема управления регистрационными данными **СЗИ НСД Dallas Lock Linux** позволяет управлять текущей лицензией и ключом технической поддержки, обновлять пользовательский и корневой сертификаты, а также просматривать номер версии и сборки, установленной **СЗИ НСД**.

> **!** Полноценное функционирование **СЗИ НСД** возможно только в случае корректной настройки и установки действующего лицензионного номера продукта.

Для перехода в подсистему управления регистрационными данными **СЗИ НСД** необходимо в консольной оболочке администрирования (*ishl*) выполнить команду *information.* После выполнения команды система перейдет в раздел *information.*

Список основных управляющих команд раздела *information*:

- *show-license* — просмотр номера лицензии **СЗИ НСД**;
- *show-version* — просмотр номера текущей версии и сборки **СЗИ НСД**;
- *set-license* — смена номера лицензии **СЗИ НСД**;

- *support-serial* — управление ключом технической поддержки;
- *change-cert* — обновление корневого и пользовательского сертификатов;
- *list* — просмотр списка доступных команд и подменю;
- *show-os-version* – просмотр версии операционной системы семейства Linux и версии ядра;
- *help* — вывод информации о встроенных командах;
- *back* — выход из подменю (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dllladmin*.

4.10.1 Просмотр номера текущей версии и сборки системы защиты

Консольная оболочка администрирования

В разделе *information* реализована возможность проверки номера текущей версии и сборки **СЗИ НСД**. Для этого необходимо выполнить команду *show-version*.

Пример:

information <enter>

show-version <enter>

Результат выполнения команды:

Installed “номер сборки”

Графическая оболочка администрирования

Для того, чтобы проверить номер текущей версии и сборки **СЗИ НСД**, необходимо открыть окно «**О программе**», вызвав его из списка дополнительных функций кнопки главного меню  . После нажатия кнопки главного меню появится окно «**О программе**». В списке найти строку «*Номер сборки*» и «*Версия GUI*» (см. Рисунок 9).

4.10.2 Просмотр установленного лицензионного номера

Консольная оболочка администрирования

Для получения информации об установленном лицензионном номере продукта в разделе *information* необходимо выполнить команду *show-license.*

Пример:

information <enter>

show-license <enter>

Результат выполнения команды:

license: <номер лицензии>

Активные модули (Active modules):

– *Система защиты от несанкционированного доступа (System of protection from unauthorized access to information)*

– *Персональный межсетевой экран (Firewall)*

– *СКН-П (Device access control)*

– *СОВ (Host based intrusion detection system)*

Графическая оболочка администрирования

Для получения информации об установленном лицензионном номере продукта необходимо открыть окно «**О программе**», вызвав его из списка дополнительных функций кнопки главного меню  . Появится окно «**О программе**». В списке просмотреть данные строки «*Номер лицензии*» (см. Рисунок 9).

4.10.3 Управление лицензионным номером

Консольная оболочка администрирования

Для смены лицензионного номера продукта в разделе *information* необходимо перейти в *set-license* и выполнить команду *set-license* с указанием в качестве атрибута нужного номера.

Для данного раздела доступны следующие команды:

- *back* — выход из подменю (на уровень выше);
- *help* — вывод информации о встроенных командах;
- *list* — просмотр списка команд раздела;
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dlladmin*;
- *set-license* — смена номера лицензии **СЗИ НСД**;
- *reboot* — *перезагрузка ОС*;

Пример:

information <enter>

set-license <enter>

set-license 0-0000-0000 <enter>

reboot yes <enter>

execute <enter>

Результат выполнения команды:

The system will reboot automatically!

The following subsystems will be disabled after reboot: -

The following subsystems will be enabled after reboot: Device access control, Firewall.

Графическая оболочка администрирования

Для смены лицензионного номера продукта необходимо открыть окно «**О программе**», вызвав его из списка дополнительных функций кнопки главного меню  . В окне «**О программе**» нажать на кнопку «**Сменить номер лицензии и код технической поддержки**». Откроется окно «Изме**нить номер лицензии или код технической поддержки**» (см. Рисунок 86). Ввести новый номер лицензии. Также, одновременно, можно ввести код активации технической поддержки.

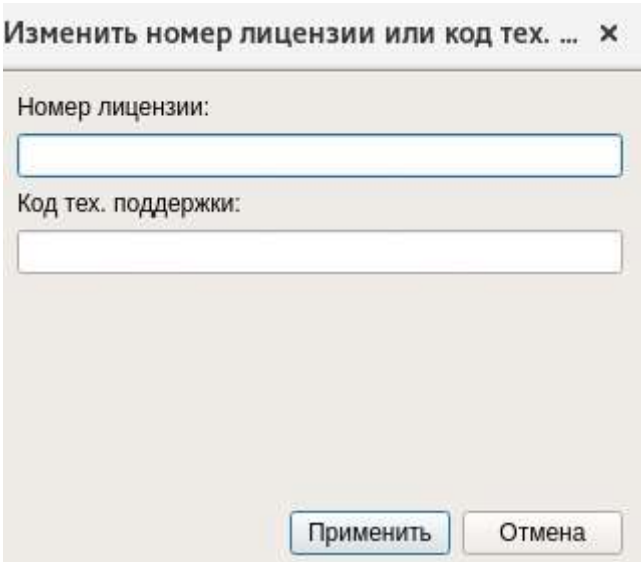


Рисунок 86. Управление лицензионным номером

При обновлении и изменении лицензии будет заблокирована возможность изменения кода технической поддержки до перезагрузки.

4.10.4 Управление ключом технической поддержки

Консольная оболочка администрирования

Для перехода к подсистеме управления ключом технической поддержки в разделе *information* необходимо выполнить команду *support-serial*.

Для данного раздела доступны следующие команды:

- *set-support-serial* — установка ключа технической поддержки;
- *get-support-serial* — просмотр номера ключа технической поддержки;
- *get-serial-date* — просмотр срока действия ключа технической поддержки;
- *list* — просмотр списка команд раздела;
- *help* — вывод информации о встроенных командах;
- *back* — выход из подменю (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dlladmin*.

Для установки ключа технической поддержки необходимо перейти в раздел *set-support-serial*, выполнив команду *set-support-serial*, затем выполнить команду *key* с указанием в качестве атрибута требуемый номер ключа технической поддержки.

Пример:

information <enter>

support-serial <enter>

set-support-serial key 00000000-000 <enter>

execute <enter>

Для получения информации о номере установленного ключа технической поддержки необходимо выполнить команду *get-support-serial.*

Пример:

information <enter>

support-serial <enter>

get-support-serial <enter>

Для получения информации о сроке действия установленного ключа технической поддержки необходимо выполнить команду *get-serial-date.*

Пример:

information <enter>

support-serial <enter>

get-serial-date <enter>

Графическая оболочка администрирования

Для установки и (или) смены кода активации технической поддержки продукта необходимо открыть окно «**О программе**», вызвав его из списка дополнительных функций кнопки главного меню  . В окне «**О программе**» нажать на кнопку «**Сменить номер лицензии и код технической поддержки**». Откроется окно «**Изменить номер лицензии или код технической поддержки**» (см. Рисунок 86). Ввести код активации технической поддержки. Код активации технической поддержки и номер лицензии можно менять одновременно.

Код активации технической поддержки указан в письме, отправленном на электронную почту.

4.11 Управление межсетевым экраном

Межсетевой экран является модулем **СЗИ НСД Dallas Lock Linux** и предназначен для защиты рабочих станций и серверов от **НСД** посредством осуществления контроля и фильтрации, проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.

Задавать ограничения можно по работе служебных и прикладных протоколов, портов и т. д. Функции МЭ осуществляются посредством контроля и фильтрации сетевых пакетов в соответствии с набором таких параметров, как параметры сетевых протоколов, профили МЭ, правила МЭ, адреса, приложения.

Управление настройками межсетевого экрана доступно пользователям, которым назначена возможность изменения настроек МЭ — администраторам **Dallas Lock Linux**. Пользователи с ролью «Аудитор» обладают всеми привилегиями на просмотр информации и настроек межсетевого экрана.

Консольная оболочка администрирования

Для перехода в подменю управления межсетевым экраном в консольной оболочке администрирования (*ishl)* необходимо выполнить команду *firewall*. После выполнения команды система перейдет в соответствующий раздел *firewall*.

Для данного раздела доступны следующие управляющие команды, представленные в таблице ниже:

Таблица 47

№	Атрибут	Описание
1	*show-netstat*	Команда вывода на экран статических сетевых соединений. После ввода команды будет выведен список сетевых соединений с полями: – *pid* – уникальный идентификатор процесса; – пользователь (*user*) – пользователь, инициализирующий соединение; – сервис (*command*) – наименование сервиса; – статус (*state*) – статус сетевого соединения; – версия (*type*) – версия интернет протокола; – протокол (*protocol*) – транспортный протокол; – адрес источника (*source address*) – IP-адрес отправителя; – порт источника (*source port*) – порт отправителя; – адрес назначения (*destination address*) – IP-адрес получателя; – порт назначения (*destination port*) – порт получателя. **Пример:** *firewall <enter>* *show-netstat <enter>* Соединения сервисов **СЗИ НСД** не отображаются в списке
2	*remove-blacklist-command <зна*	Команда удаления приложения из черного списка. Подробнее — в разделе 4.11.3.2 Удаление приложений из черного списка

№	Атрибут	Описание
	чение>	
3	*show-commands-blacklist*	Команда вывода на экран черного списка приложений. После ввода команды будет выведен список приложений, входящих в черный список приложений, с полями: – приложение (*command*); – путь (*path*) до исполняемого файла; – описание (*description*). **Пример:** *firewall <enter>* *show-commands-blacklist <enter>*
4	*remove-whitelist-command <значение>*	Команда удаления приложения из белого списка. Подробнее — в разделе 4.11.4.2 Удаление приложения из белого списка
5	*show-commands-whitelist*	Команда вывода на экран белого списка приложений. После ввода команды будет выведен список приложений, входящих в белый список приложений, с полями: – приложение (*command*); – путь (*path*) до исполняемого файла; – описание (*description*). **Пример:** *firewall <enter>* *show-commands-whitelist <enter>*
6	*remove-rule <значение>*	Команда удаления существующего правила МЭ. Подробнее — в разделе 4.11.2.3 Удаление правила межсетевого экрана
7	*show-rul*	Команда вывода на экран существующего правила МЭ. Подробнее — в разделе 4.11.2.4 Вывод правила межсетевого экрана

№	Атрибут	Описание
	e <значение>	
8	*list-rules*	Команда вывода на экран всех правил МЭ. После ввода команды будет выведен список правил МЭ с полями: – статус правила (*enable*); – приоритет обработки правила (*priority*); – имя профиля (*profile*); – операция, выполняемая при фильтрации сетевых пакетов (*action*); – направление сетевого трафика (*direction*); – протокол (*protocol*); – тип прикладного протокола (*service*); – команда прикладного протокола (*app_cmd*); – маска фильтра сетевого трафика (*content*); – мобильный код (*mobile_code*); – IP-адрес отправитель (*src_addrs*); – порт отправителя (*src_ports*); – IP-адрес получателя (*dst_addrs*); – порт получателя (*dst_ports*); – аудит (*audit*); – автоматическая блокировка адреса (*auto_block*); – текстовое сообщение с описанием правила (*message*). **Пример:** *firewall <enter>* *list-rules <enter>*
9	*test-firewall*	Команда запуска самотестирования межсетевого экрана. Подробнее — в разделе Самотестирование межсетевого экрана
1	*show-ifconfig*	Команда вывода конфигурации адресов и интерфейсов хоста. После ввода команды будет выведен список конфигурации адресов и интерфейсов хоста с полями: – идентификатор (*id*); – версия IP-адреса (*version*); – IP-адрес с маской (*address*); – имя интерфейса (*interface*). **Пример:** *firewall <enter>* *show-ifconfig <enter>*
1	*import-rules*	Команда импорта правил в формате JSON из указанного файла в базу данных правил МЭ. Подробнее — в разделе 4.11.2.6 Импорт правил
1	*export-rules*	Команда экспорта правил из базы данных МЭ в указанный файл в формате JSON. Подробнее — в разделе 4.11.2.5 Экспорт правил

№	Атрибут	Описание
1	*list-blocked-addresses*	Команда вывода списка заблокированных адресов. После ввода команды будет выведен список заблокированных адресов с полями: – идентификатор адреса (*id*); – версия IP-адреса (*version*); – IP-адрес с маской (*address*); – описание (*description*). **Пример:** *firewall <enter>* *list-blocked-addresses <enter>*
1	*unblock-address*	Команда разблокировки адреса. Подробнее — в разделе Заблокированные адреса
1	*list-profiles*	Команда вывода всех профилей правил МЭ. После ввода команды будет выведен список профилей правил МЭ с полями: – идентификатор профиля (*id*); – статус профиля (*enable*); – имя профиля (*profile*); – условие активации профиля (*activation*); – описание (*description*). **Пример:** *firewall <enter>* *list-profiles <enter>*
1	*remove-profile*	Команда удаления профиля правил МЭ. Подробнее — в разделе 4.11.7.3 Удаление профиля МЭ
1	*kill-connection*	Команда разрыва соединения
1	*set-whitelist-command*	Команда перехода в подменю для добавления приложения в белый список. Подробнее — в разделе Добавление приложений в белый список
1	*change*	Команда перехода в подменю для изменений параметров приложения белого списка. Подробнее — в разделе 4.11.4.1 Изменение параметров приложения белого списка

№	Атрибут	Описание
	-whitelist-command	
2	*set-blacklist-command*	Команда перехода в подменю для добавления приложения в черный список. Подробнее — в разделе Добавление приложений в черный список
2	*change-blacklist-command*	Команда перехода в подменю для изменений параметров приложения черного списка. Подробнее — в разделе 4.11.3.1 Изменение параметров приложений черного списка
2	*set-profile*	Команда перехода в подменю создания нового профиля правил МЭ. Подробнее — в разделе 4.11.7.1 Создание профиля МЭ
2	*change-profile*	Команда перехода в подменю для установки/изменений параметров профиля правил МЭ. Подробнее — в разделе Параметры межсетевого экрана
2	*set-rule*	Команда перехода в подменю создания нового правила. Подробнее — в разделе Параметры межсетевого экрана
2	*change-rule*	Команда перехода в подменю для установки/изменений параметров правила. Подробнее — в разделе Параметры межсетевого экрана Консольная оболочка администрирования Для настройки параметров межсетевого экрана необходимо в консольной оболочке администрирования в разделе *policies* выполнить команду *firewall-policies-set*. Система перейдет в управление параметрами межсетевого экрана.

Таблица 48

№	Атрибут	Описание
1	*firewall-is-active <значение>*	Активация межсетевого экрана. **Принимает значения:** *yes* – включение межсетевого экрана, *no* – выключение межсетевого экрана. По умолчанию установлено значение *no*
2	*ssl-analyze <значение>*	Фильтрация SSL (TLS) трафика. **Принимает значения:** *yes* – включение фильтрации трафика, *no* – выключение фильтрации трафика. По умолчанию установлено значение *yes*
3	*audit <значение>*	Подменю настройки регистрируемых событий межсетевого экрана. Для регистрации доступны следующие события: – *set-rule* – добавление нового правила; – *change-rule* – изменение правила; – *firewall-state* – изменение состояния межсетевого экрана; – *remove-rule* – удаление правила; – *block-address* – блокирование/разблокирование адресов; – *kill-connection* – разрыв соединения; – *policies-change* – изменение политик межсетевого экрана; – *testing* – самотестирование межсетевого экрана*;* – *set-profile* – добавление нового профиля; – *change-profile* – изменение профиля; – *remove-profile* – удаление профиля; – *set-blacklist-command* – добавление приложения в черный список; – *change-blacklist-command* – изменение приложения черного списка; – *remove-blacklist-command* – удаление приложения из черного списка; – *set-whitelist-command* – добавление приложения в белый список; – *change-whitelist-command* – изменение приложения из белого списка; – *remove-whitelist-command* – удаление приложения из белого списка. **Пример:** *policies <enter>* *firewall-policy-set <enter>* *audit <enter>* *remove-rule no <enter>* *e* *x* Выключен аудит события межсетевого экрана типа “Удаление правил МЭ”

№	Атрибут	Описание		
		4	*black-white-lists <значение>*	Команда включения/выключения белого и черного списков приложений
		5	*auto-block-interval <значение>*	Команда изменения интервала срабатывания правил для автоматической блокировки адресов. **Принимает значения:** от 1 до 60 минут
		6	*auto-block-burst <значение>*	Команда установки значения автоматической блокировки – количество правил, совпадающих с одним адресом источника, чтобы автоматически заблокировать его. **Принимает значения:** от 1 до 10 раз

4.11.1.1 Изменение интервала срабатывания правил для автоматической блокировки адресов

Для изменения интервала срабатывания правил для автоматической блокировки адресов необходимо в консольной оболочке администрирования, в разделе управления политиками межсетевого экрана, набрать команду *auto-block-interval* с указанием целочисленного значения интервала в минутах (от 1 до 60, шаг интервала 5 минут) и команду *auto-block-burst* с указанием целочисленного значения (от 1 до 10 раз). Для вступления изменений в силу необходимо набрать команду *execute.*

Пример:

policies <enter>

firewall-policy-set <enter>

auto-block-interval 10 <enter>

execute <enter>

policies <enter>

firewall-policy-set <enter>

auto-block-burst 10 <enter>

№	Атрибут	Описание

execute <enter>

Su

4.11.1.2 Включение белого списка приложений

ec

Для включения белого списка команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду невозможно. Для вступления изменений в силу необходимо набрать команду *execute.*

ss

se

4.11.1.3 Включение чёрного списка приложений

ip

Для включения чёрного списка команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду невозможно. Для вступления изменений в силу необходимо набрать команду *execute.*

config

4.11.1.4 Выключение чёрного и белого списков приложений

ap

Для выключения чёрного и белого списков команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду *execute*.

wa

ll

ip

Графическая оболочка администрирования

ob

Для настройки параметров межсетевого экрана с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» перейти в категорию «**Параметры**», где будут представлены параметры для настройки межсетевого экрана (см. Рисунок 88).

fi

/

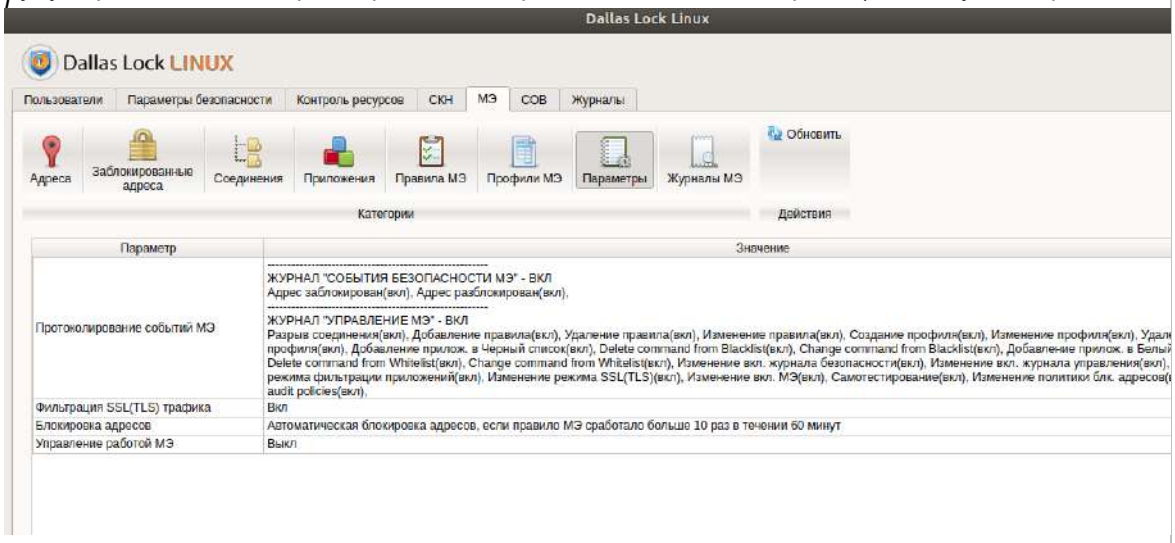


Рисунок 88. Параметры межсетевого экрана

Для настройки протоколирования событий МЭ необходимо по параметру «**Протоколирование событий МЭ**» запустить окно «**Протоколирование событий МЭ**» двойным кликом по левой кнопки мыши (см. Рисунок 89).

№	Атрибут	Описание

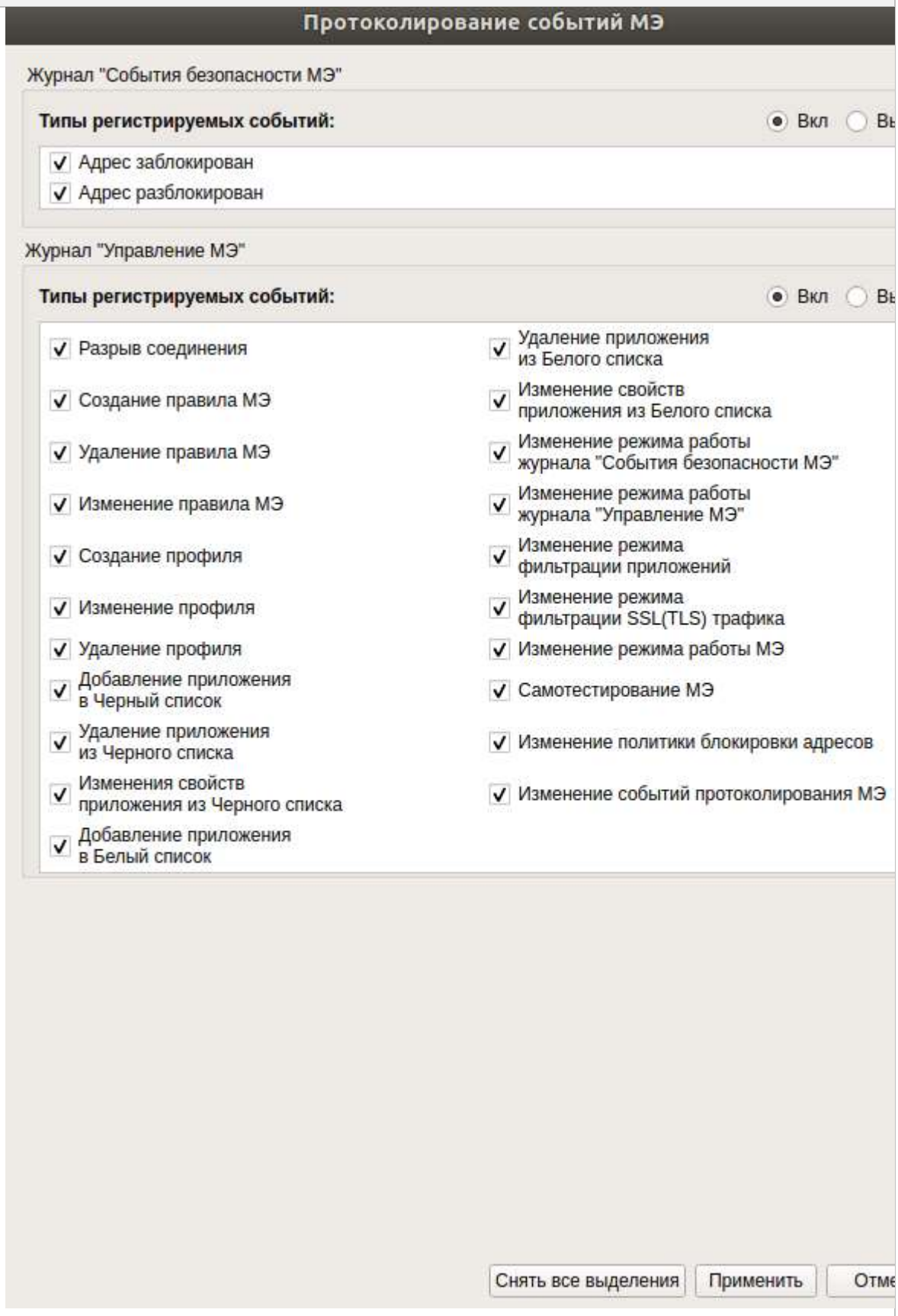


Рисунок 89. Окно «Протоколирование событий МЭ»

№	Атрибут	Описание
		Управление правилами межсетевого экрана

Графическая оболочка администрирования

Для управления межсетевым экраном **СЗИ НСД** в графической оболочке администрирования необходимо перейти во вкладку «**МЭ**» (см. Рисунок 87). На данной вкладке представлены следующие категории настраиваемых параметров системы защиты:

- «Адреса»;
- «Заблокированные адреса»;
- «Соединения»;
- «Приложения»;
- «Правила МЭ»;
- «Профили МЭ»;
- «Параметры»;
- «Журналы МЭ».

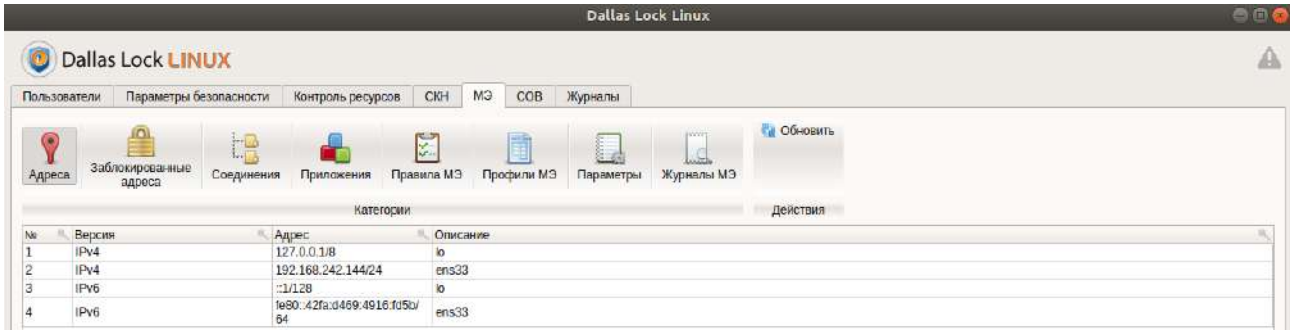


Рисунок 87. Вкладка «МЭ»

4.11.1 Параметры межсетевого экрана

Консольная оболочка администрирования

Для настройки параметров межсетевого экрана необходимо в консольной оболочке администрирования в разделе *policies* выполнить команду *firewall-policies-set*. Система перейдет в управление параметрами межсетевого экрана.

Таблица 48

№	Атрибут	Описание
1	*firewall-is-active <значе*	Активация межсетевого экрана. **Принимает значения:** *yes* – включение межсетевого экрана, *no* – выключение межсетевого экрана. По умолчанию установлено значение *no*

№	Атрибут	Описание
	ние>	
2	*ssl-analyze <значение>*	Фильтрация SSL (TLS) трафика. **Принимает значения:** *yes* – включение фильтрации трафика, *no* – выключение фильтрации трафика. По умолчанию установлено значение *yes*
3	*audit <значение>*	Подменю настройки регистрируемых событий межсетевого экрана. Для регистрации доступны следующие события: – *set-rule* – добавление нового правила; – *change-rule* – изменение правила; – *firewall-state* – изменение состояния межсетевого экрана; – *remove-rule* – удаление правила; – *block-address* – блокирование/разблокирование адресов; – *kill-connection* – разрыв соединения; – *policies-change* – изменение политик межсетевого экрана; – *testing* – самотестирование межсетевого экрана*;* – *set-profile* – добавление нового профиля; – *change-profile* – изменение профиля; – *remove-profile* – удаление профиля; – *set-blacklist-command* – добавление приложения в черный список; – *change-blacklist-command* – изменение приложения черного списка; – *remove-blacklist-command* – удаление приложения из черного списка; – *set-whitelist-command* – добавление приложения в белый список; – *change-whitelist-command* – изменение приложения из белого списка; – *remove-whitelist-command* – удаление приложения из белого списка. **Пример:** *policies <enter>* *firewall-policy-set <enter>* *audit <enter>* *remove-rule no <enter>* *e* Выключен аудит события межсетевого экрана типа “Удаление правил МЭ”
4	*black-white-lists <значение>*	Команда включения/выключения белого и черного списков приложений

№	Атрибут	Описание
5	*auto-block-interval <значение>*	Команда изменения интервала срабатывания правил для автоматической блокировки адресов. **Принимает значения:** от 1 до 60 минут
6	*auto-block-burst <значение>*	Команда установки значения автоматической блокировки – количество правил, совпадающих с одним адресом источника, чтобы автоматически заблокировать его. **Принимает значения:** от 1 до 10 раз

4.11.1.1 Изменение интервала срабатывания правил для автоматической блокировки адресов

Для изменения интервала срабатывания правил для автоматической блокировки адресов необходимо в консольной оболочке администрирования, в разделе управления политиками межсетевого экрана, набрать команду *auto-block-interval* с указанием целочисленного значения интервала в минутах (от 1 до 60, шаг интервала 5 минут) и команду *auto-block-burst* с указанием целочисленного значения (от 1 до 10 раз). Для вступления изменений в силу необходимо набрать команду *execute.*

Пример:

policies <enter>
firewall-policy-set <enter>
auto-block-interval 10 <enter>
execute <enter>
policies <enter>
firewall-policy-set <enter>
auto-block-burst 10 <enter>
execute <enter>

4.11.1.2 Включение белого списка приложений

Для включения белого списка команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду *black-white-lists* со значением Одновременно включить и чёрный, и белый список невозможно. Для вступления изменений в силу необходимо набрать команду *execute.*

4.11.1.3 Включение чёрного списка приложений

Для включения чёрного списка команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду *black-white-lists* со значением

4.11.1.4 Выключение чёрного и белого списков приложений

Для выключения чёрного и белого списков команд необходимо в консольной оболочке администрирования в разделе управления политиками межсетевого экрана набрать команду *black-*

Графическая оболочка администрирования

Для настройки параметров межсетевого экрана с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» перейти в категорию «**Параметры**», где будут представлены параметры для настройки межсетевого экрана (см. Рисунок 88).

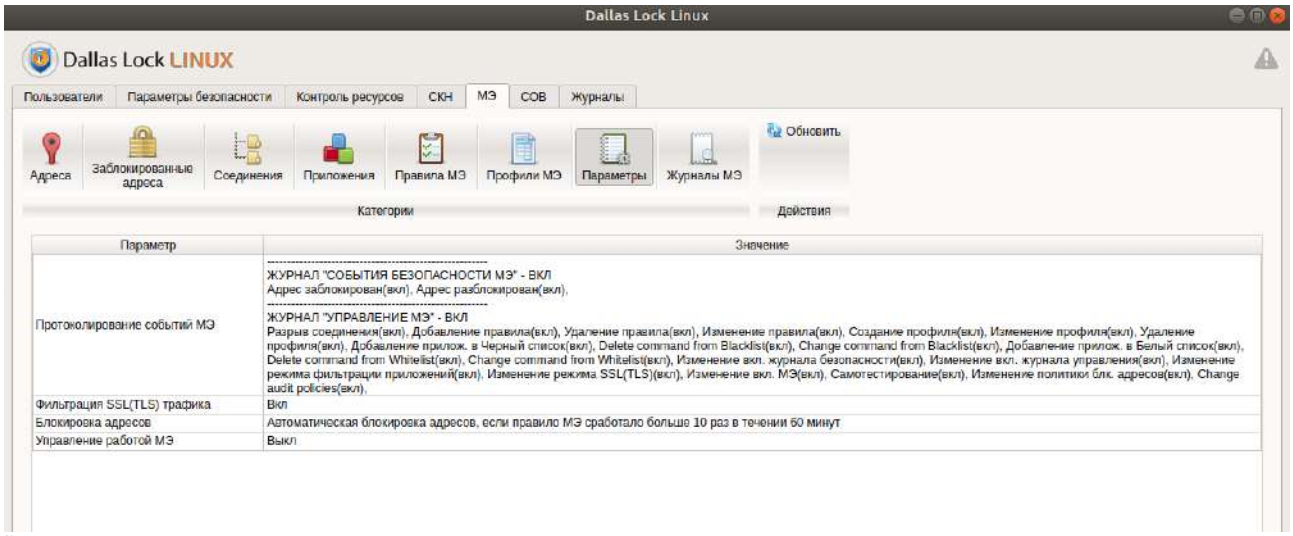


Рисунок 88. Параметры межсетевого экрана

Для настройки протоколирования событий МЭ необходимо по параметру «**Протоколирование событий МЭ**» запустить окно «**Протоколирование событий МЭ**» двойным кликом по левой кнопки мыши (см. Рисунок 89).

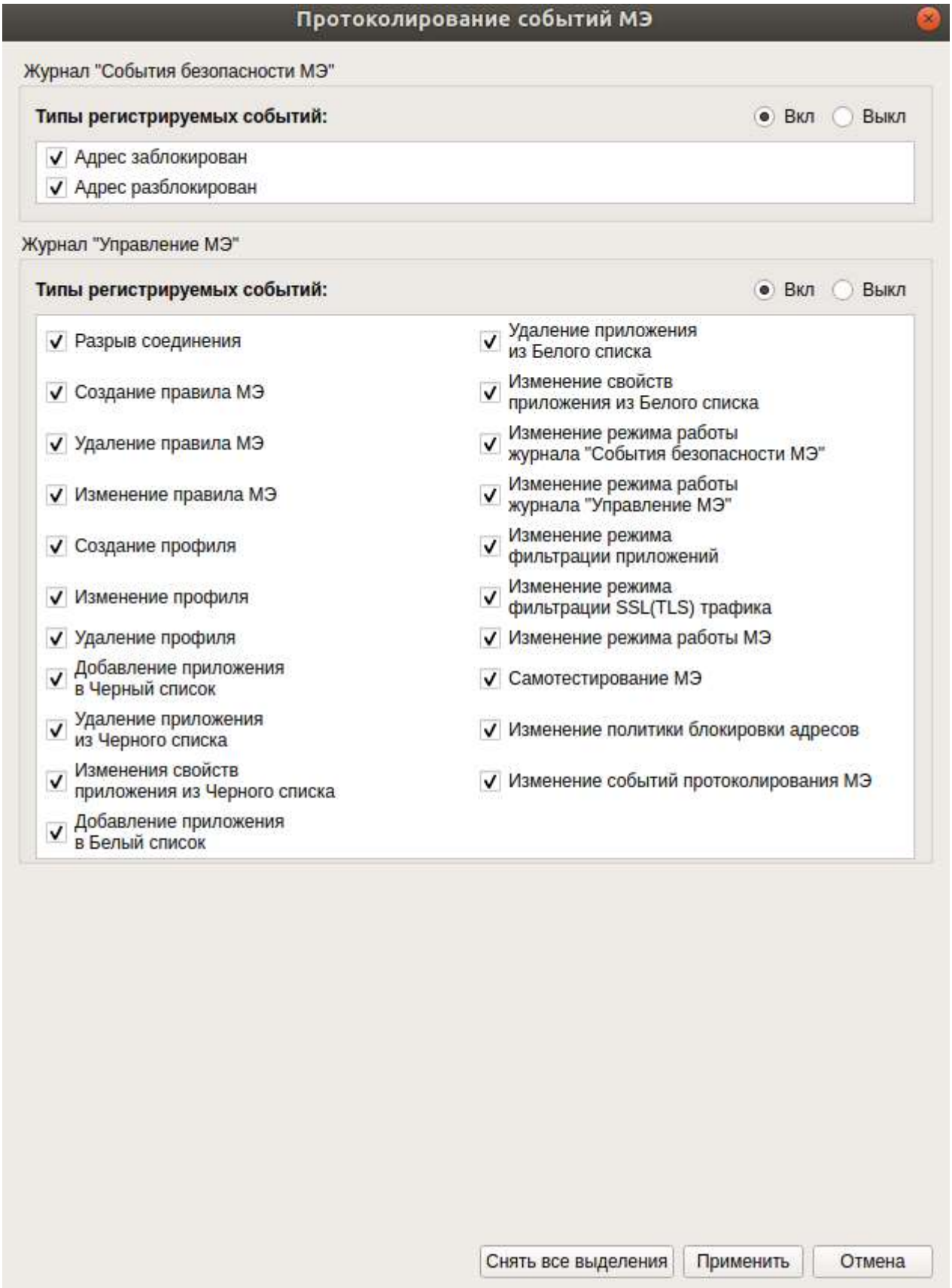


Рисунок 89. Окно «Протоколирование событий МЭ»

4.11.2 Управление правилами межсетевого экрана

4.11.2.1 Добавление правила межсетевого экрана

Пять пользовательских правил МЭ, по умолчанию входящие в профиль МЭ «Default» (см. Рисунок 90), доступны с первого включения **СЗИ НСД Dallas Lock Linux**. Данные правила МЭ доступны для редактирования и удаления. Подробнее — в разделе Управление профилями правил межсетевого экрана.

Консольная оболочка администрирования

Для добавления нового правила межсетевого экрана необходимо выполнить команду *set-rule* в разделе *firewall*. Система перейдет в подменю *set-rule*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 49.

Необходимо обратить внимание, что при задании разрешающего правила (*pass*) высокого приоритета с указанием протокола L7 и одновременным заданием запрещающего правила (*reject*) на протокол TCP с более низким приоритетом – первым будет срабатывать правило на блокировку TCP, т.к. будет сразу заблокирован сетевой пакет установки TCP-соединения, и обмен данным (при котором определяется принадлежность сетевого пакета к заданному протоколу L7) не произойдет.

В случае, если у разрешающего и запрещающего правил одинаковый приоритет, то разрешающее правило будет иметь приоритет над запрещающим.

Таблица 49

№	Атрибут	Описание
1	*profile <значение>*	Наименование профиля, который будет включать в себя настраиваемое правило. В качестве наименования указывается только существующий профиль. Является обязательным атрибутом. Подробнее — в разделе Управление профилями правил межсетевого экрана
2	*action <значение>*	Добавление операции, выполняемой при фильтрации сетевых пакетов, для которых действует правило. Является обязательным атрибутом. **Принимает значения:** – *pass* – пропустить сетевой пакет; – *reject* – отклонить сетевой пакет (при выборе значения отправителю сообщается о недоступности запрашиваемого сервиса)
3	*protocol <значение>*	Добавление типа сетевого или транспортного протокола, на основании которого осуществляется фильтрация сетевых пакетов. Является обязательным атрибутом. **Принимает значения:** – tcp; – udp; – icmp; – ip
4	*scr_addrs <значение>*	Указываются IP-адреса отправителей. Параметр включает локальные адреса, маски подсети или IP-адреса подсетей и диапазон IP-адресов, для которых действует правило.

№	Атрибут	Описание
		При вводе нескольких адресов необходимо разделять их символом «,». Для задания диапазона адресов используется сетевая маска в формате CIDR и символ «/». По умолчанию принимает значение *any*
5	*dst_addrs <значение>*	Указываются IP-адреса получателей. Параметр включает локальные адреса, маски подсети или IP-адреса подсетей и диапазон IP-адресов, для которых действует правило. При вводе нескольких адресов необходимо разделять их символом «,». Для установки диапазона адресов используется сетевая маска в формате CIDR и символ «/». По умолчанию принимает значение *any*
6	*scr_ports <значение>*	Добавление порта отправителя. Параметр включает список локальных портов или диапазон портов, для которых действует правило. **Принимает значения:** от 0 до 65535. При вводе нескольких номеров портов необходимо разделять их символом «,». Для разделения диапазона портов используется символ «:». По умолчанию используется значение *any*
7	*dst_ports <значение>*	Добавление порта получателя. Параметр включает список локальных портов или диапазон портов, для которых действует правило. **Принимает значения:** от 0 до 65535. При вводе нескольких номеров портов необходимо разделять их символом «,». Для разделения диапазона портов используется символ «:». По умолчанию используется значение *any*
8	*direction <значение>*	Настройка направления сетевого трафика, для которого действует правило. **Принимает значения:** – *out* – правило для исходящего сетевого трафика; – *inout* – направление сетевого трафика не указано. По умолчанию принимает значение *inout*
9	*message <значение>*	Параметр позволяет добавить описание правила. Описание правила МЭ должно заключаться в двойные кавычки. Является обязательным атрибутом
10	*priority <число>*	Параметр позволяет настроить, в какой последовательности будут обрабатываться правила МЭ. **Принимает значения:** от 1 до 255. Пакеты будут обрабатываться по правилам согласно их приоритету. Наивысший приоритет — 1. По умолчанию правилу присваивается низший приоритет — 255
11	*content <значение>*	Указание маски фильтра сетевого трафика на основе прямого соответствия содержимому сетевого пакета. Строка маски должна заключаться в двойные кавычки. По умолчанию параметр имеет пустое значение
12	*mobile_code <значение>*	Добавление маски фильтра сетевого трафика на основе наличия в сетевом пакете мобильного кода. **Принимает значения:**

№	Атрибут	Описание
		– *flash;* – *javascript;* – *pdf;* – *vbscript*
13	*service <значение>*	Добавление типа прикладного протокола, для которого действует правило. **Принимает значения:** – *http;* – *ftp;* – *imap;* – *pop3;* – *smtp;* – *telnet;* – *dns;* – *ntp;* – *ssh*
14	*app_cmd <значение>*	Параметр позволяет добавить команды прикладного протокола, для которого действует правило. Значение параметра можно задать, если задан прикладной протокол. **Принимает значения:** Для ***http:*** GET, POST, PUT, SEARCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, NOTIFY, POLL, BCOPY, BDELETE, BMOVE, LINK, UNLINK, OPTIONS, HEAD, DELETE, TRACE, TRACK, CONNECT, SOURCE, SUBSCRIBE, UNSUBSCRIBE, PROPFIND, PROPPATCH, BPROPFIND, BPROPPATCH, RPC_CONNECT, PROXY_SUCCESS, BITS_POST, CCM_POST, SMS_POST, RPC_IN_DATA, RPC_OUT_DATA, RPC_ECHO_DATA. Для ***smtp:*** ATRN, AUTH, BDAT, CHUNKING, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, ONEX, QUEU, QUIT, RCPT, RSET, SAML, SEND, SOML, STARTTLS, TICK, TIME, TURN, TURNME, VERB, VRFY, X-ADAT, X-DRCP, X-ERCP, X-EXCH50, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN, XUSR. Для ***ftp:*** ABOR, ACCT, ADAT, ALLO, APPE, AUTH, CCC, CDUP, CEL, CLNT, CMD, CONF, CWD, DELE, ENC, EPRT, EPSV, ESTA, ESTP, FEAT, HELP, LANG, LIST, LPRT, LPSV, MACB, MAIL, MDTM, MIC, MKD, MLSD, MLST, MODE, NLST, NOOP, OPTS, PASS, PASV, PBSZ, PORT, PROT, PWD, QUIT, REIN, REST, RETR, RMD, RNFR, RNTO, SDUP, SITE, SIZE, SMNT, STAT, STOR, STOU, STRU, SYST, TEST, TYPE, USER, XCUP, XCRC, XCWD, XMAS, XMD5, XMKD, XPWD, XRCP, XRMD, XRSQ, XSEM, XSEN, XSHA1, XSHA256. Для ***imap:*** APPEND, AUTHENTICATE, CAPABILITY, CHECK, CLOSE, COMPARATOR, COMPRESS, CONVERSIONS, COPY, CREATE, DELETE, DELETEACL, DONE, EXAMINE, EXPUNGE, FETCH, GETACL, GETMETADATA, GETQUOTA, GETQUOTAROOT, IDLE, LIST, LISTRIGHTS, LOGIN, LOGOUT, LSUB, MYRIGHTS, NOOP, NOTIFY, RENAME, SEARCH, SELECT, SETACL, SETMETADATA, SETQUOTA, SORT, STARTTLS, STATUS, STORE, SUBSCRIBE, THREAD, UID, UNSELECT, UNSUBSCRIBE, X. Для ***pop3:*** APOP, AUTH, CAPA, DELE, LIST, NOOP, PASS, QUIT, RETR, RSET, STAT, STLS, TOP, UIDL, USER.

№	Атрибут	Описание
		Для ***dns:*** A, AAAA, CNAME, SRV, TXT, MX, SOA, NS, PTR
15	*enable <значение>*	Параметр позволяет изменить статус правила. **Принимает значения:** *yes* – правило включено, *no* – правило отключено. По умолчанию установлено значение *no*
16	*audit <значение>*	Управление регистрацией событий в журнале, возникающих при срабатывании правила. **Принимает значения:** *yes* – регистрация событий включена, *no* – регистрация событий отключена. По умолчанию установлено значение *no*
17	*auto_block <значение>*	Включение/выключение автоматической блокировки адреса при кратном срабатывании правила с данным адресом. **Принимает значения:** *yes* – автоблокировка включена, *no* – автоблокировка выключена. Значение *yes* установлено по умолчанию
18	*clear <значение>*	Команда для очистки следующих настраиваемых параметров: – *content;* – *mobile_code;* – *service;* – *app_cmd*

Пример:

firewall <enter>
set-rule <enter>
action reject <enter>
protocol tcp <enter>
content “www.dallaslock.ru” <enter>
message “Reject all requests to www.dallaslock.ru” <enter>
audit yes <enter>
enable yes <enter>
profile Default <enter>
execute <enter>
New rule was successfully added

Добавлено правило для блокировки запросов, отправляемых на ресурс www.dallaslock.ru.

Нельзя одновременно задавать поля «content» и «service».

Графическая оболочка администрирования

Для добавления нового правила межсетевого экрана с помощью графической оболочки **СЗИ НСД** необходимо на вкладке «**МЭ**» выбрать категорию «**Правила МЭ**» (см. Рисунок 90) и нажать на кнопку «**Создать правило**»  на панели действий.

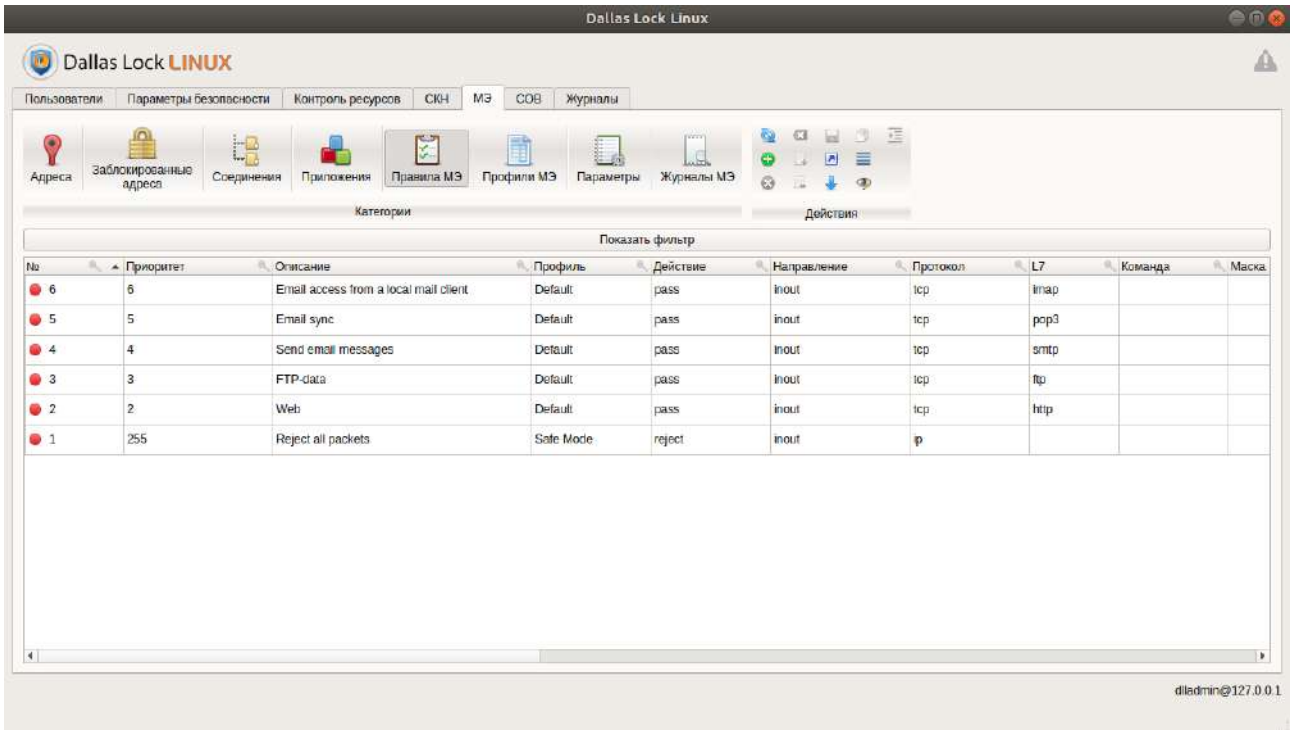


Рисунок 90. Рабочая область категории «Правила МЭ»

Пять пользовательских правил МЭ, по умолчанию входящие в профиль МЭ «Default» (см. Рисунок 90), доступны с первого включения **СЗИ НСД Dallas Lock Linux**. Данные правила МЭ доступны для редактирования и удаления.

В случае, если у разрешающего и запрещающего правил одинаковый приоритет, то разрешающее правило будет иметь приоритет над запрещающим.

Необходимо обратить внимание, что при задании разрешающего правила (*pass*) высокого приоритета с указанием протокола L7 и одновременным заданием запрещающего правила (*reject*) на протокол TCP с более низким приоритетом – первым будет срабатывать правило на блокировку TCP, т.к. будет сразу заблокирован сетевой пакет установки TCP-соединения, и обмен данным (при котором определяется принадлежность сетевого пакета к заданному протоколу L7) не произойдет.

После нажатия кнопки  «**Создать правило**» в рабочей области в категории «**Правила МЭ**» будет размещено новое правило межсетевого экрана (см. Рисунок 91). Созданное новое правило МЭ будет иметь следующие атрибуты по умолчанию:

- «№» — идентификационный номер строки правила межсетевого экрана;
- «Приоритет» — параметр позволяет настроить, в какой последовательности будут обрабатываться правила МЭ. Принимает значение: от 1 до 255. Пакеты обрабатываются по правилам согласно их приоритету. Наивысший приоритет — 1. По умолчанию установлено значение — 128;
- «Описание» — дополнительная информация по правилу. Максимальное количество символов: 128. Является обязательным атрибутом.
- «Профиль» — доступные профили проверок на выбор пользователя. По умолчанию установлено значение – *Default.* Перед выбором другого профиля правил МЭ необходимо убедиться, что он зарегистрирован в системе, подробнее — в разделе Вывод настроенных профилей МЭ;
- «Действие» — операции, выполняемые при фильтрации сетевых пакетов, для которых действует правило. Является обязательным атрибутом. Принимает значение: *pass* — пропустить сетевой пакет; *reject* — отклонить сетевой пакет. По умолчанию установлено значение *pass*;

- «Направление» — направление сетевого трафика, для которого действует правило. Принимает значение: *out* — правило для исходящего сетевого трафика; *inout* — направление сетевого трафика не указано. Значение, выставленное по умолчанию *inout*;
- «Протокол» — тип сетевого или транспортного протокола, на основании которого осуществляется фильтрация сетевых пакетов. Является обязательным атрибутом. Доступны следующие значения:
  - *tcp;*
  - *udp;*
  - *icmp;*
  - *ip.*
- «L7» — тип прикладного протокола, для которого действует правило. По умолчанию значение параметра отсутствует.
  При выборе протокола *tcp* доступны следующие прикладные протоколы:
  - *http;*
  - *ftp;*
  - *imap;*
  - *pop3;*
  - *smtp;*
  - *telnet;*
  - *dns;*
  - *ssh.*

  При выборе протокола *udp* доступны следующие прикладные протоколы:
  - *dns;*
  - *ntp.*
- «Команда» — команды прикладного протокола, для которого действует правило. Команду можно будет задать, только если задан прикладной протокол. Принимает следующие значения:

  - Для ***smtp*:** ATRN, AUTH, BDAT, CHUNKING, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, ONEX, QUEU, QUIT, RCPT, RSET, SAML, SEND, SOML, STARTTLS, TICK, TIME, TURN, TURNME, VERB, VRFY, X-ADAT, X-DRCP, X-ERCP, X-EXCH50, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN, XUSR, пустое значение;
  - Для ***ftp*:** ABOR, ACCT, ADAT, ALLO, APPE, AUTH, CCC, CDUP, CEL, CLNT, CMD, CONF, CWD, DELE, ENC, EPRT, EPSV, ESTA, ESTP, FEAT, HELP, LANG, LIST, LPRT, LPSV, MACB, MAIL, MDTM, MIC, MKD, MLSD, MLST, MODE, NLST, NOOP, OPTS, PASS, PASV, PBSZ, PORT, PROT, PWD, QUIT, REIN, REST, RETR, RMD, RNFR, RNTO, SDUP, SITE, SIZE, SMNT, STAT, STOR, STOU, STRU, SYST, TEST, TYPE, USER, XCUP, XCRC, XCWD, XMAS, XMD5, XMKD, XPWD, XRCP, XRMD, XRSQ, XSEM, XSEN, XSHA1, XSHA256, пустое значение;

  - Для ***imap*:** APPEND, AUTHENTICATE, CAPABILITY, CHECK, CLOSE, COMPARATOR, COMPRESS, CONVERSIONS, COPY, CREATE, DELETE, DELETEACL, DONE, EXAMINE, EXPUNGE, FETCH, GETACL, GETMETADATA, GETQUOTA, GETQUOTAROOT, IDLE, LIST, LISTRIGHTS, LOGIN, LOGOUT, LSUB, MYRIGHTS, NOOP, NOTIFY, RENAME, SEARCH, SELECT, SETACL, SETMETADATA, SETQUOTA, SORT, STARTTLS, STATUS, STORE, SUBSCRIBE, THREAD, UID, UNSELECT, UNSUBSCRIBE, X, пустое значение;

  - Для ***pop*:** APOP, AUTH, CAPA, DELE, LIST, NOOP, PASS, QUIT, RETR, RSET, STAT, STLS, TOP, UIDL, USER, пустое значение;

  - Для ***dns*:** A, AAAA, CNAME, SRV, TXT, MX, SOA, NS, PTR, пустое значение.

- «Маска» — маска фильтра сетевого трафика на основе прямого соответствия содержимому сетевого пакета. Максимальное количество символов — 65536. По умолчанию значение параметра отсутствует.
- «Мобильный код» — фильтрация сетевого трафика на основе наличия в сетевом пакете мобильного кода. Принимает значение: *flash, javascript, pdf, vbscript*. По умолчанию значение параметра отсутствует.
- «Адрес источника» — IP-адрес отправителя. Принимает следующее значения:
  - IPv4 — четвёртая версия интернет-протокола (IP). Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети.

–IPv6 — новая версия интернет-протокола. Длина адреса IPv6 составляет 128 бит, как и маска подсети. Диапазон адресов IPv6 составляет от 0000:0000:0000:0000:0000:0000:0000:0000 до FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Помимо обычного формата, адреса IPv6 могут быть представлены в двух других форматах:

a. Адрес IPv6 записывается с пропуском начальных нулей.
b. В адресе IPv6 на месте нескольких нулей ставится двойное двоеточие (::).

По умолчанию установлено значение *any*.

- «Порт источника» — порт отправителя. Принимает значение: от 0 до 65535. Допустимы следующие форматы записи: 1121:1256 (от и до), разделенный двоеточием, 1234, 1245 (перечисление), 1234:1238, 1267 (комбинированный вариант). По умолчанию установлено значение *any*.
- «Адрес назначения» — IP-адрес получателя. Принимает следующие значения:

  –IPv4 — четвёртая версия интернет-протокола (IP). Традиционной формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети.

  –IPv6 — новая версия интернет-протокола. Длина адреса IPv6 составляет 128 бит, как и маска подсети. Диапазон адресов IPv6 составляет от 0000:0000:0000:0000:0000:0000:0000:0000 до FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Помимо обычного формата, адреса IPv6 могут быть представлены в двух других форматах:

  a. Адрес IPv6 записывается с пропуском начальных нулей.
  b. В адресе IPv6 на месте нескольких нулей ставится двойное двоеточие (::).

  По умолчанию установлено значение *any*
- «Порт назначения» — порт получателя. Принимает значение: от 0 до 65535. Допустимы следующие форматы записи: 1121:1256 (от и до), разделенный двоеточием, 1234, 1245 (перечисление), 1234:1238, 1267 (комбинированный вариант). По умолчанию установлено значение *any*.
- «Аудит» — регистрация событий в журнале, возникающих при срабатывании правила МЭ. Принимает значения: выключено — регистрация событий производиться не будет; включено — регистрация событий производится. По умолчанию установлено значение *выключено*.
- «Автоблок» — блокировка нарушителей, возникающая при кратном срабатывании правил. Принимает значения: выключено — автоблокировка выключена; включено — автоблокировка включена. По умолчанию установлено значение *выключено*. Данный параметр работает только для запрещающих правил, на разрешающие правила оно не влияет.
  Если в атрибуте «Действия» установлено значение *pass*, параметр «Автоблок» будет недоступен.

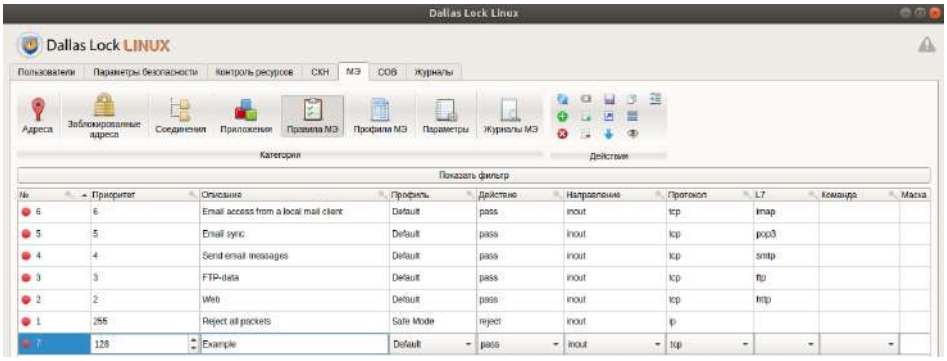


Рисунок 91. Созданное новое правило межсетевого экрана

4.11.2.2 Редактирование правила межсетевого экрана

Консольная оболочка администрирования

Для изменения правила межсетевого экрана необходимо в консольной оболочке администрирования в разделе *firewall* выполнить команду *change-rule*. После ввода команды система перейдет в подменю *change-rule*, где необходимо задать параметры правила, которые нужно изменить, используя атрибуты, приведенные в Таблица 50.

Таблица 50

№	Атрибут	Описание
1	*id <число>*	Указание идентификационного номера правила МЭ, которое необходимо изменить. Является обязательным атрибутом **Принимает значения:** от 1 до 65535
2	*profile <значение>*	Редактирование наименования профиля, который будет включать в себя настраиваемое правило. Является обязательным атрибутом
3	*action <значение>*	Изменение операции, выполняемой при фильтрации сетевых пакетов, для которых действует правило. Является обязательным атрибутом. **Принимает значения:** – *pass* – пропустить сетевой пакет; – *reject* – отклонить сетевой пакет (при выборе значения отправителю сообщается о недоступности запрашиваемого сервиса)
4	*protocol <значение>*	Изменение типа сетевого или транспортного протокола, на основании которого осуществляется фильтрация сетевых пакетов. Является обязательным атрибутом. **Принимает значения:** – *tcp;* – *udp;* – *icmp;* – *ip*
5	*scr_addrs <значение>*	Изменение IP-адреса отправителя. Параметр включает локальные адреса, маски подсети или IP-адреса подсетей и диапазон IP-адресов, для которых действует правило. При вводе нескольких адресов необходимо разделить их символом «,». Для задания диапазона адресов используется сетевая маска в формате CIDR и символ «/»
6	*dst_addrs <значение>*	Изменение IP-адреса получателя. Параметр включает локальные адреса, маски подсети или IP-адреса подсетей и диапазон IP-адресов, для которых действует правило. При вводе нескольких адресов необходимо разделить их символом «,». Для установки диапазона адресов используется сетевая маска в формате CIDR и символ «/»
7	*scr_ports <значение>*	Изменение порта отправителя. Параметр включает список локальных портов или диапазонов портов, для которых действует правило. **Принимает значения:** от 0 до 65535. При вводе нескольких номеров портов необходимо разделить их символом «,». Для разделения диапазона портов используется символ «:»
8	*dst_ports <значение>*	Изменение порта получателя. Параметр включает список локальных портов или диапазон портов, для которых действует правило. **Принимает значения:** от 0 до 65535. При вводе нескольких номеров портов необходимо разделить их символом «,». Для разделения диапазона портов используется символ «:»

№	Атрибут	Описание
9	*direction <значение>*	Настройка направления сетевого трафика, для которого действует правило. **Принимает значения:** – *out* – правило для исходящего сетевого трафика; – *inout* – направление сетевого трафика не указано. По умолчанию устанавливается значение *inout*
10	*message <значение>*	Параметр позволяет изменить описание правила. Описание правила МЭ должно заключаться в двойные кавычки. Является обязательным атрибутом
11	*priority <число>*	Изменение последовательности обработки правил. **Принимает значения:** от 1 до 255. Пакеты будут обрабатываться по правилам согласно их приоритету. Наивысший приоритет — 1. По умолчанию правилу присваивается низший приоритет — 255
12	*content <значение>*	Изменение маски фильтра сетевого трафика на основе прямого соответствия содержимому сетевого пакета. Строка маски должна заключаться в двойные кавычки.
13	*mobile_code <значение>*	Изменение маски фильтра сетевого трафика на основе наличия в сетевом пакете мобильного кода. **Принимает значения:** – *flash;* – *javascript;* – *pdf;* – *vbscript*
14	*service <значение>*	Изменение типа прикладного протокола, для которого действует правило. **Принимает значения:** – *http;* – *ftp;* – *imap;* – *pop3;* – *smtp;* – *telnet;* – *dns;* – *ntp;* – *ssh*
15	*app_cmd <значение>*	Изменение команды прикладного протокола, для которого действует правило. Значение параметра можно задать, если задан прикладной протокол. **Принимает значения:** Для ***http:*** GET, POST, PUT, SEARCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, NOTIFY, POLL, BCOPY, BDELETE, BMOVE, LINK, UNLINK, OPTIONS, HEAD, DELETE, TRACE, TRACK, CONNECT, SOURCE, SUBSCRIBE, UNSUBSCRIBE, PROPFIND, PROPPATCH, BPROPFIND, BPROPPATCH, RPC_CONNECT, PROXY_SUCCESS, BITS_POST, CCM_POST, SMS_POST, RPC_IN_DATA, RPC_OUT_DATA, RPC_ECHO_DATA. Для ***smtp:*** ATRN, AUTH, BDAT, CHUNKING, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, ONEX, QUEU, QUIT, RCPT, RSET, SAML, SEND, SOML, STARTTLS, TICK,

№	Атрибут	Описание
		TIME, TURN, TURNME, VERB, VRFY, X-ADAT, X-DRCP, X-ERCP, X-EXCH50, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN, XUSR Для ***ftp:*** ABOR, ACCT, ADAT, ALLO, APPE, AUTH, CCC, CDUP, CEL, CLNT, CMD, CONF, CWD, DELE, ENC, EPRT, EPSV, ESTA, ESTP, FEAT, HELP, LANG, LIST, LPRT, LPSV, MACB, MAIL, MDTM, MIC, MKD, MLSD, MLST, MODE, NLST, NOOP, OPTS, PASS, PASV, PBSZ, PORT, PROT, PWD, QUIT, REIN, REST, RETR, RMD, RNFR, RNTO, SDUP, SITE, SIZE, SMNT, STAT, STOR, STOU, STRU, SYST, TEST, TYPE, USER, XCUP, XCRC, XCWD, XMAS, XMD5, XMKD, XPWD, XRCP, XRMD, XRSQ, XSEM, XSEN, XSHA1, XSHA256. Для ***imap:*** APPEND, AUTHENTICATE, CAPABILITY, CHECK, CLOSE, COMPARATOR, COMPRESS, CONVERSIONS, COPY, CREATE, DELETE, DELETEACL, DONE, EXAMINE, EXPUNGE, FETCH, GETACL, GETMETADATA, GETQUOTA, GETQUOTAROOT, IDLE, LIST, LISTRIGHTS, LOGIN, LOGOUT, LSUB, MYRIGHTS, NOOP, NOTIFY, RENAME, SEARCH, SELECT, SETACL, SETMETADATA, SETQUOTA, SORT, STARTTLS, STATUS, STORE, SUBSCRIBE, THREAD, UID, UNSELECT, UNSUBSCRIBE, X. Для ***pop3:*** APOP, AUTH, CAPA, DELE, LIST, NOOP, PASS, QUIT, RETR, RSET, STAT, STLS, TOP, UIDL, USER. Для ***dns:*** A, AAAA, CNAME, SRV, TXT, MX, SOA, NS, PTR
16	*enable <значение>*	Параметр позволяет изменить статус правила. **Принимает значения:** *yes* – правило включено, *no* – правило отключено. По умолчанию установлено значение *no*
17	*audit <значение>*	Управление регистрацией событий в журнале, возникающих при срабатывании правила. **Принимает значения:** *yes* – регистрация событий включена, *no* – регистрация событий отключена. По умолчанию установлено значение *no*
18	*auto_block <значение>*	Включение/выключение автоматической блокировки адреса при кратном срабатывании правила с данным адресом. **Принимает значения:** *yes* – автоблокировка включена, *no* – автоблокировка выключена. По умолчанию установлено значение *yes*
19	*clear <значение>*	Команда для очистки следующих настраиваемых параметров: – *content;* – *mobile_code;* – *service;* – *app_cmd*

Пример:

firewall <enter>
change-rule <enter>
id 10 <enter>
app_cmd POST <enter>

message “Reject all POST-requests to example.com”

audit no <enter>

execute <enter>

Rule 10 was successfully changed

Изменено правило для блокирования GET-запросов, отправляемых на ресурс example.com. Выключено журналирование, команда прикладного протокола изменена с GET на POST, изменено сообщение.

Графическая оболочка администрирования

Для изменений правил МЭ в графической оболочке администрирования необходимо на вкладке «**МЭ**» в категории «**Правила МЭ**» в общем списке правил МЭ выделить необходимое правило и двойным кликом левой кнопки мыши запустить режим редактирования (см. Рисунок 91). Параметры правила МЭ для изменений в графической оболочке администрирования соответствуют параметрам правил в консольной оболочке администрирования.

Для редактирования доступны следующие параметры правила МЭ:

- Приоритет.
- Профиль.
- Действие.
- Направление.
- Протокол.
- L7.
- Команда.
- Маска.
- Мобильный код.
- Адрес источника.
- Порт источника.
- Адрес назначения.
- Порт назначения.
- Аудит.
- Автоблок.
- Описание.

Для сохранения всех настроенных параметров правила МЭ необходимо нажать на кнопку  «**Сохранить**» на панели действий.

4.11.2.3 Удаление правила межсетевого экрана

Консольная оболочка администрирования

Для удаления правила межсетевого экрана необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *remove-rule* с указанием идентификационного номера правила МЭ, которое необходимо удалить.

Пример:

firewall <enter>

remove-rule 2 <enter>

Rule 2 was successfully removed

Правило 2 было успешно удалено

Графическая оболочка администрирования

Для удаления правила МЭ в графической оболочке администрирования необходимо на вкладке «**МЭ**» в категории «**Правила МЭ**» в общем списке правил МЭ выделить необходимое правило и нажать на кнопку  «**Удалить**» на панели действий. После выполненных действий цвет выделения правила станет красным (см. Рисунок 92).

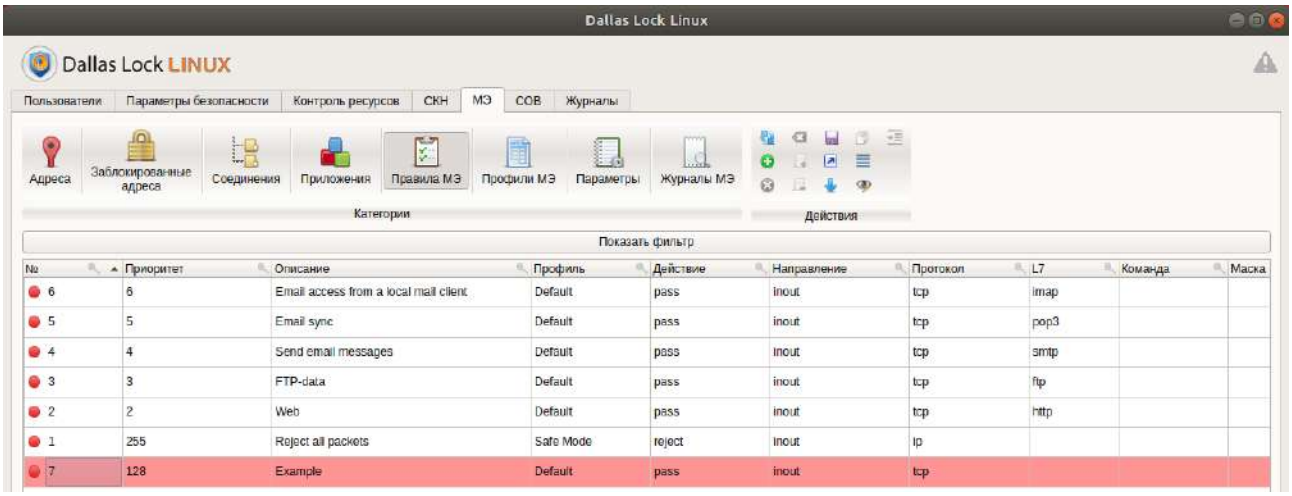


Рисунок 92. Удаление правила межсетевого экрана

Для сохранения выполненных действий необходимо нажать на кнопку «**Сохранить**» на панели действий.

4.11.2.4 Вывод правила межсетевого экрана

Консольная оболочка администрирования

Для вывода и просмотра определенного правила МЭ необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном *firewall* набрать команду *show-rule* с указанием идентификационного номера правила, информацию которого нужно просмотреть.

Пример:

firewall <enter>

show-rule 10 <enter>

При успешном завершении запроса в консольной оболочке администрирования будет выведено правило межсетевого экрана со всеми установленными ему параметрами.

Для вывода всех настроенных и имеющихся правил межсетевого экрана в консоль необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном *firewall* набрать команду *list-rules*

Пример:

firewall <enter>

list-rules <enter>

Графическая оболочка администрирования

Для просмотра всех настроенных правил межсетевого экрана с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» перейти в категорию «**Правила МЭ**». На рабочей области текущей категории будут представлены все на данный момент настроенные правила межсетевого экрана (см. Рисунок 93).

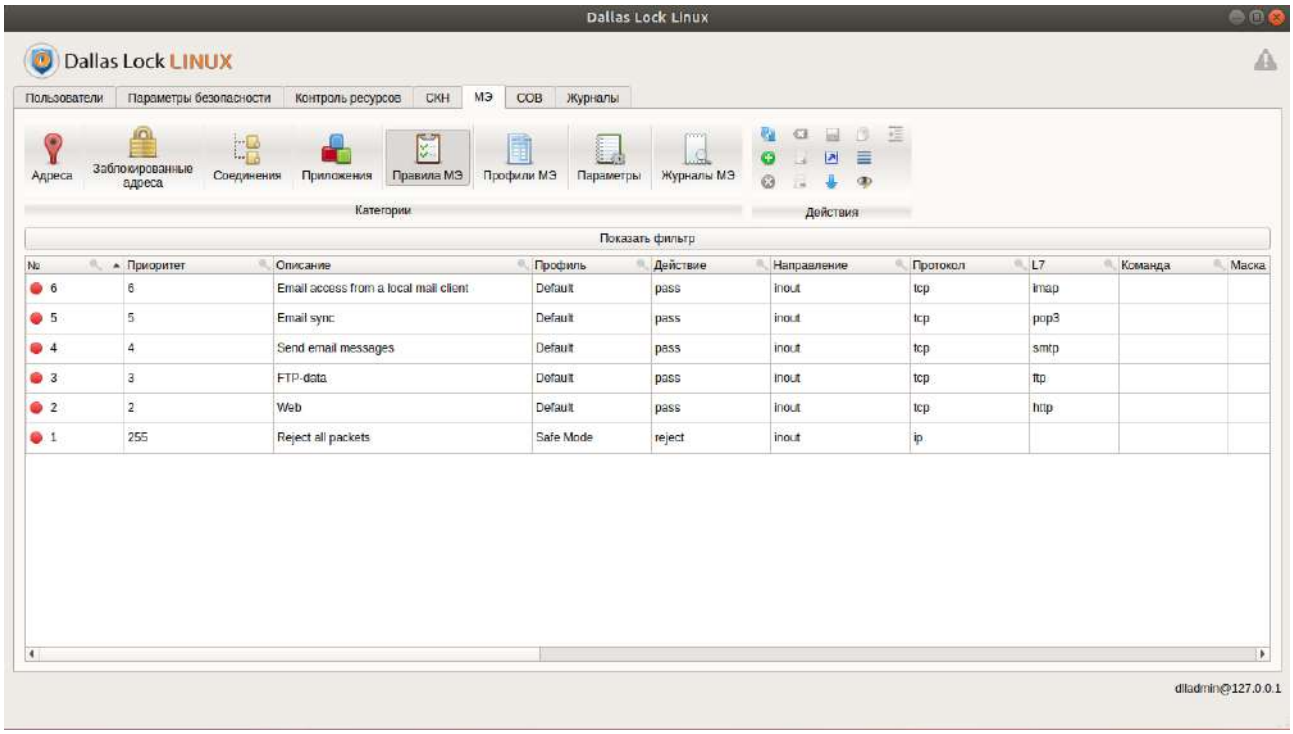


Рисунок 93. Список настроенных правил МЭ

В системе реализована настройка отображаемых столбцов, что позволяет исключить из вида некоторые столбцы параметров правил МЭ. Для этого необходимо нажать на кнопку  «**Настройка отображаемых столбцов**» на панели действий. Далее откроется окно «**Настройка отображаемых столбцов**» (см. Рисунок 94).

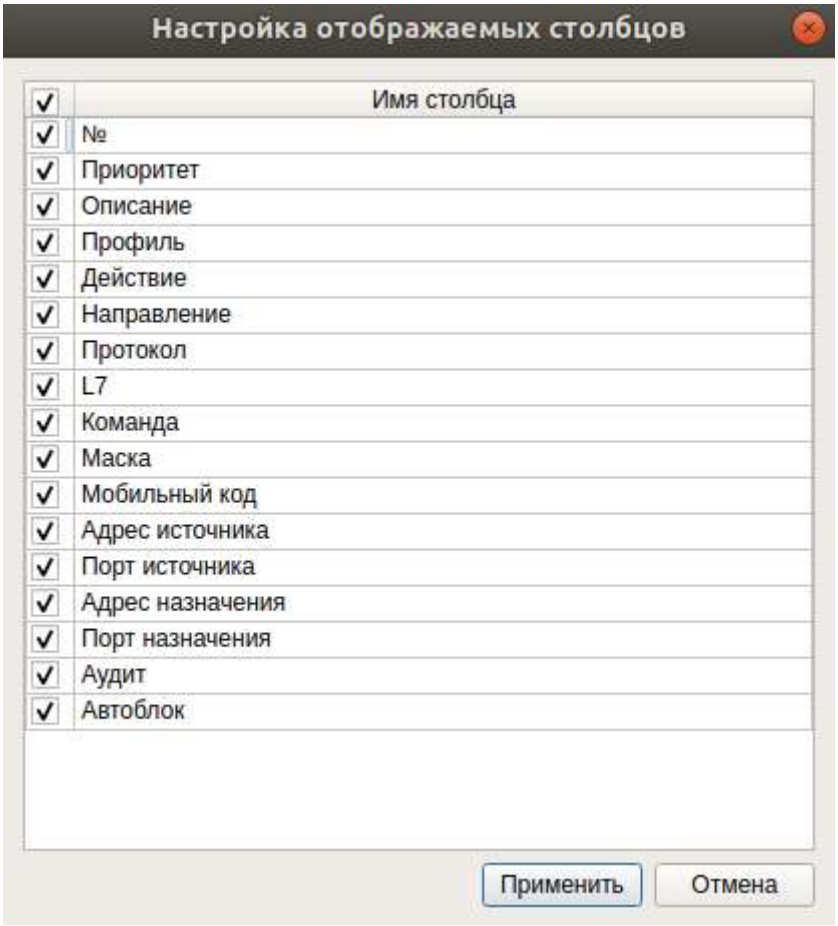


Рисунок 94. Окно «Настройка отображаемых столбцов»

После того как были исключены или добавлены из вида столбцы параметров правил категории «Правила МЭ» необходимо для подтверждения операции нажать кнопку «**Применить**». Для отмены действий — «**Отмена**».

В случае если у Администратора будет скрыт из вида столбец обязательного атрибута при настройке правила МЭ, то сохранить данное правило не удастся, так как оно будет не заполнено.

4.11.2.5 Экспорт правил

Консольная оболочка администрирования

Для экспорта правил межсетевого экрана из базы данных в файл необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *export- rules* с указанием полного пути до файла. Файл должен быть доступен для записи. Правила межсетевого экрана записываются в файл в формате json.

Пример:

firewall <enter>

export-rules /home/user/rules <enter>

Request successfully completed

Графическая оболочка администрирования

Для экспорта правил межсетевого экрана из базы данных с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» в категории «**Правила МЭ**» нажать на кнопку  «**Экспортировать**» на панели действий. Далее в открывшемся окне «**Экспорт правил**» в поле «*Каталог*» указать полный путь до файла для записи. В поле «*Имя*» ввести наименование файла. Нажать кнопку «**Экспорт**» для экспорта правил МЭ или кнопку «**Отмена**» для отмены операции экспорта (см. Рисунок 95).

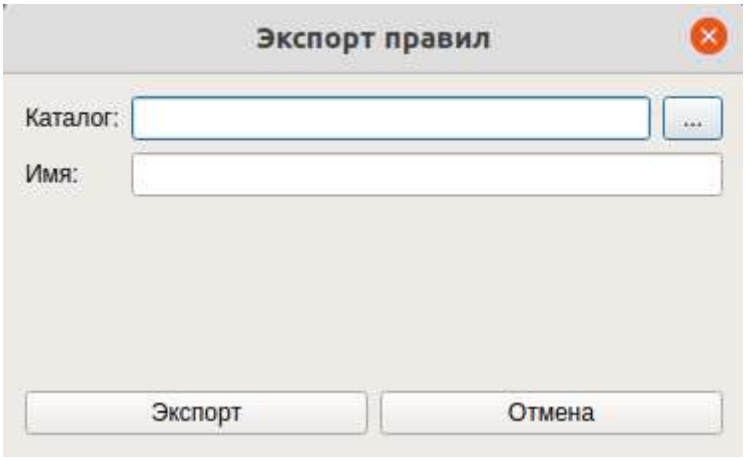


Рисунок 95. Окно «Экспорт правил»

4.11.2.6 Импорт правил

Консольная оболочка администрирования

Для импорта правил МЭ из файла в базу данных необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *import-rules* с указанием полного пути до файла. Файл должен быть доступен для чтения. Правила в файле должны быть записаны в формате json.

Пример:

firewall <enter>

import-rules /home/user/rules <enter>

Request successfully completed

Графическая оболочка администрирования

Для импорта правил межсетевого экрана в базу данных с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» в категории «**Правила МЭ**» нажать на кнопку «Загрузить» на панели действий. Далее в открывшемся окне «Выберите файл для импорта правил» в поле «*Субъект*» указать полный путь до файла для записи. Нажать кнопку «**ОК**» для импорта правил МЭ или кнопку «**Отмена**» для отмены операции импорта (см. Рисунок 96).

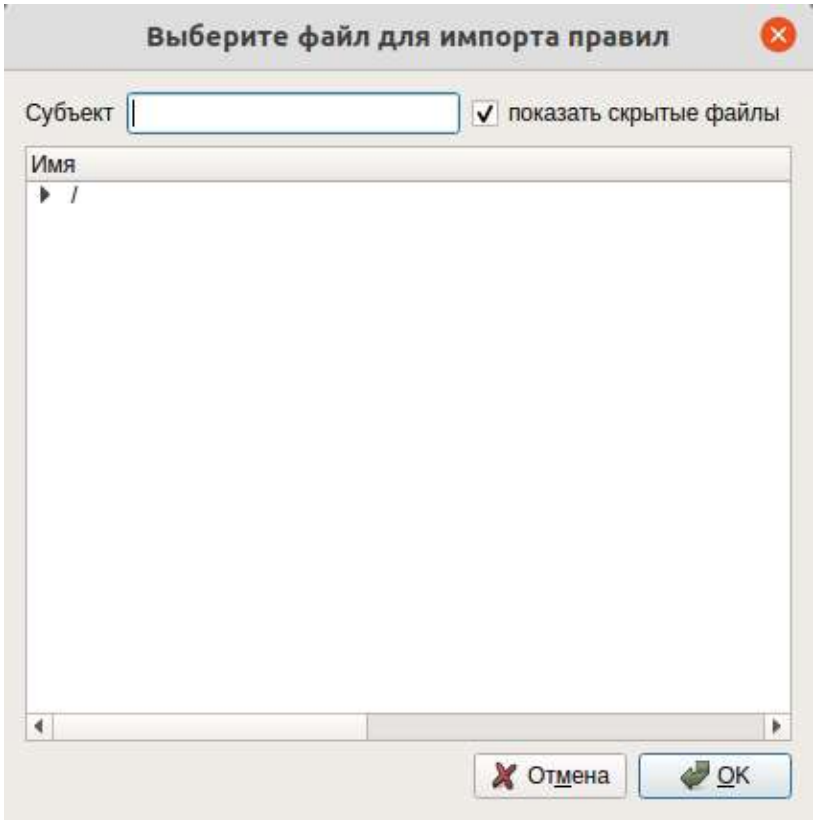


Рисунок 96. Окно «Выберите файл для импорта правил»

4.11.2.7 Вывод статистики сетевых соединений

Консольная оболочка администрирования

Соединения сервисов **СЗИ НСД Dallas Lock Linux** не отображаются в таблице соединений, чтобы Администратор не мог нарушить их работу, разорвав соединение.

Для вывода таблицы состояний сетевых соединений в консоль необходимо в консольной оболочке администрирования, в разделе управления межсетевым экраном, набрать команду *show-netstat.*

Пример:

firewall <enter>

show-netstat <enter>

Request completed successfully

	pid	user	command	state	type	protocol	source address	source port	destination address	destination port
1	41507	root	smbd	LISTEN	IPv4	TCP	0.0.0.0	SMB(139)	0.0.0.0	0
2	771	root	event-manager	LISTEN	IPv4	TCP	0.0.0.0	3889	0.0.0.0	0
3	539	systemd-resolve	systemd-resolve	LISTEN	IPv4	TCP	127.0.0.53	DNS(53)	0.0.0.0	0
4	39008	root	sshd	LISTEN	IPv4	TCP	0.0.0.0	SSH(22)	0.0.0.0	0
5	59963	root	cupsd	LISTEN	IPv4	TCP	127.0.0.1	631	0.0.0.0	0

Рисунок 97. Вывод статистики сетевых соединений

Графическая оболочка администрирования

Для просмотра состояний текущих соединений компьютера требуется на вкладке «**МЭ**» перейти в категорию «**Соединения**» (см. Рисунок 98).

Соединения сервисов **СЗИ НСД Dallas Lock Linux** не отображаются в таблице соединений, чтобы Администратор не мог нарушить их работу, разорвав соединение.

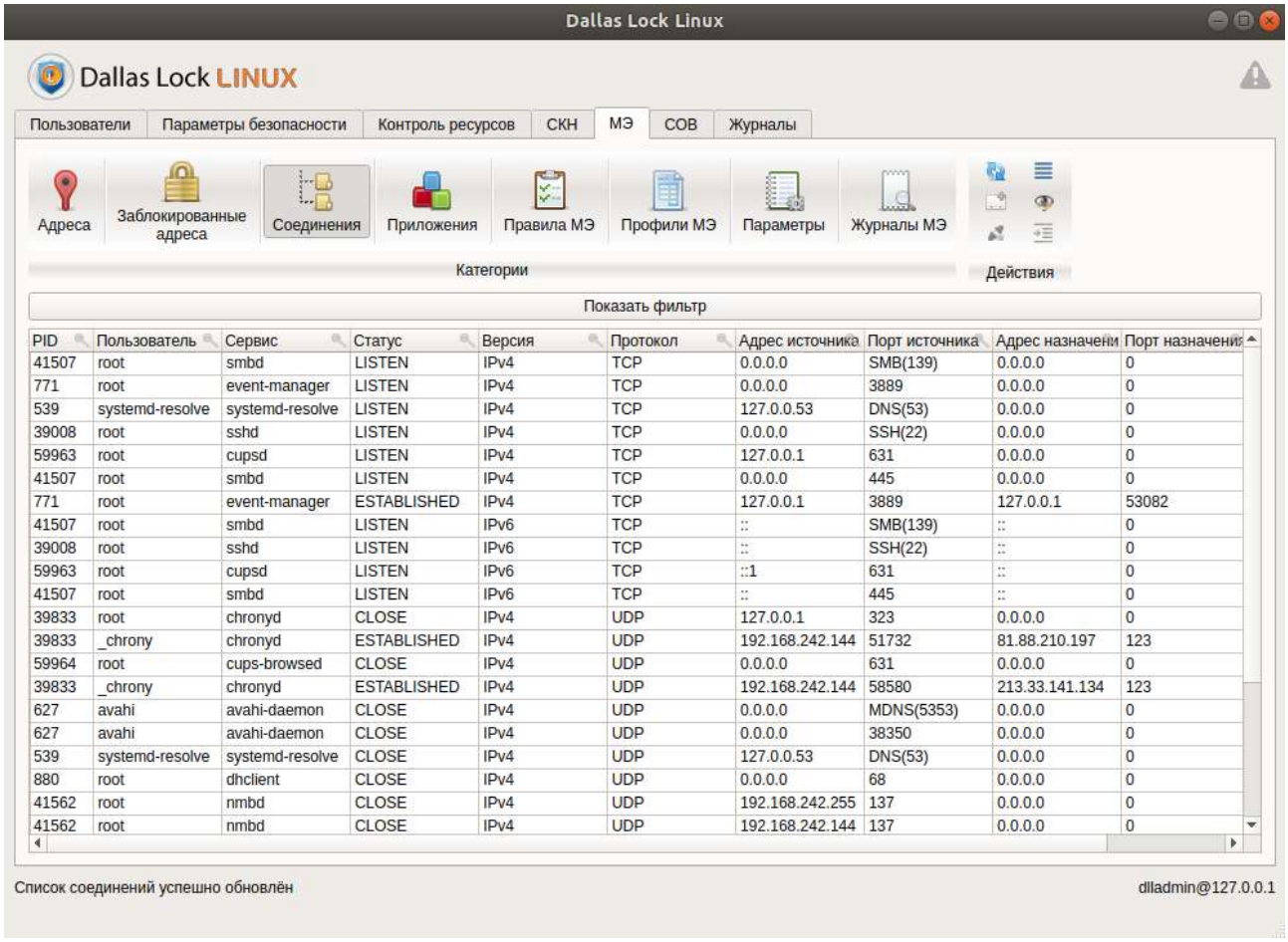


Рисунок 98. Сетевые соединения

На панели «Действия» в категории «**Соединения**» доступны следующие кнопки:

- Обновить – обновить список сетевых соединений.
- Выделить все строки .
- Создать правило МЭ – при нажатии кнопки «**Создать правило МЭ**» произойдет переход в категорию «**Правила МЭ**» для создания правила МЭ.
- Настройка отображаемых столбцов – настройка группировки столбцов.
- Разорвать соединение – прекратить обмен информацией. «Разорвать соединение» доступно только на версиях ядра 5.x.
- Отобразить в списке – отображение дополнительной информации сетевого соединения в списке.

4.11.3 Добавление приложений в черный список

Черный список приложений — список запрещенных приложений на АРМ (которые блокируются МЭ), все остальные приложения, не состоящие в списке, пропускаются МЭ.

Одновременно не могут быть включены оба списка приложений. Если включён чёрный список, то будет блокироваться весь трафик от приложений, которые включены в чёрный список, остальной трафик будет фильтроваться по правилам МЭ. Подробнее — Активация черного списка приложений.

Консольная оболочка администрирования

Категория «**Приложения**» позволяет администратору активировать фильтрацию трафика по прикладному ПО.

Для добавления приложения в черный список необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *set-blacklist-command*. После ввода команды система перейдет в раздел конструктора правил *set-blacklist-command*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 51.

Таблица 51

№	Атрибут	Описание
1	*command <значение>*	Указание приложения, которое необходимо добавить в черный список. Обязательный атрибут
2	*path <значение>*	Указание полного пути до исполняемого файла. Обязательный атрибут
3	*description <значение>*	Добавление описания приложения, которое нужно добавить в черный список. Описание должно быть заключено в двойные кавычки

Пример:

firewall <enter>
set-blacklist-command <enter>
command firefox <enter>
path /usr/lib64/firefox/firefox-bin <enter>
description “Firefox browser” <enter>
execute <enter>
Command was successfully added to blacklist

Графическая оболочка администрирования

Для добавления приложения в черный список с помощью графической оболочки **СЗИ НСД** на вкладке «**МЭ**» необходимо выбрать категорию «**Приложения**» и нажать на кнопку  «**Добавить**» на панели действий списка «Черный список».

Далее на рабочей области «Черный список» (см. Рисунок 99) появится новое правило черного списка, в которое нужно будет добавить приложение и внести соответствующие к нему атрибуты.

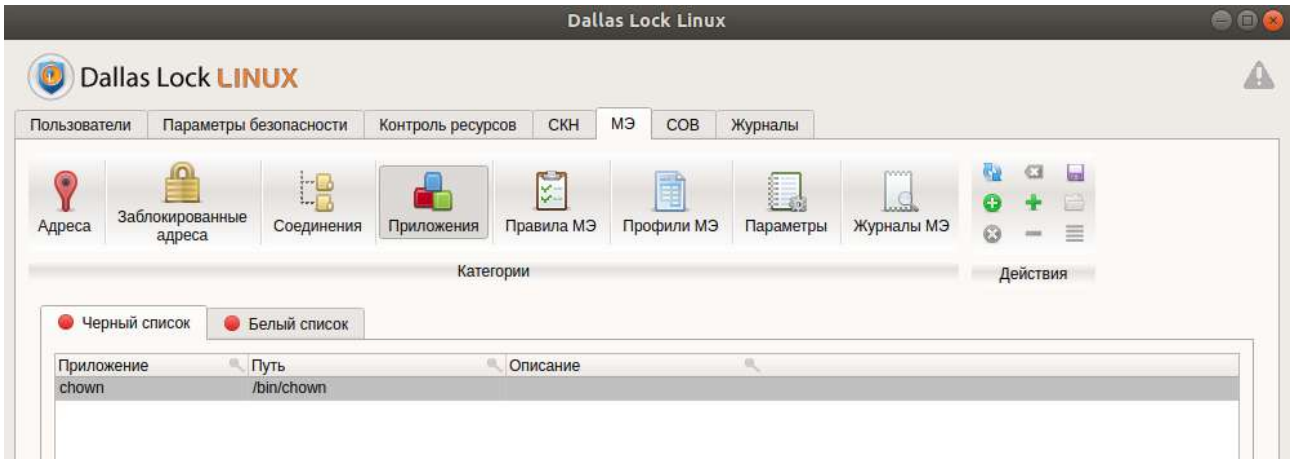


Рисунок 99. Новое правило «Черный список»

Новое правило для черного списка приложений содержит следующий список атрибутов:

- Приложение — имя приложения. Задается администратором. Максимальное количество символов: 32. Является обязательным атрибутом;
- Путь — полный путь в системе до приложения. В конечной папке должен располагаться исполняемый файл. Максимальное количество символов: 4096. Является обязательным атрибутом;
- Описание — дополнительная информация по правилу. Максимальное количество символов: 4096. По умолчанию поле остается пустым.

Необходимо указать полный путь до приложения, которое будет внесено в черный список, и его имя. Для указания пути нужно кликнуть на столбец «Путь» выделенного нового правила. Далее откроется форма «Выбрать путь к приложению» (см. Рисунок 100). В поле «Субъект» требуется прописать путь до исполняемого файла. При добавлении пути приложения система запросит подтверждение операции.

Для подтверждения операции — кнопка «**ОК**», для отмены действий — «**Отмена**».

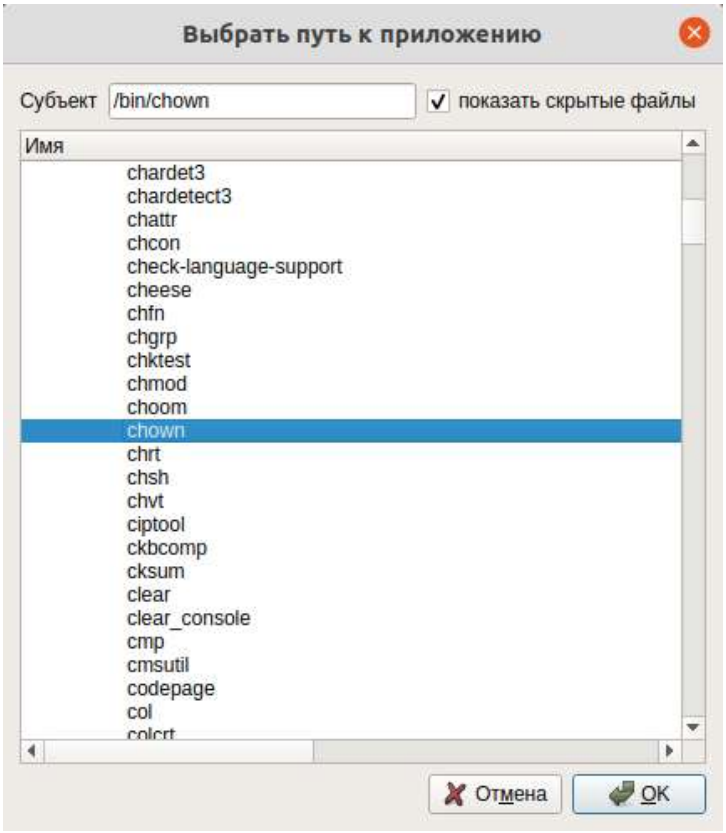


Рисунок 100. Окно «Выбрать путь к приложению»

Для добавления имени приложения нужно двойным кликом на столбец «Приложение» выделенного нового правила запустить режим редактирования и внести имя приложения черного списка (см. Рисунок 101).

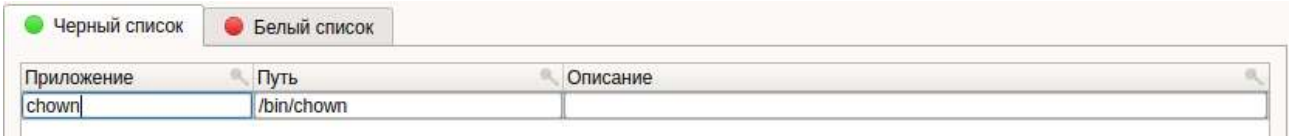


Рисунок 101. Имя приложения, внесенного в «Черный список»

Для добавления описания приложения нужно кликнуть на столбец «Описание» (см. Рисунок 102).

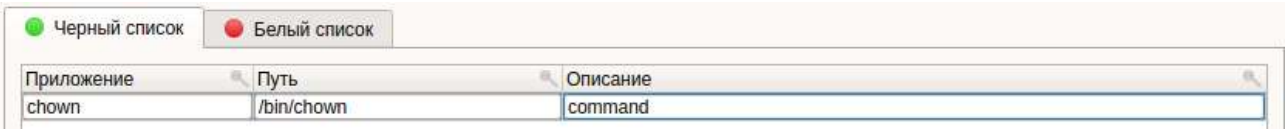


Рисунок 102. Описание приложения черного списка

После внесения всех обязательных параметров приложения для черного списка необходимо выделить настроенное правило и выбрать команду «**Сохранить**» на панели действий.

Для активации черного списка приложений необходимо нажать на кнопку «**Включить**» на панели действий, для деактивации — «**Выключить**».

4.11.3.1 Изменение параметров приложений черного списка

Консольная оболочка администрирования

Для изменения параметров приложения черного списка необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *change-blacklist-command*. После ввода команды система перейдет в раздел конструктора правил *change-blacklist-command*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 52.

Таблица 52

№	Атрибут	Описание
1	*id <значение>*	Идентификационный номер приложения черного списка. Обязательный атрибут
2	*command <значение>*	Указание имени приложения, которое необходимо изменить в черном списке. Обязательный атрибут
3	*path <значение>*	Указание пути до исполняемого файла. Обязательный атрибут
4	*description <значение>*	Редактирование описания приложения черного списка. Описание должно быть заключено в двойные кавычки

Пример:

firewall <enter>
change-blacklist-command <enter>
id 1 <enter>
path /usr/lib64/firefox/firefox <enter>
execute <enter>
Command 1 was successfully changed
Команда *firefox-bin* была изменена на команду *firefox*

Графическая оболочка администрирования

Для изменения параметров приложения в черном списке с помощью графической оболочки администратора необходимо на вкладке «**МЭ**» в категории «Приложения» в списке «Черный список»

выделить правило, в которое требуется внести изменения. Двойным кликом запустить режим редактирования требуемого параметра.

Для редактирования доступны следующие атрибуты приложения черного списка:

- приложение;
- путь;
- описание.

После изменений параметров приложения для черного списка необходимо сохранить выполненные действия, выполнив команду «**Сохранить**» на панели действий.

4.11.3.2 Удаление приложений из черного списка

Консольная оболочка администрирования

Для удаления приложения из черного списка необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *remove-blacklist-command* с указанием идентификационного номера приложения в черном списке.

Пример:

firewall <enter>

remove-blacklist-command 1 <enter>

Command 1 was successfully removed from the blacklist

Графическая оболочка администрирования

Для удаления приложения из черного списка с помощью графической оболочки администрирования необходимо в категории «**Приложения**» в списке «Черный список» выделить правило и нажать кнопку «**Удалить**» на панели действий (см. Рисунок 103).

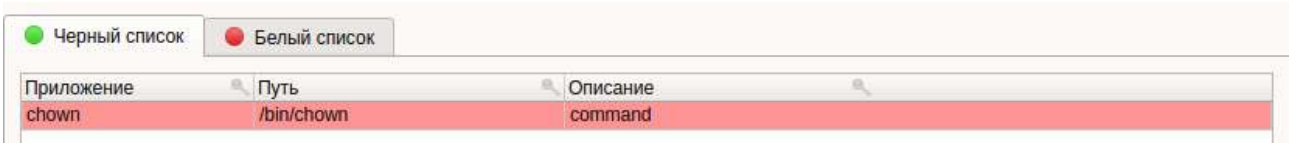


Рисунок 103. Удаление приложения из черного списка

После удаления приложения из черного списка необходимо сохранить выполненные действия, выполнив команду «**Сохранить**» на панели действий.

4.11.3.3 Вывод черного списка приложений

Консольная оболочка администрирования

Для вывода черного списка приложений в консоль необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном выполнить команду *show-commands-blacklist.*

```
firewall> show-commands-blacklist
Request successfully completed
```

	command	path	description
2	chown	/bin/chown	

Рисунок 104. Список запрещенных приложений

Графическая оболочка администрирования

Для просмотра всех правил черного списка приложений в графической оболочке администрирования необходимо перейти на вкладку «**МЭ**» в категорию «Приложения» и отрыть список «Черный список». На рабочей области текущего списка будут представлены все на данный момент приложения, занесенные в черный список (см. Рисунок 105).

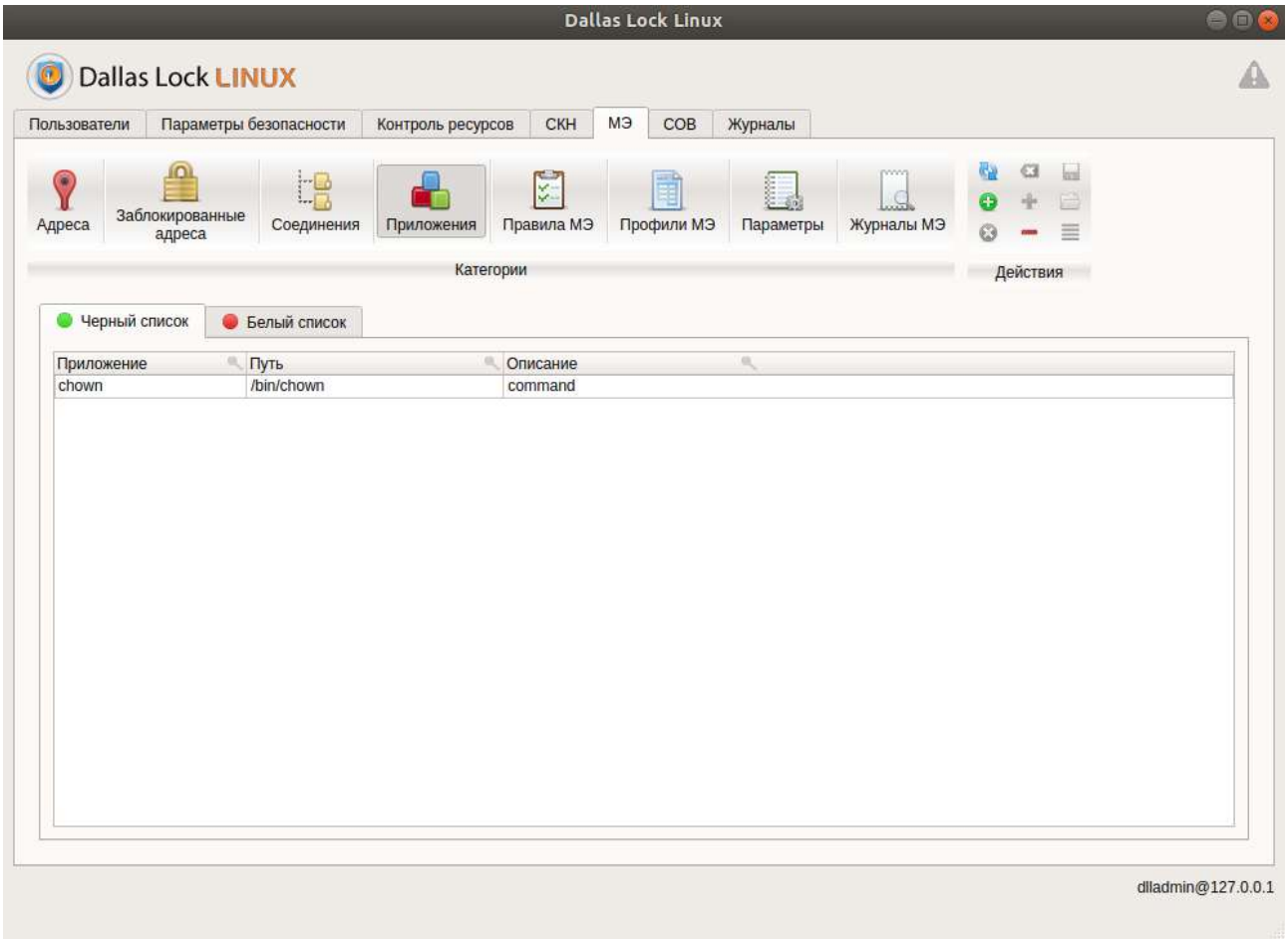


Рисунок 105. Вывод приложений черного списка

4.11.4 Добавление приложений в белый список

Белый список приложений – список разрешенных приложений на АРМ (приложения, имеющие доступ для обмена информацией). Соединения приложений, которые отсутствуют в белом списке, будут блокироваться.

Одновременно не могут быть включены оба списка приложений. Если включён белый список, то будет блокироваться трафик от всех приложений кроме тех, которые включены в белый список, трафик от приложений белого списка будет фильтроваться согласно правилам межсетевого экрана. Подробнее — Активация белого списка приложений.

Консольная оболочка администрирования

Для добавления приложения в белый список необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *set-whitelist-command*. После ввода команды система перейдет в раздел конструктора правил *set-whitelist-command*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 53.

Таблица 53

№	Атрибут	Описание
1	*command <значение>*	Указание имени приложения, которое необходимо добавить в белый список. Обязательный атрибут
2	*path <значение>*	Указание полного пути до исполняемого файла. Обязательный атрибут

№	Атрибут	Описание
3	*description <значение>*	Добавление описания приложения, которое нужно добавить в белый список. Описание должно быть заключено в двойные кавычки

Пример:

firewall <enter>
set-whitelist-command <enter>
command ping6 <enter>
path /usr/bin/ping6 <enter>
execute
Command was successfully added to whitelist

Графическая оболочка администрирования

Для добавления приложения в белый список с помощью графической оболочки **СЗИ НСД** на вкладке «МЭ» необходимо выбрать категорию «**Приложения**» и нажать на кнопку  «**Добавить**» на панели действий списка «Белый список».

Далее на рабочей области «Белый список» (см. Рисунок 106) появится новое правило белого списка, в которое нужно будет добавить приложение и настроить соответствующие ему атрибуты.

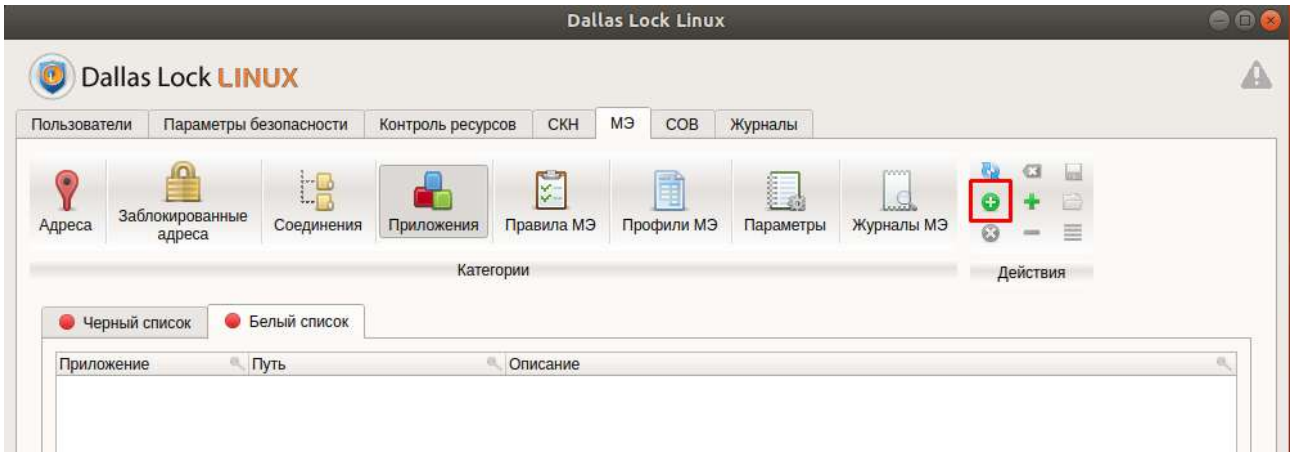


Рисунок 106. Новое правило «Белый список»

Новое правило для белого списка приложений содержит следующий список атрибутов:

- Приложение — наименование приложения. Задается администратором. Максимальное количество символов: 32. Является обязательным атрибутом;
- Путь — полный путь в системе до приложения. В конечной папке должен располагаться исполняемый файл. Максимальное количество символов: 4096. Является обязательным атрибутом;
- Описание — дополнительная информация по правилу. Максимальное количество символов: 4096. По умолчанию поле остается пустым.

Необходимо указать путь до приложения, которое будет внесено в белый список, и его имя. Для указания пути нужно кликнуть на столбец «Путь» выделенного нового правила. Далее откроется форма «**Выбрать путь к приложению**» (см. Рисунок 107). В поле «Субъект» требуется прописать путь до исполняемого файла. При добавлении пути приложения система запросит подтверждение операции.

Для подтверждения операции — кнопка «**ОК**», для отмены действий — «**Отмена**».

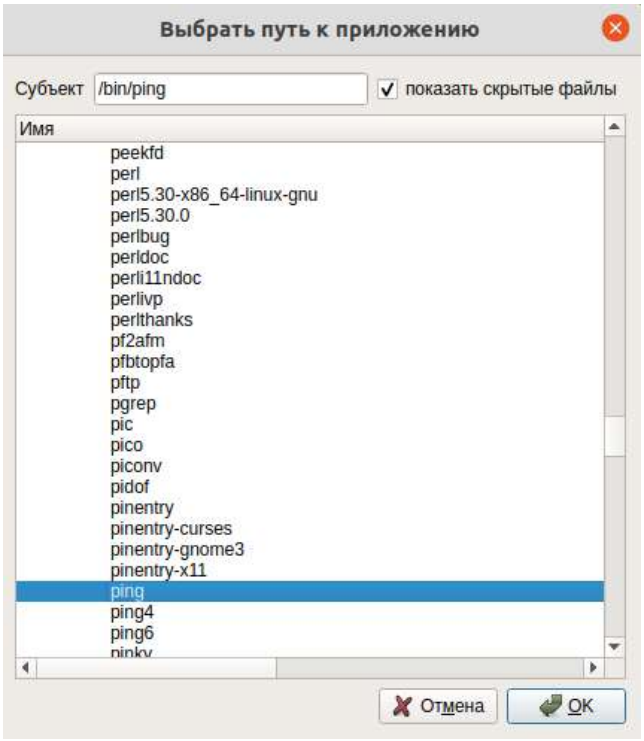


Рисунок 107. Окно «Выбрать путь к приложению»

Для добавления имени приложения нужно двойным кликом на столбец «Приложение» выделенного нового правила запустить режим редактирования и внести имя приложения белого списка (см. Рисунок 108).

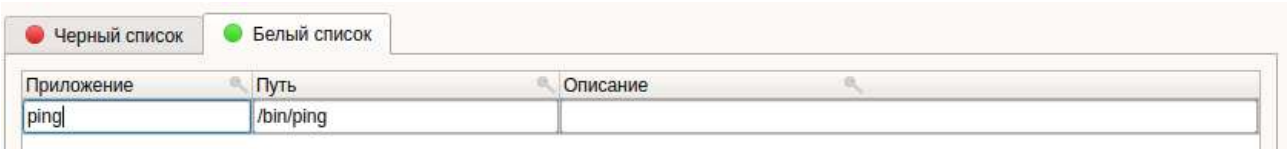


Рисунок 108. Имя приложения, внесенного в «Whitelist»

Для добавления описания приложения нужно кликнуть на столбец «Описание» (см. Рисунок 109).

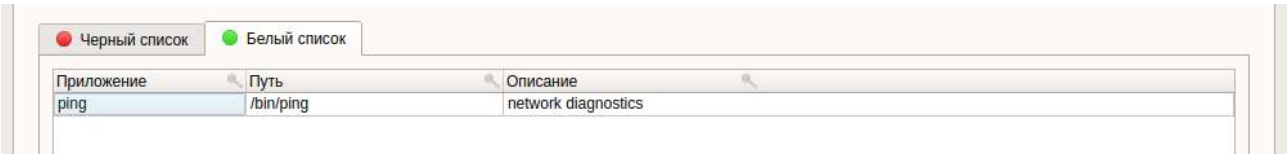


Рисунок 109. Описание приложения белого списка

После внесения всех атрибутов приложения для белого списка необходимо выделить настроенное правило и выбрать команду «**Сохранить**» на панели действий.

Для активации белого списка приложений необходимо нажать на кнопку «Включить» на панели действий, для деактивации — «**Выключить**».

4.11.4.1 Изменение параметров приложения белого списка

Консольная оболочка администрирования

Для изменения параметров приложения белого списка необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном выполнить команду *change-whitelist-command*. После ввода команды система перейдет в раздел конструктора правил *change-whitelist-command*, где необходимо задать параметры, используя атрибуты, представленные в Таблица 54.

Таблица 54

№	Атрибут	Описание
1	*id <значение>*	Идентификационный номер приложения белого списка. Обязательный атрибут
2	*command <значение>*	Указание имени приложения, которое необходимо изменить в белом списке. Обязательный атрибут
3	*path <значение>*	Указание пути до исполняемого файла. Обязательный атрибут
4	*description <значение>*	Редактирование описания приложения белого списка. Описание должно быть заключено в двойные кавычки

Пример:

firewall <enter>
change-whitelist-command <enter>
id 1 <enter>
description "Ping6 command" <enter>
execute <enter>
Command 1 was successfully changed
Было успешно изменено описание команды.

Графическая оболочка администрирования

Для изменения параметров приложения в белом списке с помощью графической оболочки администрирования необходимо на вкладке «**МЭ**» в категории «**Приложения**» в списке «Белый список» выделить правило, в которое требуется внести изменения. Двойным кликом запустить текстовую строку требуемого параметра для редактирования.

Для редактирования доступны следующие атрибуты приложения белого списка:

- приложение;
- путь;
- описание.

После изменений параметров приложения для белого списка необходимо сохранить выполненные действия, выполнив команду  «**Сохранить**» на панели действий.

4.11.4.2 Удаление приложения из белого списка

Консольная оболочка администрирования

Для удаления приложения из белого списка необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *remove-whitelist-command* с указанием идентификационного номера приложения в белом списке.

Пример:

firewall <enter>
remove-whitelist-command 1<enter>
Command 1 was successfully removed from the whitelist

Графическая оболочка администрирования

Для удаления приложения из белого списка с помощью графической оболочки администрирования необходимо в категории «**Приложения**» в списке «Белый список» выделить правило и нажать кнопку  «**Удалить**» на панели действий (см. Рисунок 110).

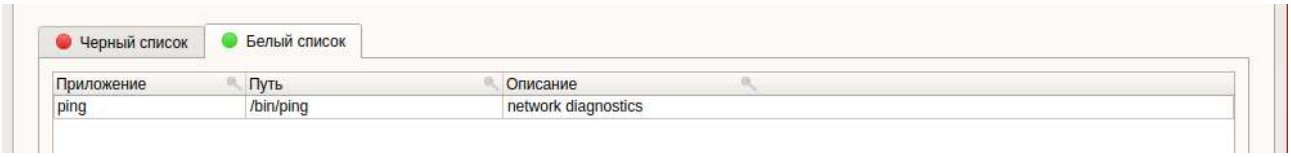


Рисунок 110. Удаление приложения из белого списка

После удаления приложения из белого списка необходимо сохранить выполненные действия, выполнив команду «**Сохранить**» на панели действий.

4.11.4.3 Вывод белого списка приложений

Консольная оболочка администрирования

Для вывода белого списка приложений в консоль необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *show-commands-whitelist* (Рисунок 111).

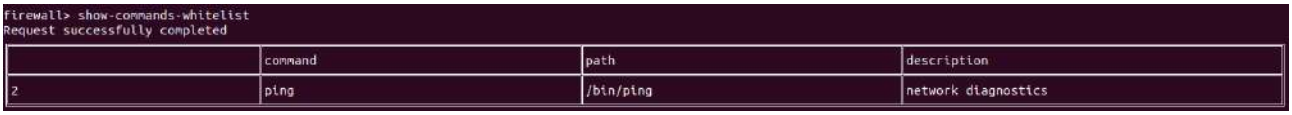


Рисунок 111. Список разрешенных приложений

Графическая оболочка администрирования

Для просмотра всех правил белого списка приложений в графической оболочке администрирования необходимо перейти на вкладку «**МЭ**» в категорию «**Приложения**» и отрыть список «Белый список». На рабочей области текущего списка будут представлены все на данный момент приложения, занесенные в белый список (см. Рисунок 112).

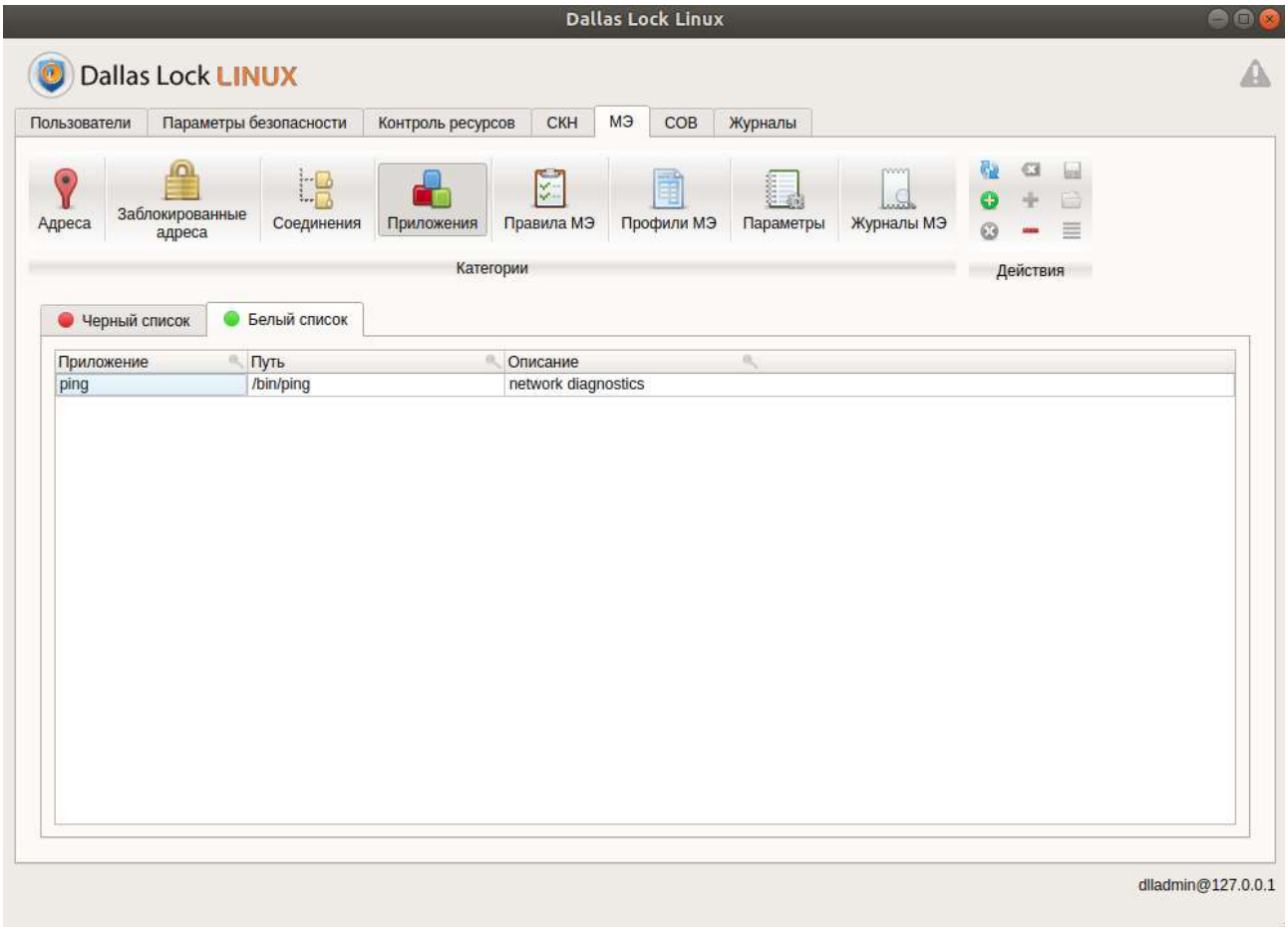


Рисунок 112. Вывод приложений белого списка

4.11.5 Вывод конфигурации адресов и интерфейсов АРМ

Консольная оболочка администрирования

Для вывода конфигурации адресов и интерфейсов АРМ в консольной оболочке администрирования необходимо в разделе управления межсетевым экраном выполнить команду *show-ifconfig* (Рисунок 113).

```
firewall> show-ifconfig
Request completed successfully
```

	version	address	interface
1	IPv4	127.0.0.1/8	lo
2	IPv4	192.168.242.144/24	ens33
3	IPv6	::1/128	lo
4	IPv6	fe80::42fa:d469:4916:fd5b/64	ens33

```
firewall>
```

Рисунок 113. Вывод конфигурации адресов и интерфейсов АРМ

Графическая оболочка администрирования

Для просмотра адресов с помощью графической оболочки администрирования необходимо перейти во вкладку «МЭ» в категорию «**Адреса**». Категория «**Адреса**» выдает информацию об активных интерфейсах АРМ. Рабочая область категории «**Адреса**» (см. Рисунок 114) содержит следующий список параметров:

- № — идентификационный номер адреса;
- Версия — версия интернет протокола. Принимает значения: IPv4 и IPv6;
- Адрес — локальный адрес АРМ;
- Описание — наименование сетевой точки для построения соединений.

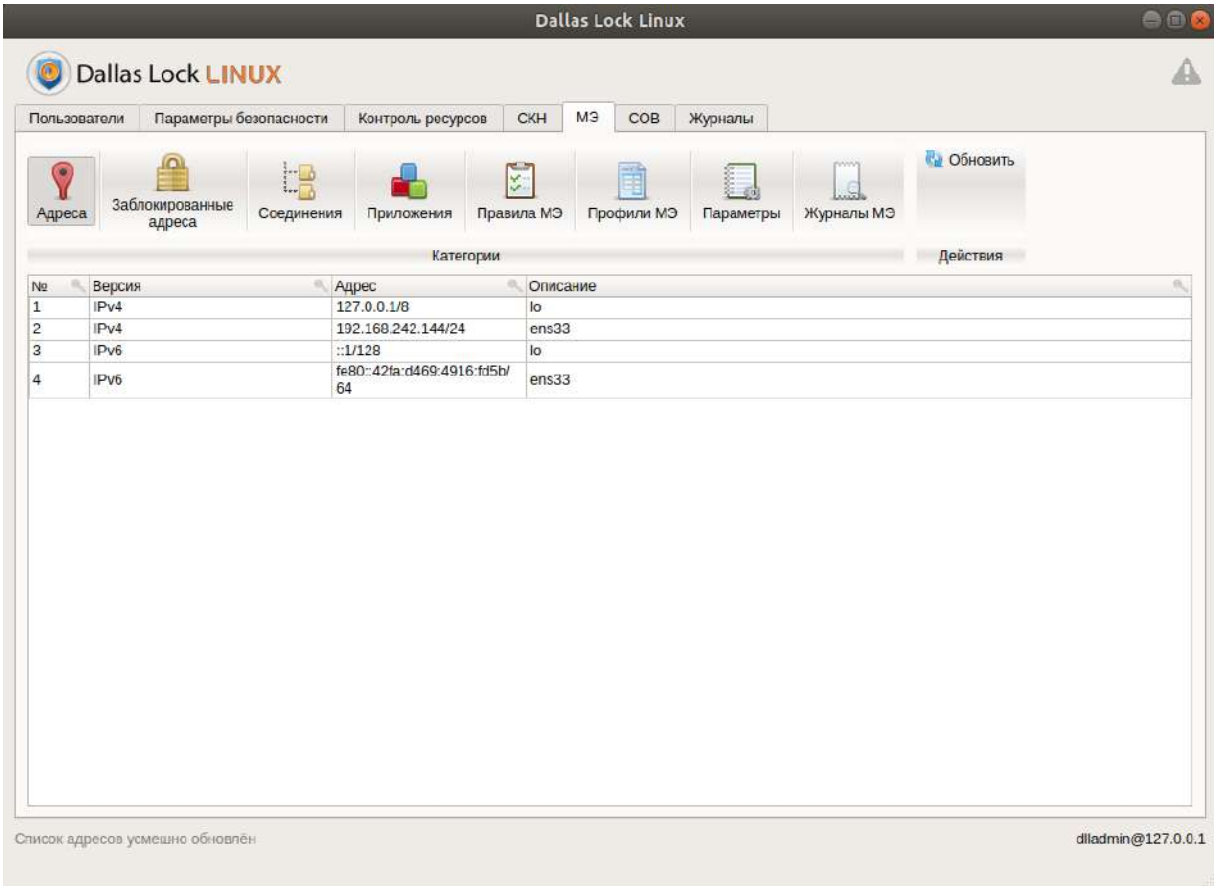


Рисунок 114. Адреса

4.11.6 Заблокированные адреса

Консольная оболочка администрирования

Для отмены блокировки адреса необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *unblock-address* с указанием идентификационного номера адреса из таблицы заблокированных адресов.

После разблокировки адреса счетчики для него обнуляются.

Пример:

firewall <enter>
unblock-address 1 <enter>
Request successfully completed

Графическая оболочка администрирования

Для просмотра заблокированных адресов требуется на вкладке «**МЭ**» перейти в категорию «**Заблокированные адреса**». Категория «**Заблокированные адреса**» отображает список заблокированных адресов межсетевым экраном автоматически при кратном срабатывании правил со включенной автоблокировкой (см. Рисунок 115).

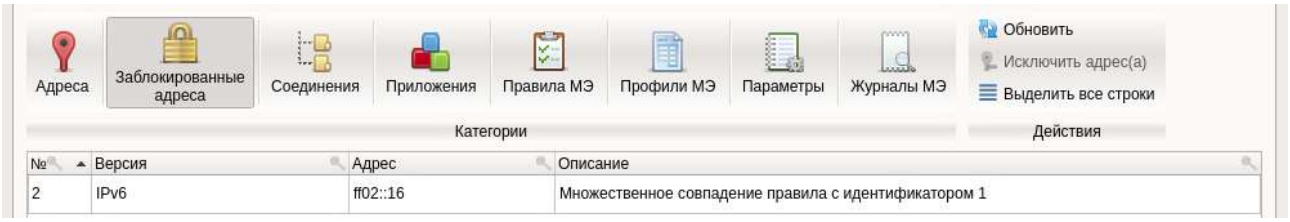


Рисунок 115. Заблокированные адреса

Адреса будут разблокированы при удалении или отключении автоблокировки правил, по которым они заблокированы.

Заблокированные адреса имеют следующие параметры:

- № — идентификационный номер заблокированного адреса;
- Версия — версия интернет-протокола. Принимает значения: IPv4 и IPv6;
- Адрес — сетевой адрес АРМ. Принимает значения: IPv4 и IPv6;
- Описание — указывается причина блокировки адреса.

Для того, чтобы убрать адрес из списка заблокированных адресов, нужно выделить заблокированный адрес и на панели действий нажать на кнопку «**Исключить адрес (а)**». При удалении заблокированного адреса система запросит подтверждение операции (см. Рисунок 116).

Для подтверждения операции — кнопка «Да**»,** для отмены действий — «**Нет**».

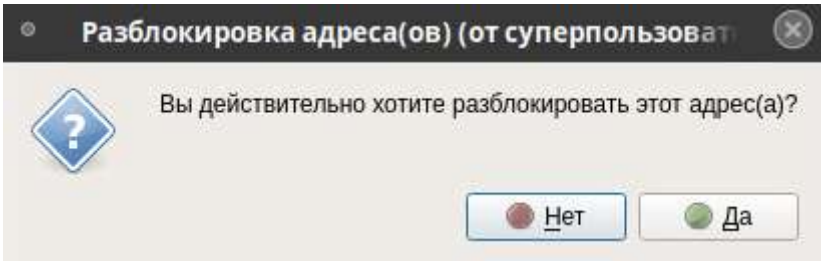


Рисунок 116. Исключение адреса(-ов) из списка заблокированных адресов

4.11.7 Управление профилями правил межсетевого экрана

Профиль правил отображает набор правил межсетевого экрана. При активации или деактивации профиля все правила, входящие в данный профиль, активируются или деактивируются. При удалении профиля, удаляются все входящие в него правила межсетевого экрана.

В МЭ **Dallas Lock Linux** по умолчанию доступны два профиля правил межсетевого экрана: «Default» и «Safe Mode».

Профиль «Default» включает в себя пять пользовательских правил по умолчанию, которые доступны с первого включения **СЗИ НСД Dallas Lock Linux**. Данные правила МЭ доступны для редактирования и удаления.

Профиль «Safe Mode» включает в себя одно правило межсетевого экрана, блокирующее трафик при критическом сбое работы МЭ. Данный профиль доступен для активации и деактивации, но недоступен для удаления и редактирования. Правила межсетевого экрана в профиле «Safe Mode» рекомендуется настроить таким образом, чтобы обеспечить безопасное состояние защищенного АРМ, разрешив только минимально необходимый набор подключений, в частности для централизованного управления **СЗИ НСД** с помощью **ЕЦУ Dallas Lock** и т.д.

4.11.7.1 Создание профиля МЭ

Консольная оболочка администрирования

Для добавления нового профиля правил необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *set-profile*. После ввода команды система перейдет в раздел конструктора правил *set-profile*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 55.

Таблица 55

№	Атрибут	Описание
1	*name <значение>*	Указывает название профиля правил. Обязательный атрибут
2	*activation <значение>*	Добавление условия активации нового профиля правил. **Принимает значения:** *yes* – профиль активируется при отсутствии запущенного антивирусного ПО в системе (проверяется Dr. Web и Kaspersky), *no* – отсутствует условие активации. По умолчанию установлено условие активации для профиля *no*
3	*enable <значение>*	Указание состояния профиля правил. **Принимает значения:** *yes* – профиль включен, *no* – профиль выключен. По умолчанию установлено значение профиля *yes*
4	*description <значение>*	Добавление описания для нового профиля. Описание профиля должно быть заключено в двойные кавычки

Пример:

firewall <enter>

set-profile <enter>

name "HTTP profile" <enter>

activation yes <enter>

execute <enter>

New profile was successfully added

Графическая оболочка администрирования

Для создания нового профиля правил межсетевого экрана с помощью графической оболочки **СЗИ НСД** необходимо на вкладке «**МЭ**» выбрать категорию «**Профили МЭ**» (см. Рисунок 117) и нажать на кнопку «**Создать профиль**»  на панели действий.

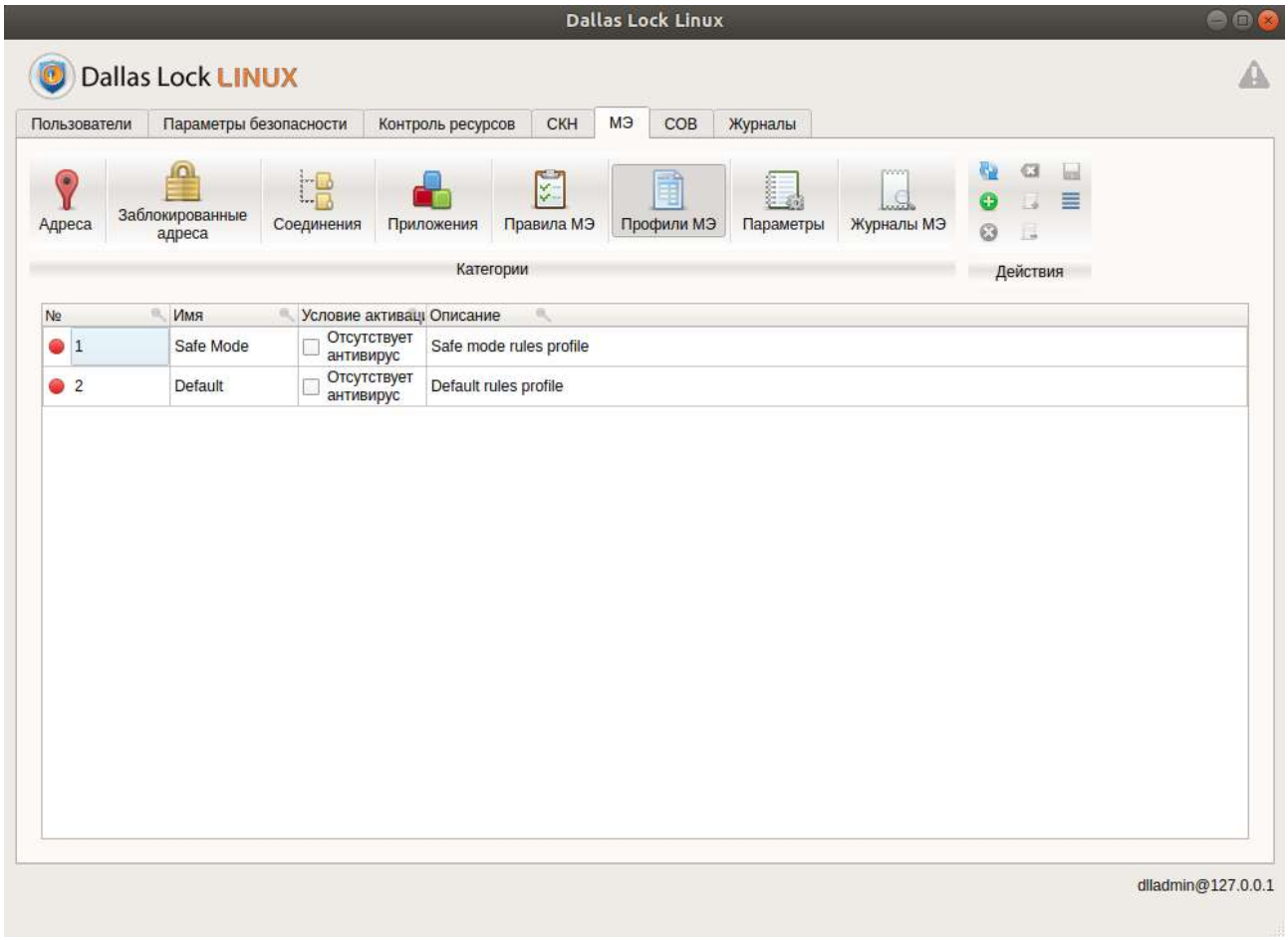


Рисунок 117. Рабочая область категории «Профили МЭ»

После нажатия кнопки «**Создать профиль**» в рабочей области в категории «**Профиль МЭ**» будет размещен новый профиль межсетевого экрана.

Созданный новый профиль правил МЭ будет иметь следующие параметры по умолчанию:

- «№» — идентификационный номер профиля правил МЭ. Также указывается статус профиля правил МЭ. **Принимает значение:** *включен* – профиль и все входящие в него правила включены, *выключен* – профиль и все входящие в него правила выключены. По умолчанию установлено значение *выключен*;
- «Имя» — указывается имя профиля правил МЭ. Максимальное количество символов: 32. Является обязательным параметром;
- Условие автоактивации профиля — условия, при которых профиль правил активируется. **Принимает значение:** *отключено* – антивирус отсутствует на АРМ, *включено* – осуществляется проверка установленного антивируса на АРМ. Модуль МЭ взаимодействует со следующими антивирусами: DrWeb и Kaspersky. По умолчанию установлено значение *отключено*.
- Описание — указывается дополнительная информация по профилю правил. Максимальное количество символов: 128. По умолчанию параметр имеет *пустое значение*.

4.11.7.2 Изменение профиля МЭ

Консольная оболочка администрирования

Для изменения профиля правил МЭ необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *change-profile*. После ввода команды система перейдет в раздел конструктора правил *change-profile*, где необходимо задать параметры, используя атрибуты, приведенные в Таблица 56.

Таблица 56

№	Атрибут	Описание
1	*id <значение>*	Идентификационный номер профиля правил. Обязательный атрибут. Идентификационный номер профиля правил можно узнать, выполнив команду *list-profiles.* **Пример:** *firewall <enter>* *list-profiles <enter>*
2	*name <значение>*	Наименование профиля правил МЭ. Обязательный атрибут
3	*activation <значение>*	Изменение условия активации профиля правил. **Принимает значения:** *yes* – профиль активируется при отсутствии запущенного антивирусного ПО в системе (проверяется Dr. Web и Kaspersky), *no* – отсутствует условие активации
4	*enable <значение>*	Изменение состояния профиля правил. **Принимает значение:** *yes* – профиль включен, *no* – профиль выключен
5	*description <значение>*	Редактирование описания профиля правил МЭ. Описание профиля должно быть заключено в двойные кавычки

Пример:

firewall <enter>
change-profile <enter>
id 1 <enter>
description "Profile for HTTP rules" <enter>
enable yes <enter>
execute <enter>
Profile 1 was successfully changed

Графическая оболочка администрирования

В режиме редактирования профиля правил МЭ доступны следующие атрибуты:

- наименование профиля;
- условие активации профиля;
- описание.

Для перехода в режим редактирования профиля правил межсетевого экрана необходимо выделить требуемый профиль и двойным кликом на столбец атрибута, в который требуется внести изменения, запустить режим редактирования.

Функции активация и деактивация профиля правил реализованы только на панели действий категории «**Профили МЭ**» (см. Рисунок 118). «**Активировать профиль**» — включить профиль и все входящие в него правила, «**Деактивировать профиль**» — выключить профиль и все входящие в него правила.

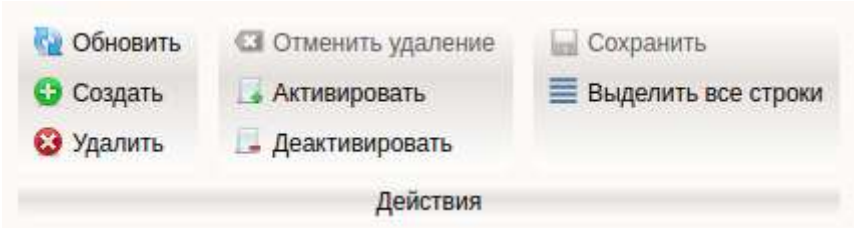


Рисунок 118. Панель действий категории «Профили МЭ»

Для сохранения всех изменений профиля правил межсетевого экрана необходимо нажать на кнопку  «**Сохранить**».

4.11.7.3 Удаление профиля МЭ

Консольная оболочка администрирования

Для удаления профиля правил межсетевого экрана необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном набрать команду *remove-profile* с указанием целочисленного идентификатора профиля.

Пример:

firewall <enter>

remove-profile 1 <enter>

Графическая оболочка администрирования

Для удаления профиля правил с помощью графической оболочки администрирования необходимо перейти в категорию «**Профили МЭ**» вкладки «**МЭ**», одним кликом выделить требуемый для удаления профиль и нажать на кнопку «**Удалить профиль**» на панели действий (см. Рисунок 118). При удалении профиля МЭ, все входящие в него правила будут также удалены.

Для сохранения выполненных действий необходимо нажать на кнопку  «**Сохранить**».

4.11.7.4 Вывод настроенных профилей МЭ

Консольная оболочка администрирования

Для вывода всех настроенных профилей правил межсетевого экрана в консоль необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном выполнить команду *list-profiles* (Рисунок 119).

```
cli> firewall
firewall> list-profiles
Request successfully completed
```

	enable	profile	activation	description
1	0	Safe Mode	0	Safe mode rules profile
2	0	Default	0	Default rules profile

Рисунок 119. Вывод настроенных профилей правил

Графическая оболочка администрирования

Для просмотра настроенных и имеющихся по умолчанию профилей правил с помощью графической оболочки администрирования нужно перейти в категорию «**Профили МЭ**» вкладки «**МЭ**» (см. Рисунок 120).

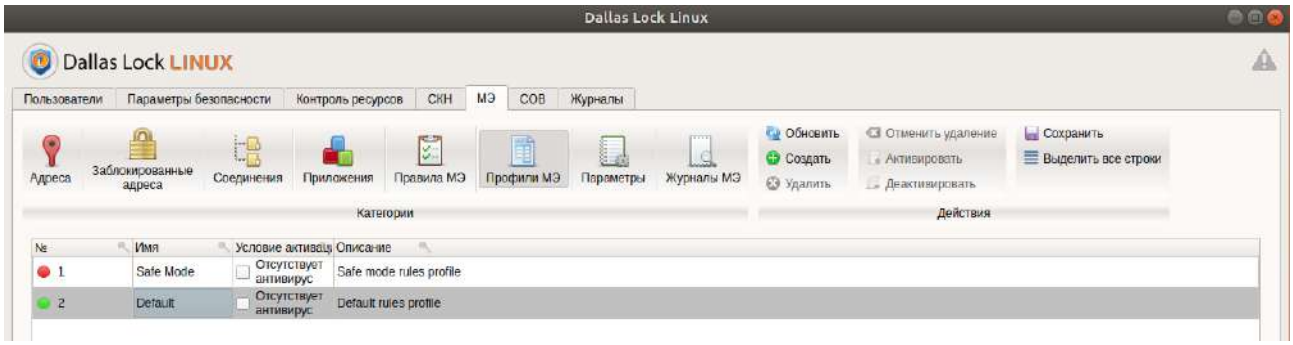


Рисунок 120. Просмотр профилей правил МЭ

4.11.8 Самотестирование межсетевого экрана

Консольная оболочка администрирования

Для запуска самотестирования межсетевого экрана необходимо в консольной оболочке администрирования в разделе управления межсетевым экраном выполнить команду *test-firewall.* Самотестирование межсетевого экрана занимает от 20 секунд до 1,5 минуты.

Пример:

firewall <enter>

test-firewall <enter>

```
firewall> test-firewall
Firewall test successfully completed
        Firewall start test.....................OK
        Firewall common rule test...............OK
        Firewall L7 protocol rule test..........OK
        Firewall blacklisted command test.......OK
        Firewall SSL rule test..................OK
        Firewall stop test......................OK
firewall>
```

Рисунок 121. Результат самотестирования МЭ

4.12 Управление системой обнаружения вторжений

СОВ **Dallas Lock Linux** является модулем **СЗИ НСД Dallas Lock Linux**, расширяющим функциональные возможности модуля «Межсетевой экран» **СЗИ НСД Dallas Lock Linux**. СОВ **Dallas Lock Linux** обеспечивает обнаружение и блокирование основных угроз безопасности, выполняя одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализируя некоторые отдельные сетевые протоколы.

В рамках модуля СОВ реализуются следующие функциональные возможности:

- управление параметрами СОВ;
- управление работой СОВ;
- управление установкой (актуализация) обновлений базы решающих правил (сигнатуры трафика) СОВ;
- обнаружение и (или) блокирование основных угроз безопасности информации, относящихся к вторжениям (атакам);
- разграничение доступа к управлению СОВ;
- регистрация событий СОВ в журналах безопасности;
- управление журналами безопасности СОВ.

Консольная оболочка администрирования

Для управления системой обнаружения вторжений с помощью консольной оболочки администрирования (далее – *ishl*) присутствует управляющая команда *hids.* Команда *hids* осуществляет переход в раздел управления системой обнаружения вторжений *hids*.

Раздел *hids* представлен в Таблица 57 и имеет следующие основные команды:

Таблица 57

№	Атрибут	Описание
1	*back*	Выход из подменю (на уровень выше).
2	*help*	Вывод информации о встроенных командах.
3	*list*	Просмотр списка управляющих команд.
4	*exit*	Выход из консольной оболочки администрирования и закрытие сессии Администратора (Аудитора).
5	*hids-policies-set*	Команда перехода в меню установки политик (параметров) безопасности СОВ.
6	*hids-policies-get*	Команда просмотра установленных политик (параметров) безопасности СОВ.
7	*profiles*	Команда управления профилем СОВ.
8	*update-sources*	Команда управления источником обновления набора сигнатур трафика.
9	*hids-control*	Команда управления режимом работы СОВ.
10	*signatures*	Команда перехода в подраздел управления журнальными сигнатурами, сигнатурами трафика, эвристикой.
11	*list-blocked-addresses*	Команда просмотра заблокированных IP-адресов.
12	*unblock-addresses*	Команда разблокировки IP-адреса.

Графическая оболочка администрирования

Для управления системой обнаружения вторжений **СЗИ НСД** в графической оболочке администрирования необходимо перейти во вкладку «СОВ» (см. Рисунок 122). На данной вкладке представлены следующие категории настраиваемых параметров системы защиты:

- «Информация о СОВ»;
- «Параметры СОВ»;
- «Сигнатуры»;
- «Блокировки»;
- «Журналы СОВ»;
- «Статистика»;
- «Обновления».

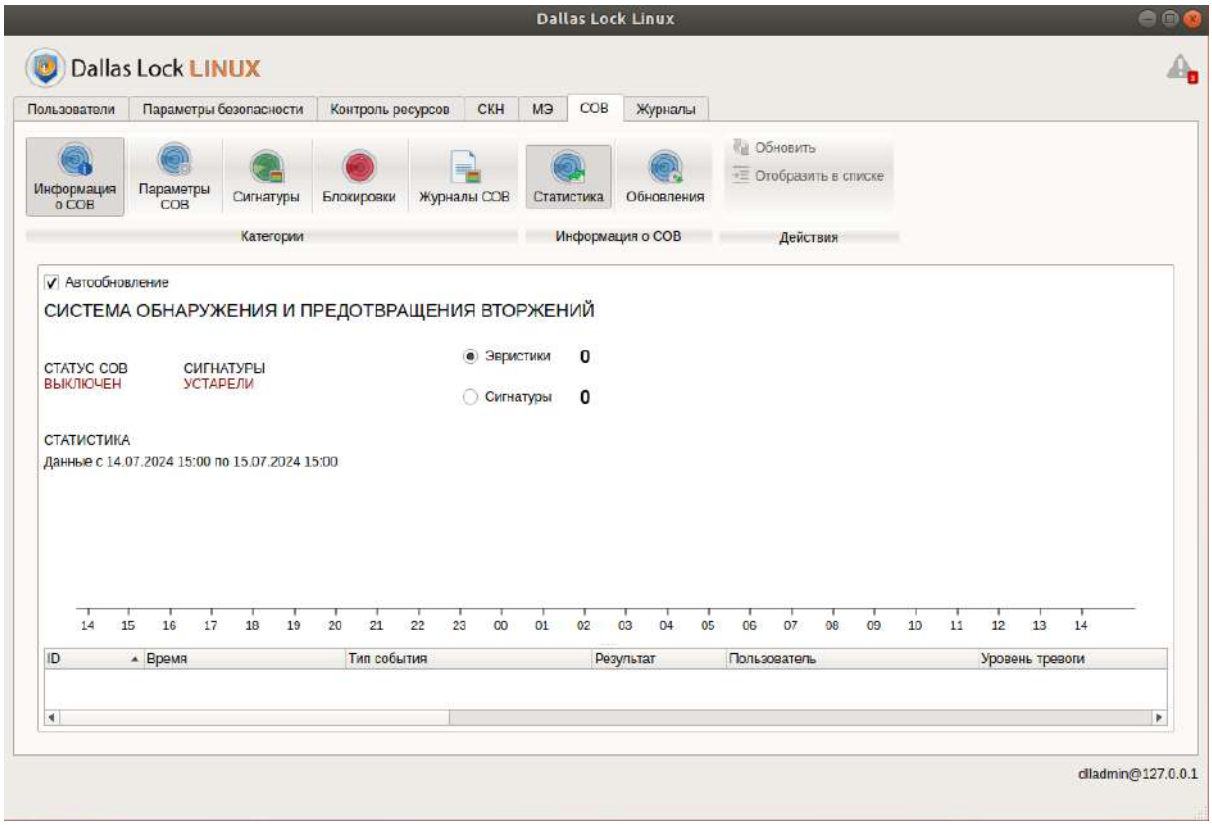


Рисунок 122. Вкладка «СОВ» в графической оболочке администрирования

При переходе на вкладку СОВ в графической оболочке администрирования **СЗИ НСД Dallas Lock Linux** по умолчанию отображается категория «**Информация о СОВ – Статистика**».

Категория «**Информация о СОВ – Статистика**» является информационной панелью в графической оболочке администрирования **СЗИ НСД**.

Рабочая панель категории «**Информация о СОВ – Статистика**» вкладки СОВ содержит:

Автообновление – чекбокс, который определяет, должна ли обновляться таблица со статистикой СОВ (по умолчанию включен). При переходе в другую вкладку/категорию состояние чекбокса сохраняется.

Статус СОВ – режим работы СОВ. Информирует о состоянии работы СОВ, а именно:

- включен;
- выключен;

Сигнатуры – информируют об актуальности сигнатур трафика, имеющихся в **БД СЗИ НСД**.

Доступные значения статуса сигнатур: актуальны и устарели.

- Актуальны – статус отображается, когда набор сигнатур трафика обновился, и с момента обновления прошло меньше, чем две недели.
- Устарели – статус отображается, если с момента последнего обновления набора сигнатур трафика прошло больше, чем две недели.

Таблица – таблица регистрирует подробную информацию событий по срабатываниям сигнатур и эвристики.

В блоке «Статистика» отображаются события в соответствии с настройками журналирования. Подробнее в разделе – **Управление категорией «Параметры СОВ – Глобальные параметры»**.

Идентификатор события безопасности в столбце ID на вкладке «**Основное – Статистика**» может не соответствовать уникальному идентификатору события безопасности из журнала «События безопасности СОВ». Столбец ID на вкладке «**Основное – Статистика**» будет отображать порядковый номер полученного события.

Счетчик эвристики – количество событий срабатываний эвристик за 24 часа.

Счетчик сигнатур – количество событий срабатываний журнальных сигнатур и сигнатур трафика за 24 часа.

С помощью радио-кнопок напротив счетчиков «Эвристика» и «Сигнатуры» система позволяет переключать и демонстрировать информацию по срабатываниям сигнатур или эвристики. По умолчанию радио-кнопка включена на счетчике эвристики.

Статистика по количеству срабатываний сигнатур и эвристик за последние 24 часа также отображается в виде гистограммы с осями времени ценой деления 1 час и количества срабатываний.

Администратору и Аудитору доступно следующее действие:

Обновить () – обновить информацию на панели категории «**Информация о СОВ – Статистика**». Кнопка «Обновить» недоступна при включенном Автообновлении.

4.12.1 Управление параметром «Включить СОВ/Отключить СОВ»

Консольная оболочка администрирования

Для управления режимом работы СОВ с помощью *ishl* необходимо в разделе *hids* перейти в подраздел *hids-control*.

Команда перехода для управления режимом работы СОВ *hids-control* содержит следующие команды:

Таблица 58

№	Атрибут	Описание
1	*start*	Команда включения работы СОВ **Пример:** *cli> hids <enter>* *hids>hids-control <enter>* *start <enter>* *Success enabling HIDS*
2	*stop*	Команда выключения работы СОВ **Пример:** *cli> hids <enter>* *hids>hids-control <enter>* *stop<enter>* *Success disabling HIDS*

Графическая оболочка администрирования

Управлять работой СОВ имеет право Администратор. По умолчанию модуль СОВ выключен.

Для включения СОВ необходимо во вкладке «**Параметры СОВ**» нажать левой кнопкой мыши по кнопке «Включить СОВ» расположенная на панели «**Параметры СОВ**» (см. Рисунок 123).

СЗИ НСД предупреждает Администратора о включении СОВ. Функциональная реализация представлена ниже (Рисунок 124):

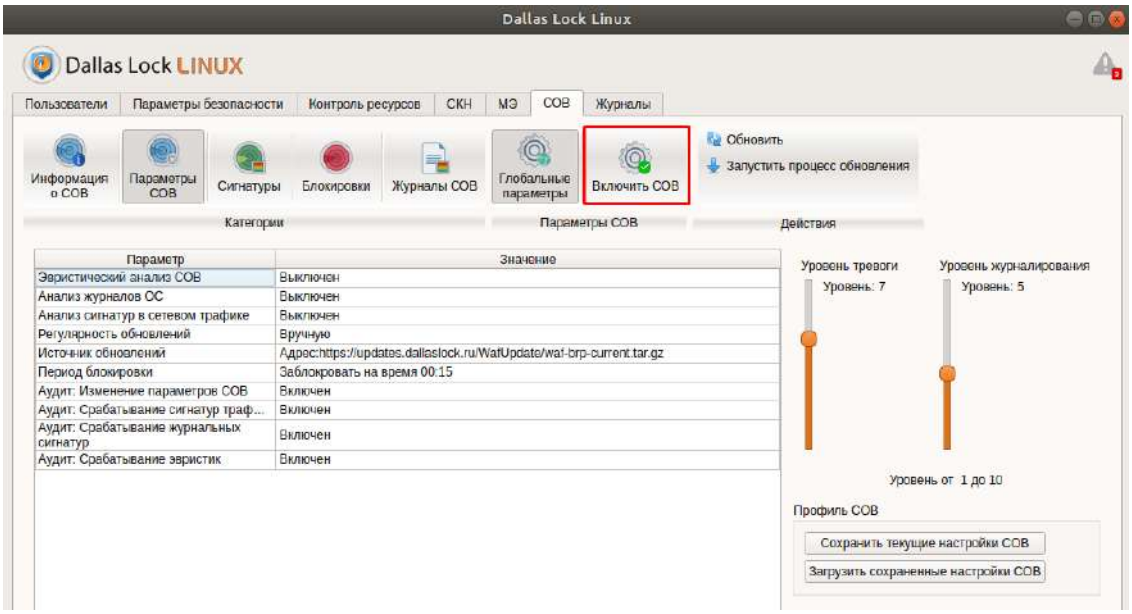


Рисунок 123. Включение СОВ

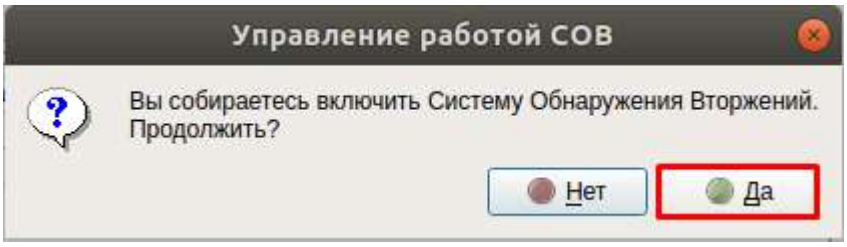


Рисунок 124. Окно «Управление работой СОВ»

4.12.2 Управление категорией «Параметры СОВ – Глобальные параметры»

Консольная оболочка администрирования

Для управления политиками (параметрами) безопасности СОВ с помощью *ishl* необходимо в разделе *hids* ввести команду *hids-policies-set*.

Команда перехода для установки политик/параметров безопасности СОВ *hids-policies-set* содержит следующие атрибуты и их значения (см. Таблица 59):

Таблица 59

№	Атрибут	Описание
1	*audit-lvl <значение>*	Команда установки уровня журналирования в системе, который считается подлежащим проверке. Уровень журналирования в системе по умолчанию 5. **Принимает значения:** от 1 до 10 **Пример:** *cli>hids <enter>* *hids>set-policies<enter>* *set-policies> audit-lvl 2 <enter>* *set-policies> execute <enter>* *Success setting HIDS policies*
2	*threat-lvl <значение>*	Команда установки уровня тревоги в системе. Уровень тревоги в системе по умолчанию 7. **Принимает значения:** от 1 до 10

№	Атрибут	Описание
		Пример: *cli>hids <enter>* *hids>hids-policies-set<enter>* *threat-lvl 2 <enter>* *hids-policies-set> execute <enter>* *Success setting HIDS policies* В случае, если Администратор установил уровень журналирования выше, чем уровень тревоги, то система не сохраняет введенное значение уровня тревоги и выдаст сообщение об ошибке. **Пример:** *cli>hids <enter>* *hids>hids-policies-set<enter>* *hids-policies-set> audit-lvl 2 <enter>* *hids-policies-set> execute <enter>* *Success setting HIDS policies* *hids>hids-policies-set<enter>* *threat-lvl 2 <enter>* *hids-policies-set> execute <enter>* *Error setting HIDS policies*
3	*ip-block-time <значение>*	Команда установки времени блокировки вредоносного IP-адреса (в минутах). Время блокировки вредоносного IP-адреса по умолчанию 15 минут. **Принимает значения:** 0 – навсегда, от 1 до 1440 (в минутах) **Пример:** *cli>hids <enter>* *hids>hids-policies-set<enter>* *hids-policies-set> ip-block-time 15 <enter>* *hids-policies-set> execute <enter>* *Success setting HIDS policies*
4	*update-sources*	Установленный источник обновлений. Данный параметр позволяет задать временной интервал для блокирования IP-адреса(-ов), с которого произошло тревоги или произошла атака. **Пример:** *cli> hids <enter>* *hids> hids-policies-get <enter>* *“update-sources”: online https://updates.dallaslock.ru/Update, или* *“update-sources”: offline “/home/user/signatures_dir”* *hids-policies-set> execute <enter>*
5	*heuristic-analysis <значение>*	Команда включения и отключения эвристического анализа СОВ. **Принимает значения:** yes – включить эвристический анализ СОВ, no – отключить эвристический анализ СОВ. **Пример:** *cli>hids <enter>*

№	Атрибут	Описание
		hids>hids-policies-set<enter> *hids-policies-set> heuristic-analysis no <enter>* *hids-policies-set> execute <enter>* *Success setting HIDS policies*
6	*network-analysis <значение>*	Команда включения и отключения сетевого анализа. **Принимает значения:** yes – включить сетевой анализ, no – отключить сетевой анализ. **Пример:** *cli>hids <enter>* *hids>hids-policies-set <enter>* *hids-policies-set>network-analysis no <enter>* *hids-policies-set>execute <enter>* *Success setting HIDS policies*
7	*syslog-analysis <значение>*	Команда включения и отключения системного анализа. **Принимает значения:** yes – включить системный анализ, no – отключить системный анализ. **Пример:** *cli>hids <enter>* *hids>hids-policies-set<enter>* *hids-policies-set> syslog-analysis no <enter>* *hids-policies-set> execute <enter>* *Success setting HIDS policies*
8	*update-mode*	Установленное значение «Регулярность обновлений СОВ». Данный параметр позволяет устанавливать регулярность обновления набора сигнатур трафика. Значение по умолчанию – раз в сутки. **Принимает значения** – вручную, раз в сутки, раз в 2 недели.
9	*journal-change-parametrs-hids*	Режим работы журналирования (аудит) изменения параметров СОВ. Данный параметр управляет журналированием событий связанных с настройками СОВ. Значение по умолчанию – Включен. **Принимает значения** – включен, выключен.
10	*journal-network-signatures <значение>*	Команда управления журналированием событий срабатывания сигнатур трафика. **Принимает значения:** yes – включить журналирование событий срабатываний сигнатур трафика, no – отключить журналирование событий срабатываний сигнатур трафика.
11	*journal-syslog-signatures <значение>*	Команда управления журналированием событий срабатывания журнальных сигнатур. **Принимает значения:** yes – включить журналирование событий срабатываний журнальных сигнатур, no – отключить журналирование событий срабатываний журнальных сигнатур.
12	*journal-heuristics <значение>*	Команда управления журналированием событий связанных срабатываний эвристики. **Принимает значения:** yes – включить журналирование событий срабатываний эвристики, no – отключить журналирование событий срабатываний эвристики.

Также **СЗИ НСД** позволяет просматривать установленные политики (параметры) безопасности СОВ с помощью команды *show-all* в разделе управления политиками безопасности – *policies*), (см. Рисунок 125):

```
cli> policies
policies> show-all

Password policies:
min-len => '8'
retries => '3'
has-spec-sym => 'no'
has-digit-sym => 'no'
has-upperlower-sym => 'no'
pswd-min-days => '-1'
pswd-max-days => '42'
pswd-wrn-days => '3'

Session policies:
max-sessions => '10'
lock-timeout => '0'
schedule-force-shutdown => '0'
```

Рисунок 125. Просмотр установленных политик (параметров)

Графическая оболочка администрирования

После перехода в категорию «**Параметры СОВ**» в графической оболочке администрирования **СЗИ НСД** по умолчанию отображена подкатегория «*Глобальные параметры*» (см. Рисунок 126).

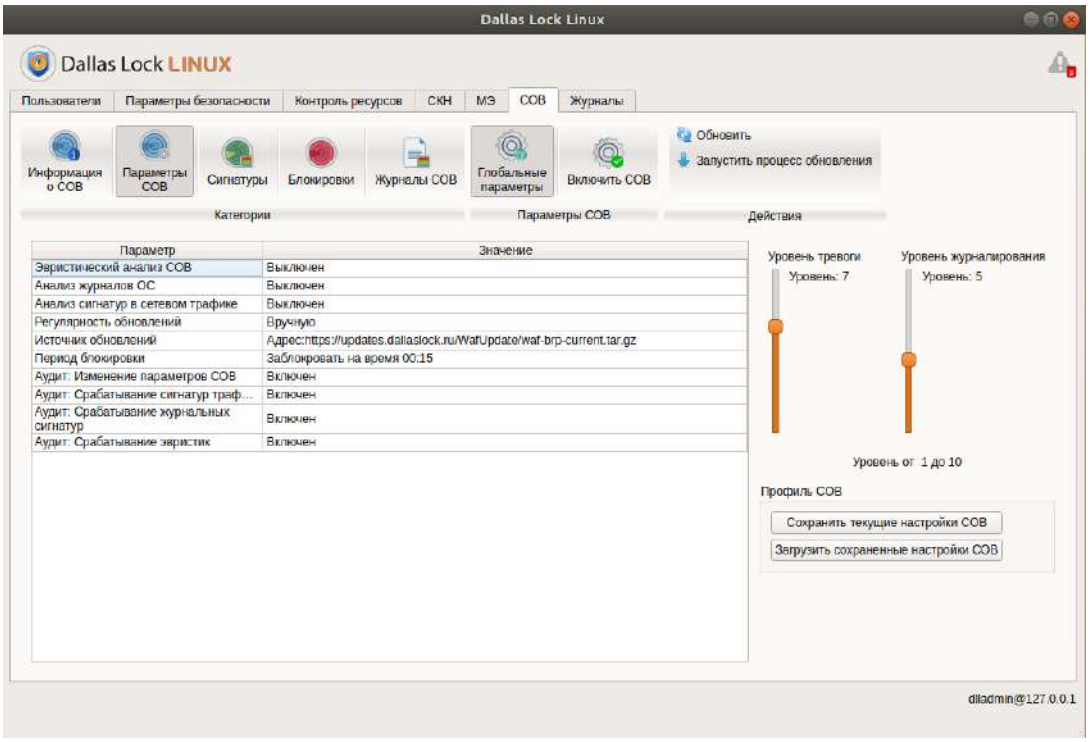


Рисунок 126. Глобальные параметры СОВ

Подкатегория «Глобальные параметры» содержит таблицу со следующими столбцами (атрибутами):

- параметр – наименование политики;
- значение – значение, присваиваемое политике.

Эвристический анализ СОВ – данный параметр позволяет включать/отключать блокировку, журналирование атак на протоколы и сканирование портов (независимо от анализа сигнатур сетевого трафика). Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлено ниже (Рисунок 127):

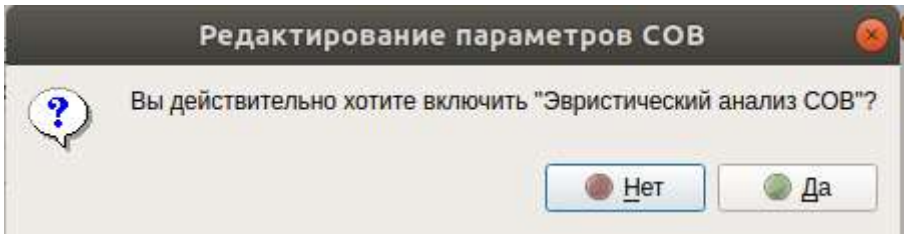


Рисунок 127. Окно «Редактирование параметров СОВ», «Эвристический анализ СОВ»

Анализ журналов ОС – данный параметр позволяет включать/отключать сигнатурный анализ, использующий «Журнальные сигнатуры». Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлено ниже (Рисунок 128):

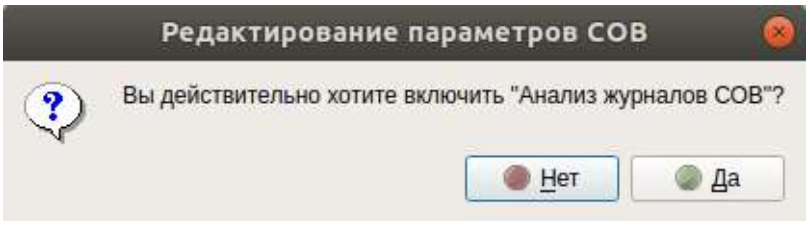


Рисунок 128. Окно «Редактирование параметров СОВ», «Анализ журналов СОВ»

Анализ сигнатур атак в сетевом трафике – данный параметр позволяет включать/отключать сигнатурный анализ, использующий «Сигнатуры трафика». Для установки значения для анализа сигнатур атак в сетевом трафике, появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлено ниже (Рисунок 129):

Рисунок 129. Окно «Редактирование параметров СОВ», «Анализ сигнатур атак»

Регулярность обновлений – данный параметр позволяет устанавливать регулярность обновления набора сигнатур трафика. Принимает значения – вручную, раз в сутки, раз в 2 недели. Появляется вспомогательное окно при двойном нажатии левой кнопки мыши по значению или параметру. Вспомогательное окно представлено ниже (Рисунок 130):

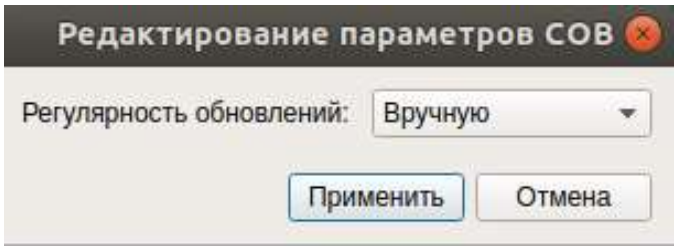


Рисунок 130. Окно «Редактирование параметров СОВ», «Регулярность обновлений»

Источник обновлений – данный параметр позволяет устанавливать источник обновлений набора сигнатур трафика. Значение по умолчанию – HTTPS-адрес. Для установки значения см. Параметр «Источник обновлений».

Период блокировки – данный параметр позволяет задать временной интервал для блокирования IP-адреса(-ов), с которого произошло вторжение или произошла атака.

Значение «**Заблокировать навсегда**» срабатывает, если для журнальной сигнатуры, сигнатуры трафика или эвристики установлено действие – «**Блокировать**». Для установки значения появляется вспомогательное окно «**Период блокировки**» при двойном нажатии левой кнопки мыши по Значению или Параметру (Рисунок 131):

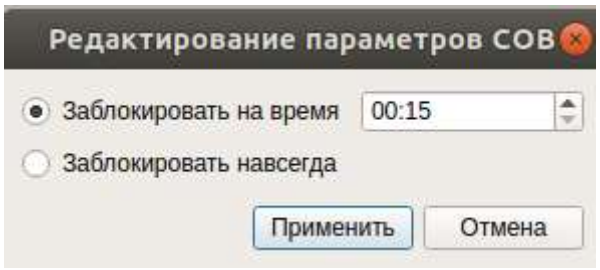


Рисунок 131. Окно «Редактирование параметров СОВ», «Период блокировки»

Аудит: Изменение параметров СОВ – данный параметр управляет журналированием событий связанных с настройками СОВ. Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «Редактирование параметров СОВ» представлены ниже (Рисунок 132):

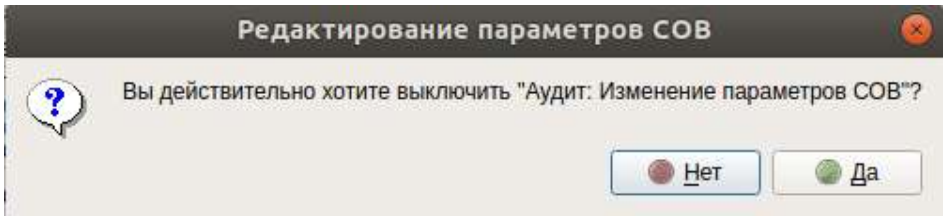


Рисунок 132. Окно «Редактирование параметров СОВ», «Аудит: Изменение параметров СОВ»

Аудит: Срабатывание сигнатур трафика – данный параметр позволяет управлять журналированием событий. Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлены ниже (Рисунок 133):

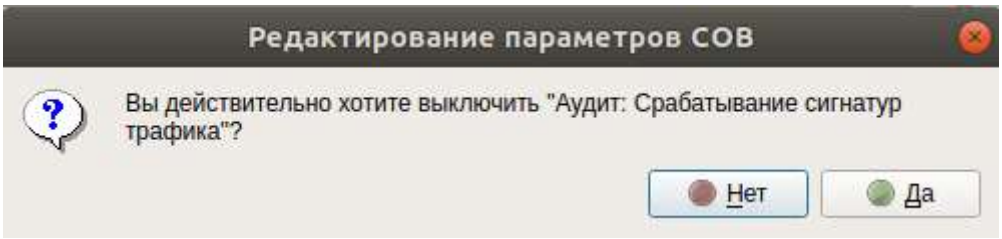


Рисунок 133. Окно «Редактирование параметров СОВ», «Аудит: Срабатывание сигнатур трафика»

Аудит: Срабатывание журнальных сигнатур – данный параметр позволяет управлять журналированием событий срабатывания журнальных сигнатур. Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлены ниже (Рисунок 134):

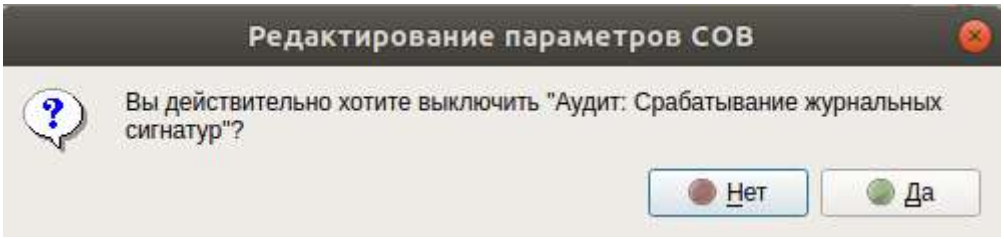


Рисунок 134. Окно «Редактирование параметров СОВ», «Аудит: Срабатывание журнальных сигнатур»

Аудит: Срабатывание эвристики – данный параметр позволяет управлять журналированием событий связанных срабатываний эвристики. Для установки значения появляется вспомогательное окно «**Редактирование параметров СОВ**» при двойном нажатии левой кнопки мыши по значению или параметру. Окно «**Редактирование параметров СОВ**» представлены ниже (Рисунок 135):

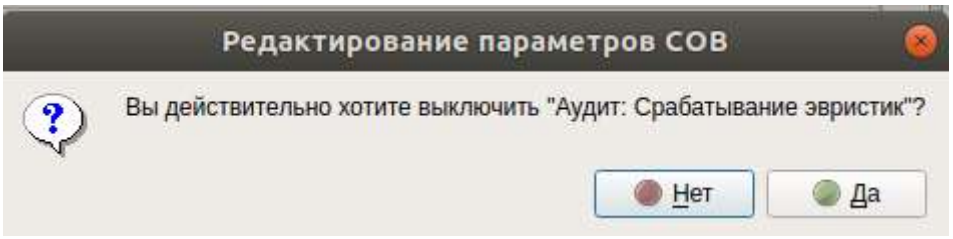


Рисунок 135. Окно «Редактирование параметров СОВ», «Аудит: Срабатывание эвристики»

Уровень журналирования и Уровень тревоги доступны для редактирования Администратору.

В случае установки значений в соответствии с условием: уровень журналирования > уровень тревоги Администратором, то система не разрешит устанавливать уровень журналирования выше уровня тревоги (Рисунок 136):

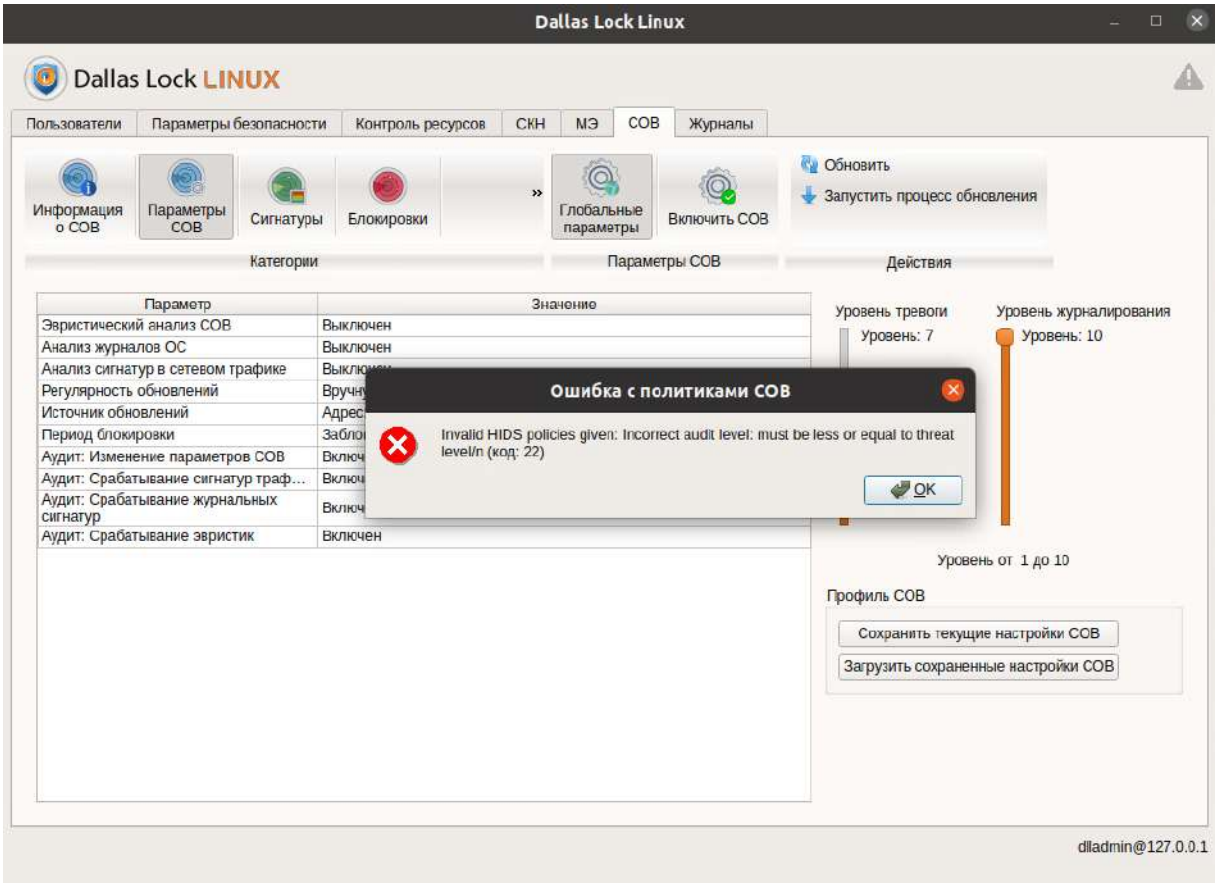


Рисунок 136. Ошибка редактирования политик СОВ

4.12.2.1 Параметр «Источник обновлений»

Консольная оболочка администрирования

Для установки источника обновления сигнатур трафика в разделе *hids* нужно выбрать подраздел *update-sources*. При выполнении команды *update-sources* открывается конструктор установки источника обновления с доступными управляющими командами:

update-source-online <path>, где *<path>* – путь для дальнейшей установки адреса веб-ресурса с обновлениями базы сигнатур,

update-source-offline <path>, где *<path>* – путь для дальнейшей установки пути к файлу с обновлениями базы сигнатур.

Конструктор *update-sources* содержит следующие команды и их значения в Таблица 60:

Таблица 60

№	Атрибут	Описание
1	*update-source-online <path>*	Адрес веб-ресурса с обновлениями базы сигнатур трафика **Пример:** *cli> hids <enter>* *hids> update-sources <enter>* *update-sources> update-source-online http://dallaslock/<enter>* *execute <enter>*
2	*update-source-offline <path>*	Путь к файлу с обновлениями базы сигнатур трафика **Пример:** *cli> hids <enter>* *hids> update-sources <enter>* *update-sources> update-source-offline “/home/user/signatures_dir”<enter>* *execute <enter>*
3	*update-mode <значение>*	Команда установки времени обновления сигнатур трафика. Значение по умолчанию 1. **Принимает значения:** 0 – выключено, 1 – раз в сутки, 2 – раз в 2 недели **Пример:** *cli>hids <enter>* *hids>update-sources<enter>* *update-sources> update-mode 1 <enter>* *update-sources> execute <enter>* Success setting HIDS policies

Графическая оболочка администрирования

Для редактирования источника обновлений набора сигнатур трафика в интерфейсе **Dallas Lock Linux** во вкладке «**СОВ**» присутствует настройка «Источник обновлений» (Рисунок 137).

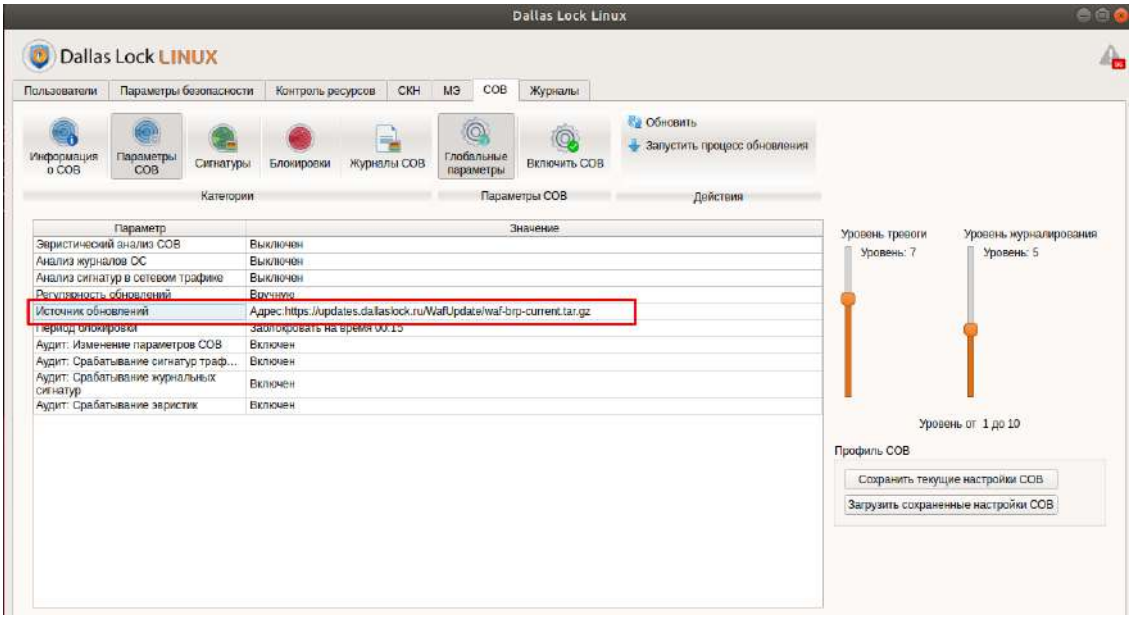


Рисунок 137. Параметр «Источник обновлений»

При нажатии левой кнопки мыши по Значению или Параметру «**Источник обновлений**» появляется окно «**Редактирование параметров СОВ**». Окно настройки «**Источник обновлений**» представлен ниже (Рисунок 138):

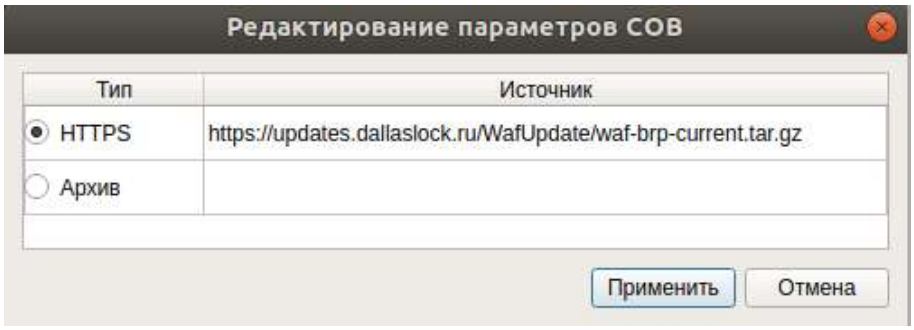


Рисунок 138. Редактирование параметра «Источник обновлений»

Тип источника обновлений набора сигнатур трафика по умолчанию установлен HTTPS. В столбце «Источник» по умолчанию прописан адрес для загрузки набора сигнатур трафика с официального сайта **ООО** «**Конфидент**».

Также доступен для выбора источник обновлений набора сигнатур трафика по пути расположения архива набора сигнатур трафика в системе Linux, загруженных с официального сайта вручную Администратором.

Для установки данного типа источника обновлений открывается вспомогательное окно для установки пути к архиву, содержащему набор сигнатур трафика (Рисунок 139).

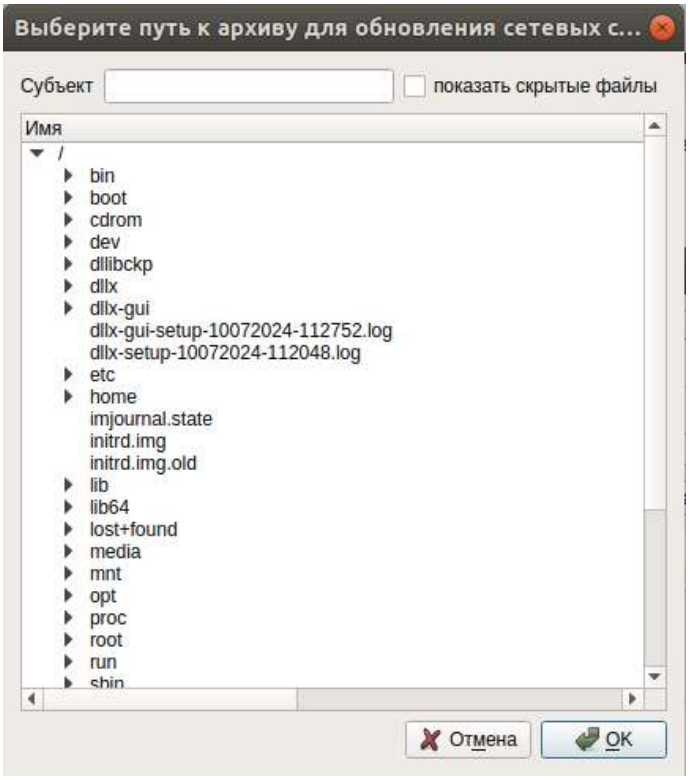


Рисунок 139. Вспомогательное окно выбора каталога для обновления набора сигнатур трафика

1. **СЗИ НСД** разрешает Администратору подтвердить установленный источник обновлений кнопкой «**Ок**», не подтвердить – «**Отмена**».
2. Для запуска процесса обновления набора сигнатур трафика, на панели «Действия» необходимо нажать на кнопку «**Запустить процесс обновления**».
3. Обновление и (или) загрузка набора сигнатур трафика происходят в ходе фонового обновления сигнатур.
4. **СЗИ НСД** не разрешает оставлять источник обновлений незаданным (радио-кнопки в «Источнике обновлений» нет возможности снять).
5. В случае, если один из типов источника обновлений указан неверно, нет подключения к сети и др., **СЗИ НСД** сообщает об ошибке: «*Ошибка загрузки обновлений СОВ. Ошибка подключения к серверу*».
6. В случае, если происходят внутренние ошибки при обновлении набора сигнатур трафика, то система выводит соответствующее сообщение об ошибке.

7. При истечении срока действия кода технической поддержки источник обновления набора сигнатур трафика заблокирован для обновлений.
8. При продлении срока действия кода технической поддержки источник обновлений набора сигнатур трафика разблокирован для обновлений.

Администратору доступны следующие действия на категории Управление категорией «Параметры СОВ – Глобальные параметры»:

- обновить ( ) – обновить таблицу;
- запустить процесс обновления ( ) – действие позволяет запустить процесс обновления набора сигнатура трафика.

4.12.2.2 Управление Профилем СОВ

Консольная оболочка администрирования

Для сохранения и загрузки настроек СОВ с помощью *ishl* в разделе *hids* необходимо перейти в подраздел *profiles*.

Команда перехода для сохранения и (или) загрузки настроек СОВ *profiles* содержит следующие команды (см. Таблица 61):

Таблица 61

№	Атрибут	Описание
1	*save-default*	Команда сохранения текущих настроек СОВ, как заводские, предусмотренные в СОВ, так и выполненные Администратором. **Пример:** *cli> hids <enter>* *hids> profiles <enter>* *profiles> save-default <enter>* Success saving HIDS policies
2	*load-default*	Команда загрузки сохраненных настроек СОВ (импортировать и применить ранее сохраненные настройки СОВ Администратором). **Пример:** *cli> hids <enter>* *hids> profiles <enter>* *profiles> load-default <enter>* Success setting HIDS policies

Графическая оболочка администрирования

Кнопка «**Сохранить текущие настройки СОВ**» – действие позволяет сохранить текущие настройки СОВ, как заводские, предусмотренные в СОВ, так и выполненные Администратором.

Аудитору недоступно действие «**Сохранить текущие настройки СОВ**».

Кнопка «**Загрузить сохраненные настройки СОВ**» – действие позволяет импортировать и применить ранее сохраненные настройки СОВ Администратором. Сохраненные настройки СОВ должны импортироваться из **БД СЗИ НСД** в фоновом обновлении (Рисунок 140).

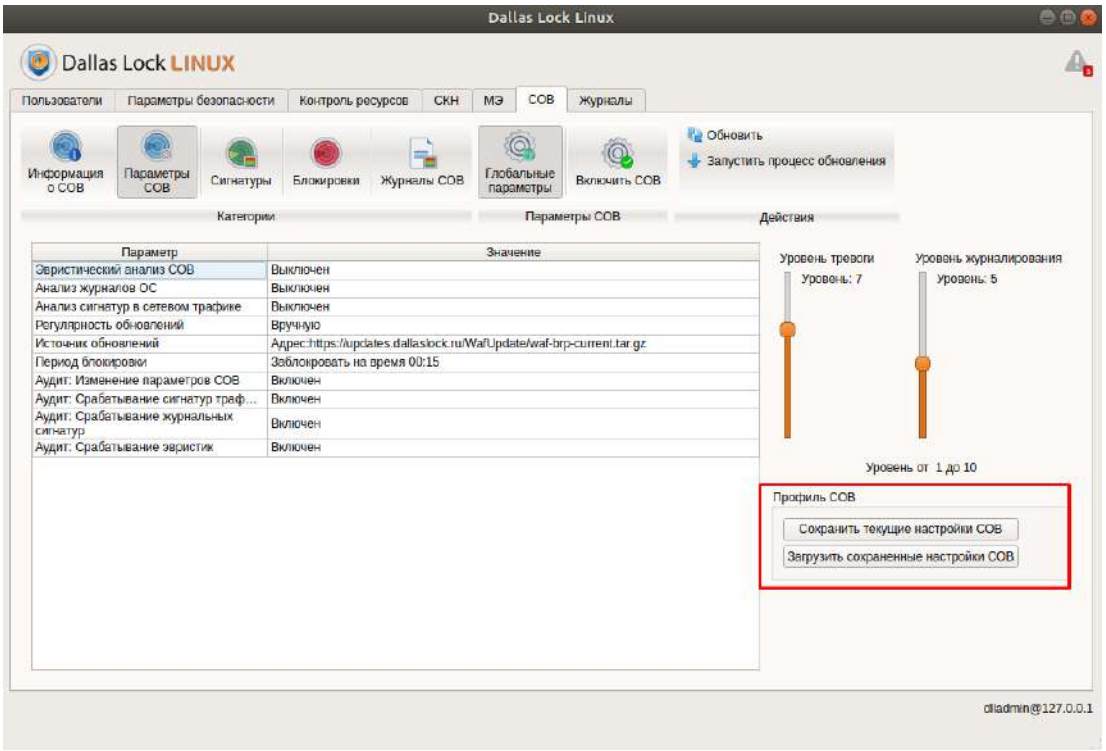


Рисунок 140. Управление профилем СОВ

4.12.3 Управление категорией «Сигнатуры»

Консольная оболочка администрирования

Журнальные сигнатуры – сигнатуры, вхождение которых исследуются в системном журнале. Они являются детекторами локальной подозрительной активности.

Для управления журнальными сигнатурами необходимо перейти в меню управления *syslog-signatures* в подразделе *signatures*.

Меню управления *syslog-signatures* содержит следующие команды в Таблица 62:

Таблица 62

№	Атрибут	Описание
1	*list-syslog-signatures*	Команда вывода списка журнальных сигнатур. При выполнении команды в консольную оболочку администрирования выводится список журнальных сигнатур со следующими полями: – ID – Идентификационный номер журнальной сигнатуры; – Name – наименование журнальной сигнатуры; – Status – режим работы журнальной сигнатуры; – event-lvl – установленный уровень угрозы для журнальной сигнатуры; – Action – операция, выполняемая при срабатывании журнальных сигнатур; – Description – описание журнальной сигнатуры. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> list-syslog-signatures <enter>*

№	Атрибут	Описание
2	*change-syslog-signatures*	Команда для перехода в конструктор изменений параметров журнальной сигнатуры **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> syslog-signatures <enter>* *syslog-signatures> change-syslog-signatures <enter>* *change-syslog-signatures>*

Графическая оболочка администрирования

При переходе в категорию «**Сигнатуры**» в графической оболочке администрирования **СЗИ НСД** по умолчанию отображена подкатегория «*Сигнатуры журналов*» (Рисунок 142).

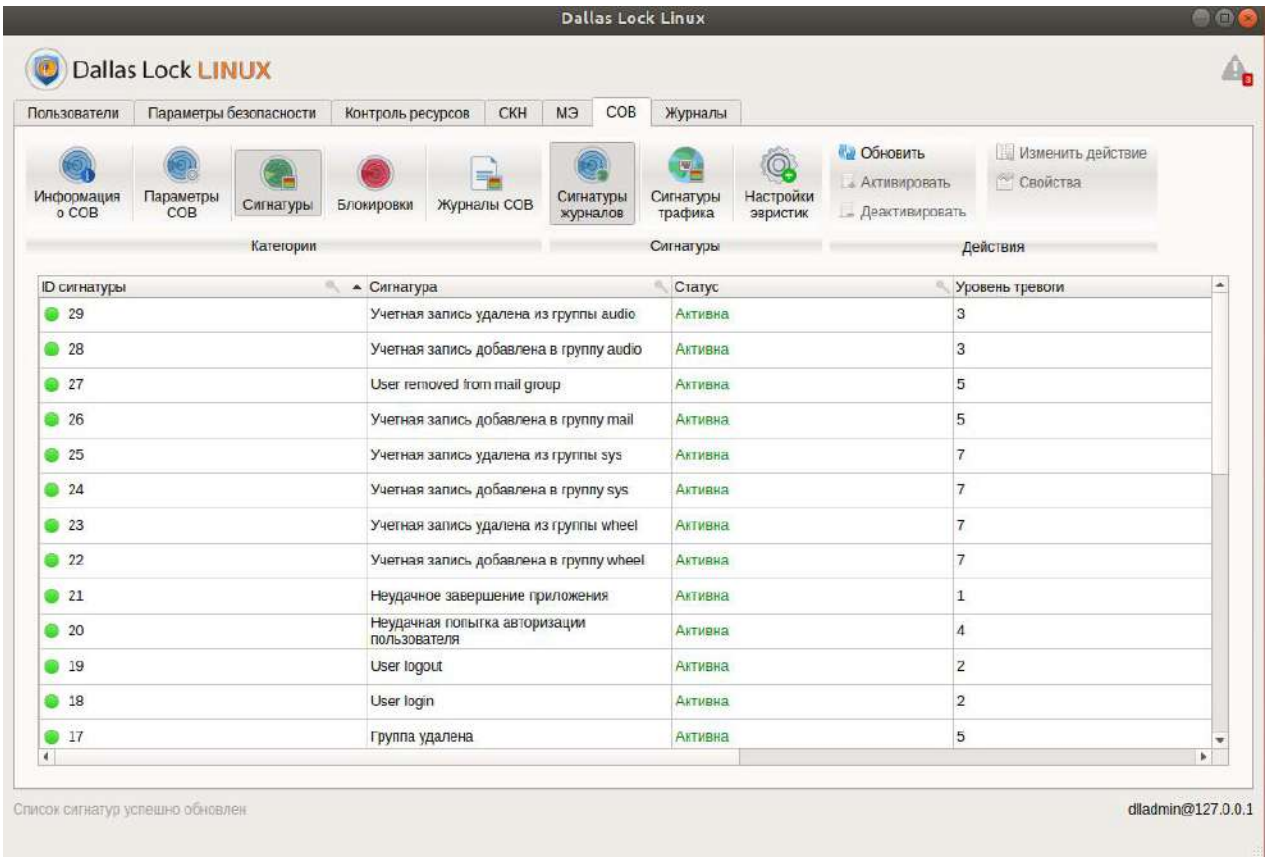


Рисунок 141. Категория «Сигнатуры»

4.12.3.1. Вкладка «Сигнатуры журналов»

Консольная оболочка администрирования

Для изменений параметров журнальной сигнатуры СОВ с помощью *ishl* в разделе *syslog-signatures*, необходимо ввести команду *change-syslog-signature*, выполнение которой осуществляется переход в конструктор *change-syslog-signature*, где необходимо будет задать параметры, используя атрибуты, приведенные в таблице ниже:

Таблица 63

№	Атрибут	Описание	Дополнительно
1	*id <значение>*	Указание целочисленного идентификационного номера журнальной сигнатуры. Является обязательным параметром.	**Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> syslog-signatures <enter>* *syslog-signatures> change-syslog-signatures <enter>* *change-syslog-signatures> id 29 <enter>* *change-syslog-signatures> status no <enter>* *change-syslog-signatures> event-lvl 7 <enter>* *change-syslog-signatures> execute <enter>* *System response:* Журнальная сигнатура с идентификационным номером 29 была выключена. Установлен новый уровень тревоги 7 для журнальной сигнатуры. Также с помощью конструктора *change-syslog-signature* система позволяет изменить режим работы и действие для нескольких журнальных сигнатур с указанием целочисленных идентификационных номеров журнальных сигнатур через запятую. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> syslog-signatures <enter>* *syslog-signatures> change-syslog-signatures <enter>* *change-syslog-signatures> id 29, 24, 27 <enter>* *change-syslog-signatures> status no <enter>* *change-syslog-signatures> execute <enter>* *System response:* Журнальные сигнатуры с идентификационными номерами 29, 24, 27 выключены *syslog-signatures> changed*
2	*status <значение>*	Изменение режима работы журнальной сигнатуры. Является обязательным параметром. **Принимает значения**: yes — включить	

№	Атрибут	Описание	Дополнительно
		журнальную сигнатуру, no – выключить журнальную сигнатуру	
3	*event-lvl <значение>*	Изменение уровня угрозы для журнальной сигнатуры. Является обязательным параметром. **Принимает значения**: от 1 до 10	
4	*action <значение>*	Изменение операции, выполняемой при срабатывании журнальной сигна	

№	Атрибут	Описание	Дополнительно
		туры. Является обязательным параметром. **Принимает значения:** – –	

В конструкторе *change-syslog-signature* необходимо ввести команду *preview* для вывода внесённых изменений. Также в конструкторе присутствует команда *execute* для сохранения внесённых изменений.

Графическая оболочка администрирования

При переходе в категорию «**Сигнатуры**» в графической оболочке администрирования **СЗИ НСД** по умолчанию отображена подкатегория «Сигнатуры журналов» (Рисунок 142).

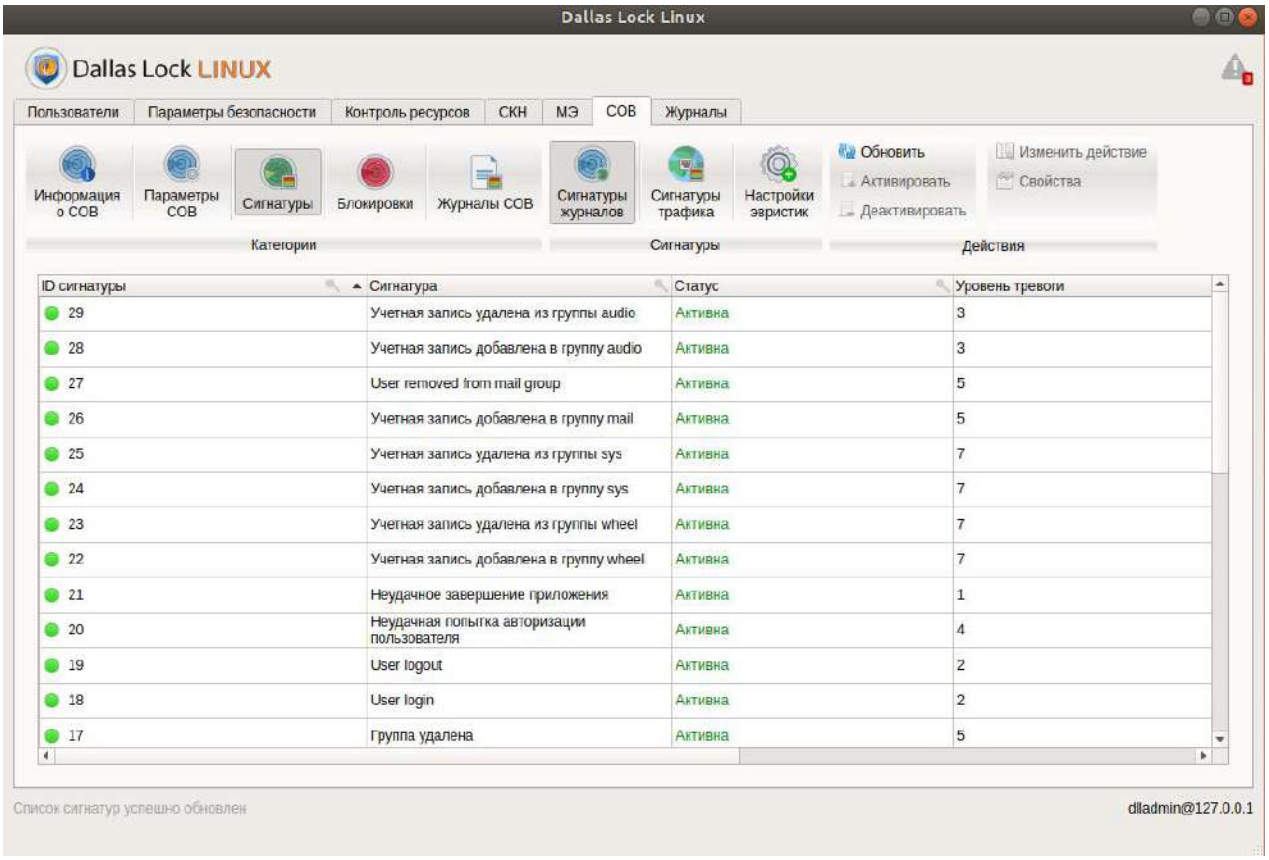


Рисунок 142. Вкладка «Сигнатуры журналов»

ID сигнатуры – Идентификационный номер журнальной сигнатуры.

Сигнатура – Наименование журнальной сигнатуры.

Статус – Режим работы журнальной сигнатуры. Принимает значения: Активен, Неактивен.

Уровень тревоги – Установленный уровень угрозы для журнальной сигнатуры. Принимает значения: от 1 до 10.

Действие – Операции, выполняемые при срабатывании журнальных сигнатур. Допустимые значения: блокировать, журналировать.

Описание – Дополнительная информация о журнальной сигнатуре.

Для редактирования параметров журнальной сигнатуры (журнальных сигнатур) необходимо выбрать редактор во вкладке «**Действия**» – «**Свойства**» (см. Рисунок 143).

Окно свойств журнальной сигнатуры (журнальных сигнатур) содержит:

- ID сигнатуры;
- Сигнатура;
- Выпадающий список «Статус». Позволяет устанавливать режим работы журнальной сигнатуры;
- Спинбокс «Уровень тревоги». Позволяет установить уровень тревоги для журнальной сигнатуры;
- Выпадающий список «**Действие**». Позволяет устанавливать действие для журнальной сигнатуры;
- Кнопка «**Применить**». Кнопка «**Применить**» позволяет применить внесенные изменения для журнальной сигнатуры;
- Кнопка «**Отмена**». Позволяет отменить действия, вносимые Администратором и (или) закрывать окно редактора настроек «Свойства».

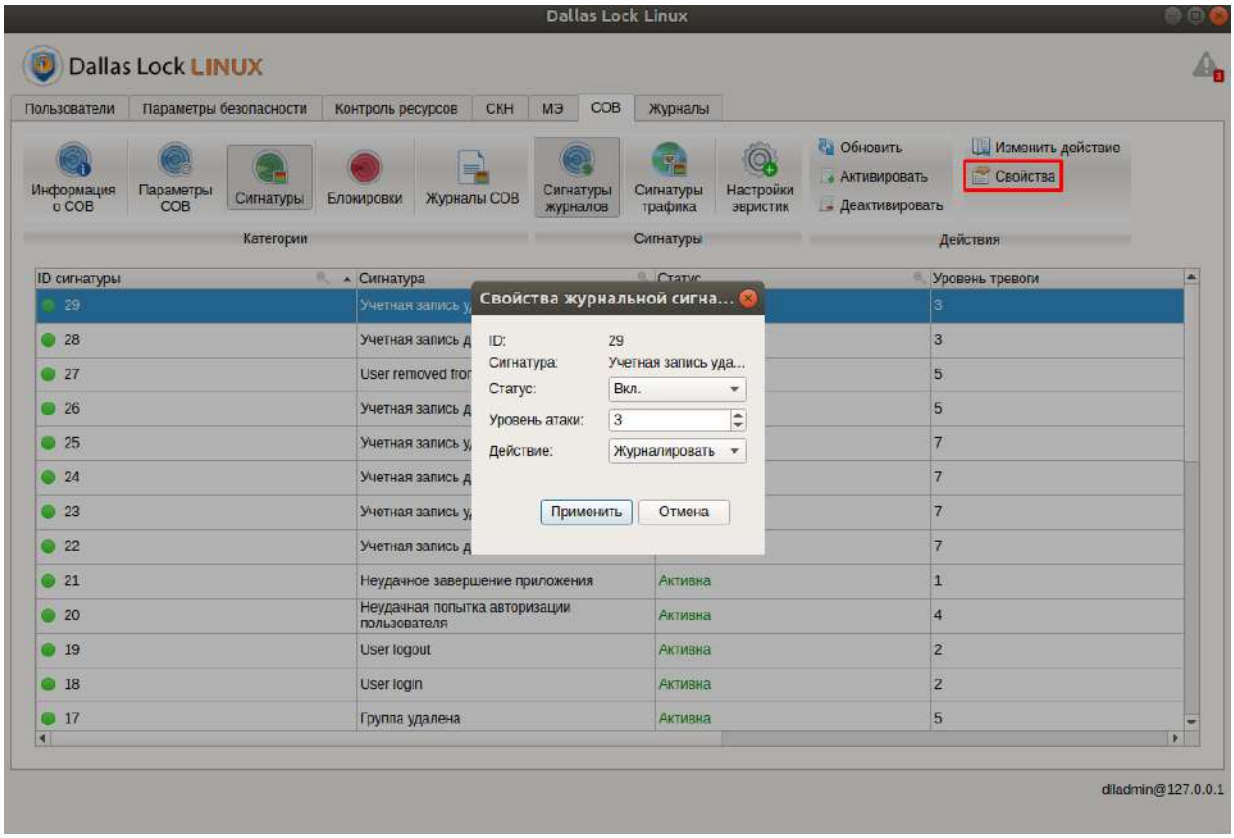


Рисунок 143. Свойства журнальной сигнатуры

Администратору доступны следующие действия (полные права) в категории «**Сигнатуры – Сигнатуры журналов**»:

Изменить действие ( ) – изменить действие для журнальной сигнатуры или журнальных сигнатур. Для внесения изменений система выдает окно «**Изменение действия**» для выбранной журнальной сигнатуры или несколько выбранных журнальных сигнатур (см. Рисунок 144).

Рисунок 144. Окно «Изменить действие»

Активировать ( ) – включить журнальную(-ые) сигнатуру (-ы) СОВ;

Деактивировать ( ) – выключить журнальную (-ые) сигнатуру (-ы) СОВ;

После выполнения активации и (или) деактивации сигнатур (-ы) **СЗИ НСД** принимает изменения.

Свойства ( ) – просмотр установленных параметров для журнальных сигнатур. Выпадающий список «Статус», спинбокс «Уровень тревоги», выпадающий список «Действие» неактивный.

Обновить ( ) – обновить таблицу категории «Сигнатуры – Сигнатуры журналов».

Поиск ( ) – в категории «Сигнатуры журналов» реализована фильтрация данных (поиск) по столбцам «ID сигнатуры», «Сигнатура» (см. Рисунок 145). При нажатии на изображение лупы, появиться текстовое поле, где пользователь сможет осуществить поиск ID сигнатуры и (или) Сигнатуры. После ввода информации пользователю необходимо нажать «**Enter**». Поиск происходит по вхождениям введенной строки.

Рисунок 145. Фильтрация сигнатур журналов

СЗИ НСД позволяет Администратору выделить несколько журнальных сигнатур с помощью горячих клавиш: Ctrl и Shift. В случае, если Администратор выделил несколько журнальных сигнатур, то кнопка Свойства ( ) становится неактивной.

Также присутствует сортировка информации по следующим столбцам: Статус, Уровень тревоги, Действие.

Реализация сортировки обозначена ниже (см. Рисунок 146, Рисунок 147, Рисунок 148):

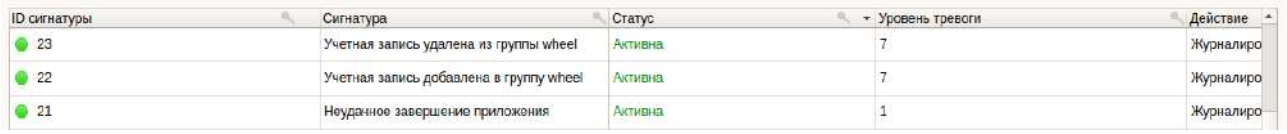


Рисунок 146. Сортировка по столбу «Статус»

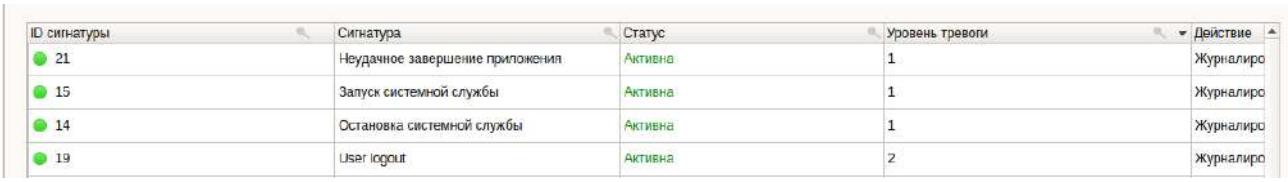


Рисунок 147. Сортировка по столбцу «Уровень тревоги»

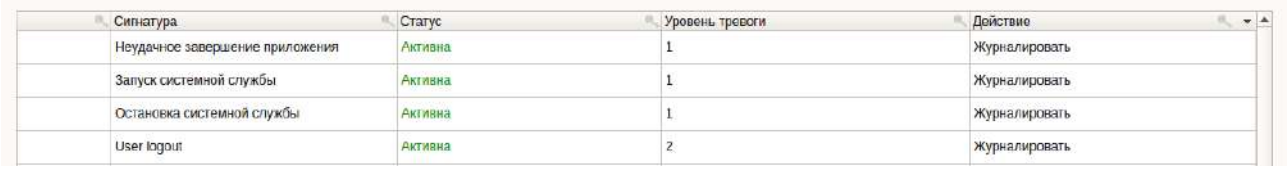


Рисунок 148. Сортировка по столбцу «Действие»

4.12.3.2. Вкладка «Сигнатуры трафика»

Консольная оболочка администрирования

Сигнатуры трафика – сигнатуры, вхождение которых исследуются в исходящем или входящем сетевом трафике. Они являются детекторами потенциального сетевого вторжения.

Для управления сигнатурами трафика необходимо указать меню управления *network-signatures* в подразделе *signatures*.

Меню управления *network-signatures* содержит следующие команды:

Таблица 64

№	Атрибут	Описание
1	*list-network-signatures*	Команда вывода списка сигнатур трафика. При выполнении команды в консольную оболочку администрирования выводится список сигнатур трафика со следующими полями: – ID – Идентификационный номер сигнатуры трафика; – Status – режим работы сигнатуры трафика; – event-lvl – установленный уровень угрозы для сигнатуры трафика; – Action – операция, выполняемая при срабатывании сигнатуры трафика; – Description – описание сигнатуры трафика. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> network-signatures <enter>* *network-signatures > list-network-signatures <enter>*
2	*change-network-signatures*	Команда для перехода в конструктор изменений параметров сигнатуры трафика **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> network-signatures <enter>* *network-signatures> change-network-signatures <enter>* *change-network-signatures>*

Для изменений параметров сигнатуры трафика СОВ с помощью *ishl* в разделе *network-signatures*, необходимо выбрать команду *change-network-signature*, выполнение которой осуществляется переход в конструктор *change-network-signature*, где необходимо задать параметры, используя атрибуты, приведенные в таблице ниже:

Таблица 65

№	Атрибут	Описание	Дополнительно
1	*id <значение>*	Указание целочисленного идентификационного номера	**Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> network-signatures <enter>* *network-signatures> change-network-signatures <enter>* *change-network-signatures> id 65001 <enter>* *change-network-signatures> status no <enter>* *change-network-signatures> event-lvl 7 <enter>* *change-network-signatures> execute <enter>*

№	Атрибут	Описание	Дополнительно
		сигнатуры трафика, которую необходимо изменить. Является обязательным параметром.	Сигнатура трафика с идентификационным номером 65001 выключена. Установлен новый уровень тревоги 7 для сигнатуры трафика. Также с помощью конструктора *change-network-signature* система позволяет изменить режим работы и действие для нескольких сигнатур трафика с указанием целочисленных идентификационных номеров сигнатур трафика через запятую. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> network-signatures <enter>* *network-signatures> change-network-signatures <enter>* *change-network-signatures> id 38933, 65000 <enter>* *change-network-signatures> status no <enter>* *change-network-signatures> execute <enter>* *N* Сигнатуры трафика с идентификационными номерами 38933, 65000 выключены.
2	*status <значение>*	Изменение режима работы сигнатуры трафика. Является обязательным параметром. **Принимает значения:** yes – включить сигн	*e* *t* *w* *o* *r* *k* *s* *i* *g* *n* *a* *t* *u* *r* *e* *s* *s* *u* *c* *c* *e* *s* *s* *f* *u* *l* *l* *y* *changed*

№	Атрибут	Описание	Дополнительно
		атуру трафика, no – выключить сигнатуру трафика	
3	*event-lvl <значение>*	Изменение уровня угрозы для сигнатуры трафика. Является обязательным параметром. **Принимает значения**: от 1 до 10	
4	*action <значение>*	Изменение операции, выпо	

№	Атрибут	Описание	Дополнительно
		лняемой при срабатывании сигнатуры трафика. Является обязательным параметром. **Принимает значения**: idle – журналировать, block ip – блокировать	

В конструкторе *change-network-signature* имеется команда *preview* для вывода внесённых изменений. Также в конструкторе есть команда *execute* для сохранения внесённых изменений.

Графическая оболочка администрирования

Для того чтобы войти в сигнатуры трафика, нужно перейти во вкладку «**СОВ**», далее нажать на категорию «**Сигнатуры**», «**Сигнатуры трафика**» (см. Рисунок 149).

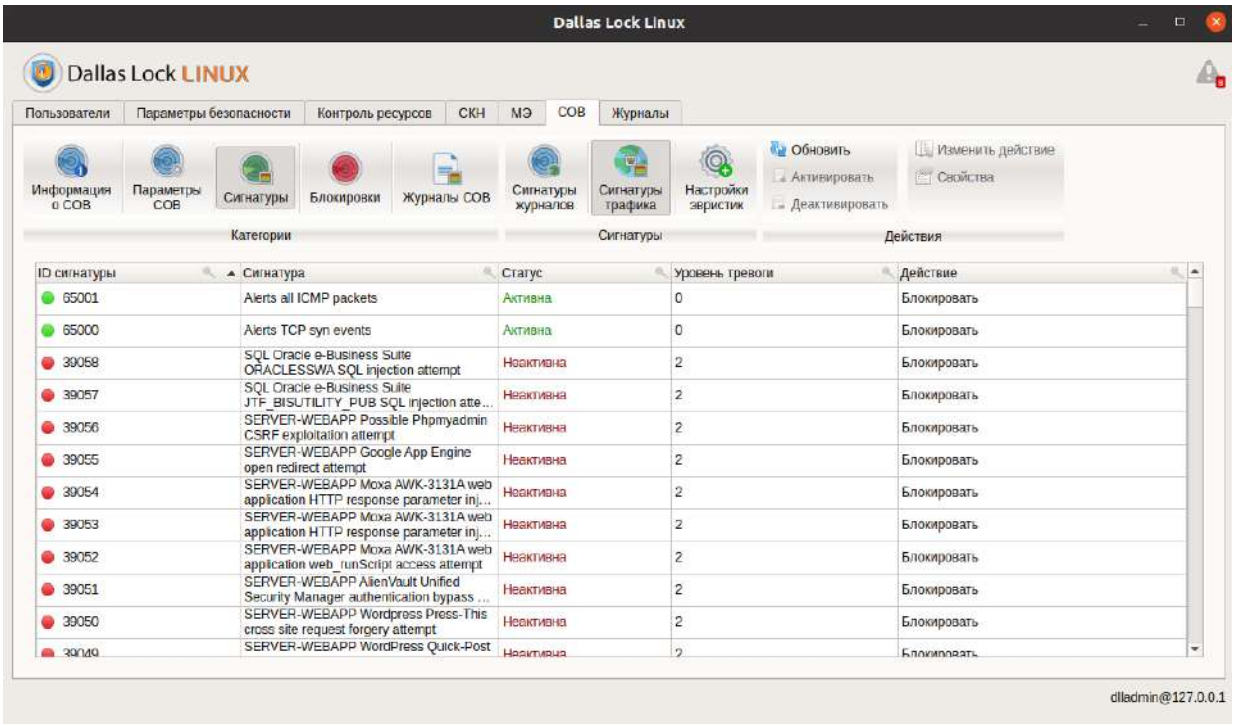


Рисунок 149. Вкладка «Сигнатуры трафика»

Для редактирования параметров сигнатуры трафика необходимо выбрать редактор общих настроек (- Свойства), (см. Рисунок 150).

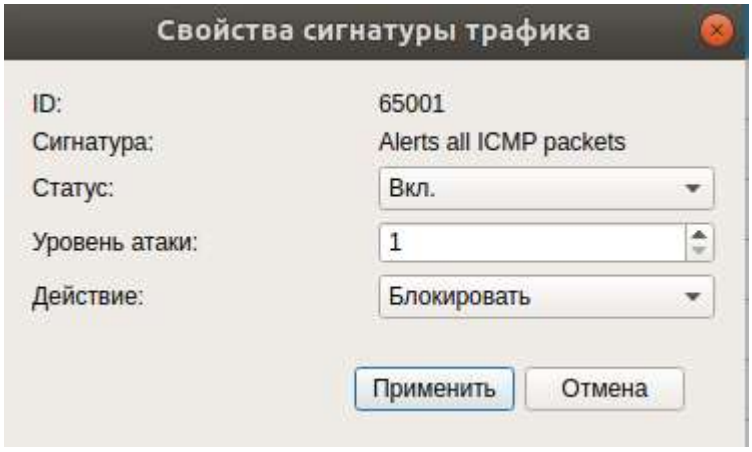


Рисунок 150. Свойства сигнатуры трафика

Окно редактора настроек сигнатуры трафика содержит:

- ID сигнатуры;
- Описание;
- Выпадающий список «Статус». Позволяет устанавливать режим работы сигнатуры трафика;
- Спинбокс «Уровень тревоги». Позволяет установить уровень тревоги для сигнатуры трафика;
- Выпадающий список «**Действие**». Позволяет устанавливать действие для сигнатуры трафика;
- Кнопка «**Применить**». Позволяет применить внесенные изменения для сигнатуры трафика;
- Кнопка «**Отмена**». Кнопка «**Отмена**» позволяет отменить действия, вносимые Администратором и (или) закрывать окно редактора настроек «**Свойства**».

При первой установке СОВ, и ее включении, система содержит базовый набор сигнатур трафика. Статус для «Сигнатуры» на вкладке «**Информация о СОВ – Статистка**» остается «Устарели» до первого обновления набора сигнатур трафика.

В случае истечения срока действия кода технической поддержки будет блокироваться автоматизированное и ручное обновление сигнатур трафика. Ранее загруженные сигнатуры трафика в **СЗИ НСД** при истечении кода технической поддержки будут продолжать работать.

В случае истечения срока действия кода технической поддержки строка состояния в категории «**Сигнатуры – Сигнатуры трафика**» будет отображать информационное сообщение об истечении срока действия кода технической поддержки:

«Нет возможности обновить набор сигнатур трафика. Техническая поддержка завершена. Необходимо продлить техническую поддержку Dallas Lock Linux».

4.12.3.3. Вкладка «Настройки эвристик»

Консольная оболочка администрирования

Управление сигнатурами и эвристикой в *ishl* осуществляется подразделом *signatures*, разработанным в разделе *hids*. Подраздел *signatures* имеет три меню управления: управление сигнатурами трафика – *network-signatures*, управление журнальными сигнатурами – *syslog-signatures*, управление эвристикой – *heuristics*.

Идентификационные номера журнальных сигнатур, сигнатур трафика, эвристики не совпадают.

Уровень угрозы сигнатуры или эристики – угрозы, определенные разработчиками ООО «Конфидент», как угрозы с определенным уровнем риска для информационной безопасности АРМ.

Для управления эвристикой необходимо войти в меню управления *heuristics* в подразделе *signatures*.

Меню управления *heuristics* содержит следующие команды:

Таблица 66

№	Атрибут	Описание
1	*list-heuristics*	Команда вывода списка эвристики. При выполнении команды в консольную оболочку администрирования выводится список эвристики со следующими полями: – ID – Идентификационный номер эвристики; – Name – наименование эвристики; – Status – режим работы эвристики; – event-lvl – установленный уровень угрозы для эвристики; – Action – операция, выполняемая при срабатывании эвристики; – Description – описание эвристики. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures>heuristics <enter>* *heurisrics> list-heuristics<enter>* *list-heuristics>*
2	*change-heuristics*	Команда для перехода в конструктор изменений параметров эвристики **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures>heuristics <enter>* *heurisrics> change-heuristics<enter>* *change-heuristics>*

Для изменений параметров эвристики СОВ с помощью *ishl* в разделе *heuristics* необходимо выбрать команду *change-heuristics*, выполнение которой осуществляется переход в конструктор *change-heuristics*, где необходимо будет задать параметры, используя атрибуты, приведенные в таблице ниже:

Таблица 67

№	Атрибут	Описание	Дополнительно
1	*id <значение>*	Указание целочисленного идентификационного номера эвристики,	**Пример:**

№	Атрибут	Описание	Дополнительно
		которую необходимо изменить. Является обязательным параметром.	*cli>hids <enter>* *hids>signatures <enter>* *signatures>heuristics <enter>* *heurisrics> change-heuristics <enter>* *change-heuristics> id 6 <enter>* *change-heuristics> status on <enter>* *change-heuristics> execute <enter>* *Heuristics 6 successfully changed* Эвристика с идентификационным номером 6 включена. Также с помощью конструктора *change-heuristics* система позволяет изменить режим работы и действие для нескольких эвристик с указанием целочисленных идентификационных номеров эвристик через запятую. **Пример:** *cli>hids <enter>* *hids>signatures <enter>* *signatures> heuristics <enter>* *heuristics> change-heuristics <enter>* *change-heuristics> id 6, 5 <enter>* *change-heuristics> status no <enter>* *change-heuristics> execute <enter>* *Heuristics 6, 5 successfully changed* Эвристики с идентификационными номерами 6, 5 выключены.
2	*status <значение>*	Изменение режима работы эвристики. Является обязательным параметром. **Принимает значения:** yes – включить эвристику, no – выключить эвристику	
3	*event-lvl <значение>*	Изменение уровня угрозы для эвристики. Является обязательным параметром. **Принимает значения:** от 1 до 10	
4	*action <значение>*	Изменение операции, выполняемой при срабатывании эвристики. Является обязательным параметром. **Принимает значения**: Journal – журналировать, Block – блокировать	

Для эвристик типа «flood» обязательно должна стоять реакция блокирование адреса.

В конструкторе *change-heuristics* имеется команда *preview* для вывода внесённых изменений. Также в конструкторе есть команда *execute* для сохранения внесённых изменений.

Графическая оболочка администрирования

Для того чтобы перейти в настройки эвристик, нужно перейти во вкладку «СОВ», далее нажать на категорию «**Сигнатуры**», «**Настройки эвристик**» (см. Рисунок 151):

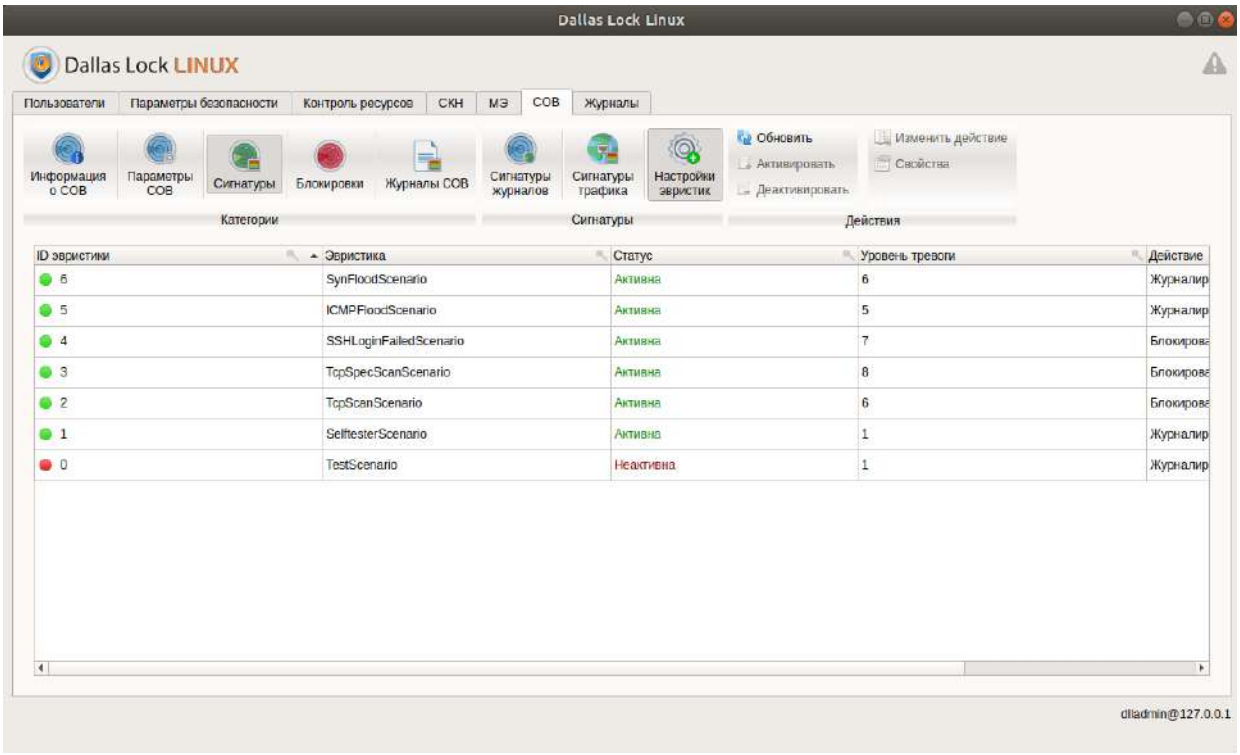


Рисунок 151. Окно «Настройки эвристик»

Для редактирования параметров эвристики необходимо найти редактор общих настроек (– Свойства) (см. Рисунок 152), выбрать нужную эвристику из списка и нажать левой кнопкой мыши по нужной иконке. Далее выбрать на панели «**Действия**» вкладку «**Свойства**» (см. Рисунок 153).

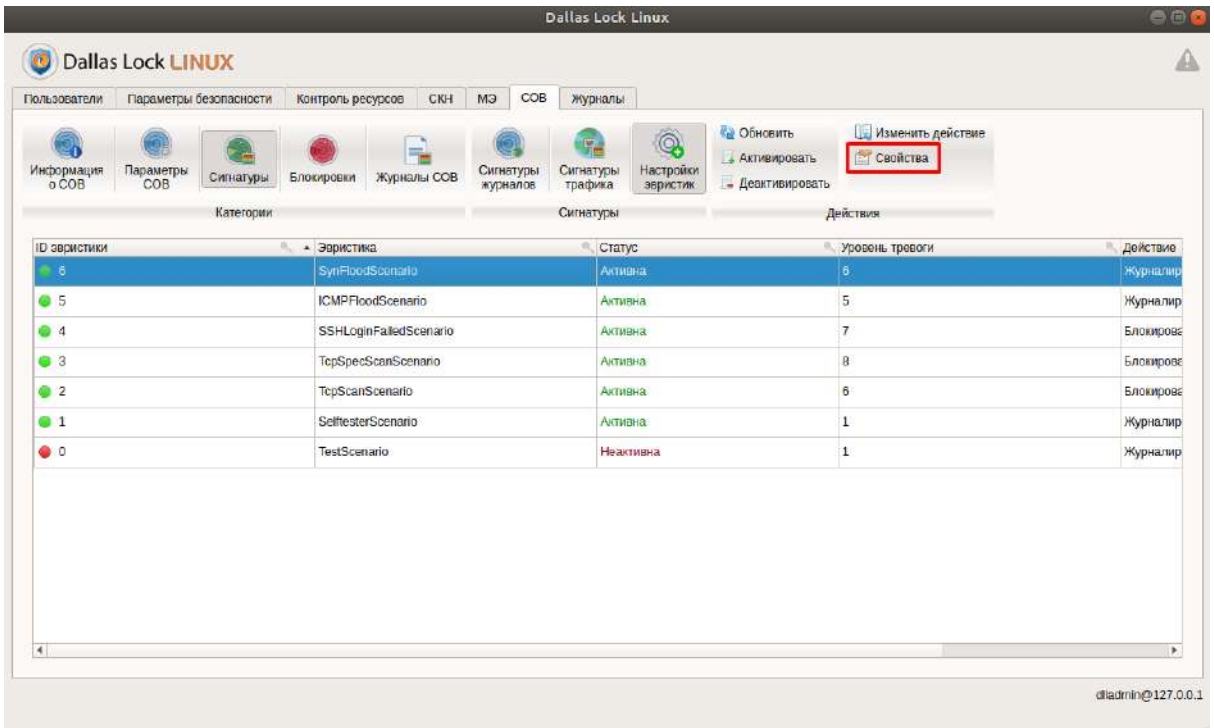


Рисунок 152. Свойства эвристик на панели «Действия»

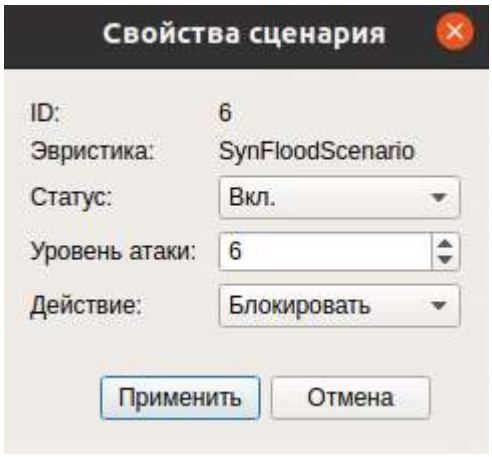


Рисунок 153. Свойства эвристики

Окно редактора настроек эвристики содержит:

- ID;
- Название эвристики;
- Выпадающий список «Статус». Позволяет устанавливать режим работы эвристики;
- Спинбокс «Уровень тревоги». Позволяет установить уровень тревоги для эвристики;
- Выпадающий список «**Действие**». Позволяет устанавливать действие для эвристики;
- Кнопка «**Применить**». Позволяет применить внесенные изменения для эвристики;
- Кнопка «**Отмена**». Кнопка «**Отмена**» позволяет отменить действия, вносимые Администратором и (или) закрывать окно редактора настроек «**Свойства**».

Для эвристик типа «flood» обязательно должна стоять реакция блокирование адреса.

Администратору доступны следующие действия (полные права) в категории «**Сигнатуры – Настройки эвристик**»:

Изменить действие ( ) – изменить действие для эвристики или эвристик. Для внесения изменений система выдает окно «**Изменение действия**» для выбранной эвристики или несколько выбранных эвристик. Окно «**Изменение действия**» содержит выпадающий список «Действие» (см. Рисунок 154).

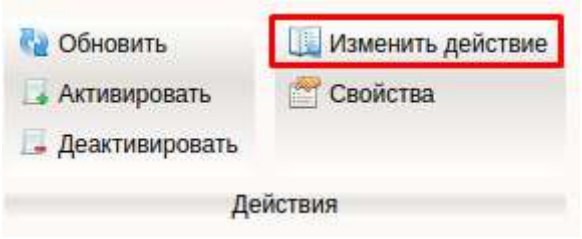


Рисунок 154. Кнопка «Изменить действие» на панели «Действия»

Выпадающий список позволяет выбрать действие для эвристики или эвристик. Кнопка «**Применить**» позволяет применить внесенные изменения для эвристики. Кнопка «**Отмена**» позволяет отменить действия, вносимые Администратором и (или) закрывать окно редактора настроек «**Изменение действия**».

Активировать ( ) – включить эвристики СОВ.

Деактивировать ( ) – выключить эвристики СОВ.

После выполнения активации и (или) деактивации эвристик (-и) **СЗИ НСД** принимает изменения.

При переходе в категорию «**Сигнатуры – Настройки эвристики**» следующие действия будут неактивными:

Активировать ( ), Деактивировать ( ), Свойства ( ), Изменить действие ( ).

Данные действия система активирует при условии, если Администратор в списке «Настройки эвристик» выделил эвристику и (или) эвристики для дальнейших действий: Активировать, Деактивировать, Изменить действие, Свойства.

В случае, если Администратор выделил несколько эвристик, то кнопка Свойства ( ) станет неактивной.

Обновить ( ) – обновить таблицу.

4.12.4 Управление категорией «Блокировки»

Консольная оболочка администрирования

Для вывода списка заблокированных адресов в консольной оболочке администрирования реализована команда *list-blocked-addresses* в разделе *hids*.

IP-адреса вносятся в список *list-blocked-addresses* при выполнении условия:

- *L2 <= I.*

При выполнении команды *list-blocked-addresses* в консольную оболочку администрирования выводится список заблокированных IP-адресов со следующими полями:

- № – номер строки;
- Version – версия интернет протокола. Допустимые значения: IPv4 и IPv6;
- Address – сетевой адрес компьютера. Допустимый формат: IPv4 и IPv6;
- ID – идентификационный номер журнальной сигнатуры, сигнатуры трафика, эвристики;
- Unlock time – время разблокировки IP-адреса;
- Description – причина блокировки.

Где, I – уровень тревоги сигнатуры и (или) эвристики, L1 – уровень журналирования, L2 – уровень тревоги в системе.

Для разблокировки адреса в консольной оболочке администрирования реализована команда *unblock-address* в разделе *hids*.

Разблокировка адреса происходит при выполнении команды *unblock-address* с указанием целочисленного номера строки адреса из таблицы заблокированных адресов (*list-blocked-addresses*).

Пример:

hids <enter>

unblock-address 1 <enter>

Request successfully completed

Графическая оболочка администрирования

При переходе в категорию «**Блокировки**», на вкладке «**СОВ**» в графической оболочке администрирования **СЗИ НСД** отображается окно заблокированных адресов со следующими столбцами (Рисунок 155):

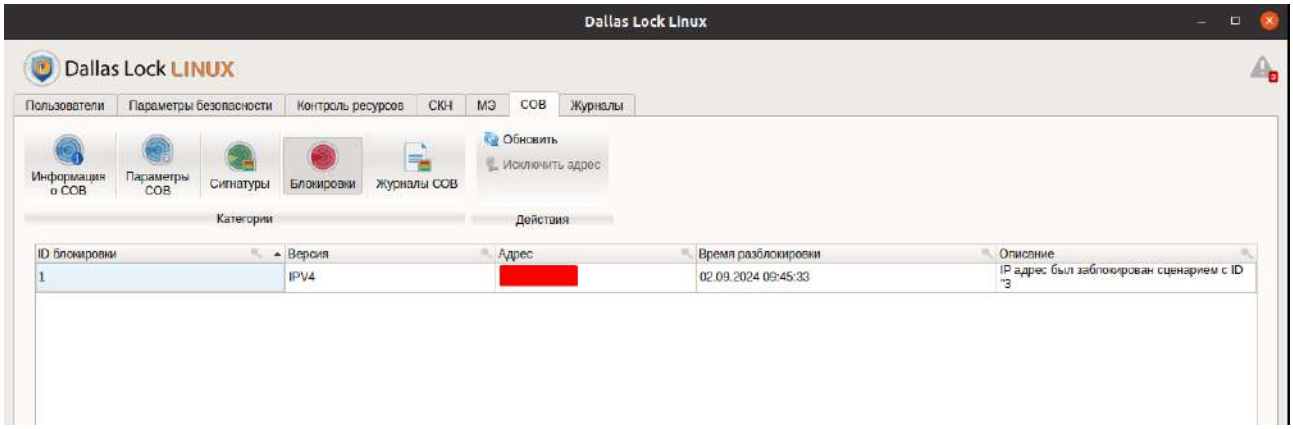


Рисунок 155. Окно заблокированных адресов

- ID блокировки – номер строки.
- Версия – Версия интернет протокола. Допустимые значения: IPv4 и IPv6.
- Адрес – Сетевой адрес компьютера. Допустимый формат: IPv4 и IPv6.
- Время разблокировки – Время, когда IP-адрес разблокируется.
- Описание – Причина блокировки (также другая дополнительная информация).

При установленной глобальной политике «Заблокировать навсегда» в столбец «Время разблокировки» система ставит прочерк "–". В столбце «Описание» содержится дополнительная информация, что IP-адрес заблокирован навсегда.

События НСД и заблокированные адреса регистрируются автоматически при срабатываниях следующих настроек глобальных параметров СОВ:

- *L2 <= I.*

Где I – уровень тревоги сигнатуры и (или) эвристики, L1 – уровень журналирования, L2 – уровень тревоги в системе.

Администратору доступны следующие действия (полные права) в категории «Блокировки»:

Обновить () – обновить таблицу категории «Блокировки».

Исключить адрес (-а) () – убрать IP-адрес из списка заблокированных, в том числе IP-адреса заблокированных при установленной глобальной политики «Заблокировать навсегда».

Выделить все строки () – выделение всего списка заблокированных адресов.

СЗИ НСД позволяет Администратору выделить несколько заблокированных адресов с помощью горячих клавиш: **Ctrl** и **Shift**.

4.12.5 Управление категорией «Журналы СОВ»

Консольная оболочка администрирования

В подсистеме регистрации и учета **СЗИ НСД** (*audit*) присутствует возможность просмотра журналов безопасности СОВ: *hids-sec-events* (события безопасности СОВ), *hids-management* (управление СОВ), а именно использования инструментов *audit: archivate, export-ods, export-pdf, export-xml u get-journal: journal, event-type, from-time, till-time, resilt, archive-path*.

Пример:

cli> audit <enter>

audit> get-journal <enter>

get-journal> journal hids-management <enter>

g
e

Графическая оболочка администрирования

j
При переходе в категорию «**Журналы СОВ**» в графической оболочке администрирования **СЗИ НСД** по умолчанию отображен журнал «**События безопасности СОВ**» (см. Рисунок 77).

u
Администратору доступны следующие действия (полные права) во вкладках «**Журналы СОВ**» для журналов «**События безопасности СОВ**» и «**Управление СОВ**»:

a
l
e
Обновить () – обновить таблицу с событиями.

x
e
c
u
t
e
e
n
t
e
r
Экспортировать () – экспортировать события в ОС. При нажатии появляется системное окно, которое позволяет Администратору записать события в необходимую папку. В **СЗИ НСД** присутствует возможность экспорта записей журнала или отфильтрованных записей журнала в следующие форматы: PDF, ODS, XML (Рисунок 156).

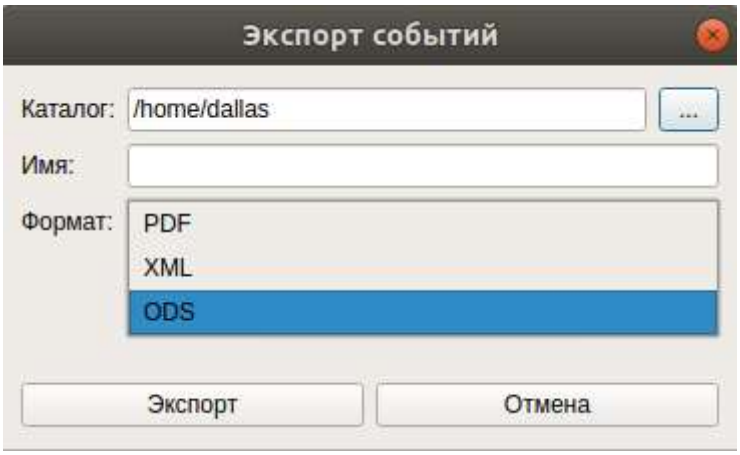


Рисунок 156. Экспорт событий в ОС

Настройка отображаемых столбцов ( ) – позволяет Администратору исключить из вида некоторые столбцы (атрибуты).

Архивировать (очистить) ( ) – действие архивации журналов безопасности СОВ.

Во вкладке «**Журналов СОВ**» для журналов «**События безопасности СОВ**» и «**Управление СОВ**» имеется общая фильтрация данных (Рисунок 157):

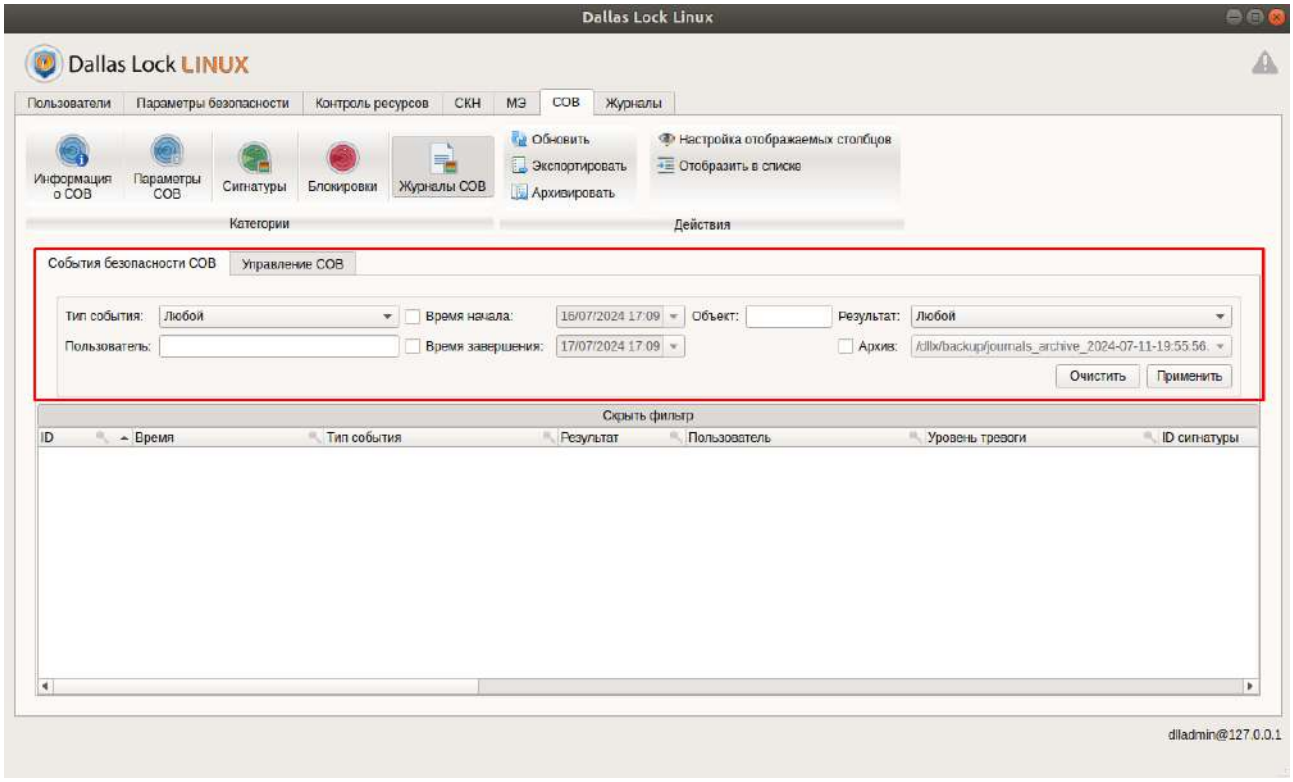


Рисунок 157. Фильтрация данных в категории «Журналы СОВ»

4.13 Автоматическое тестирование функциональных возможностей

Данная функция позволяет выполнить автоматическое тестирование основных функциональных возможностей системы защиты (создание/удаление пользователя, проверки параметров доступа к ресурсам и пр.).

Консольная оболочка администрирования

Для перехода в подсистему автоматического тестирования функциональных возможностей необходимо в консольной оболочке администрирования (*ishl*) выполнить команду *testing.*

Далее консольное приложение будет ожидать ввода управляющих команд подсистемы автоматического тестирования, список команд представлен в Таблица 68.

Таблица 68

№	Команда	Описание
1	*start-self-test*	Команда запуска самотестирования системы. Процесс самотестирования занимает до двух минут. **Проверка функционирования подсистемы идентификации и аутентификации.** Описание теста. Тест включает в себя авторизацию пользователя в системе. **Проверка функционирования подсистемы управления доступом**. Описание теста. Тест включает в себя следующие проверки и действия: – создание тестовой группы и пользователя; – создание тестового файла; – назначение прав «только чтение» на тестовый файл для тестового пользователя; – попытка произвести запись в тестовый файл от имени тестового пользователя; – удаление тестового файла, тестовых пользователя и группы. **Проверка подсистемы контроля целостности.** Описание теста. Тест включает в себя следующие проверки и действия: – изменение одного из подконтрольных файлов; – запуск службы проверки контроля целостности; – проверка факта восстановления измененного в тесте файла. **Проверка подсистемы межсетевого экрана.** Описание теста. Тест включает в себя следующие проверки и действия: – запуск/выключение межсетевого экрана; – запуск проверки общих правил, правил протокола L7, правил SSL; – запуск тестирования приложений черного списка **Проверка системы обнаружения вторжений.** Описание теста. Тест включает в себя следующие проверки и действия: – срабатывание тестовой сигнатуры
2	*stop-self-test*	Команда завершения самотестирования системы
3	*get-self-test-result*	Команда вывода результата теста самотестирования системы. **Ожидаемый результат проверки функционирования подсистемы идентификации и аутентификации.** Сообщение в CLI об удачном/неудачном выполнении команды. Соответствующие записи в системе аудита в журнале Entries: – запись о попытке аутентификации. **Ожидаемый результат проверки функционирования подсистемы управления доступом.**

№	Команда	Описание
		Сообщение в CLI об удачном/неудачном выполнении команды. Соответствующие записи в системе аудита в журналах Entries, Users, Resources: – запись о создании группы и пользователя; – запись о назначении прав на тестовый файл; – запись о попытке изменения файла со стороны пользователя; – запись о результате теста системы самотестирования. **Ожидаемый результат проверки подсистемы контроля целостности.** Сообщение в CLI об удачном/неудачном выполнении команды. Соответствующие записи в системе аудита в журналах *Entries, Resources*: – запись об изменении подконтрольного файла со стороны пользователя. **Ожидаемый результат проверки подсистемы межсетевого экрана.** Сообщение в CLI об удачном/неудачном выполнении команды. Соответствующие записи в системе аудита в журнале *Fw-management:* – запись о результатах теста системы самотестирования. **Ожидаемый результат проверки системы обнаружения вторжений.** Сообщение в CLI об удачном/неудачном выполнении команды: – проверка прошла успешно (успех). Тест пройден. – проверка прошла безуспешно (отказ). Тест не пройден.

Пример:

testing <enter>

start-self-test <enter>

get-self-test-result <enter>

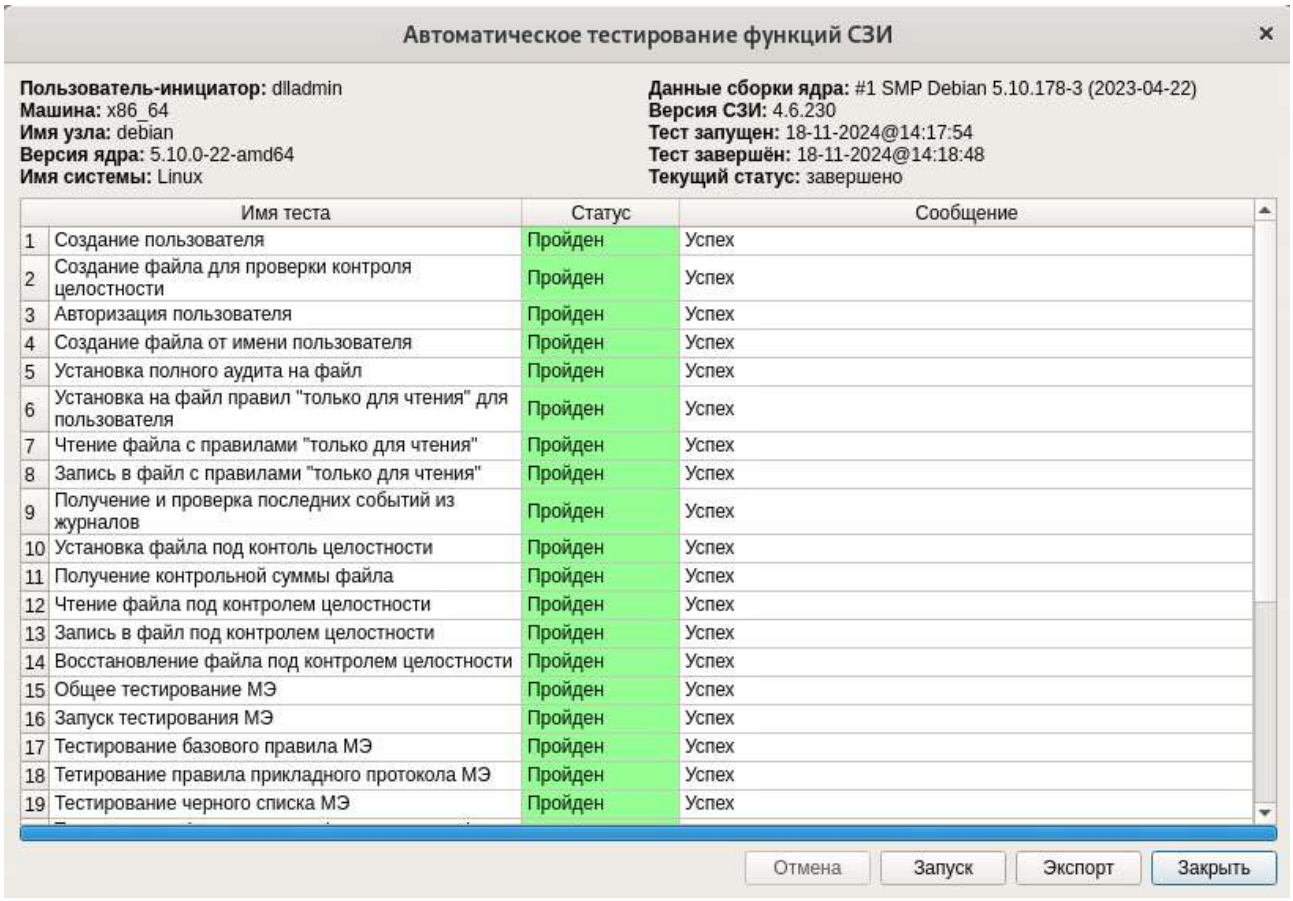
Графическая оболочка администрирования

Для запуска автоматического тестирования функциональных возможностей в графической оболочке **СЗИ НСД** необходимо нажать кнопку  основного меню и в списке функций выбрать пункт «**Тестирование функций СЗИ**» (см. Рисунок 158).

Рисунок 158. Тестирование функций СЗИ

В появившемся окне нужно нажать кнопку «**Запуск**».

При окончании тестирования, при необходимости, можно сохранить отчет, нажав кнопку «**Экспорт**» (см. Рисунок 159).



	Имя теста	Статус	Сообщение
1	Создание пользователя	Пройден	Успех
2	Создание файла для проверки контроля целостности	Пройден	Успех
3	Авторизация пользователя	Пройден	Успех
4	Создание файла от имени пользователя	Пройден	Успех
5	Установка полного аудита на файл	Пройден	Успех
6	Установка на файл правил "только для чтения" для пользователя	Пройден	Успех
7	Чтение файла с правилами "только для чтения"	Пройден	Успех
8	Запись в файл с правилами "только для чтения"	Пройден	Успех
9	Получение и проверка последних событий из журналов	Пройден	Успех
10	Установка файла под контоль целостности	Пройден	Успех
11	Получение контрольной суммы файла	Пройден	Успех
12	Чтение файла под контролем целостности	Пройден	Успех
13	Запись в файл под контролем целостности	Пройден	Успех
14	Восстановление файла под контролем целостности	Пройден	Успех
15	Общее тестирование МЭ	Пройден	Успех
16	Запуск тестирования МЭ	Пройден	Успех
17	Тестирование базового правила МЭ	Пройден	Успех
18	Тетирование правила прикладного протокола МЭ	Пройден	Успех
19	Тестирование черного списка МЭ	Пройден	Успех

Рисунок 159. Автоматическое тестирование функций СЗИ

Для экспорта отчета системой будет предложено выбрать папку для текстового файла. По умолчанию отчет сохраняется в формате *.pdf (см. Рисунок 160).

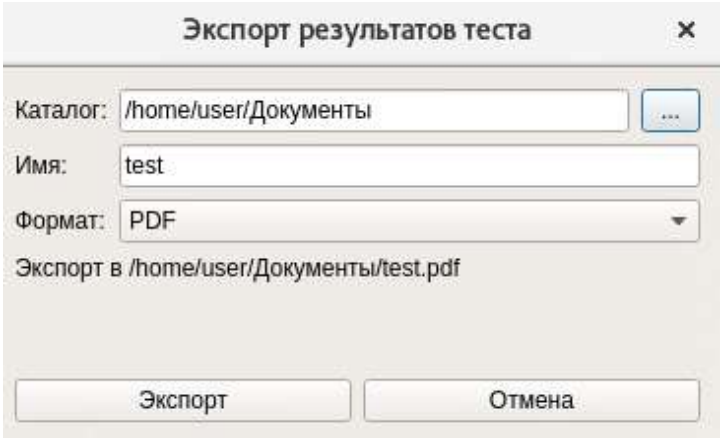


Рисунок 160. Экспорт результатов тестирования

4.14 Централизованное управление системой защиты

Возможности централизованного управления **СЗИ НСД** предоставляют Сервер безопасности Dallas Lock и Единый центр управления **Dallas Lock** (**ЕЦУ Dallas Lock**), управление которым осуществляется отдельным приложением «**Консоль ЕЦУ**».

Единый Центр Управления **Dallas Lock** позволяет просматривать журналы событий и настраивать систему защиты в части:

- управления политиками безопасности;
- управления атрибутами пользователей и групп;
- управления параметрами аудита событий.

Любой компонент продуктовой линейки **ООО «Конфидент»** (**СЗИ Dallas Lock 8.0**, **СДЗ Dallas Lock**, **СДЗ УБ Dallas Lock**, **СЗИ НСД Dallas Lock Linux**, **СЗИ ВИ Dallas Lock**, **WAF Dallas Lock**), находящийся под управлением Домена безопасности **ЕЦУ** (далее — **ДБ**, **ДБ ЕЦУ**), — это модуль.

СЗИ НСД не может находиться под управлением **ЕЦУ Dallas Lock** и Сервера безопасности **Dallas Lock** одновременно.

С подробным описанием **ЕЦУ Dallas Lock** можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock ПФНА.501410.002 И3.

С подробным описанием СБ Dallas Lock можно ознакомиться в Руководстве по эксплуатации RU.48957919.501410-01 92 и RU.48957919.501410-02 92.

При вводе в Сервер безопасности **Dallas Lock** количество пользователей в группе Linux клиента ограничено. В группе должно быть зарегистрировано не более 21 пользователя. В ином случае, могут возникнуть ошибки при синхронизации групп с **СБ**.

Консольная оболочка администрирования

Для перехода в подменю централизованного управления **СЗИ НСД** с помощью **ЕЦУ Dallas Lock** необходимо выполнить команду *management-dll*.

Для данного раздела доступны следующие управляющие команды:

- *connect-domain* — переход в подменю подключения к домену безопасности;
- *disconnect-domain* — отключение от домена безопасности;
- *synchronize* — синхронизировать журналы безопасности с **ЕЦУ**;
- *journals-synchronize* — синхронизировать журналы с **ЕЦУ**;
- *disconnect-sb* — отключение от сервера безопасности в одностороннем порядке;
- *list* — просмотр списка управляющих команд раздела;
- *info* — отображение информации о сервере, если **СЗИ НСД** находится под управлением Сервера безопасности **Dallas Lock** или **ЕЦУ Dallas Lock**;
- *help* — вывод информации о встроенных командах консольной оболочки администрирования;
- *back* — выход из подраздела (на уровень выше);
- *exit* — выход из консольной оболочки администрирования и закрытие сессии *dlladmin*.

Для подключения модуля DLL к домену безопасности **ЕЦУ** необходимо в разделе *management-dll* выполнить команду *connect-domain.* После ввода команды система перейдет в раздел *connect-domain* (подменю подключения к домену безопасности). Далее консольное приложение будет ожидать ввода управляющих команд данной подсистемы, список команд приведен в Таблица 69.

Таблица 69

№	Команда	Описание
1	*net-name <значение>*	Сетевое имя или IP-адрес сетевого узла, на котором установлена Служба **ЕЦУ**. При указании сетевого имени или IP-адреса важно указать номер порта
2	*name <значение>*	Сетевое имя или прочее говорящее название для сетевого узла, которое будет отображаться в панели **ЕЦУ** в списке управляемых объектов
3	*key <значение>*	Ключ доступа к ДБ **ЕЦУ**

Пример:

net-name <ip-address>:<port> <enter>

name <hostname> <enter>

key <значение> <enter>

execute <enter>

В случае ошибки при подключении к домену безопасности **ЕЦУ Dallas Lock** отобразится соответствующее сообщение.

Для отключения от домена безопасности необходимо выполнить команду *disconnect-domain* с атрибутом:

- *force* — принудительное отключение от домена безопасности без связи **ЕЦУ**. При выполнении команды оповещение **ЕЦУ** не происходит;
- *yes* — вывод из домена безопасности с оповещением **ЕЦУ**.

В случае выполнения команды *disconnect-domain* с установленным неверным атрибутом или пустым, отобразятся соответствующие сообщения об ошибках: «*There is no connection to UCC and no "force" flag. Aborting* — отсутствует соединение с **ЕЦУ** и атрибут '*force*'. Прерывание.», «*wrong command* — неверная команда».

Пример:

management-dll <enter>

disconnect-domain force <enter>

В результате успешного выполнения команды появится сообщение: «*Unregistration success*» — модуль успешно выведен из **ДБ**.

Графическая оболочка администрирования

Для настройки управления **СЗИ НСД** с помощью графической оболочки **СЗИ НСД** на вкладке «**Параметры безопасности**» необходимо выбрать категорию «**Основные настройки**» и запустить поле «*Настройка домена безопасности*» на панели действий. После запуска поля «Настройка домена безопасности» откроется окно настройки централизованного управления системы защиты (см. Рисунок 161).

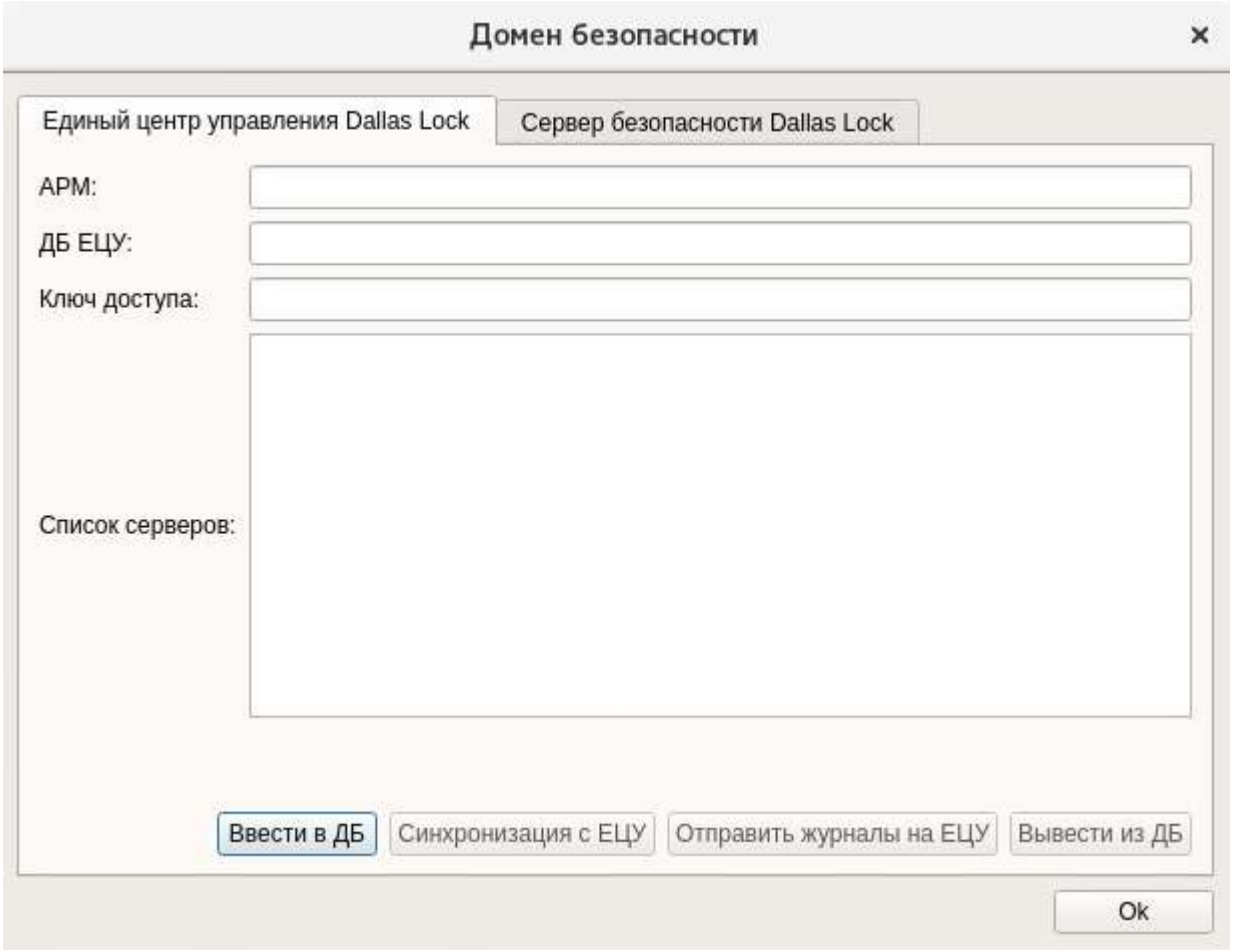


Рисунок 161. Централизованное управление системы защиты

1. В том случае, если **СЗИ НСД** находится под управлением Сервера безопасности (**СБ**), в значении поля «*СБ*» будет отображено имя компьютера в сети или IP-адрес, на котором установлен **СБ**. Поля для ввода, относящиеся к **ЕЦУ**, и кнопки «**Ввести в ДБ**», «**Вывести из ДБ**» будут недоступны для ввода и нажатия.

2. Если **СЗИ НСД** не находится под управлением **СБ**, необходимо будет заполнить следующие поля:

- «АРМ» — сетевое имя или прочее говорящее название для сетевого узла, которое будет

отображаться в панели **ЕЦУ** в списке управляемых объектов;

- «ДБ ЕЦУ» — сетевое имя или IP-адрес сетевого узла, на котором установлена Служба **ЕЦУ**;
- «Ключ доступа» — ключ доступа к **ДБ** (может быть пустым).

Далее нужно нажать кнопку «**Ввести в ДБ**». Если указанные поля не заполнены, кнопка «**Ввести в ДБ**» будет недоступна для нажатия».

Результат успешного выполнения: *«Модуль успешно зарегистрирован в Домене Безопасности»*.

Результат ошибочного выполнения:

- *«На указанном АРМ уже зарегистрирован модуль этого типа»* — АРМ с указанным именем найдено, и на нем уже зарегистрировано **СЗИ НСД Dallas Lock Linux**;
- *«Модуль уже находится под управлением Сервера безопасности*» — **СЗИ НСД Dallas Lock Linux** уже находится под управлением СБ;
- *«Превышено максимально допустимое число АРМ»* — превышено максимально допустимое число АРМ;
- *«Сетевой доступ к серверу ЕЦУ отсутствует»* — сервер **ЕЦУ** не доступен по сети;
- *«Доступ к серверу ЕЦУ отсутствует»* — в случае иных ошибок (например, ввод неправильного ключа доступа к **ДБ**).

В результате выполнения операции ввода **СЗИ НСД Dallas Lock Linux** получает от **ЕЦУ** список серверов, он будет отображен в поле «*Список серверов*». Этот список будет обновляться в процессе синхронизации с **ЕЦУ Dallas Lock** и будет пустым, если **СЗИ НСД Dallas Lock Linux** не введена в Домен безопасности **ЕЦУ**.

5 ХРАНЕНИЕ И ТРАНСПОРТИРОВАНИЕ ИЗДЕЛИЯ

Изделие поставляется в составе, указанном в Таблица 1 (см. Состав изделия).

Хранение и транспортирование изделия осуществляется в соответствии с требованиями документа «Технические условия» ПФНА.501410.002 ТУ.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Полная формулировка
АИ	Аппаратный идентификатор
АРМ	Автоматизированное рабочее место
ДБ	Домен безопасности
ЕЦУ	Единый центр управления
МЭ	Межсетевой экран
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
СБ	Сервер безопасности
СЗИ НСД	Система защиты информации от несанкционированного доступа
СЗИ	Система защиты информации
СКН	Средство контроля съемных машинных носителей информации
СОВ	Система обнаружения вторжений
ТС	Техническое средство
УЗ	Учетные записи
ФС	Файловая система
ЦЗИ	Центр защиты информации
SSH	Протокол прикладного уровня удаленного управления компьютером с операционной системой Linux
DLL	Dallas Lock Linux
PIN	Персональный идентификационный номер
GUI	Графическая оболочка администрирования
CLI	Интерфейс командной строки