ПАО «ГАЗПРОМ АВТОМАТИЗАЦИЯ»

СИСТЕМА ЛИНЕЙНОЙ ТЕЛЕМЕХАНИКИ «МАГИСТРАЛЬ-ДУ» (SCADA «ПОТОК-ДУ»)

ОПЫТНЫЙ ОБРАЗЕЦ

Эксплуатационная документация

Руководство администратора информационной безопасности

00159093.28.99.39.190.СЛТМ.2850.И13-02

2022

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
12853				

Содержание

Перв. примен.

Справ. №

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл. 12853

Изм	Лист	№ докум.	Подпись	Дата
Разраб.		Семенников		12.22
Пров.		Панкова		12.22
Н.контр.		Колесникова		12.22
Утв.		Мирошников		12.22

00159093.28.99.39.190.СЛТМ.2850.И13-02

СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ»)

Руководство администратора информационной безопасности

Лит.	Лист	Листов
	2	74

ГАЗПРОМ АВТОМАТИЗАЦИЯ

1 Введение

1.1 Основные понятия

Система линейной телемеханики «Магистраль-ДУ» (SCADA «Поток-ДУ») (далее по тексту – Система) предназначена для обеспечения автоматического контроля и автоматизированного управления технологическими процессами и оборудованием линейной части магистральных газопроводов (ЛЧ МГ) в условиях периодического технического обслуживания и в период эксплуатации и проведения ремонтных работ на объектах магистральных газопроводов.

Согласно п. 2.4.5. ГОСТ Р 50922-2006, под **безопасностью информации (данных)** понимается состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность. В Системе предусмотрены меры защиты информации от неправильных действий персонала и от случайных изменений, а также от несанкционированного доступа к информации.

Администратор информационной безопасности (ИБ) Системы назначается приказом и является лицом, выполняющим функции по защите информации обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в пределах зоны своей ответственности.

К задачам администратора ИБ относится:

– поддержание системы в рамках выбранной политики безопасности;

– обеспечение должного уровня конфиденциальности и целостности данных;

– подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;

– создание и поддержание в актуальном состоянии пользовательских учётных записей;

– отслеживание информации об уязвимостях Системы и своевременное принятие мер;

– периодическое практическое тестирование защищенности Системы.

1.2 Уровень подготовки пользователя

Администратор информационной безопасности должен:

– обладать базовыми знаниями и навыками пользователя ОС Astra Linux Special Edition (версия 1.7);

– знать предметную область, в которой осуществляется управление и, в частности, знать и понимать все технологические процессы, проходящие на объекте автоматизации;

– иметь опыт администрирования ОС Astra Linux в объеме курсов:

– ALSE-1701. Astra Linux для пользователей;

– ALSE-1702. Astra Linux. Базовое администрирование.

– ALSE-1703. Astra Linux. Расширенное администрирование.

– ALSE-1705. Astra Linux. Специальный курс.

1.3 Перечень эксплуатационной документации

В процессе работы администраторы информационной безопасности должны руководствоваться следующими документами на Систему:

– ведомость эксплуатационных документов (00159093.28.99.39.190.СЛТМ.2850.ВЭ-02);

– ведомость программного обеспечения, лицензий и ключей, код В9 (00159093.28.99.39.190.СЛТМ.2850.В9-02);

– руководство пользователя (00159093.28.99.39.190.СЛТМ.2850.И3-02);

– руководство администратора информационной безопасности (00159093.28.99.39.190.СЛТМ.2850.И13-02);

– инструкция по эксплуатации КТС (00159093.28.99.39.190.СЛТМ.2850.ИЭ-02);

– паспорт (00159093.28.99.39.190.СЛТМ.2850.ПС…-02);

– формуляр (00159093.28.99.39.190.СЛТМ.2850.ФО-02);

– шаблон документа (00159093.28.99.39.190.СЛТМ.2850.С9-02).

– Документация ОС специального назначения Astra Linux Special Edition (версия 1.7).

– Документация к программному комплексу Альфа-платформа.

– Документация к программному обеспечению Kaspersky Endpoint Security для Linux.

2 Перечень программного обеспечения

Для нормального функционирования на серверах и АРМ оператора должно быть установлено следующее программное обеспечение (ПО):

– ОС специального назначения Astra Linux Special Edition («Смоленск») версии 1.7 Разрядность ОС: x64 или x32;

– Проект SCADA-системы технологического объекта, площадки;

– ПО защиты компьютеров под управлением операционных систем Linux от вредоносных программ Kaspersky Endpoint Security для Linux;

– ПО резервного копирования и восстановления Astra Linux Lucky backup.

ОС специального назначения Astra Linux Special Edition предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

3 Программное обеспечение Kaspersky Endpoint Security

3.1 Установка и настройка программы

Процесс установки программного обеспечения Kaspersky Endpoint Security (KES) выполняется с использованием программы «Терминал Fly». Для запуска программы «Терминал Fly» перейдите в меню «Пуск», «Системные» и выберите «Терминал Fly» (см. Рисунок 1).

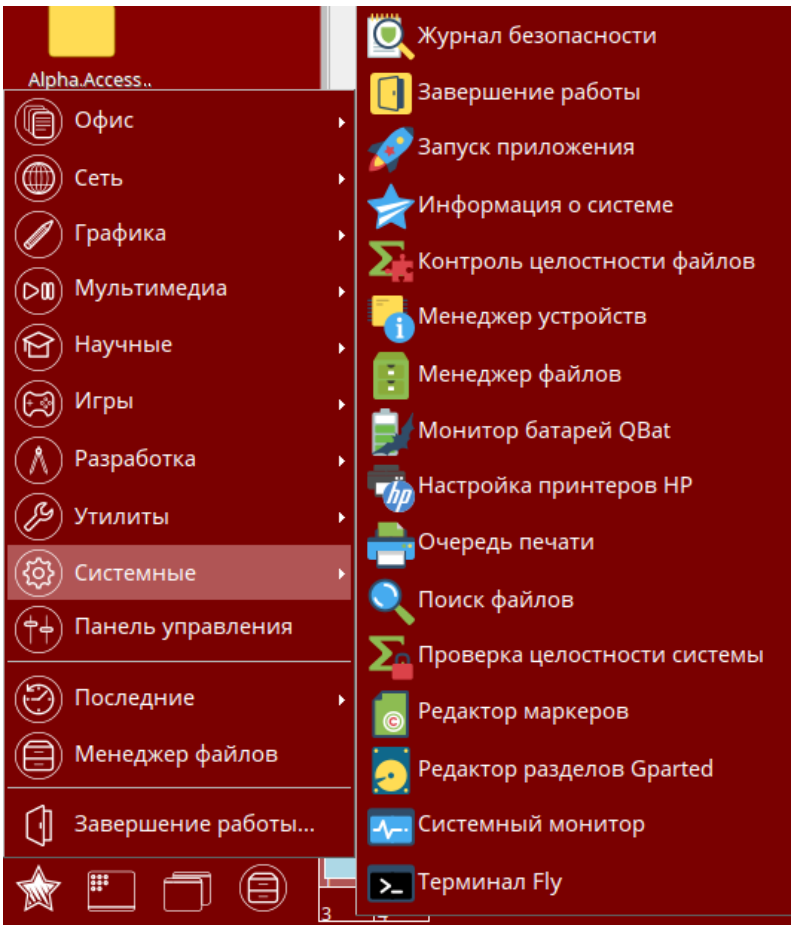


Рисунок 1

Антивирус Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM. В ОС Astra Linux используются пакеты форматов DEB.

Выполните установку антивируса Kaspersky Endpoint Security с помощью команды (см. Рисунок 2)

`sudo dpkg –i /home/administrator/kesl-astra_<номер сборки>_amd64.deb`,

где `/home/administrator/kesl-astra_<номер сборки>_amd64.deb` – путь до установочного файла и сам установочный файл.

```
administrator@astraSDK:~$ sudo dpkg -i /home/administrator/kesl-astra_11.2.0-
4528_amd64.deb
Выбор ранее не выбранного пакета kesl-astra.
(Чтение базы данных … на данный момент установлено 139110 файлов и каталогов.)
Подготовка к распаковке …/kesl-astra_11.2.0-4528_amd64.deb …
Распаковывается kesl-astra (11.2.0-4528) …
Настраивается пакет kesl-astra (11.2.0-4528) …
Created symlink /etc/systemd/system/kesl-supervisor.service -> /lib/systemd/system/kesl-
supervisor.service.
Created symlink /etc/systemd/system/kesl.service -> /lib/systemd/system/kesl-
supervisor.service.
Created symlink /etc/systemd/system/multi-user.target.wants/kesl-supervisor.service ->
/lib/systemd/system/kesl-supervisor.service.

Kaspersky Endpoint Security 11.2.0 for Linux has been installed successfully,
but it must be properly configured before using.
Please run "/opt/kaspersky/kesl/bin/kesl-setup.pl" script
manually to configure it.

Обрабатываются триггеры для man-db (2.7.6.1-2) …
administrator@astraSDK:~$
```

Рисунок 2

После установки антивируса Kaspersky Endpoint Security требуется запустить скрипт первоначальной настройки Kaspersky Endpoint Security, входящий в пакет Kaspersky Endpoint Security. Для этого выполните следующую команду (см. Рисунок 3).

```
sudo /opt/kaspersky/kesl/bin/kesl-setup.pl.
```

Скрипт первоначальной настройки необходимо запустить с правами суперпользователя (root). Скрипт пошагово запрашивает значения параметров Kaspersky Endpoint Security.

```
administrator@astraSDK:~$ sudo /opt/kaspersky/kesl/bin/kesl-setup.pl

Kaspersky Endpoint Security 11.2.0 for Linux version 11.2.0.4528


Setting up the Anti-Virus Service default locale

Specified locale will be used to show user agreements in this script and
send events to Kaspersky Security Center.
List of available locales:
- ru_RU.UTF-8
- de_DE.UTF-8 [not supported by OS]
- en_US.UTF-8 [not supported by OS]
- fr_FR.UTF-8 [not supported by OS]
- ja_JP.UTF-8 [not supported by OS]
[ru_RU.UTF-8]:
administrator@astraSDK:~$
```

Рисунок 3

На первом шаге вам нужно задать обозначение языкового стандарта, который будет использоваться при работе антивируса Kaspersky Endpoint Security. По умолчанию программа предлагает использовать языковой стандарт, установленный для суперпользователя (root). Подтвердите клавишей **Enter** выбор стандартного языка при появлении сообщения.

Далее нажмите клавишу **Enter**, чтобы ознакомиться с лицензионным соглашением и политикой конфиденциальности (Рисунок 4). Чтобы переходить по разделам текста, используйте клавиши со стрелками или клавиши **B** (чтобы перейти на один экран назад) и **F** (чтобы перейти на один экран вперед). Для получения справки нажмите на клавишу **H**. Чтобы завершить просмотр, нажмите на клавишу **Q**.

```
Anti-Virus Service default locale is changed to 'ru_RU.UTF-8'.
Service will be restarted if it is already running.

Accepting the End User License Agreement (EULA) and Privacy Policy

Please confirm that you have fully read, understand, and accept the End
User License Agreement (EULA) and Privacy Policy to continue.

NOTE: To quit the EULA and Privacy Policy viewer, press the Q key.

Press ENTER to display the EULA and Privacy Policy:
```

Рисунок 4

Примите лицензионное соглашение, для этого нажмите клавиши «y» и **Enter** (Рисунок 5).

```
Read EULA and Privacy Policy from file "/opt/kaspersky/kesl/doc/license.ru"
(utf-8) if it cannot be read here.

I confirm that I have fully read, understand, and accept the terms and
conditions of this End User License Agreement [y/n]: y
```

Рисунок 5

Повторно подтвердите, что принимаете лицензионное соглашение, для этого нажмите клавиши «y» и **Enter** (Рисунок 6).

```
Please answer either 'y' or 'n'.
I confirm that I have fully read, understand, and accept the terms and
conditions of this End User License Agreement [y/n]: y
```

Рисунок 6

Примите политику конфиденциальности, для этого нажмите клавиши «y» и **Enter** (Рисунок 7).

```
I am aware and agree that my data will be handled and transmitted
(including to third countries) as described in the Privacy Policy. I
confirm that I have fully read and understand the Privacy Policy [y/n]: y
```

Рисунок 7

Ознакомьтесь и примите заявление KASPERSKY SECURITY NETWORK (KSN Statement), для этого нажмите клавиши «y» и **Enter** (Рисунок 8).

```
Configuring KSN

I confirm that I have fully read, understand, and accept the terms and
conditions of the Kaspersky Security Network Statement (KSN Statement is
available here: '/opt/kaspersky/kesl/doc/ksn_license.ru') [y/n]: y
```

Рисунок 8

Установите графический интерфейс пользователя (GUI), для этого нажмите клавиши «y» и **Enter** (Рисунок 9).

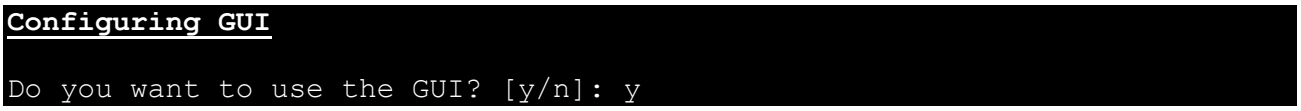


Рисунок 9

Введите логин для учетной записи администратора – **administrator**, и нажмите клавишу **Enter** (Рисунок 10).

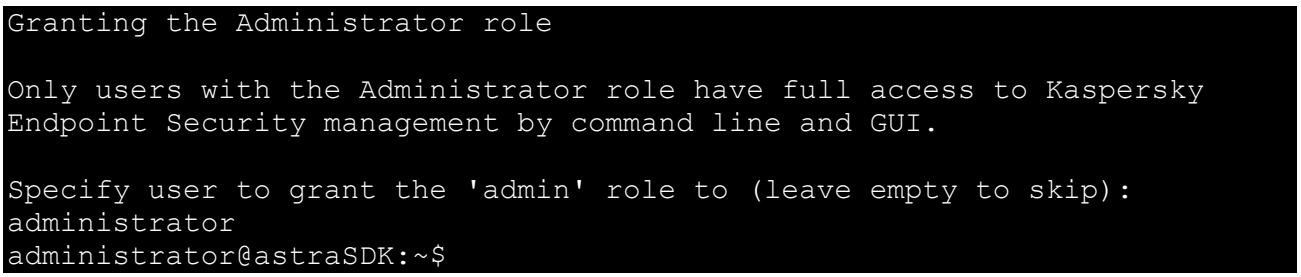


Рисунок 10

Укажите источник обновлений баз и модулей антивируса (Рисунок 11) и нажмите клавишу **Enter**:

- KLServers — с одного из серверов обновлений «Лаборатории Касперского»;
- SCServer — с установленного в локальной сети Сервера администрирования Kaspersky Security Center;
- <Url> — вы можете указать адрес пользовательского источника обновлений в локальной сети или в сети Интернет.

Внимание! Если вы планируете управлять Kaspersky Endpoint Security и обновлять базы данных и модулей антивируса с помощью Kaspersky Security Center, необходима установка на серверах и АРМ программы Агента администрирования.

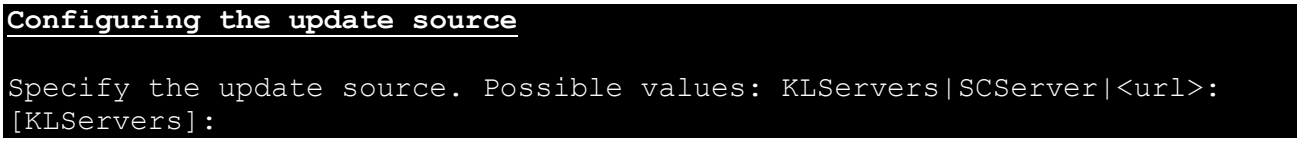


Рисунок 11 – Запрос источника обновлений

Далее предлагается ввести настройки прокси-сервера — откажитесь, нажав клавиши «n» и **Enter** (Рисунок 34).

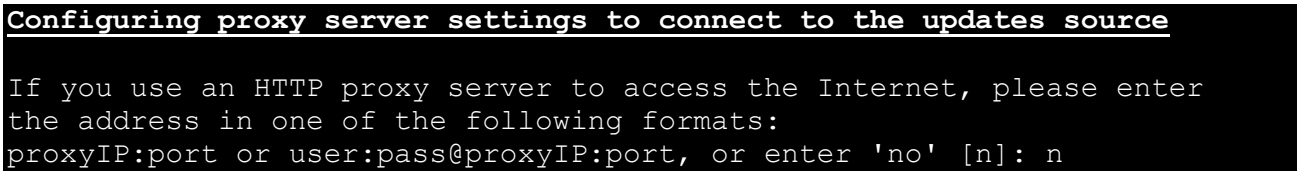


Рисунок 12 – Запрос на настройки прокси-сервера

На следующем этапе предлагается обновить базы данных антивируса, нажмите клавиши «y» (согласиться на обновление) или «n» (отказаться от обновления) и **Enter** (Рисунок 13).

```
Please note that the application may be restarted during the update
process.
Do you want to download the latest databases now? [y]: n
```

Рисунок 13 – Запрос обновления баз данных антивируса

Далее предлагается включить автоматическое обновление, нажмите клавиши «y» (включить автоматическое обновление) или «n» (отказаться от автоматического обновления) и **Enter** (Рисунок 14).

```
Enabling automatic updates of the application databases

Do you want to enable scheduled updates? [y]: y
```

Рисунок 14 – Запрос на автоматическое обновление баз данных антивируса

На завершающем этапе установки и настройки антивируса Kaspersky Endpoint Security необходимо выполнить его активацию, для этого введите ключ и нажмите клавишу **Enter** (Рисунок 15).

```
Activate the application

You must activate the application to use it.
To activate the application now, enter the path to your key file or an
activation code. Enter an empty string to add the built-in trial key:
```

Рисунок 15 – Запрос активации антивируса

3.2 Запуск и остановка программы

По умолчанию программа Kaspersky Endpoint Security запускается автоматически при запуске ОС (на уровнях выполнения по умолчанию, принятых для каждой ОС). Программа Kaspersky Endpoint Security запускает все служебные задачи, а также пользовательские задачи, в параметрах расписания которых задан режим запуска PS (запускать задачу после запуска программы).

Если вы остановите программу Kaspersky Endpoint Security, все выполняющиеся задачи будут прерваны. После повторного запуска Kaspersky Endpoint Security прерванные пользовательские задачи автоматически не возобновляются. Будут запущены снова только те пользовательские задачи, в параметрах расписания которых задан режим запуска PS.

Чтобы запустить программу Kaspersky Endpoint Security в ОС Astra Linux, выполните команду:

```
systemctl start kesl
```

Чтобы остановить программу Kaspersky Endpoint Security, выполните команду:

```
systemctl stop kesl
```

Чтобы перезапустить программу Kaspersky Endpoint Security, выполните команду:

```
systemctl restart kesl
```

Чтобы вывести текущий статус программы Kaspersky Endpoint Security, выполните команду:

```
systemctl status kesl
```

Работающая программа должна иметь статус **active** (running).

3.3 Управление задачами с помощью командной строки

Для работы с программой Kaspersky Endpoint Security предусмотрено два типа задач:

– *Предустановленная задача* – задача, которая создается во время установки программы. Вы не можете удалять предустановленные задачи, но можете изменять параметры этих задач.

– *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно.

Идентификатор (ID) задачи – номер задачи, который программа присваивает задаче при ее создании. Идентификаторы пользовательских задач начинаются с 100. Все задачи, включая удаленные, имеют уникальные идентификаторы. Программа не использует повторно идентификаторы удаленных задач. Идентификатор новой задачи представляет собой номер, следующий по порядку за идентификатором последней созданной задачи.

Чтобы просмотреть список задач программы Kaspersky Endpoint Security, выполните следующую команду:

```
kesl-control --get-task-list
```

Отобразится список задач программы Kaspersky Endpoint Security.

Чтобы изменить параметры задачи с помощью командной строки, выполните следующие действия:

1. Укажите нужное значение параметра

```
kesl-control --set-settings <ID задачи>|<имя задачи> <параметр=значение >
```

2. Убедитесь, что значение параметра изменено в конфигурационном файле задачи

```
kesl-control --get-settings <ID задачи>|<имя задачи>
```

3.4 Управление задачами путем изменения конфигурационного файла

Чтобы изменить параметры задачи путем изменения конфигурационного файла, выполните следующие действия:

1. Сохраните параметры задачи в конфигурационный файл:

```
kesl-control --get-settings <ID задачи>|<имя задачи> --file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Измените нужный параметр в конфигурационном файле.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте в задачу параметры из конфигурационного файла:

```
kesl-control --set-settings <ID задачи>|<имя задачи> --file <полный путь к файлу>
```

3.5 Настройка задачи «Обновление»

Источник обновлений — это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security. Источником обновлений могут быть FTP- или HTTP-серверы (например, серверы обновлений Kaspersky Security Center и «Лаборатории Касперского») и локальные или сетевые каталоги, смонтированные пользователем.

В предустановленной задаче «Обновление» в качестве источника обновлений по умолчанию выбраны серверы обновлений «Лаборатории Касперского». Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений «Лаборатории Касперского», существует возможность получения обновлений из ***пользовательского источника обновлений*** – из указанной локальной или сетевой папки, смонтированной по протоколу SMB или NFS, или с FTP- или HTTP-сервера. Вы можете указать пользовательский источник обновлений в параметрах задачи «Обновление».

Все доступные значения и значения по умолчанию для всех параметров задачи «Обновление» описаны в Таблица 1.

Таблица 1 – Параметры задачи «Обновление»

Параметр	Описание	Значение
SourceType	Источник получения обновлений	**KLServers** — с одного из серверов обновлений «Лаборатории Касперского» по протоколу HTTPS **SCServer** — с установленного в

Параметр	Описание	Значение
		локальной сети Сервера администрирования Kaspersky Security Center **Custom** — программа загружает обновления из пользовательского источника, указанного в секции [CustomSources.item_#]. Вы можете указывать разделы HTTP-серверов или каталога на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.
UseKLServersWhenUnavailable	Обращение программы к серверам обновлений «Лаборатории Касперского» в случае, если все пользовательские источники недоступны	**Yes** (значение по умолчанию) – программа подключается к серверам обновлений «Лаборатории Касперского», если все пользовательские источники обновлений недоступны. **No** – программа не подключается к серверам обновлений «Лаборатории Касперского», если все пользовательские источники обновлений недоступны
ApplicationUpdateMode	Режим загрузки и установки обновлений программы	**Disabled** – не загружать и не устанавливать обновления программы **DownloadOnly** (значение по умолчанию) – загружать обновления программы, но не устанавливать их **DownloadAndInstall** – автоматически загружать и устанавливать обновления программы
ConnectionTimeout	Время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера – при попытке соединения с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, программа обращается к другому указанному источнику обновлений.	Вы можете указывать только целые числа в диапазоне от 0 до 120. Значение по умолчанию: 10
Секция [CustomSources.item_#] содержит следующие параметры:		
URL	Адрес пользовательского источника	Значение по умолчанию: Не задано Содержит адрес HTTP-сервера, на котором расположен раздел с

Параметр	Описание	Значение
	обновлений в локальной сети или в сети Интернет	обновлениями или каталог на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS
Enabled	Включение использования источника обновлений, указанного в параметре URL. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.	Значение по умолчанию: Не задано Yes — программа использует источник обновлений, указанный ранее в параметре URL. No — программа не использует источник обновлений

Рассмотрим пример конфигурационного файла задачи обновления для случая, когда программа должна загружать обновления из пользовательского источника — локального каталога `/home/bases`:

```
SourceType=Custom
UseKLServersWhenUnavailable=No
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
[CustomSources.item_0000]
URL=/home/bases
Enabled=Yes
```

Импортируйте в задачу параметры из конфигурационного файла 6-update.ini командой

```
kesl-control --get-settings 6 --file 6-update.ini
```

Для программно-аппаратных средств, работающих в режиме реального времени, предусмотрено ручное обновление антивирусных баз Kaspersky Endpoint Security в рамках проведения ТО4.

3.6 Настройка расписания задачи «Обновление»

Чтобы настроить параметры расписания задачи путем изменения конфигурационного файла, выполните следующие действия:

1. Сохраните параметры расписания задачи в конфигурационный файл с помощью следующей команды:

```
kesl-control --get-schedule <ID задачи>|<имя задачи> --file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Задайте параметры расписания.
4. Сохраните изменения в конфигурационном файле.

5. Импортируйте параметры расписания задачи из конфигурационного файла с помощью следующей команды:

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <полный путь к файлу>
```

Предусмотрены следующие параметры для настройки расписания запуска задачи:

```
RuleType= Once | Monthly | Weekly | Daily | Hourly | Minutely | Manual |
PS | BR
```

где:

PS – запускать задачу после запуска программы.

BR – запускать задачу после обновления баз программы.

Время запуска задачи:

```
StartTime=[year/month/month_day] [hh]:[mm]:[ss];
[<month_day>|<week_day>]; [<period>]
```

`RandomInterval=<мин.>` – интервал запуска задачи, если несколько задач запущены одновременно (в минутах).

`RunMissedStartRules=Yes|No` – включение запуска пропущенной задачи после запуска программы.

Рассмотрим пример конфигурационного файла, обеспечивающего запуск задачи обновления каждые 10 часов:

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:00:00; 10
RandomInterval=0
```

Чтобы настроить запуск задачи каждые 10 минут, укажите следующие параметры:

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00; 10
RandomInterval=0
```

Импортируйте параметры расписания задачи из конфигурационного файла 6–schedule.ini командой

```
kesl-control --set-schedule 6 --file 6-schedule.ini
```

3.7 Настройка режима работы Kaspersky Endpoint Security

Исключение из проверки – совокупность условий, при выполнении которых программа Kaspersky Endpoint Security не проверяет объект на вирусы и другие угрозы.

Таблица 2 – Возможные параметры исключений из проверки

Блок параметров	Описание
Исключения*	Блок параметров содержит кнопку «Настроить», по нажатию на которую открывается окно «Области исключения». В этом окне можно задать список областей исключений из проверки.
Исключения по маске	Блок параметров содержит кнопку «Настроить», по нажатию на которую открывается окно «Исключение по маске». В этом окне можно настроить исключение объектов из проверки по маске.
Исключения по названию угрозы	Блок параметров содержит кнопку «Настроить», по нажатию на которую открывается окно «Исключения по названию угрозы». В этом окне можно настроить исключение объектов из проверки по названию угрозы.

*Примечание: * – В СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») применяется исключение из проверки Kaspersky Endpoint Security при помощи «Области исключения».*

Окно «Название области исключения»

В данном окне добавляется и настраивается область исключения из проверки.

Таблица 3 – Параметры области исключения

Параметр	Описание
Название области исключения	Поле ввода названия области исключения. Данное называние будет отображаться в таблице окна «Области исключения»
Использовать эту область	Флажок включает или выключает исключение области из проверки во время работы программы. Если флажок установлен – программа исключает проверку.
Файловая система, протокол доступа и путь	Блок параметров позволяет задать исключения. В раскрывающемся списке файловых систем выбирается тип файловой системы, на которой

Параметр	Описание
	расположены директории, исключаемые из проверки: Локальная – локальные директории; Смонтированная – смонтированные директории;
Имя файловой системы	Поле ввода названия файловой системы, на которой расположены директории. Поле доступно, если в разрывающемся списке файловых систем выбран тип «смонтированная» и в раскрывающемся списке справа выбран элемент «Пользовательская».

Далее приведена настройка исключения «Области исключения» СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») при помощи командной строки.

Пользователь имеет возможность формировать глобальную область исключения. Объекты в данной области исключаются из области проверки, заданных в задаче постоянной проверки по требованию

Необходимо выполнить следующие действия:

– Сохранить параметры задачи постоянной проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/Kaspersky/kesl/bin/kesl-control --file /Automiq
```

– Открыть созданный конфигурационный файл для редактирования.

– Добавить в созданный конфигурационный файл секцию `[ExcludedFromScanScope.item_#].`

– В секции `[ExcludedFromScanScope.item_#]` указать значения следующих параметров:

– `AreaDesc` – задает уникальное имя области исключения;

– `UseScanArea` – указывает, будет ли Kaspersky Endpoint Security исключать область из проверки во время выполнения задачи;

– `Path` – задает путь к объектам, исключаемых из проверки;

– Сохранить изменения в конфигурационном файле.

– Импортировать параметры из конфигурационного файла в задачу постоянной проверки по требованию с помощью следующей строки:

```
/opt/Kaspersky/kesl/bin/kesl-control –set-settings--file /Automiq
```

4 Управление политикой безопасности

В данном разделе описана программа ОС Astra Linux «Управление политикой безопасности» (fly-admin-smc), осуществляющая управление протоколированием, привилегиями и мандатными атрибутами пользователей, работа с пользователями и группами;

Программа предназначена для управления политикой безопасности (ПБ), а также управления единым пространством пользователя. В частности, позволяет управлять:

– пользователями, группами, настройками и атрибутами: мандатным разграничением доступа (МРД) пользователя, параметрами протоколирования, привилегиями, политикой срока действия пароля, политикой блокировки;

– базами данных PARSEC (аудитом, мандатными атрибутами и привилегиями);

– политикой создания пользователей;

– настройками безопасности (устанавливать параметры монтирования для очистки блоков памяти при их освобождении, настраивать очистку разделов страничного обмена при выключении системы);

– параметрами подключения внешних устройств (учитывать носители и управлять их принадлежностью, протоколированием и мандатными атрибутам.

Программа запускается в режиме администратора. Для вызова привилегированных действий запрашивается дополнительная авторизация.

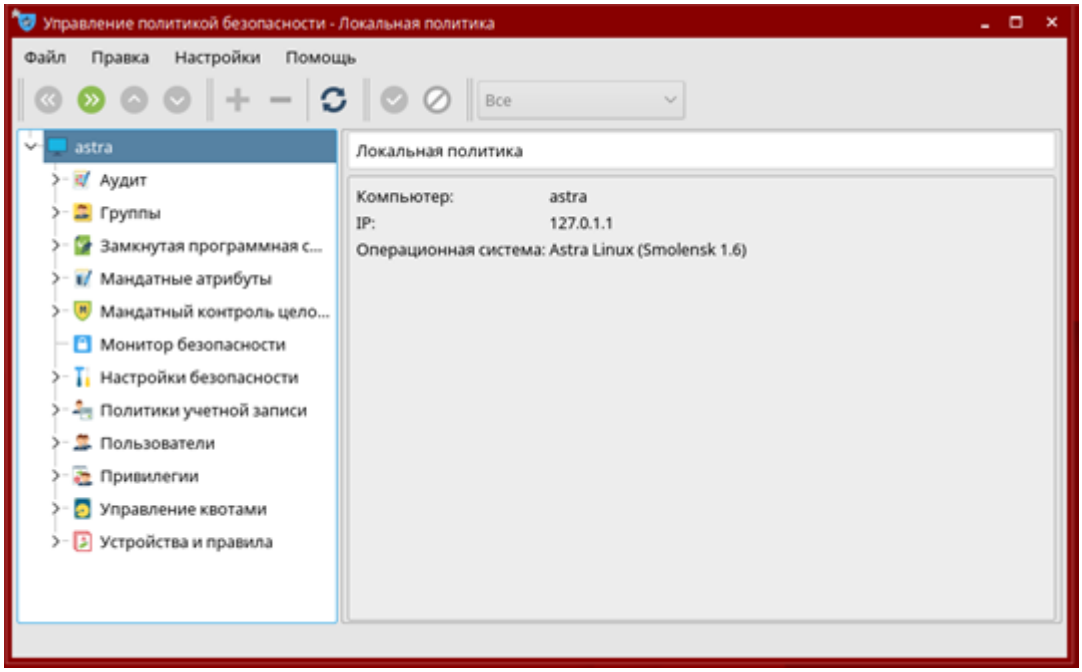


Рисунок 16 – Панель управления политикой безопасности

Главное окно программы содержит меню (Меню), панель инструментов (Панель инструментов) и боковую панель для навигации по дереву настроек ПБ (Панель навигации) с рабочей панелью справа (см. Рисунок 16).

Меню программы содержит следующие пункты:

- «Файл»:
  - «Выход» — работа программы завершается;
  - «Правка» — пунктами подменю добавляется/удаляется раздел в дереве настроек ПБ на боковой панели «Элементы» (Панель навигации), а также изменяются соответствующие ему значения параметров настройки:
    - «Обновить» — содержимое панелей обновляется;
    - «Удалить» (активируется при выделении раздела) — появляется окно с запросом на подтверждение удаления. После подтверждения или отмены окно закрывается и раздел, соответственно, удаляется или не удаляется;
    - «Создать» (активируется при выделении раздела или объединения разделов) — позволяет создать новый раздел, а также рабочую панель с элементами настройки этого нового раздела. На панели «Свойства» появляется новая форма или вспомогательное окно для установки необходимых параметров;
    - «Применить» — установленные настройки применяются;
    - «Отмена» — отмена изменения настроек;
- «Настройки»:
  - «Плагины» — открывается окно «Плагины и модули», во вкладках «Плагины» и «Модули» которого отображаются, соответственно, загружаемые плагины и модули, а в строке «Путь» отображается маршрутное имя каталога с файлами для их хранения. Управляющие элементы:
    - [Изменить] — открывается диалоговое окно для установки нового имени каталога с файлами для хранения. После подтверждения или отмены окно закрывается, и новое имя каталога, соответственно, устанавливается или не устанавливается;
    - [Закрыть] — окно закрывается;
- «Помощь»:
  - «Содержание» — вызов окна справки;
  - «О программе…» — вызов окна с краткой информацией о программе.

На панели инструментов располагаются подвижные панели с кнопками быстрой навигации по дереву функциональных категорий данных на боковой панели ([Перейти к родительскому элементу дерева], [Перейти к первому дочернему элементу дерева], [Перейти к предыдущему или родительскому элементу дерева], [Перейти к следующему элементу дерева]), кнопками, которые повторяют аналогичные пункты меню «Правка» (см. Меню) и выпадающим списком для установки фильтра отображения категорий данный на рабочей панели.

Щелчком правой кнопки мыши на панели меню или на панели инструментов открывается контекстное меню с флагами установки показа на панели инструментов соответствующих подвижных панелей с этими кнопками.

Настройки политики безопасности по своему функциональному и смысловому значению объединяются в группы и структурно организуются в дереве настроек ПБ, которое отображается на боковой панели навигации:

- Аудит;
- Группы;
- Замкнутая программная среда;
- Мандатные атрибуты;
- Мандатный контроль целостности;
- Монитор безопасности;
- Настройки безопасности;
- Политики учетной записи;
- Пользователи;
- Привилегии;
- Устройства и правила.

Щелчком левой кнопки мыши на знаке в вершине дерева или щелчком левой кнопки мыши на названии вершины эта вершина разворачивается, если была свернута и, наоборот, сворачивается, если была развернута. После разворачивания вершины появляются названия разделов и/или сводов разделов, входящих в эту вершину.

Для оперативного перемещения по дереву используются кнопки панели инструментов (см. Панель инструментов).

Терминальная вершина дерева настроек политики безопасности называется разделом, а нетерминальная вершина — сводом разделов. Раздел или свод разделов выделяется щелчком левой кнопки мыши на нем. После выделения справа на появляется соответствующая форма рабочей панели с элементами для настройки соответствующих параметров ПБ. При наведении курсора на элемент

управления появляется подсказка. Значения параметров устанавливаются в режиме администратора.

4.1 Аудит

В ОС Astra Linux имеется собственная система аудита, позволяющая настраивать 17 видов событий по группам: по умолчанию, для отдельных пользователей и для отдельных групп.

Назначение флагов журналирования происходит следующим образом:

1) если указана специальная запись для пользователя, то используется эта запись;

2) если записи нет, то складываются флаги журналирования для первичной группы (если она указана) и для всех явно указанных групп, членом которых является данный пользователь. Таким образом, если пользователь входит в несколько групп, указанных в файле, для него будут регистрироваться все события, указанные для этих групп;

3) если пользователь не является членом ни одной из явно указанных групп, то используется запись "other" (остальные);

4) если записи "other" нет, то используется политика, принятая для системы по умолчанию, а в журнале регистрируется предупреждение.

Для настройки отдельных параметров аудита используйте консольную команду useraud или графическую утилиту fly-admin-smc.

Чтобы добавить параметры аудита для пользователя, используйте команду

```
sudo useraud <пользователь> <флаги_аудита>
```

Чтобы добавить параметры аудита для группы, используйте команду

```
sudo useraud –g <группа> <флаги_аудита>
```

Например, чтобы добавить для пользователя oper успешного события open, успешного события exec и отменить протоколирование неуспешного события open, используйте команду

```
sudo useraud oper +open+exec:-open
```

Перечень протоколируемых событий приведен в Таблица 2.

Таблица 2 – Перечень протоколируемых событий ОС Astra Linux

Разряд	Ключ	Событие	Описание события	Успех	Отказ
16	W	Net	Сетевые события	Нет флага	Флаг

Разряд	Ключ	Событие	Описание события	Успех	Отказ
15	E	Rename	Переименование	Нет флага	Флаг
14	H	Chroot	Изменение корневого каталога	Флаг	Флаг
13	P	Cap	Изменение привилегий	Нет флага	Флаг
12	M	Mac	Смена мандатных атрибутов	Нет флага	Флаг
11	R	Acl	Управление списком прав доступа	Нет флага	Флаг
10	A	Audit	Изменение списка протоколируемых событий	Нет флага	Флаг
9	G	Gid	Изменение GID	Нет флага	Флаг
8	I	Uid	Изменение UID	Нет флага	Флаг
7	L	Module	Загрузка-выгрузка модуля	Нет флага	Флаг
6	T	Mount	Монтирование/размонтирование файловой системы	Флаг	Флаг
5	N	Chown	Изменение владельца файла	Нет флага	Флаг
4	D	Chmod	Изменение прав доступа к файлу	Нет флага	Флаг
3	U	Delete	Удаление файла	Нет флага	Флаг
2	X	Exec	Запуск программы	Нет флага	Флаг
1	C	Create	Создание файла	Нет флага	Флаг
0	O	Open	Открытие файла	Нет флага	Флаг

Для настройки протоколирования с помощью графической утилиты fly-admin-smc перейдите в рабочую панель *Аудит → Настройки аудита*. Панель «Настройки аудита» содержит вкладки:

1) «По умолчанию» (см. Рисунок 17) - настройки аудита по умолчанию:

– флаг «Настройка аудита по умолчанию» - включает настройки аудита по умолчанию;

– «Аудит успехов» и «Аудит отказов» - список флагов включения регистрации событий в журнале операций, в случае их, соответственно, успешного и неуспешного выполнения. Флаг переключается щелчком левой кнопки мыши на нем.

2) «Группы» (Рисунок 18) - список групп с персональными настройками аудита. Двойным щелчком левой кнопки мыши на элементе списка на рабочей панели отображаются настройки аудита соответствующей группы;

3) «Пользователи» (см. Рисунок 19) - список пользователей с персональными настройками аудита. Двойным щелчком левой кнопки мыши на

элементе списка на рабочей панели отображаются настройки аудита соответствующего пользователя.

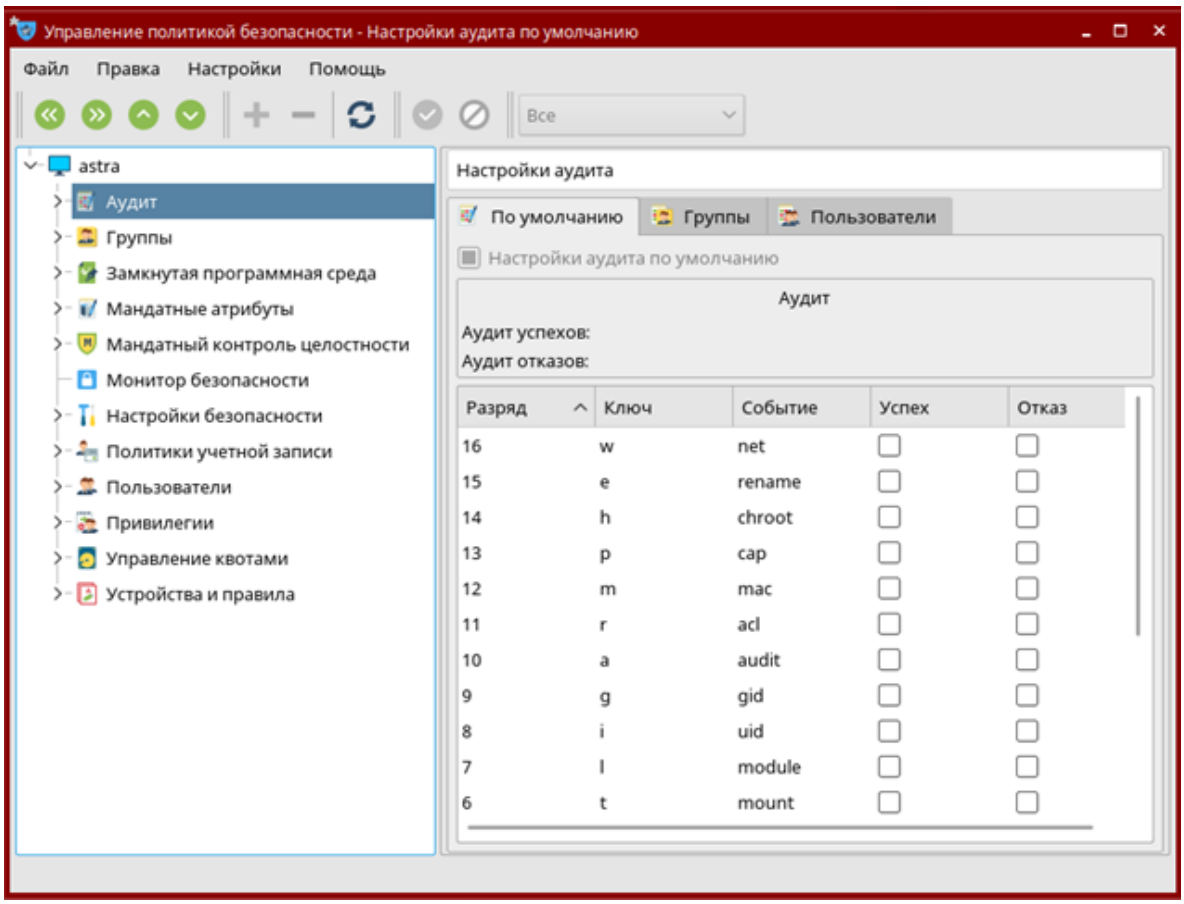


Рисунок 17 – Настройка аудита

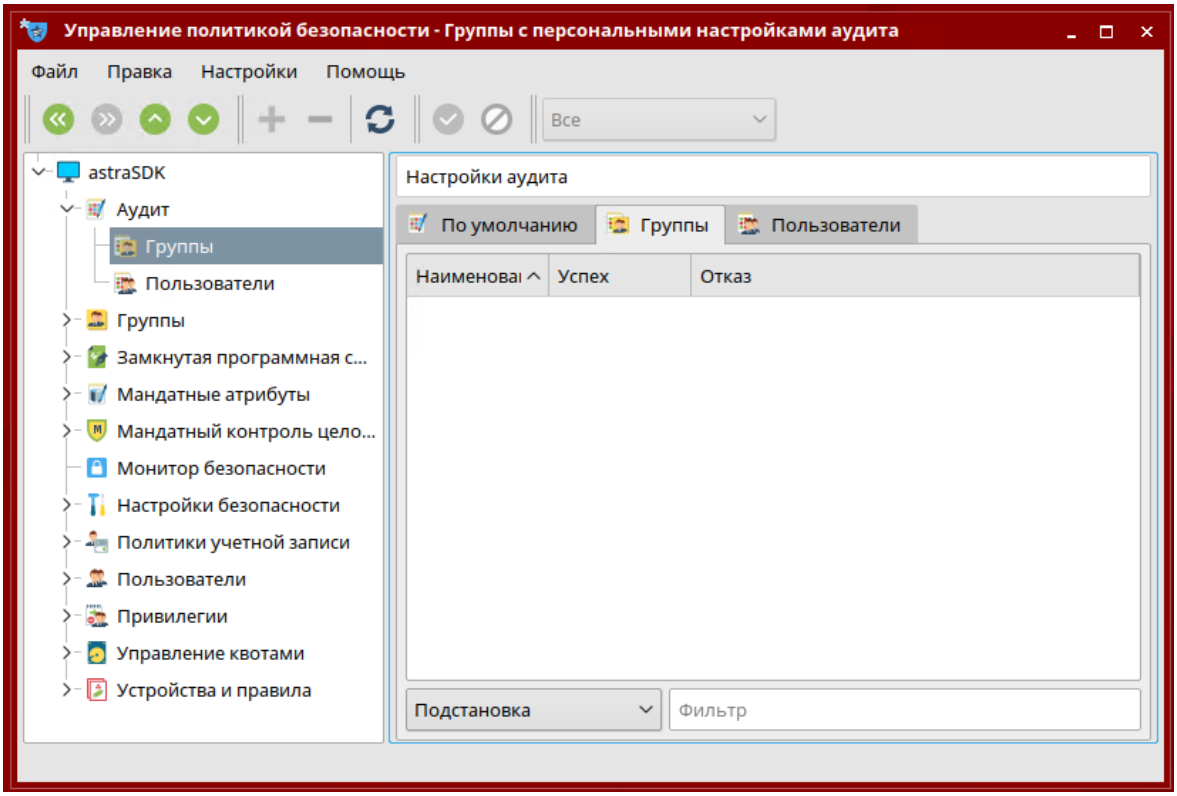


Рисунок 18 – Настройки аудита групп

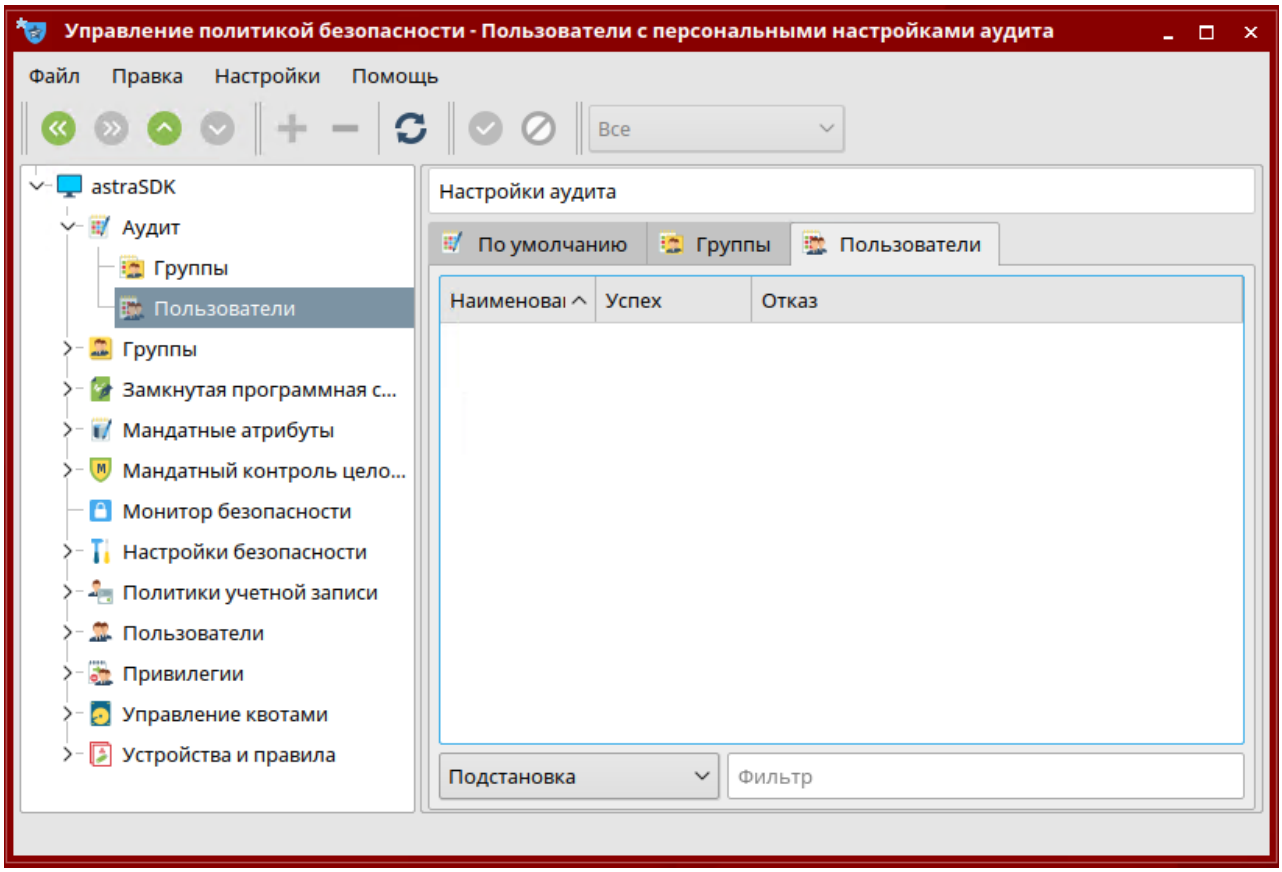


Рисунок 19 – Настройки аудита пользователей

4.2 Группы

На рабочей панели (см. Рисунок 20) в табличном виде отображается список групп пользователей.

Столбцы: «Наименование» (со значком порядка сортировки справа) - имя группы; «GID» - идентификационный номер группы; «Системная» - принадлежность к системным группам.

Двойным щелчком левой кнопки мыши на названии группы на рабочей панели появляются вкладки со значениями настроек политики безопасности для пользователя этой группы (см. Рисунок 21):

1) вкладка «Общие»:

– «Имя» - отображается имя члена группы;

– «UID» - отображается идентификационный номер члена группы;

– «GECOS» - отображается информация из учетной записи члена группы;

– «Системный» - принадлежность к системным группам;

– кнопки управления списком (внизу):

– [Добавить] - открывается окно со списком пользователей. Элемент списка выделяется щелчком левой кнопки мыши на нем. [Да] - окно закрывается, и

имя выделенного пользователя отображается в поле «Пользователи», [Отмена] - окно закрывается;

– [Удалить из группы]) - выделенный в поле «Имя» элемент удаляется;

2) вкладка «Аудит» - настройки аудита группы (см. Рисунок 22):

– флаг «Настройка аудита по умолчанию» включает настройки аудита по умолчанию;

– «Аудит успехов» и «Аудит отказов» - список флагов включения регистрации событий в журнале операций, в случае их, соответственно, успешного и неуспешного выполнения членом группы. Флаг переключается щелчком левой кнопки мыши на нем.

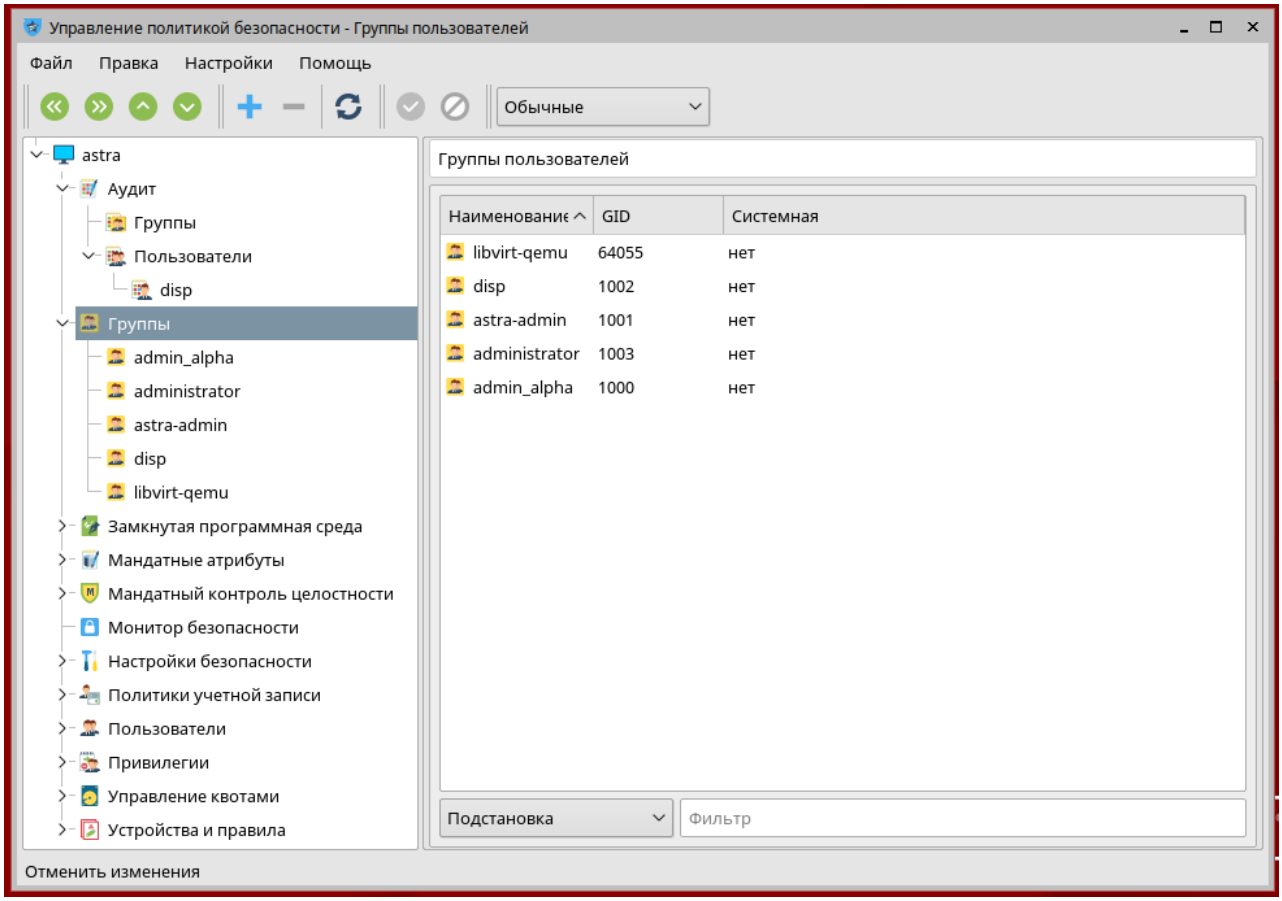


Рисунок 20 – Группы пользователей

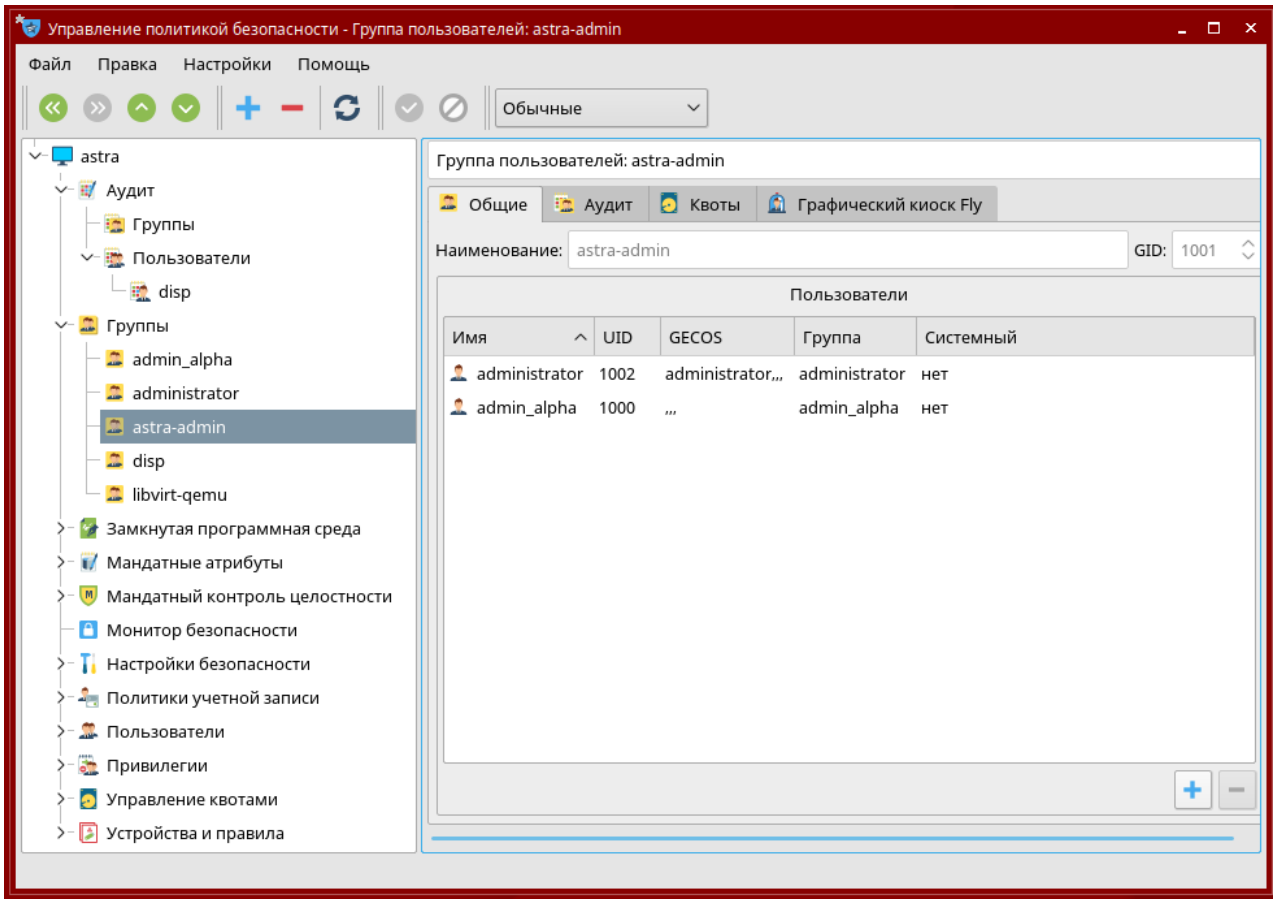


Рисунок 21 – Общие настройки группы пользователей

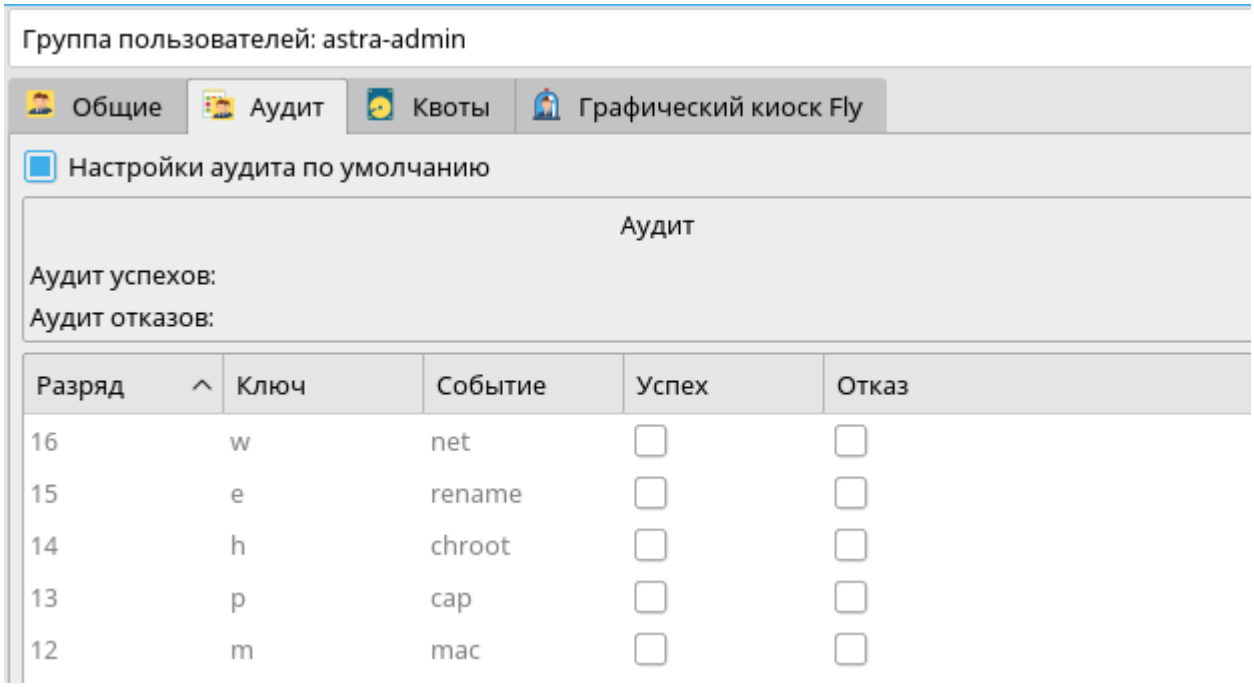


Рисунок 22 - Настройки аудита группы пользователей

3) вкладка «Квоты» (см. Рисунок 23) - настройки параметров квот для групп:

– «Устройства (из fstab)» - установка устройства из выпадающего списка. Отображается список из файла /etc/fstab с устройствами, которые поддерживают квотирование;

– «Файловая система», «Дисковые квоты на данном устройстве», «Квоты для групп на данном устройстве» - отображается соответствующая информация об установленном устройстве;

– поле «Память» - элементы для настройки текущего использования памяти («Используется»); лимита памяти, при превышении которого начинается отсчет времени в периоде отсрочки («Мягкое ограничение»); лимита памяти, который не может быть превышен ни при каких обстоятельствах («Жесткое ограничение») и интервала времени, при превышении которого мягкое ограничение становится жестким («Время наступления жесткого ограничения»);

– поле «Файлы» - элементы для настройки текущего использования файлов («Используется»); лимита файлов, при превышении которого начинается отсчет времени в периоде отсрочки («Мягкое ограничение»); лимита файлов, который не может быть превышен ни при каких обстоятельствах («Жесткое ограничение») и интервала времени, при превышении которого мягкое ограничение становится жестким («Время наступления жесткого ограничения»).

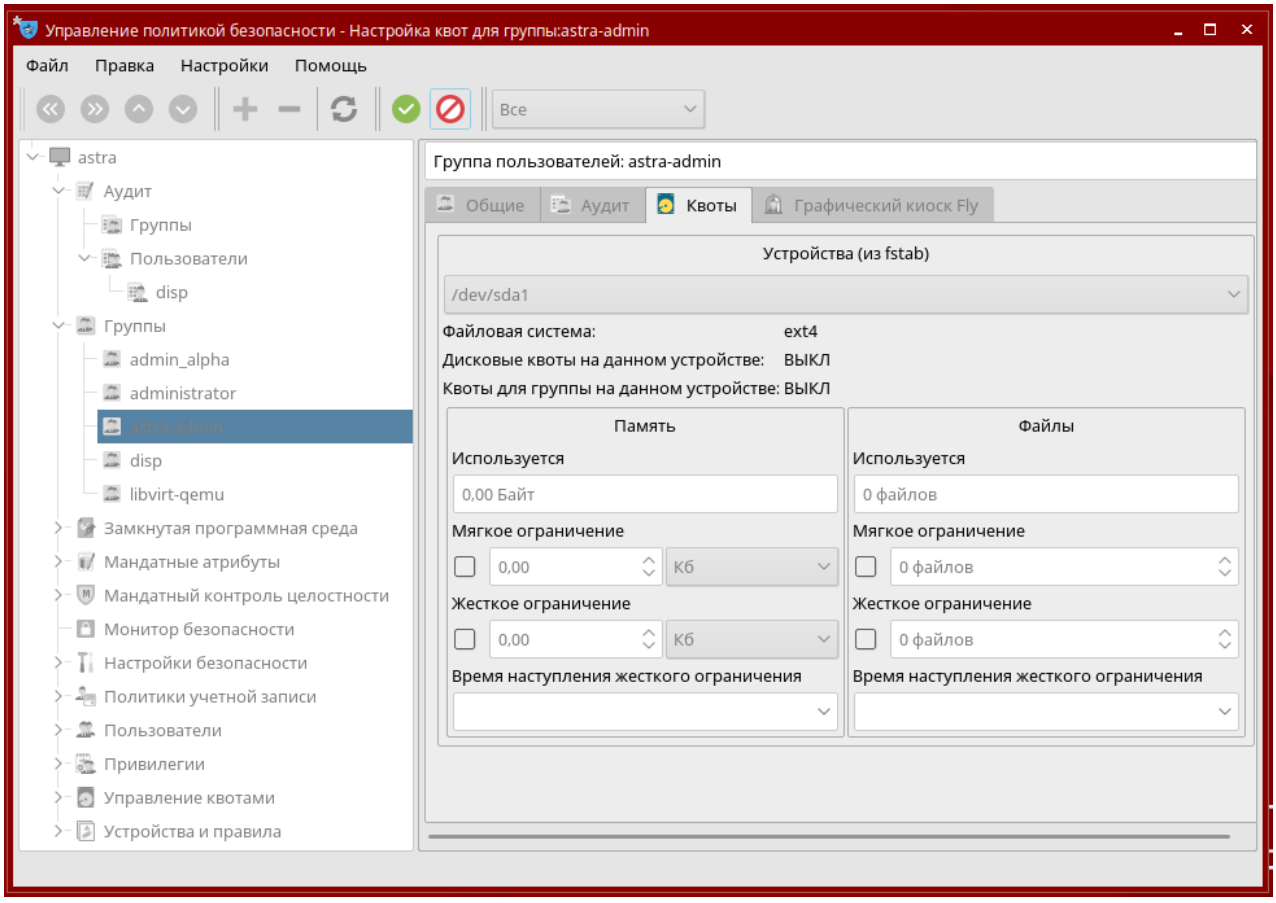


Рисунок 23 - Настройка квот групп пользователей

4.3 Пользователи

Войдите в систему как суперпользователь (root), откройте Панель управления (меню «Пуск»). Перейдите в группу «Безопасность» и откройте раздел «Политика безопасности» (см. Рисунок 16). Перейдите на узел «Пользователи» (см. Рисунок 24).

На рабочей панели в табличном виде отображается список пользователей.

Столбцы: «Наименование» (со значком порядка сортировки справа) — имя пользователя; «UID» — идентификационный номер пользователя; «GECOS» — информация из учетной записи пользователя; «Группа» — группа пользователя; «Системная» — отметка для системных групп; «Дом. каталог» — домашний каталог пользователя; «Оболочка» — имя оболочки.

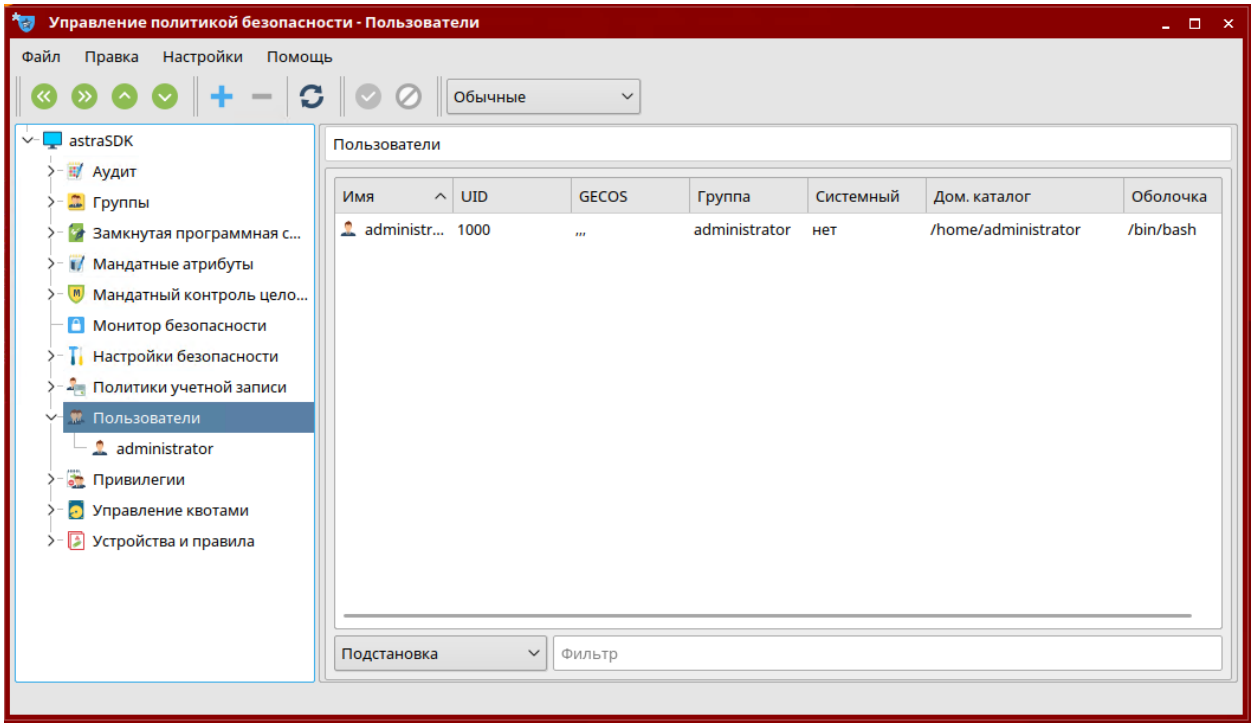


Рисунок 24 – Рабочая панель «Пользователи»

Двойным щелчком левой кнопки мыши на имени пользователя на рабочей панели появляются вкладки со значениями настроек политики безопасности для пользователя этой группы (см. Рисунок 25):

1) вкладка «Общие»:

– «Имя» - отображается имя пользователя;

– «UID» - отображается идентификационный номер пользователя;

– «Дом. каталог» - строка ввода маршрутного имени домашнего каталога пользователя;

– флаг «Переместить» — включает перенос содержимого домашнего каталога пользователя при изменении имени домашнего каталога;

– «Оболочка» — строка ввода маршрутного имени каталога с оболочкой;

– поле «Пароль»: [Изменить] — открывается окно для ввода нового пароля с последующим его подтверждением. После подтверждения или отмены окно закрывается и новый пароль, соответственно, устанавливается или не устанавливается. Флаг «Печать» — включает отображение учетной карточки пользователя с возможностью ее печати;

– флаг «GECOS» — строка ввода информации из учетной записи пользователя. […] (справа) — открывается окно для заполнения отдельных полей учетной записи с информацией о пользователе. После подтверждения или отмены окно закрывается и новый информация о пользователе, соответственно, устанавливается или не устанавливается;

– поле «Группы» — в табличном виде отображается список групп. Щелчком кнопки мыши на строке элемент списка выделяется. [Добавить] и [Удалить] (внизу) — пользователь, соответственно, добавляется в или исключается из выделенной группы.

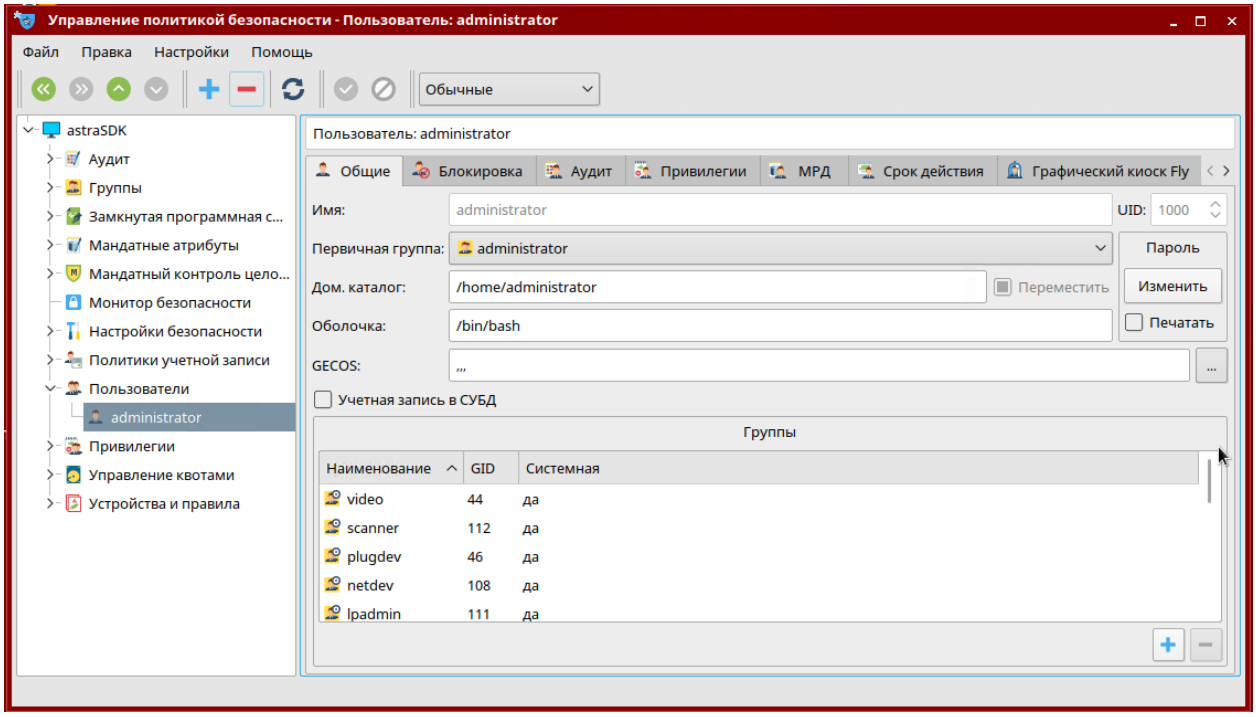


Рисунок 25 – Общие свойства пользователя

2) вкладка «Блокировка» (см. Рисунок 26)

– «Счетчик неудачных входов» — отображается количество неуспешных входов пользователя и установленных политикой блокировки количество неуспешных попыток входа. [Сброс] (справа) — количество неуспешных входов обнуляется;

– «Максимальное количество неудачных попыток входа» — в числовом поле устанавливается максимальное неудачное количество попыток входа для пользователя;

– флаг «Удаление пароля и блокировка входа» — разрешает блокировку входа без пароля;

– флаг «Блокировать пароль» — включает блокировку пароля;

– флаг «Блокировать учетную запись» — включает блокировку учетной записи;

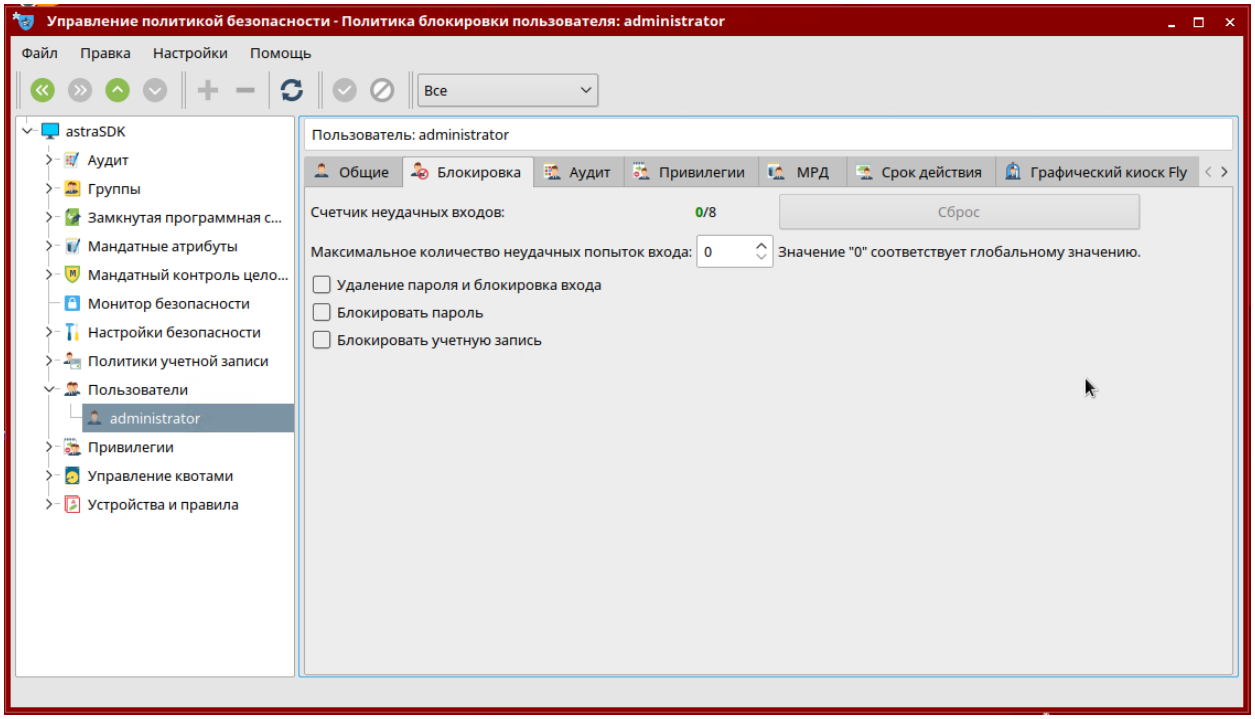


Рисунок 26 – Вкладка «Блокировка»

3) вкладка «Аудит» - настройки аудита группы (см. Рисунок 27):

– флаг «Настройка аудита по умолчанию» включает настройки аудита по умолчанию;

– «Аудит успехов» и «Аудит отказов» - список флагов включения регистрации событий в журнале операций, в случае их, соответственно, успешного и неуспешного выполнения членом группы. Флаг переключается щелчком левой кнопки мыши на знаке слева от него.

4) вкладка «Привилегии» - настройки привилегий пользователя (см. Рисунок 28). В списках «Linux-привилегии:» и «Parsec привилегии:» — отображается список флагов включения, соответственно, Linux- и Parsec-привилегий для пользователя (Флаги включения Linux- и Parsec привилегий). Флаг переключается щелчком левой кнопки мыши на знаке слева от него.

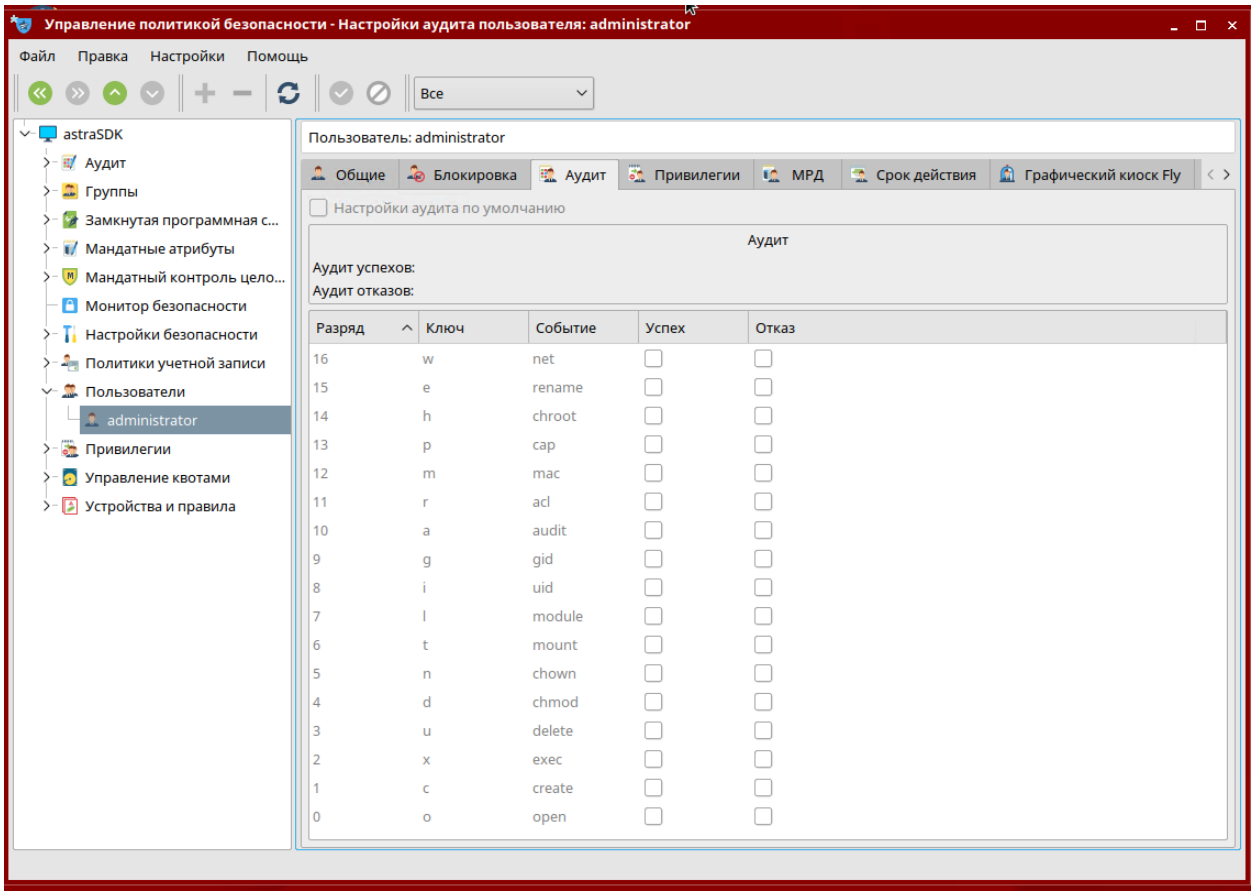


Рисунок 27 – Настройки аудита пользователя

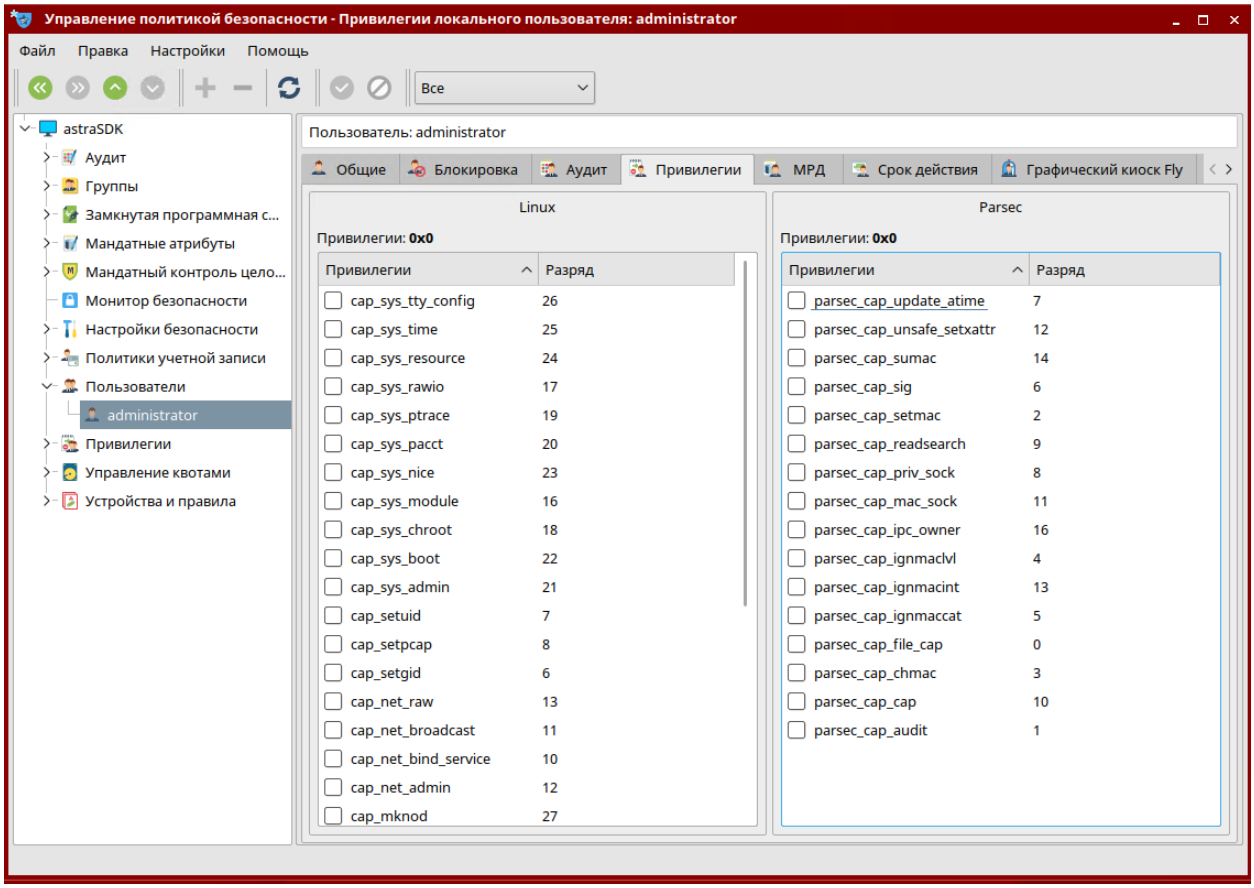


Рисунок 28 – Настройка Linux- и Parsec-привилегий пользователя

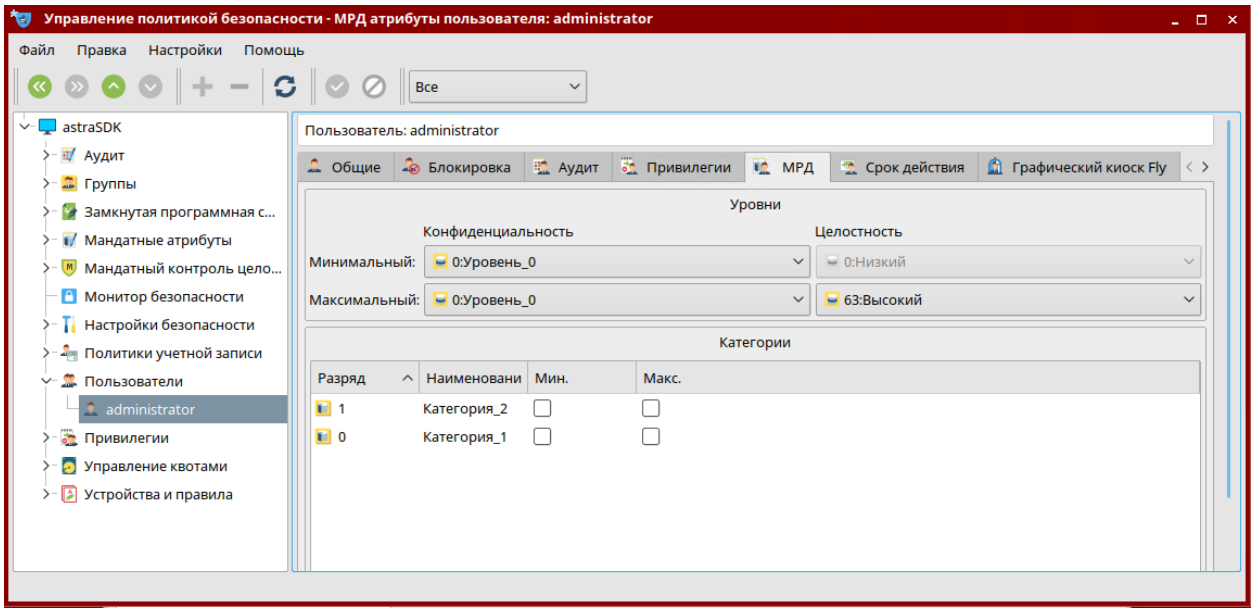


Рисунок 29 – Мандатное разграничение доступа для пользователя

5) Вкладка «МРД» (мандатное разграничение доступа) (см. Рисунок 29). Элементы управления:

– «Минимальный уровень:» — из выпадающего списка «Конфиденциальность» устанавливается минимальный уровень мандатного доступа, а из списка «Целостность» — минимальный уровень целостности;

– «Максимальный уровень:» — из выпадающего списка «Конфиденциальность» устанавливается максимальный уровень мандатного доступа, а из списка «Целостность» — максимальный уровень целостности;

– поле «Категории» — в табличном виде отображаются категории и их атрибуты. Флагами включается минимальный и максимальный уровень категории.

6) Вкладка «Срок действия пароля» (см. Рисунок 30). Элементы управления:

– флаг «Минимальное количество дней между сменой пароля» — включает числовое поле для установки минимального количества дней между сменой пароля;

– флаг «Максимальное количество дней между сменой пароля» — включает числовое поле для установки максимального количества дней между сменой пароля;

– флаг «Число дней выдачи предупреждения до смены пароля» — включает числовое поле для установки числа дней выдачи предупреждения до смены пароля;

– флаг «Число дней неактивности после устаревания пароля до блокировки учетной записи» — включает числовое поле для установки числа дней неактивности после устаревания пароля до блокировки учетной записи;

– флаг «Срок действия учетной записи пользователя» — включает календарь для установки срока действия учетной записи пользователя;

–  [Импорт из шаблона] — открывается окно для установки шаблона политики пароля и последующего импорта параметров из установленного шаблона.

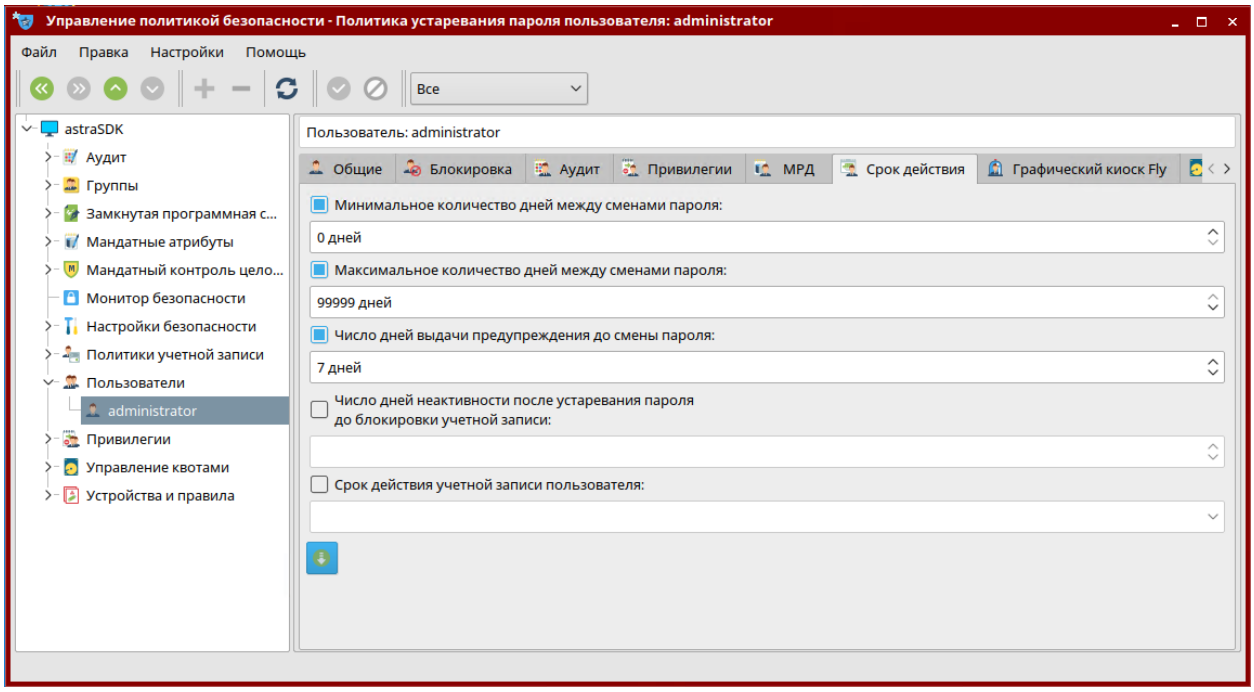


Рисунок 30 – Срок действия пароля пользователя

7) Вкладка «Графический киоск Fly» (см. Рисунок 31) позволяет ограничивать доступность для запуска программ локальным пользователям. Настройка режима киоска осуществляется администратором на максимальном уровне мандатного контроля целостности, установленного в ОС Astra Linux. Элементы управления:

– флаг «Режим киоска графического киоска Fly» — включает режим киоска при работе с приложениями из списка. Если в списке одно приложение, то режим киоска включается при работе с этим приложением. Если в списке несколько приложений, то запускается Рабочий стол с этими приложениями. Все доступные каталоги, ярлыки и т.д. устанавливаются в соответствии с предоставленным доступом;

– список «Разрешенные приложения» — список приложений для запуска в режиме киоска. Элемент списка выделяется щелчком мыши на нем. Кнопки управления для формирования списка:  [Добавить] (внизу и справа) — открывается окно для установки имени программы (см. Рисунок 32). После подтверждения или отмены окно закрывается и имя программы, соответственно, появляется или не появляется в списке. [Удалить] — программа, выделенная в списке, удаляется;

– кнопка [Системный киоск], при нажатии которой запускается программа «Системный киоск» (управление ограничением среды).

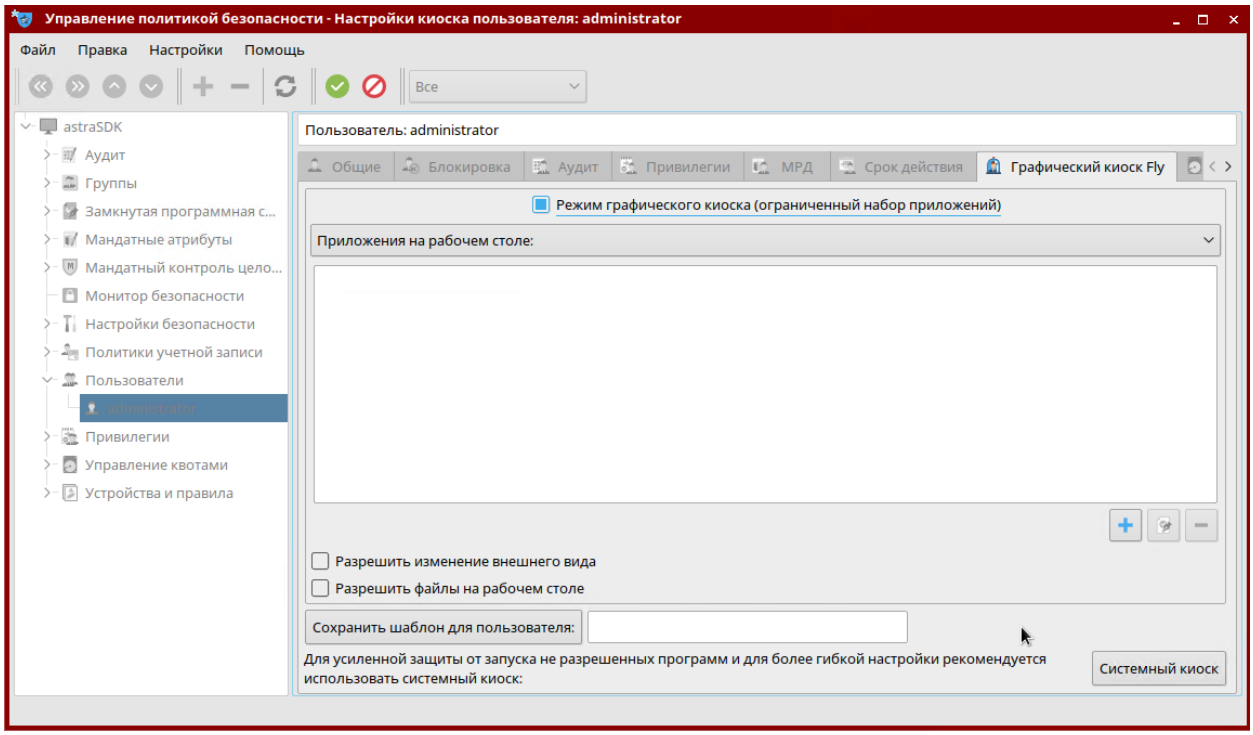


Рисунок 31 – Настройка режима графического киоска

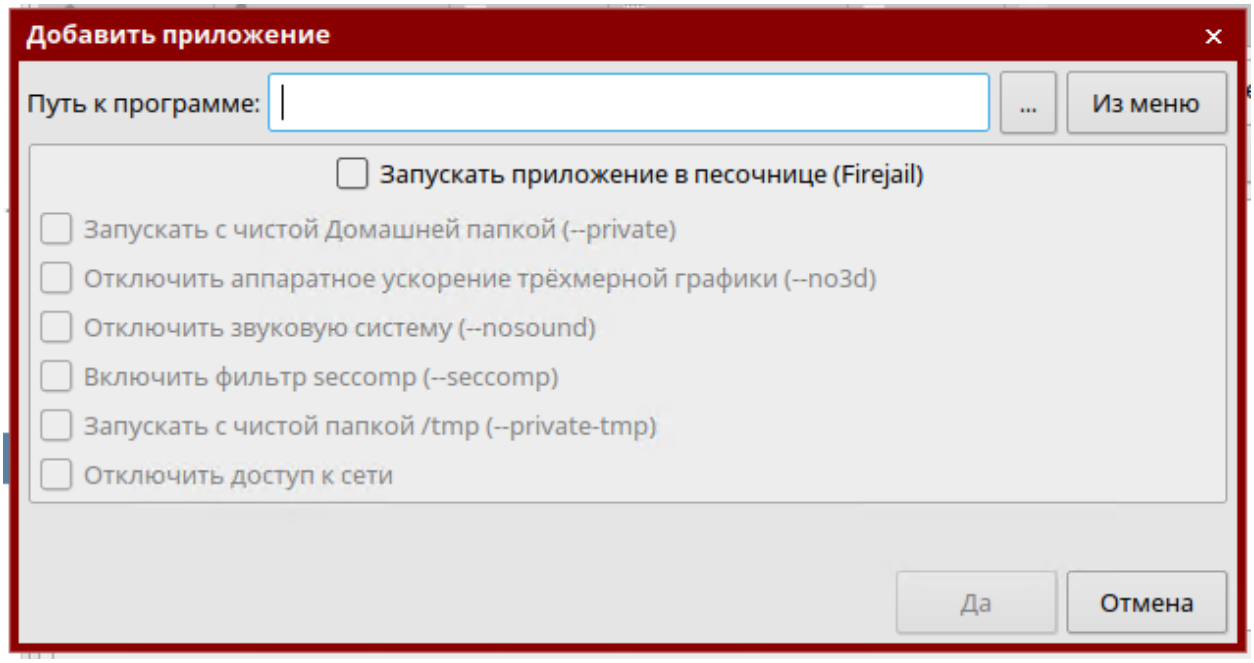


Рисунок 32

При создании графического киоска следует также ознакомиться с разд. 16.2 «Режим киоска» документа «РУСБ.10015-01 97 01-1 «Руководство по комплексу средств защиты информации, часть 1».

В качестве примера рассмотрим создание пользователя oper с ограниченными правами, от имени которого должен будет работать оператор Системы.

Добавьте нового пользователя, нажав на кнопку  , введите имя пользователя «oper» и подтвердите изменения, нажав на кнопку  .

Задайте первоначальный пароль пользователя, нажав кнопку *Пароль* → *Изменить*.

Установите права пользователя.

Внимание! Для создания домашнего каталога нового пользователя необходимо хотя бы один раз войти в систему как этот пользователь.

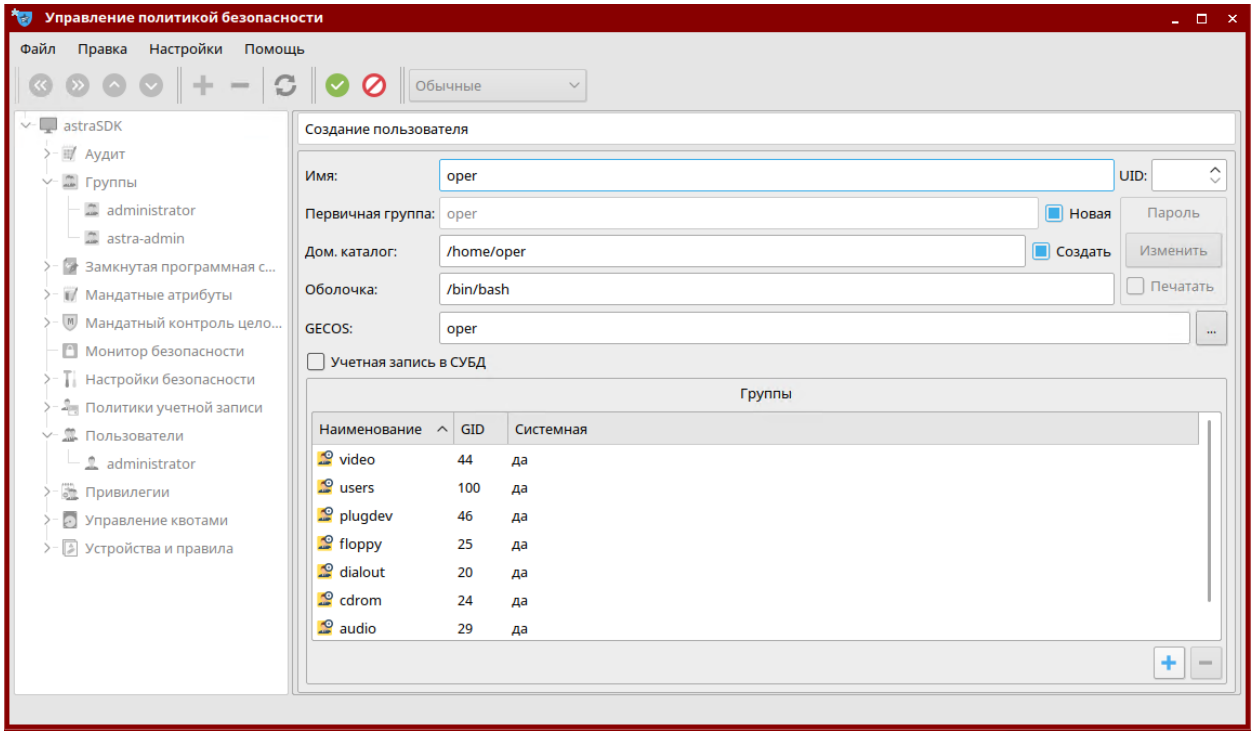


Рисунок 33 – Создание пользователя oper

Создайте файл с расширением sh, например, Start.sh, для запуска визуализатора Alpha.HMI.Viewer.

Добавьте разрешенное для выполнения приложения, нажав на кнопку  и выбрав созданный BASH-скрипт (см. Рисунок 34).

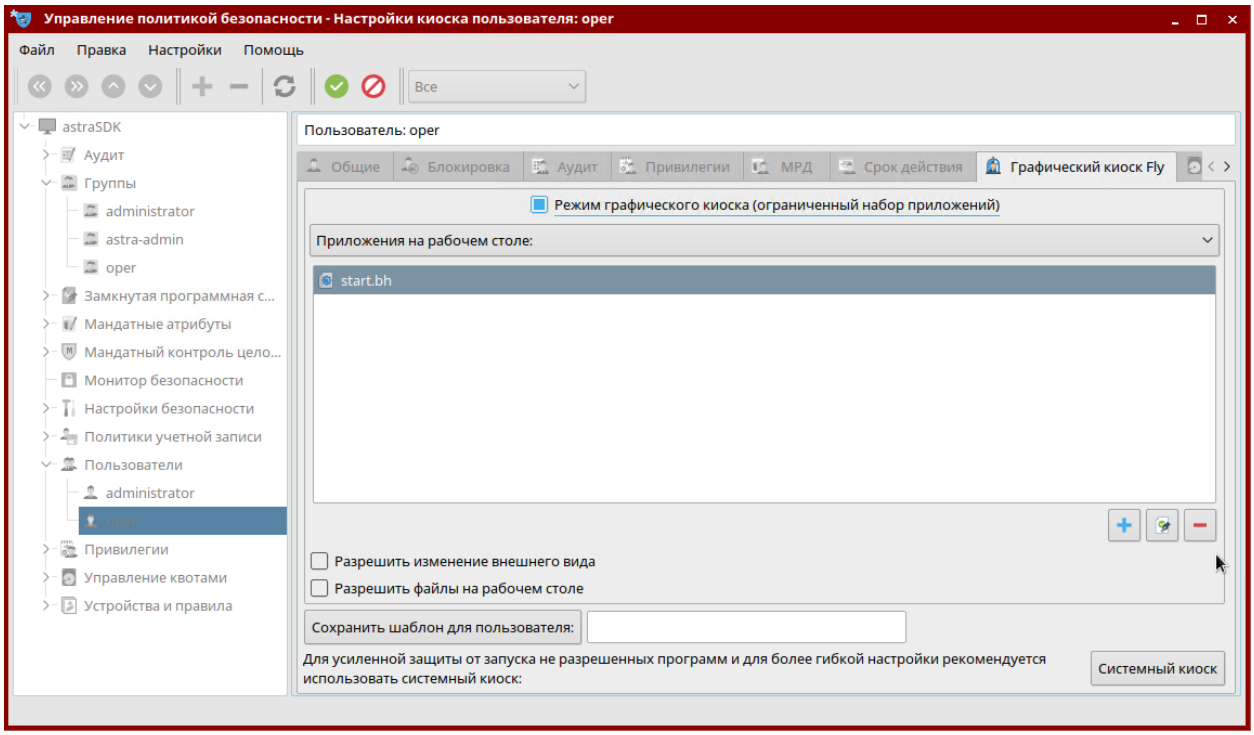


Рисунок 34

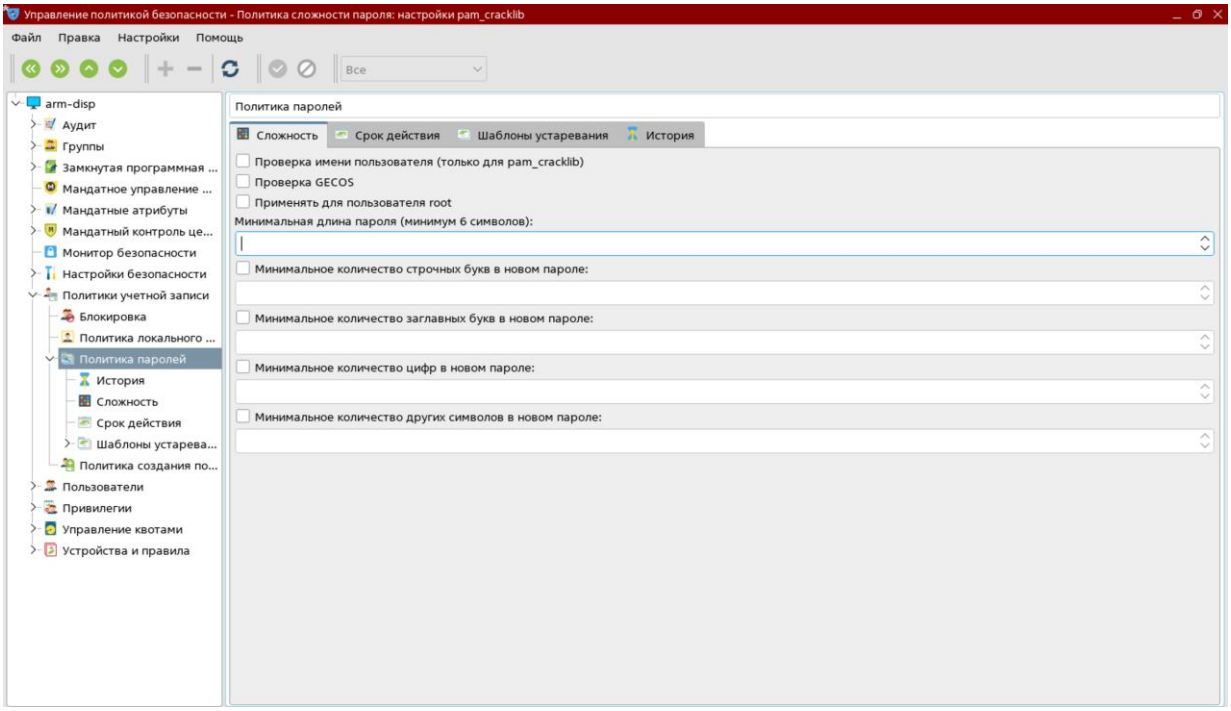


Рисунок 35 – Политика паролей

Общие правила формирования паролей:

- Минимальная длина:
  - Длина пароля пользователя не менее 12 символов;
  - Длина пароля администратора не менее 16 символов;
- Минимальное количество строчных букв не менее 1;
- Минимальное количество заглавных букв не менее 1;
- Минимальное количество цифр не менее 1;

– Минимальное количество специальных символов не менее 1.

4.4 Ограничение доступа к внешним носителям

В настоящем разделе описаны меры по ограничению использования внешних USB-накопителей (Flash-память, внешние переносные жесткие диски и другие устройства) на серверах и АРМ Системы.

Внимание! Разграничение доступа возможно только для файловых систем, поддерживающих расширенные атрибуты. Для USB-носителей это файловые системы Ext2/Ext3/Ext4.

Разграничение доступа к устройству осуществляется на основе соответствующего правила для менеджера устройств udev, которое хранится в файле в каталоге /etc/udev/rules.d. Обычно имя каждого файла правил начинается с двух цифр и имеет расширение *.rules, например, 99-local.rules.

Перед выполнением файлы упорядочиваются по алфавиту. Файлы с одинаковыми именами переписываются последним найденным файлом, т.е. файл, найденный последним, заменит собой ранее найденный файл с таким же именем.

Каждая строка в файле с правилами содержит хотя бы одну пару ключ/значение. Существует два типа ключей: ключ-условие и ключ присваивания. Если ключ-условие совпал при обработке события, то данное правило выполняется и с помощью ключей присваивания устанавливаются указанные переменные.

Далее приведен пример правила для съемного USB-накопителя.

```
ENV{ID_SERIAL}=="JetFlash_TS256MJF120_OYLIXNA6-0:0", OWNER="user", GROUP="users" PDPL="3:0:f:0!:"
```

В данном примере для съемного USB-накопителя с серийным номером JetFlash_TS256MJF120_OYLIXNA6-0:0 разрешено его использование владельцу устройства – пользователю user и пользователям, входящим в группу users. Здесь ENV{key} задает значение переменной окружения.

Ключи OWNER и GROUP позволяют вам назначить владельца устройства и группу, владеющую устройством.

По умолчанию, udev создает устройства с правами доступа 0660 (чтение/запись для владельца и группы). Если потребуется, вы можете изменить настройки по умолчанию для определенных устройств, используя в правилах ключ назначения MODE. Ключ MODE=”0666” устанавливает, что устройство будет доступно на чтение и запись для всех:

Для устройства установлены мандатные атрибуты: уровень конфиденциальности — 3, уровень целостности — 0, категории — f, роли и административные роли отсутствуют.

Узнать путь к USB устройству можно, выполнив команду lsblk. Результат команды будет примерно следующий:

```
NAME       MAJ:MIN    RM    SIZE  RO    TYPE MOUNTPOINT
sda        8:0        0     20G   0     disk
├─sda2     8:2        0     1K    0     part
├─sda5     8:5        0     1022M 0     part [SWAP]
├─sda3     8:3        0     7.9G  0     part
└─sda1     8:1        0     9G    0     part /
sr0        11:0       1     1024M 0     rom
sdb        8:32       1     14.9G 0     disk
├─sdb2     8:34       1     2.3M  0     part
└─sdb1     8:33       1     1.7G  0     part /media/linoxide/SANDISK
```

В списке найдите смонтированный раздел вашего USB-накопителя, в данном случае это устройство /dev/sdb1. Чтобы запросить атрибуты устройства из базы данных udev, используйте команду

```
udevadm info /dev/sdb1 | grep ID_SERIAL
```

Благодаря возможности автоматического формирования файлов правил системой udev подсистема безопасности PARSEC в ОС Astra Linux SE реализует следующие дополнительные функции по работе с устройствами:

– регистрация устройств в локальной базе учёта (в случае автономной рабочей станции) или базе учёта, хранящейся в базе учёта контроллера домена ALD;

– управление доступом к зарегистрированным устройствам на основе политики безопасности, основанной на их уровнях конфиденциальности и целостности.

Внимание! В Системе контроллер домена ALD не используется.

В случае локальной регистрации устройств база учёта создаётся в конфигурационном файле /etc/parsec/PDAC/devices.cfg. Для каждого из зарегистрированных устройств формируется отдельная секция, ограниченная блоком вида

```
flashdisk1
{
      enabled = true;
      description = ”Флэш диск 1”;
      user = ”administrator”;
      group =”Astra-admin”;
```

```
        mode = "774";
        pdpl = "3:0:0x3:0x0!:";
        audit = "0x31d:0x31d";
        expressions=( "ENV{ID_SERIAL}==\"JetFlash_TS256MJF120_OYLIXNA6-0:0\"" );
        access_rules = ();
}
```

Наряду с идентификационными данными устройства соответствующая ему секция содержит данные о дискреционных правах доступа к нему, а также о его мандатных уровнях конфиденциальности и неиерархических категориях.

Для устройств, учитываемых в локальной базе учета, генерация осуществляется при сохранении информации об устройстве с использованием программы «Управление политикой безопасности» (fly-admin-smc).

Для установки прав доступа к устройству необходимо вначале его зарегистрировать. Для этого следует выбрать в главном меню ОС Astra Linux *Пуск* пункты *Панель управления* и далее *Политика безопасности* (см. Рисунок 16).

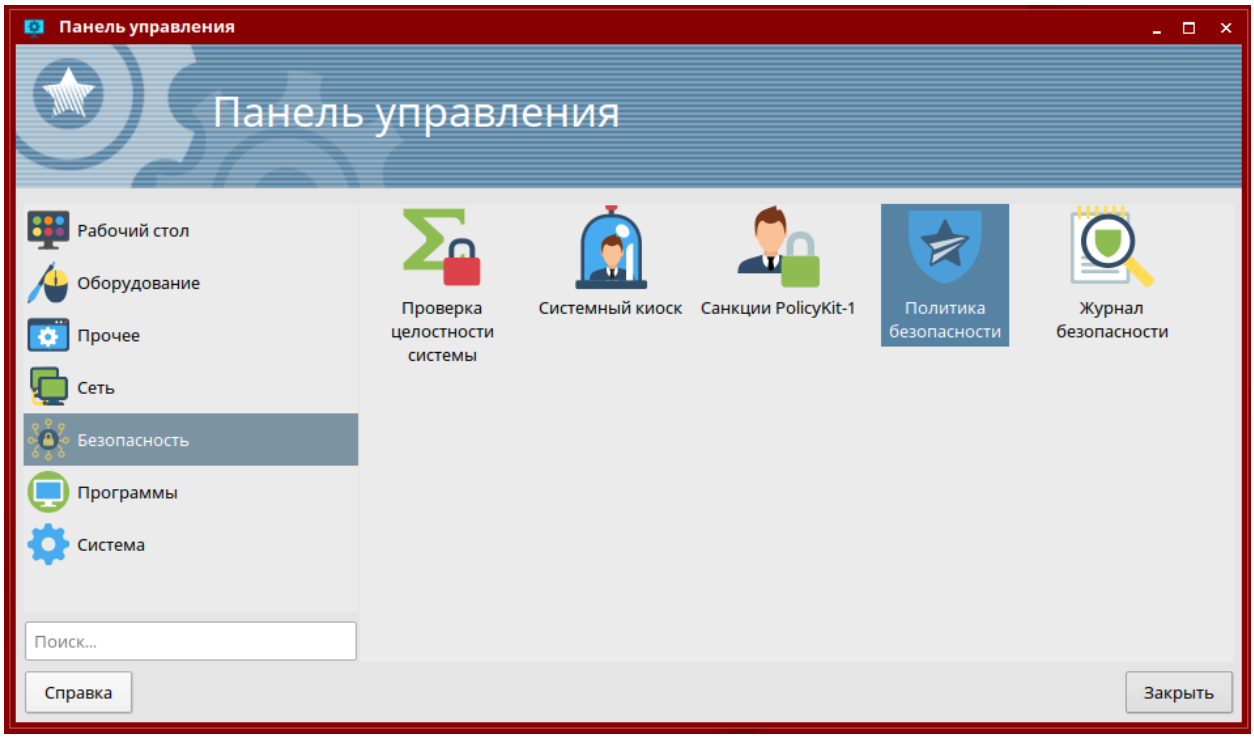


Рисунок 35 – Панель управления

Далее следует выбрать в дереве настроек политики безопасности, которое отображается на боковой панели навигации, пункты *Устройства и правила* → *Устройства* (см. Рисунок 36).

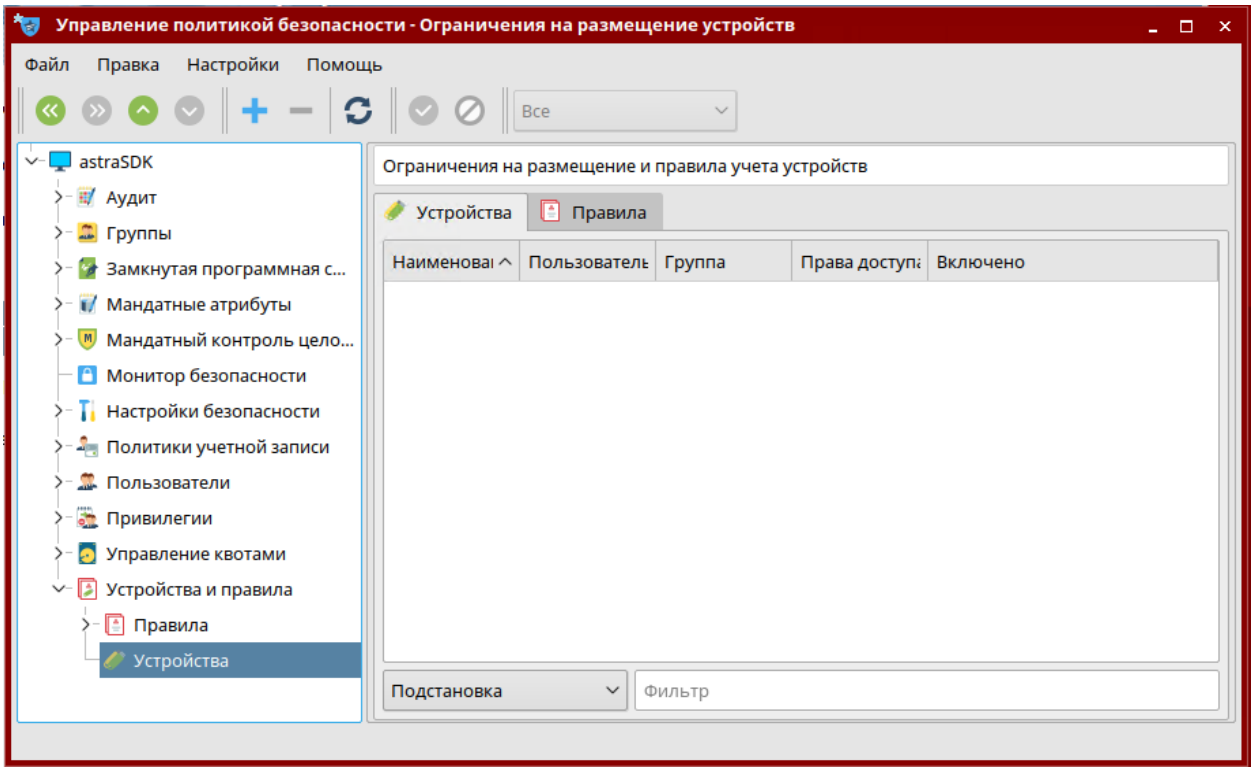


Рисунок 36 – Рабочая панель «Устройства»

Нажмите на панели инструментов кнопку  [Создать новый элемент]. Дождитесь появления графического окна «Добавить устройство» (см. Рисунок 37) и подключите USB-накопитель к USB-порту компьютера.

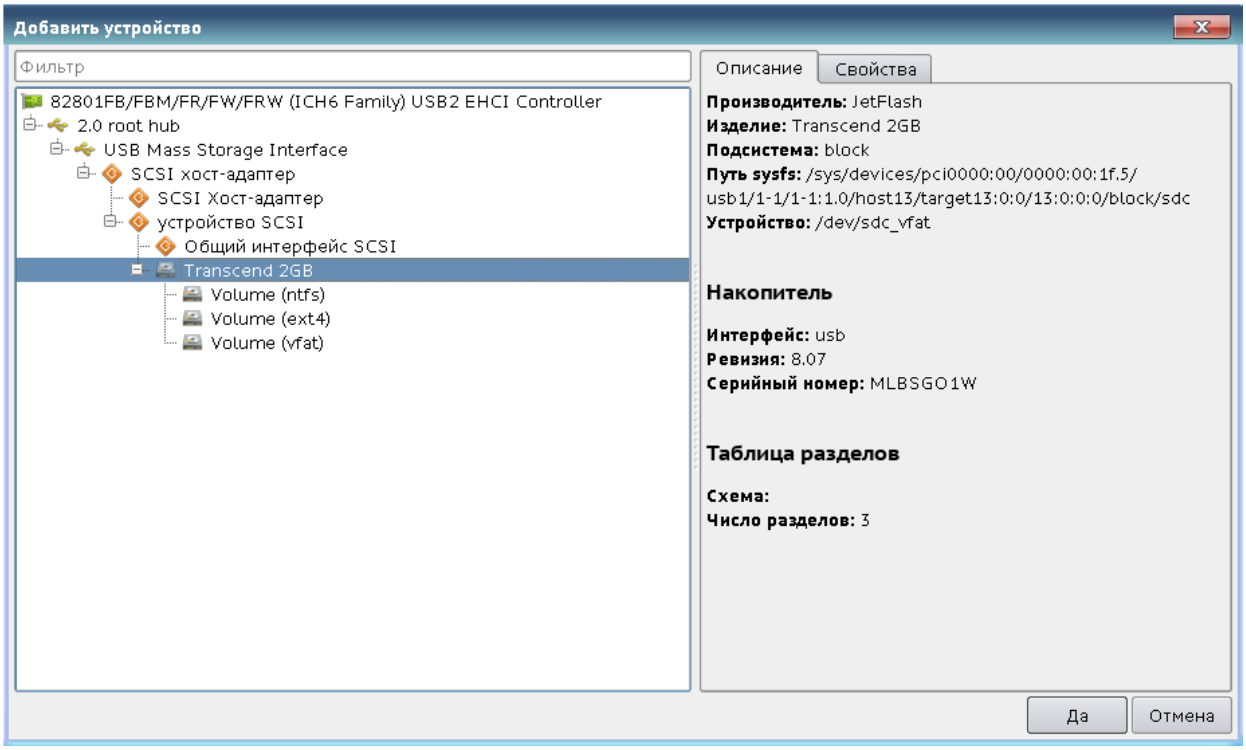


Рисунок 37 – Окно регистрации нового устройства

Перейти к вкладке «Общие» (Рисунок 39). В свойствах устройства следует:

– установить флажок «Включено»;

– ввести имя носителя в поле «Наименование»;

– создать новое свойство ID_SERIAL и ввести в столбце «Значение» серийный номер USB-накопителя, например, JetFlash_TS256MJF120_OYLIXNA6-0:0;

– выбрать в выпадающих меню пользователя и группу (владельца устройства), установить флажки (задать дискреционные права доступа) владельца, группы и всех остальных пользователей;

– в поле «Описание» можно ввести краткий комментарий.

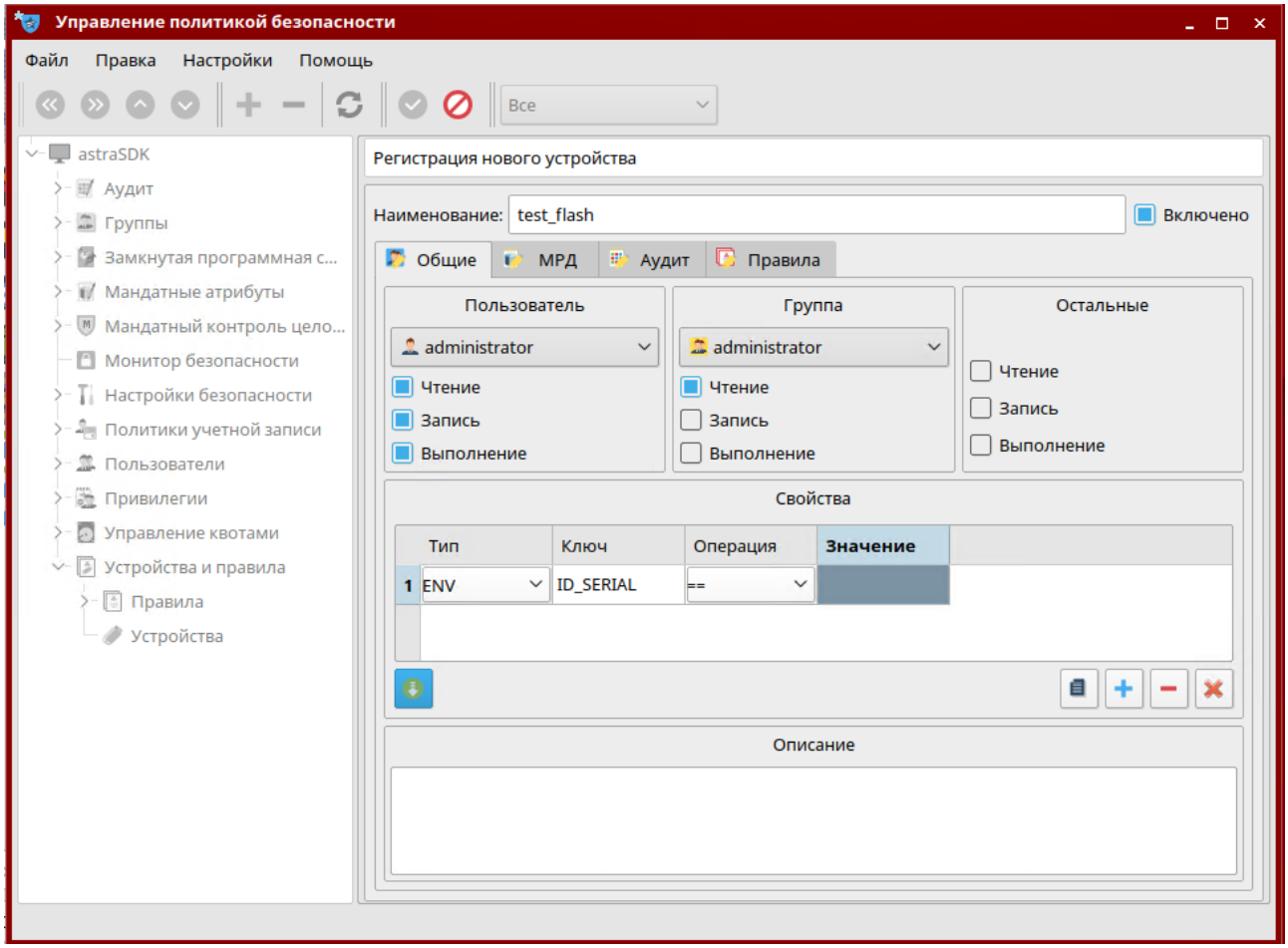


Рисунок 38 – Общие свойства нового устройства

Далее следует перейти к вкладке «МРД», выбрать мандатный уровень из выпадающего списка, далее указать набор мандатных категорий (**Рисунок 39**).

Назначить дополнительные наборы правил для устройства из списка правил, созданных во вкладке боковой панели *Устройства и правила* → *Правила* (в данной вкладке создается набор правил для менеджера устройств udev.

На основе данных из базы учёта устройств подсистема безопасности PARSEC автоматически генерирует файлы правил системы udev, соответствующие учтённым устройствам, в состав которых будет добавлено соответствие

ENV{ID_SERIAL}, включающее действия OWNER, GROUP и MACLABEL, связанные с управлением доступом к устройству. Пример формата такого правила следующий:

```
ENV{ID_SERIAL}=="JetFlash TS256MJF120 OYLIXNA6-0:0", OWNER="user", GROUP="users"
MACLABEL="1:0:r-xr-x"
```

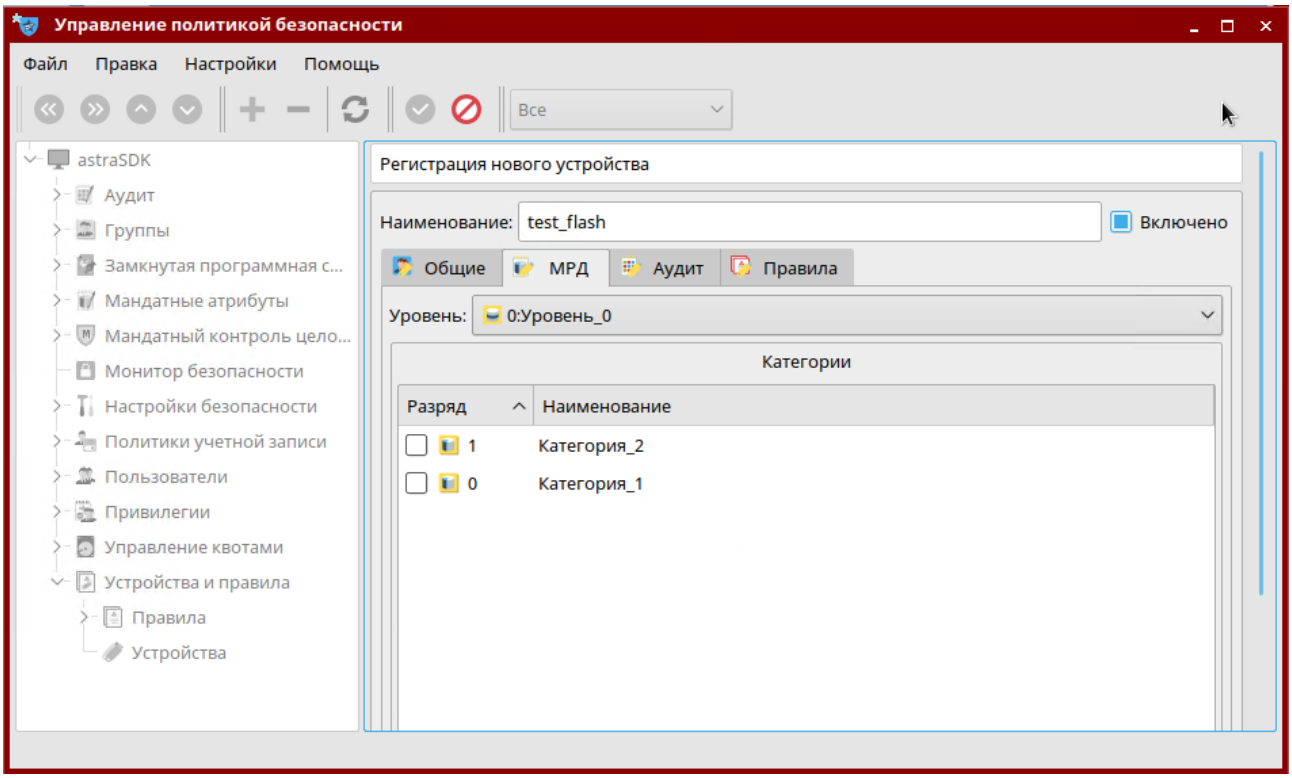


Рисунок 39 – Мандатный доступ

Далее следует назначить параметры регистрации событий, связанных с устройством, для этого во вкладке «Аудит» необходимо выбрать событие и результат (успех, отказ), подлежащие регистрации (**Рисунок 40**).

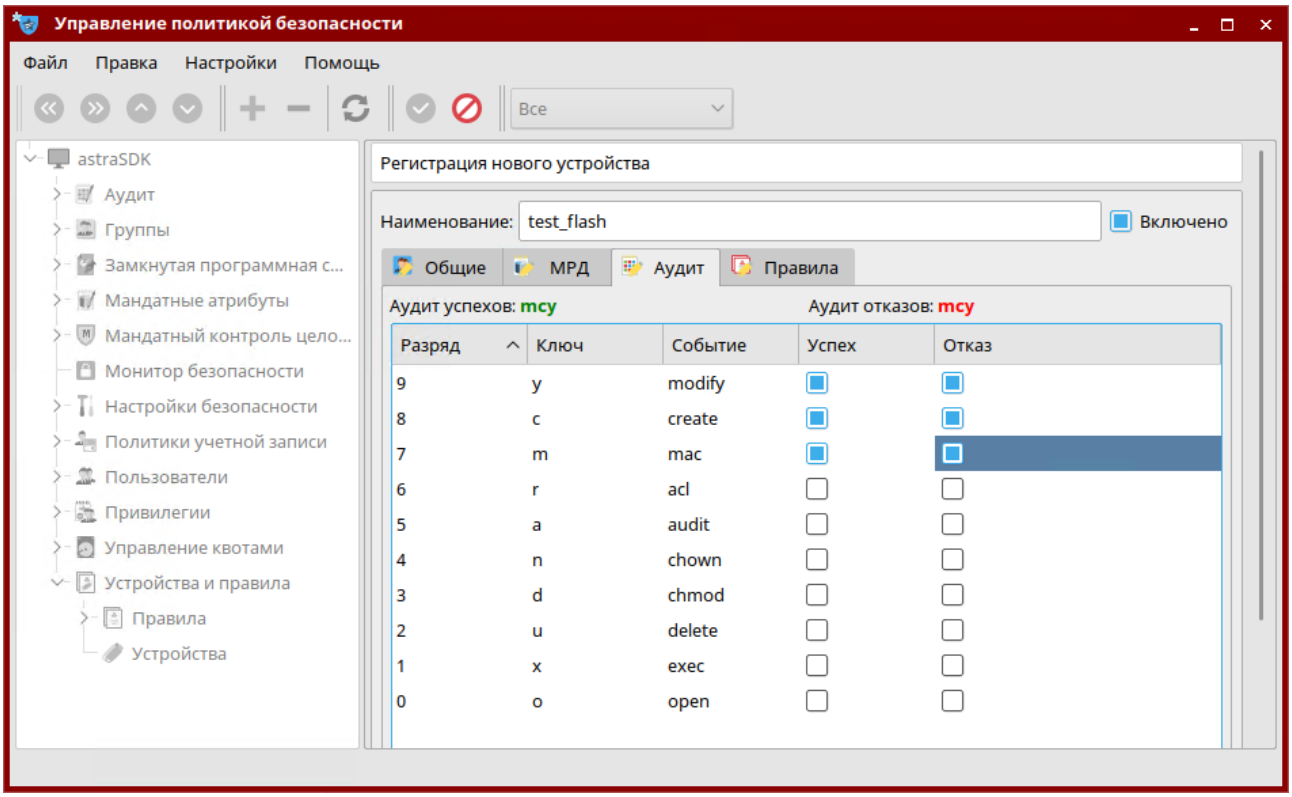


Рисунок 40 – Параметры аудита событий, связанных с USB-накопителем

Далее следует применить изменения, нажав кнопку  [Применить изменения] на панели инструментов.

После переподключения устройства владелец устройства или пользователи из группы могут монтировать устройство, и на точку монтирования будут устанавливаться указанный мандатный уровень и категории.

5 Управление системой безопасности АРМ оператора

Доступ к функциям управления системой информационной безопасности АРМ оператора осуществляется через **Панель администратора**. Для запуска Панели администратора следует в Панели режимов, расположенной в правой верхней части основного экрана АРМ оператора (см. Рисунок 41), и нажать на кнопку **Панель администратора**  .

Рисунок 41 – Панель режимов АРМ оператора

5.1 Журнал информационной безопасности

В журнале информационной безопасности АРМ оператора фиксируются попытки открытия окон мнемосхем, трендов, запуск программ контроля целостности файлов и т.д. Для просмотра журнала информационной безопасности следует нажать на кнопку **Журнал информационной безопасности** (см. Рисунок 42):

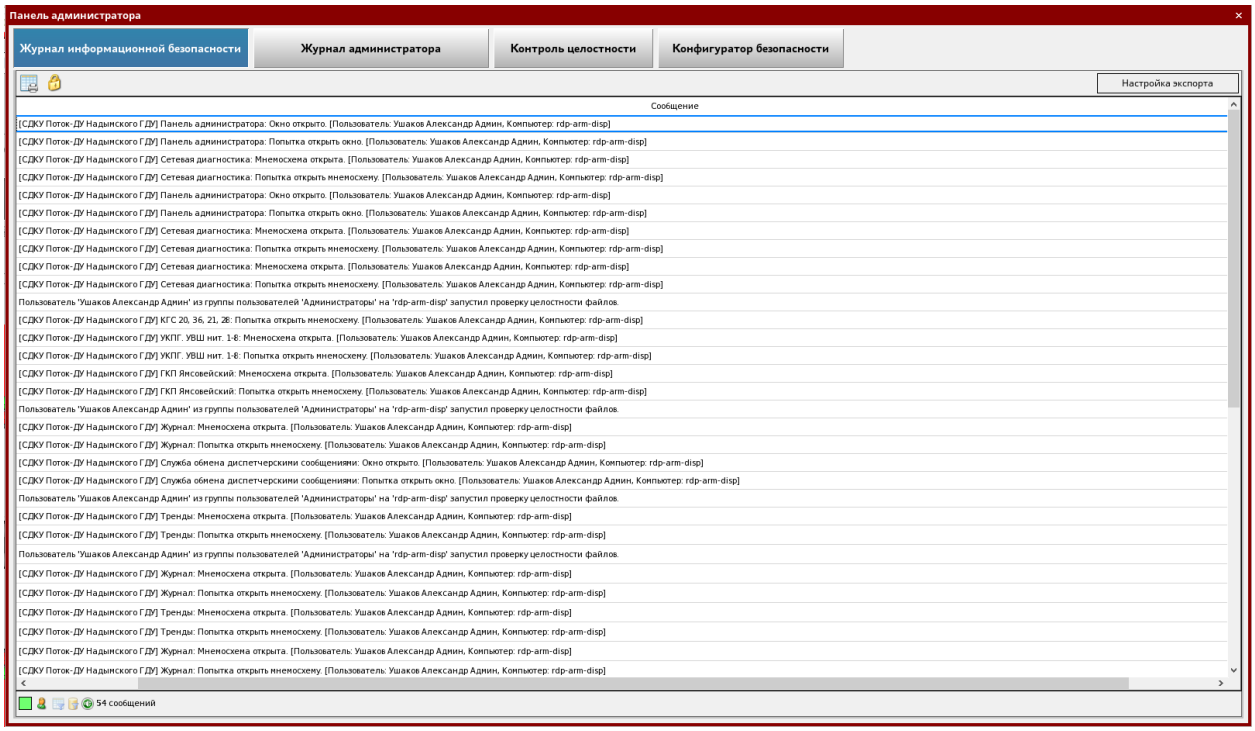


Рисунок 42 - Журнал информационной безопасности

Журнал информационной безопасности может быть сохранен в файле. Для настройки режима сохранения журнала следует нажать кнопку Настройка экспорта. На экран будет выведена панель настроек (см. Рисунок 43).

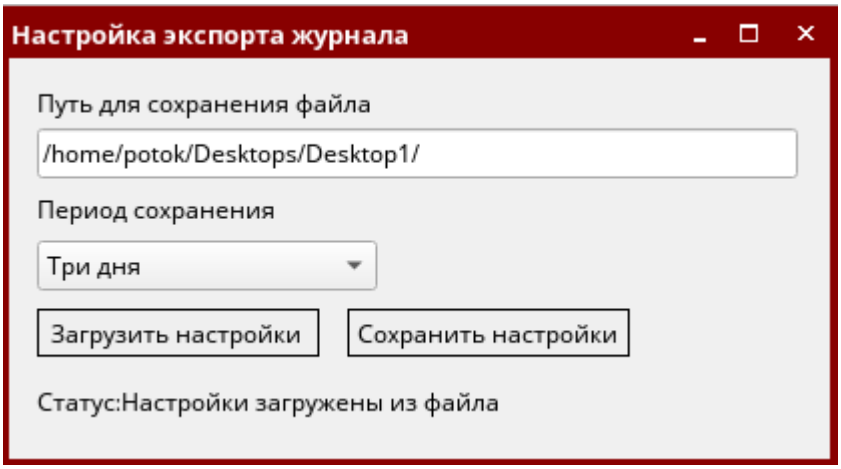


Рисунок 43 – Настройка экспорта журнала информационной безопасности

5.2 Журнал администратора

Для просмотра журнала администратора АРМ оператора следует в Панели администратора нажать кнопку **Журнал администратора** (см. Рисунок 44). Как и другие журналы Альфа-платформы, журнал администратора может работать в оперативном или в историческом режиме.

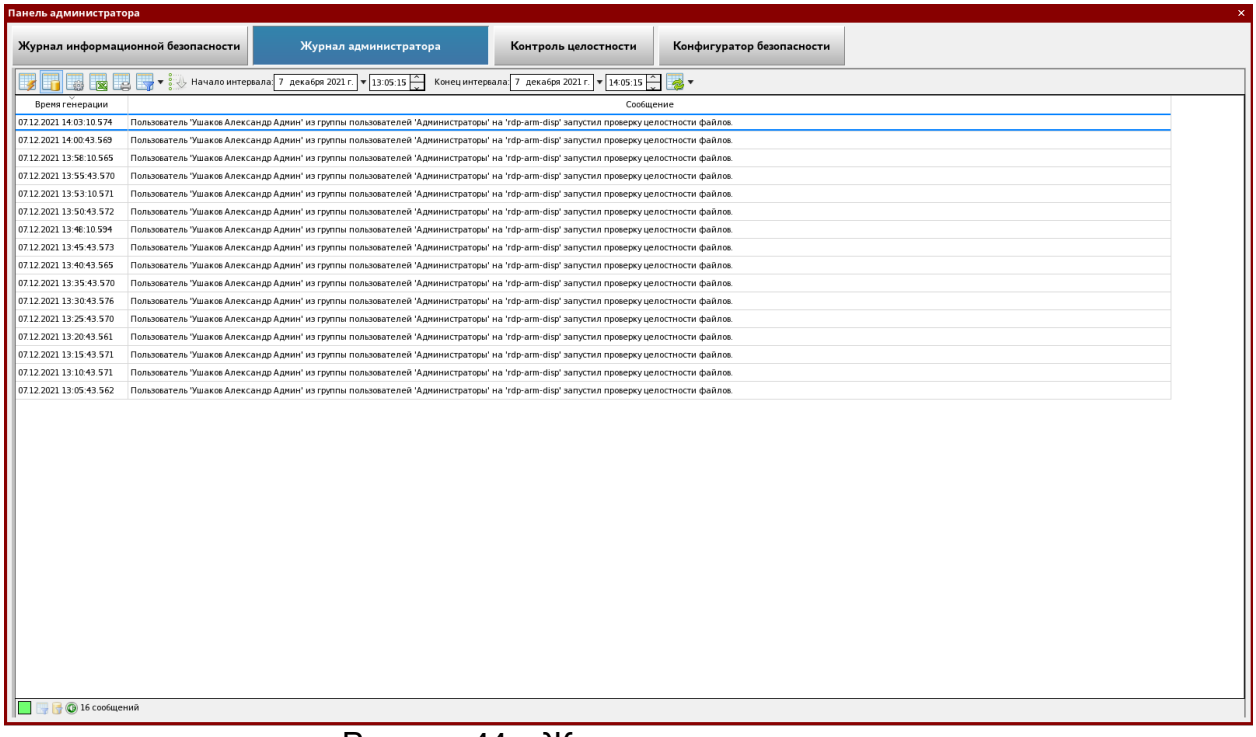


Рисунок 44 – Журнал администратора

Оперативный режим предназначен для поступления оповещений о событиях в режиме реального времени. Для перехода в оперативный режим предназначена кнопка  на панели инструментов. Исторический режим предназначен для

просмотра событий за прошедший период. Для перехода в исторический режим нажмите кнопку  на панели инструментов.

Полное описание панели инструментов журнала приведено в документе «Руководство пользователя» (00159093.28.99.39.190.СЛТМ.2850.И3-02).

5.3 Конфигуратор безопасности

В качестве инструмента администратора ИБ для настройки системы безопасности АРМ оператора используется **Конфигуратор безопасности**. В конфигураторе можно задать пользователей, группы пользователей, отслеживаемые приложения, а также определить для приложений права для пользователей, групп пользователей и ролей. Для доступа к функциям Конфигуратора следует в Панели администратора нажать кнопку **Конфигуратор безопасности (см.** Рисунок 45**).**

Администратору, обладающему правами на изменение конфигурации безопасности, строго запрещено добавление, удаление и изменение прав в своей учетной записи. Все вносимые изменения фиксируются в журнале действия администратора

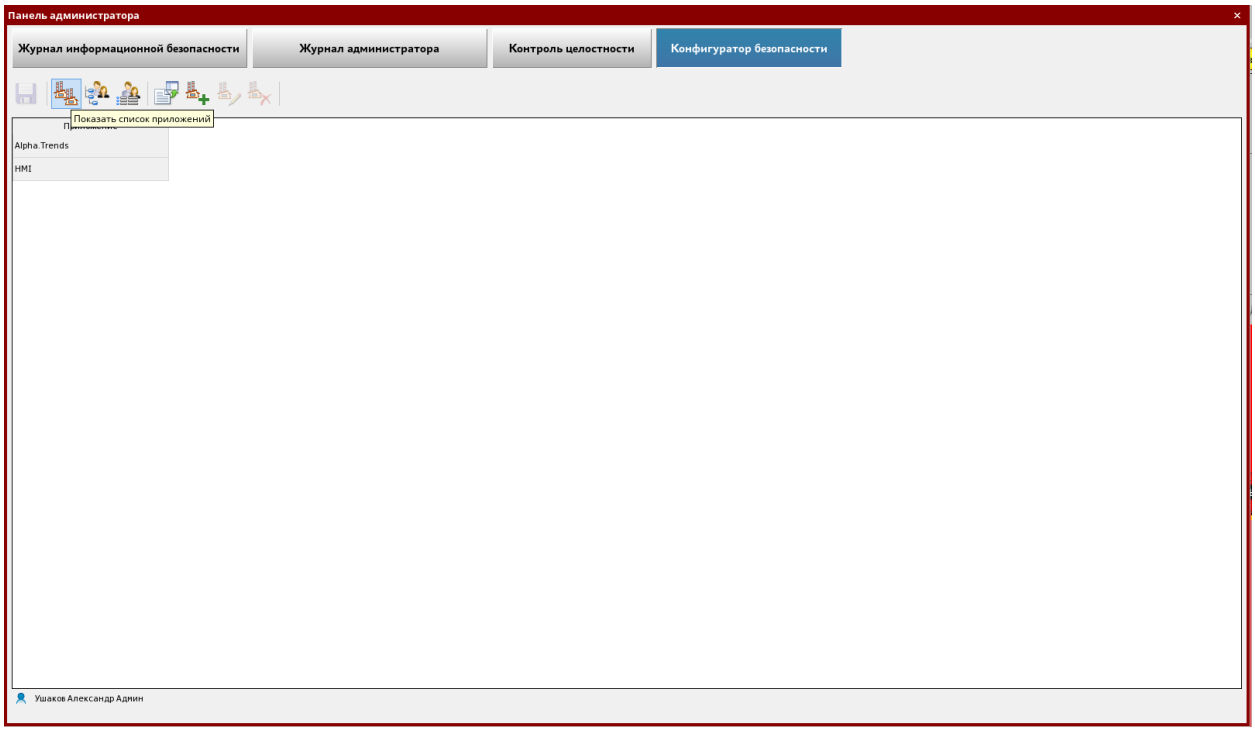


Рисунок 45 – Панель конфигуратора безопасности

5.3.1 Пользователи

Работа с пользователями ведется в Конфигураторе безопасности в разделе **Пользователи**.

Создание пользователей в системе безопасности производится для назначения пользователям прав доступа к определенным функциям приложений.

Чтобы перейти в раздел **Пользователи**, нажмите на панели управления Конфигуратора безопасности кнопку **Пользователи**  . На панели будет отображен список пользователей АРМ оператора, зарегистрированных в компоненте Alpha.Security (см. Рисунок 46).

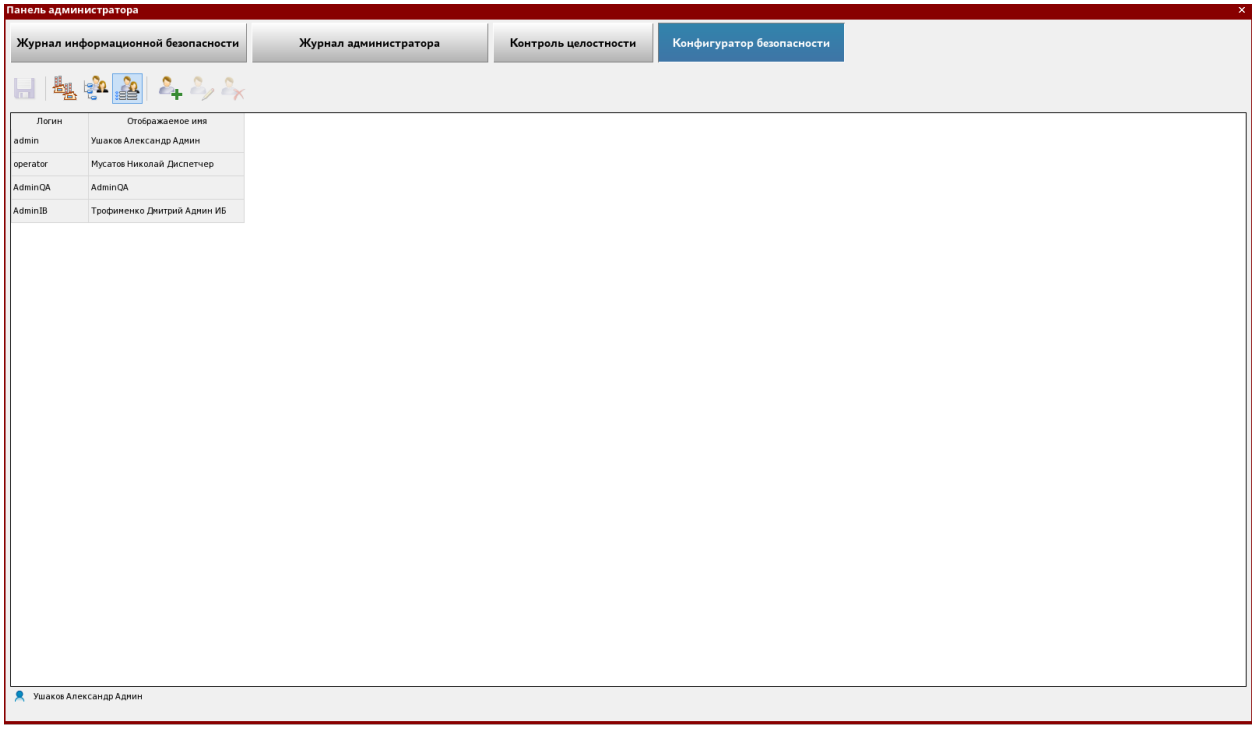


Рисунок 46 – Конфигуратор безопасности – список пользователей

1. Для добавления нового пользователя следует:

а). На панели инструментов (группа **Пользователи**) нажмите кнопку **Добавить пользователя**  .

б). В появившейся форме (см. Рисунок 47) заполните информацию о пользователе. Обязательные поля – **Логин**, **Пароль**, **Фамилия** и **Отображаемое имя** (в форме ввода подсвечены красным).

Чтобы пользователь при первом своем входе сменил пароль, поставьте флажок «**Требовать смены пароля при следующем входе в систему»**.

2. Для редактирования существующего пользователя следует:

а). Выделить курсором пользователя в списке (см. Рисунок 48).

б). На панели инструментов (группа **Пользователи**) нажмите кнопку **Редактировать пользователя**  .

б). В появившейся форме (см. Рисунок 49) отредактируйте информацию о пользователе.

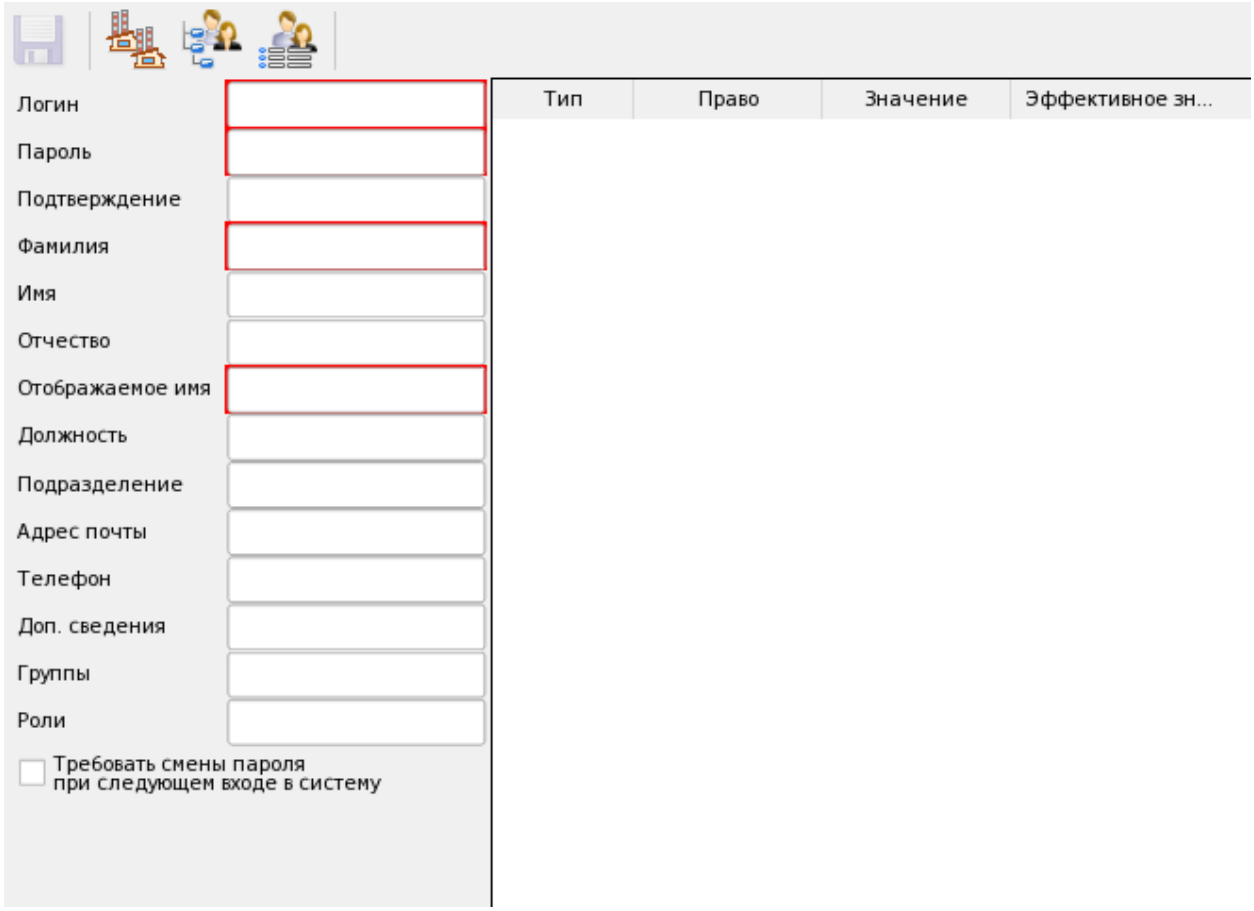


Рисунок 47 – Форма ввода нового пользователя

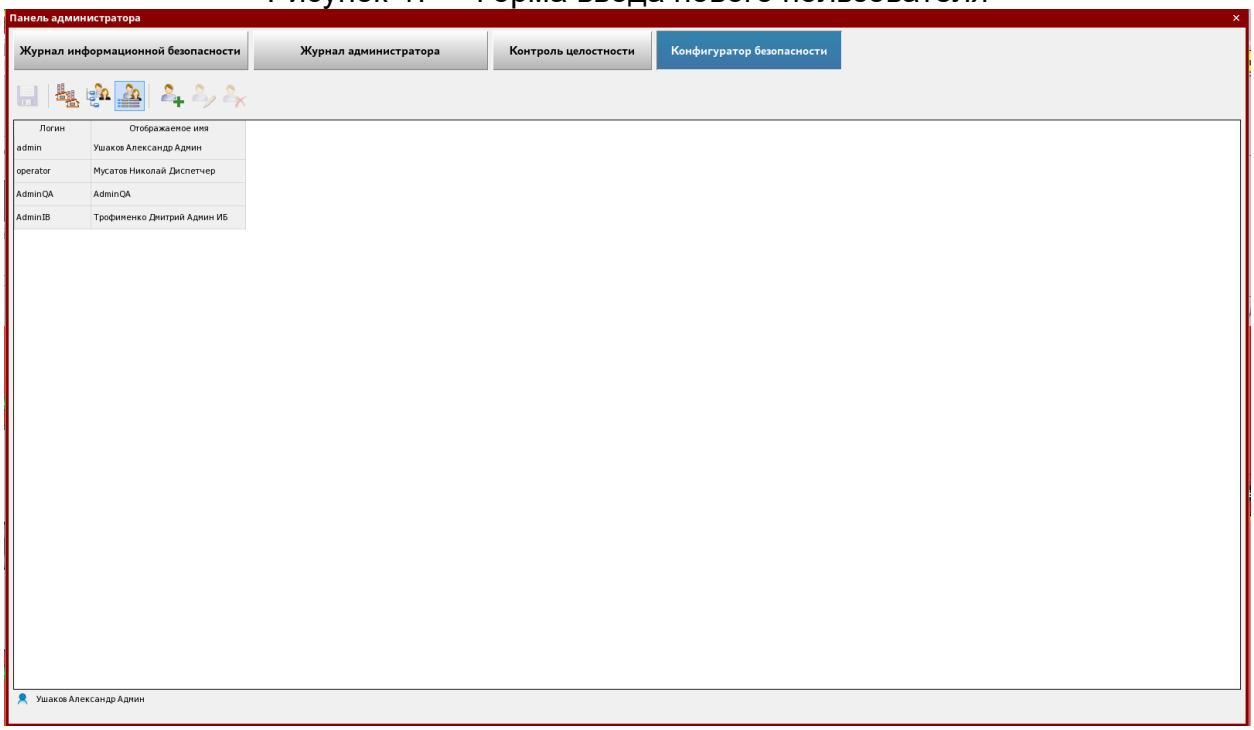


Рисунок 48 – Выделение пользователя

3. Для установки пароля пользователя следует:

а). В режиме редактирования на панели инструментов (группа **Пользователи**) нажмите кнопку **Задать пароль**  .

б). В появившейся форме **Смена пароля** (см. Рисунок 50) задайте пароль и подтвердите его.

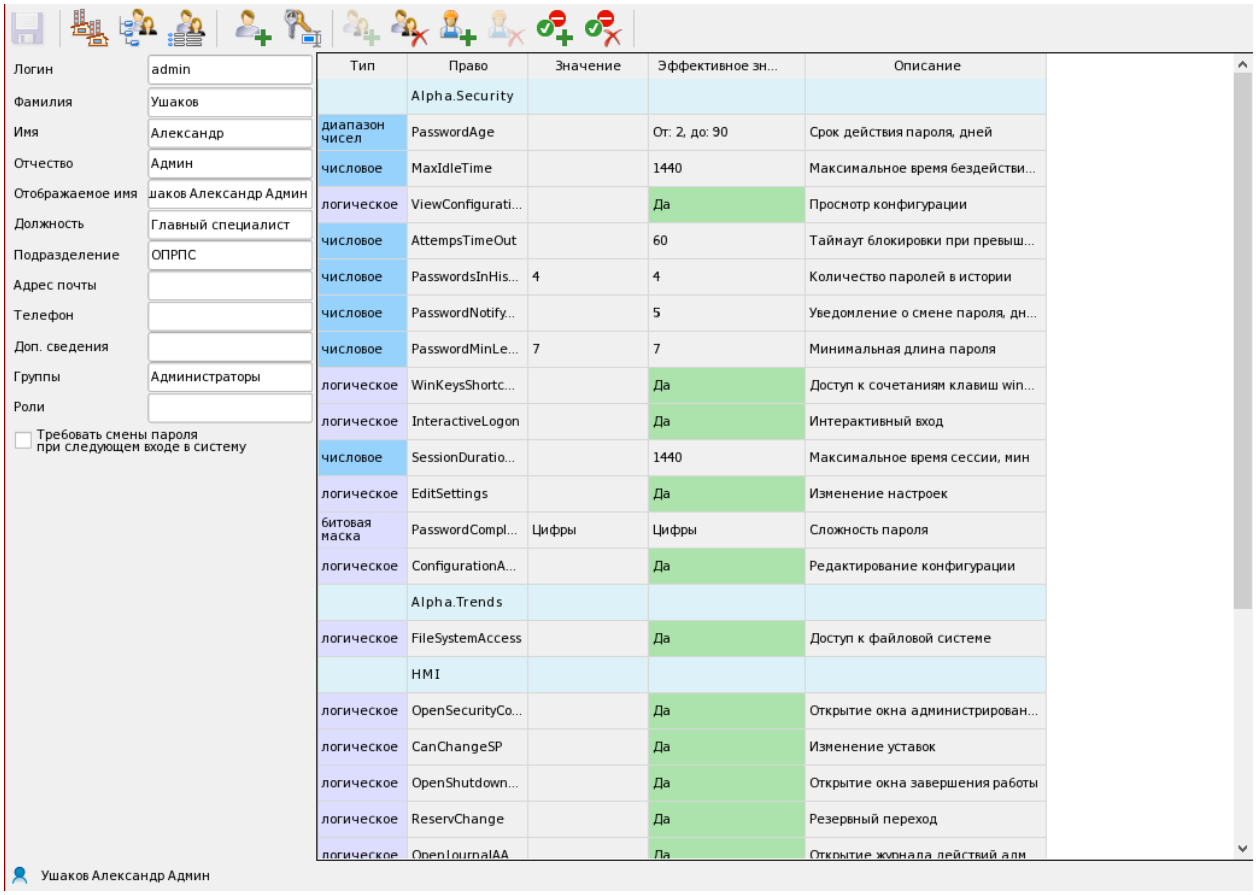


Рисунок 49 – Редактирование пользователя

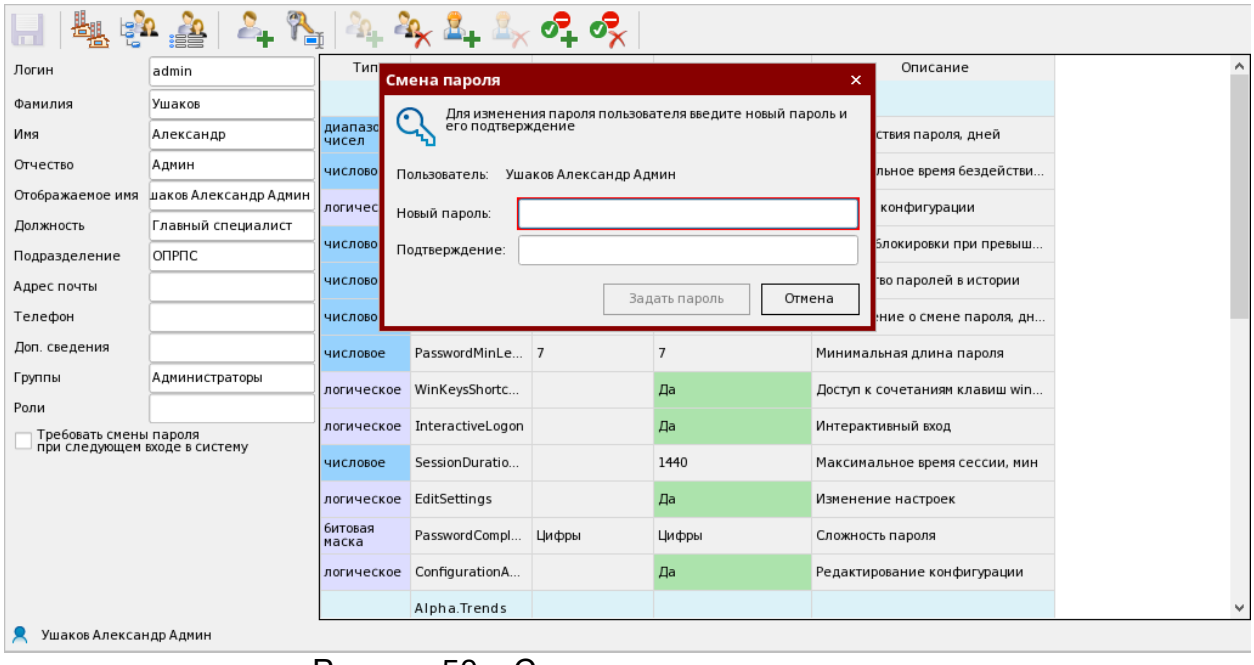


Рисунок 50 – Смена пароля пользователя

4. Роль приложения – совокупность прав приложений, присущих пользователю или группе пользователей в рамках конкретного приложения. Для добавления пользователю роли следует:

а). В режиме редактирования на панели инструментов (группа **Пользователи**) нажмите кнопку **Добавить роль**  .

б). В появившейся форме **Выбор роли** (см. Рисунок 51) выберите роль и нажмите кнопку **Добавить**.

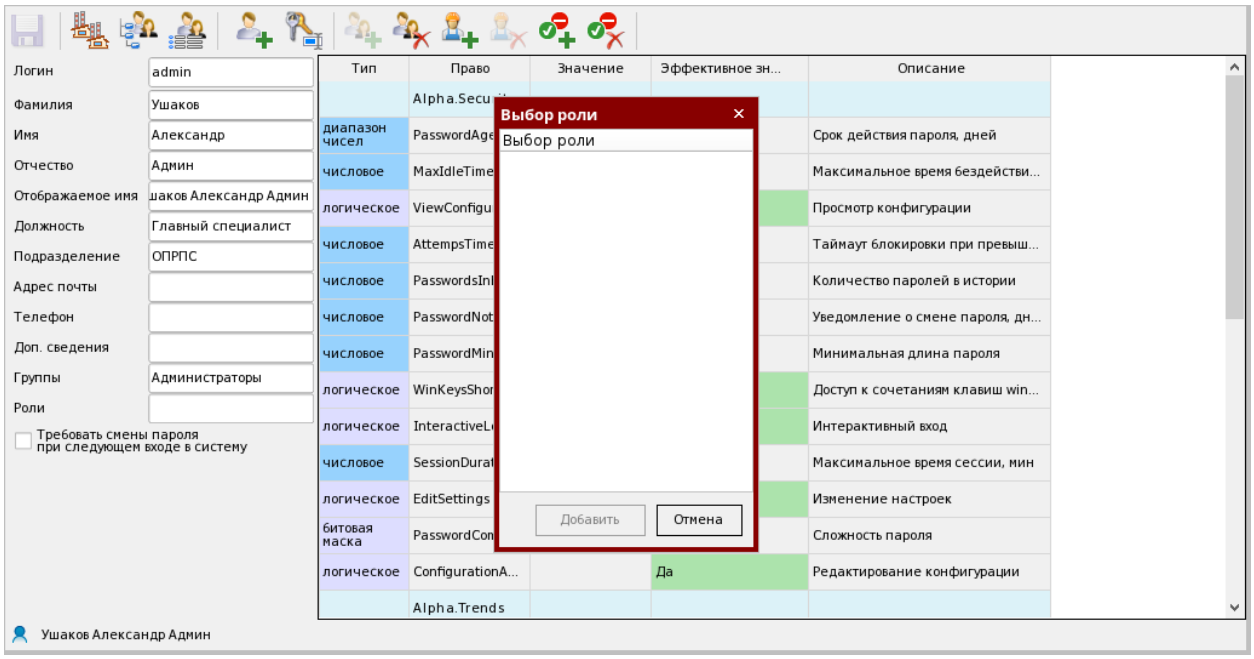


Рисунок 51 – Добавление пользователю роли

5. Для удаления существующего пользователя следует:

а). Выделить курсором пользователя в списке (см. Рисунок 48).

б). На панели инструментов (группа **Пользователи**) нажмите кнопку **Удалить пользователя**  .

Матрица прав доступа пользователей представлена в таблице 4.

Таблица 4 – Матрица прав доступа пользователей

Имя функции	Приложение	Описание	Диспетчер	Администратор	Администратор ИБ
SS_Level	SCADA	Предоставление пользователю прав на отправку сигналов	Предоставление пользователю прав на: - отправку сигналов ТУ; - редактирование путем ручной замены. Запрет отправки сигналов ТР	Предоставление пользователю прав на: - отправку сигналов ТР; - редактирование путем ручной замены. Запрет отправки сигналов ТУ	Запрет для пользователя на: - отправку сигналов ТУ; - отправку сигналов ТР; - редактирование путем ручной замены.
Запуск Alpha.Alarms	Alpha.Alarms	Предоставление пользователю прав на запуск программы Alpha.Alarms	Разрешить	Разрешить	Разрешить
Запуск Alpha.HMIя	Alpha.HMI	Предоставление пользователю прав на запуск программы Alpha.HMI	Разрешить	Разрешить	Разрешить
Запуск Alpha.Trends	Alpha.Trends	Предоставление пользователю прав на запуск программы Alpha.Trends	Разрешить	Разрешить	Разрешить
Запуск редактора скриптов	Alpha.HMI.designer	Предоставление пользователю прав на запуск редактора скриптов	Запретить	Разрешить	Запретить
Квитирование	Alpha.Alarms	Предоставление пользователю прав на Квитирование аварийных сообщений	Разрешить	Разрешить	Разрешить
Настройка фильтров	Alpha.Alarms	Предоставление пользователю прав на настройку фильтров в программе Alpha.Alarms	Разрешить	Разрешить	Разрешить
Просмотр мнемосхем Alpha.HMI	Alpha.HMI	Предоставление пользователю прав на просмотр мнемосхем в приложении Alpha.HMI	Разрешить	Разрешить	Разрешить
Просмотр тегов	Alpha.Trends	Предоставление пользователю прав на просмотр тегов в приложении Alpha.Trends	Разрешить	Разрешить	Разрешить

Имя функции	Приложение	Описание	Диспетчер	Администратор	Администратор ИБ
Упрощенный стиль диалогов	Alpha.Trends	Предоставление пользователю прав на открытие только упрощенных диалогов программы Alpha.Trends (отсутствуют функции настройки и определения системных параметров)	Разрешить	Правило не задано. Можно открывать как полноформатные так и упрощенные диалоги программы Alpha.Trends	Правило не задано. Можно открывать как полноформатные так и упрощенные диалоги программы Alpha.Trends
Упрощенный стиль диалогов	Alpha.Alarms	Предоставление пользователю прав на открытие только упрощенных диалогов программы Alpha.Alarms (отсутствуют функции настройки и определения параметров)	Разрешить	Правило не задано. Можно открывать как полноформатные так и упрощенные диалоги программы Alpha.Alarms	Разрешить
Администрирование Alpha.Alarms	Alpha.Alarms	Предоставление пользователю прав на администрирование программы Alpha.Alarms	Запретить	Запретить	Разрешить
Администрирование Alpha.Security	Alpha.Security	Предоставление пользователю прав на администрирование программы Alpha.Security	Запретить	Разрешить	Запретить
Администрирование Alpha.Trends	Alpha.Trends	Предоставление пользователю прав на администрирование программы Alpha.Trends	Запретить	Разрешить	Запретить
Закрытие приложения	Alpha.HMI	Предоставление пользователю прав на закрытие приложения Alpha.HMI	Запретить	Разрешить	Запретить
Настройка параметров Alpha.Alarms	Alpha.Alarms	Предоставление пользователю прав на настройку параметров в программе Alpha.Alarms	Запретить	Разрешить	Запретить
Настройка параметров Alpha.Trends	Alpha.Trends	Предоставление пользователю прав на настройку параметров в программе Alpha.Trends	Запретить	Разрешить	Запретить
Переход в режим разработки	Alpha.HMI.designer	Предоставление пользователю прав на переход в режим разработки в программе Alpha.HMI.designer	Запретить	Разрешить	Запретить
Разрешить блокировку экрана	Операционная система	Предоставление пользователю прав на блокировку экрана в операционной системе (ОС)	Запретить	Разрешить	Запретить

Имя функции	Приложение	Описание	Диспетчер	Администратор	Администратор ИБ
Разрешить вызов горячей клавиши Win	Операционная система	Предоставление пользователю прав на вызов горячей клавиши Win в ОС	Запретить	Разрешить	Запретить
Разрешить вызов диспетчера задач	Операционная система	Предоставление пользователю прав на вызов диспетчера задач в ОС	Запретить	Разрешить	Запретить
Разрешить вызов командной строки	Операционная система	Предоставление пользователю прав на вызов командной строки в ОС	Запретить	Разрешить	Запретить
Разрешить вызов меню Пуск	Операционная система	Предоставление пользователю прав на вызов меню «Пуск» в ОС	Запретить	Разрешить	Запретить
Разрешить выход из операционной системы	Операционная система	Предоставление пользователю прав на выход из ОС	Запретить	Разрешить	Запретить
Разрешить завершение работы операционной системы	Операционная система	Предоставление пользователю прав на завершение работы ОС	Запретить	Разрешить	Запретить
Разрешить запуск консоли управления Windows	Операционная система	Предоставление пользователю прав на запуск консоли управления ОС	Запретить	Разрешить	Запретить
Разрешить переключение между приложениями	Операционная система	Предоставление пользователю прав на переключение между приложениями в ОС	Запретить	Разрешить	Запретить

Имя функции	Приложение	Описание	Диспетчер	Администратор	Администратор ИБ
Разрешить свертывание окон приложений	Операционная система	Предоставление пользователю прав на свертывание окон в ОС	Запретить	Разрешить	Запретить
Разрешить смену пользователя	Операционная система	Предоставление пользователю прав на смену пользователя в ОС	Запретить	Разрешить	Запретить
Разрешить смену пароля своей учетной записи	Alpha.Security	Предоставление пользователю прав на смену пароля учетной записи в рамках ОС и СПО	Запретить	Разрешить	Запретить
Разрешить смену пароля любой учетной записи	Alpha.Security	Предоставление пользователю прав на смену пароля учетной записи в рамках ОС и СПО	Запретить	Разрешить	Запретить
Создание/Удаление/Блокировка пользователя	Alpha.Security	Создание пользователя в ОС и СПО	Запретить	Разрешить	Запретить
Редактирование политик паролей	Alpha.Security	Редактирование политик паролей ОС которые также распространяются на пользователей СПО	Запретить	Разрешить	Запретить
Настройка параметров журналов ИБ	Alpha.Security	Настройка размера, параметров архивирования, собираемых системных журналов для Административного и Общего журналов безопасности	Запретить	Разрешить	Разрешить
Просмотр журналов ИБ	Alpha.Alarms	Просмотр Административного и Общего журналов безопасности	Запретить	Запретить	Разрешить
Контроль состояния узлов ИБ	Alpha.Security	Возможность запуска и просмотра состояния узлов ИБ. Узлом ИБ являются все ПК принадлежащие СДКУ	Запретить	Разрешить допуск и просмотр	Разрешить просмотр

Имя функции	Приложение	Описание	Диспетчер	Администратор	Администратор ИБ
Смена текущего пользователя любого узла в рамках СПО	Alpha.Security	Возможность перехода в гостевой режим любого узла ИБ. Узлом ИБ являются все ПК принадлежащие СДКУ	Запретить	Разрешить	Запретить
Перезагрузка/ Выключение любого узла в рамках СПО	ОС	Возможность удаленной/локальной перезагрузки/выключения любого узла ИБ. Узлом ИБ являются все ПК принадлежащие СДКУ	Запретить	Разрешить	Запретить

5.3.2 Группы

Чтобы перейти в раздел **Группы пользователей**, нажмите иконку **Группы**  . На панели будет отображен список групп пользователей Альфа-платформы (см. Рисунок 52), зарегистрированных в компоненте Alpha.Security.

Рисунок 52 – Группы пользователей

1. Для добавления новой группы пользователей следует:

а). На панели инструментов (группа **Группы пользователей**) нажмите кнопку **Добавить группу**  .

б). В появившейся форме (см. Рисунок 53) заполните информацию о группе пользователей. Группа характеризуется следующими данными:

– **Идентификатор** (идентификация группы в LDAP-сервере).

– **Описание** (отображаемое имя группы).

– **Роли** – совокупность прав приложений, присущих группе пользователей в рамках конкретного приложения.

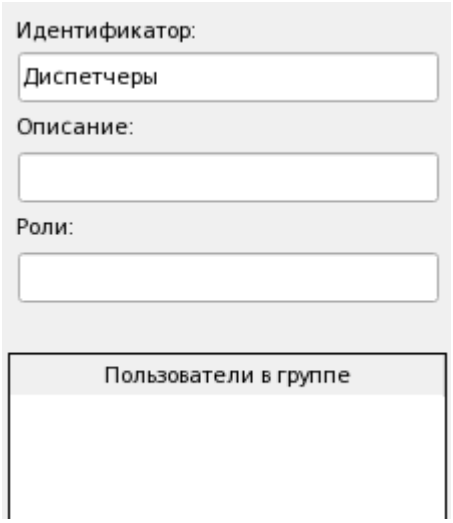


Рисунок 53 – Форма ввода новой группы пользователей

2. Для редактирования существующей группы пользователей следует:

а). Выделить курсором группу в списке (см. Рисунок 54)

б). На панели инструментов (группа **Группы пользователей**) нажмите кнопку **Редактировать группу**  .

в). В появившейся форме (см. Рисунок 55) отредактируйте информацию о группе пользователей.

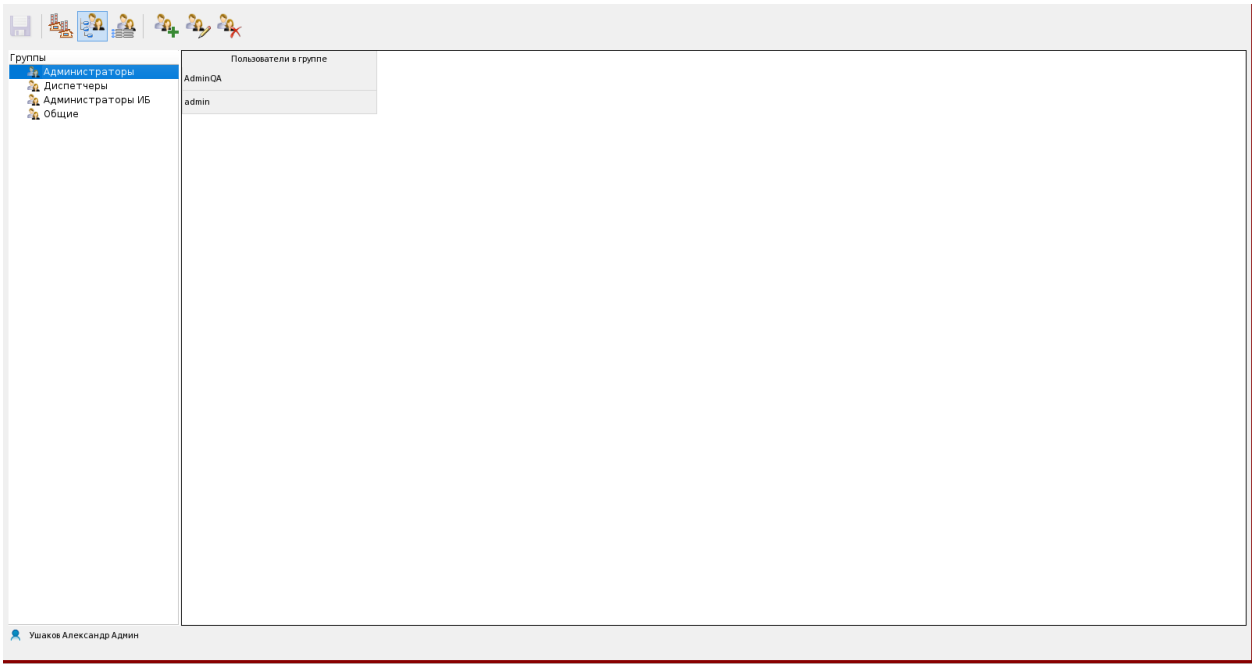


Рисунок 54 – Выделение группы пользователей

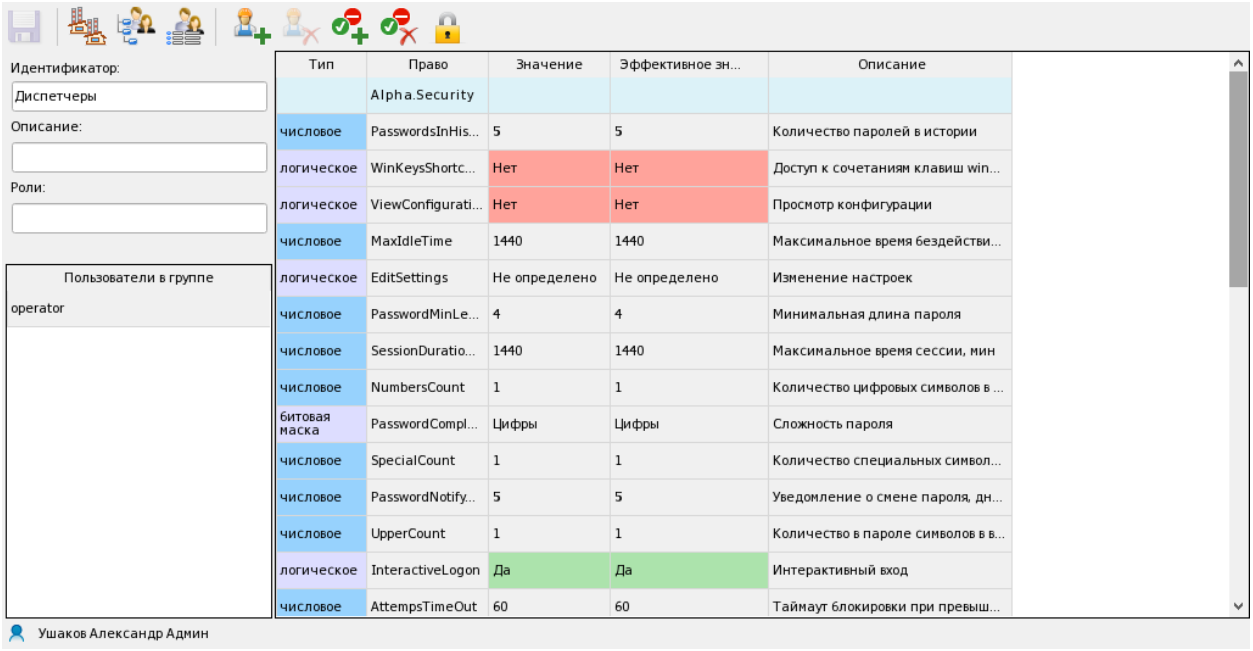


Рисунок 55 – Редактирование группы пользователей

3. Для добавления группе пользователей роли следует:

а). В режиме редактирования на панели инструментов нажмите кнопку **Добавить роль**  (см. Рисунок 55).

б). В появившейся форме **Выбор роли** выберите роль и нажмите кнопку **Добавить**.

4. Для удаления существующей группы пользователей следует:

а). Выделить курсором группу в списке (см. Рисунок 54).

б). На панели инструментов (группа **Группы пользователей**) нажмите кнопку **Удалить группу**  .

5.3.3 Приложения

Приложения добавляются в систему безопасности для отслеживания и контроля доступа пользователей к ним.

Чтобы перейти в раздел **Приложения**, нажмите кнопку **Показать список приложений**  .

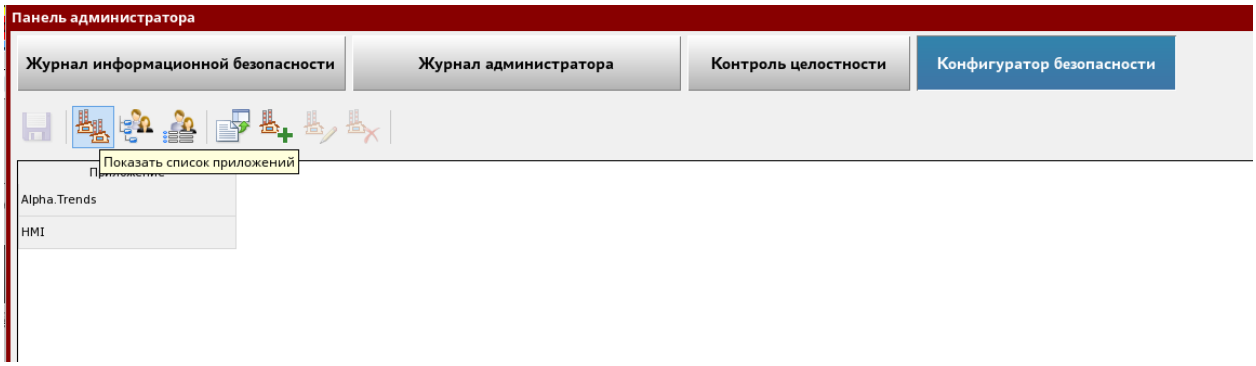


Рисунок 56 – Список приложений

Приложение характеризуется следующими данными:

– **Наименование** – имя приложения.

– **Право** приложений: логическое право/строковое право.

– **Значение права**: разрешить/запретить.

1. Для добавления нового приложения следует:

а). На панели инструментов (группа **Приложения**) нажмите кнопку **Добавить приложение**  .

б). В появившейся форме (см. Рисунок 57) введите название приложения и нажмите клавишу **Enter**.

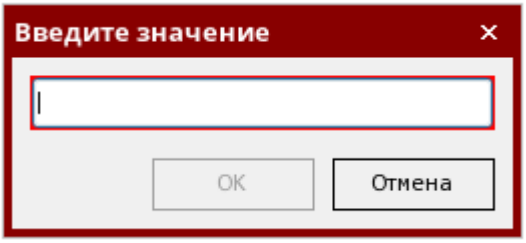


Рисунок 57 – Наименование нового приложения

2. Для удаления приложения:

а). Из списка приложений выберите приложение.

б). На панели инструментов (группа **Приложения**) нажмите кнопку **Удалить приложение**  .

3. Права приложений назначаются администратором и отвечают за защиту функций приложения. Логическое право принимает значения:

– разрешить;

– запретить;

– неопределенное значение, которое означает «не разрешено и не запрещено».

Логическое право вычисляется по формуле «разрешено и не запрещено». Для появления у пользователя прав доступа к определенной функции приложения, у пользователя должно быть явное разрешение и не должно быть явного запрета.

Для добавления логического права следует:

а). Выбрать приложение из списка приложений и нажать кнопку **Редактировать приложение**  . Появится перечень прав, присвоенный данному приложению (см. Рисунок 58).

б). Нажать кнопку **Логическое право**  .

в). В появившемся окне **Добавить логическое право** (см. Рисунок 59) ввести название и описание логического права.

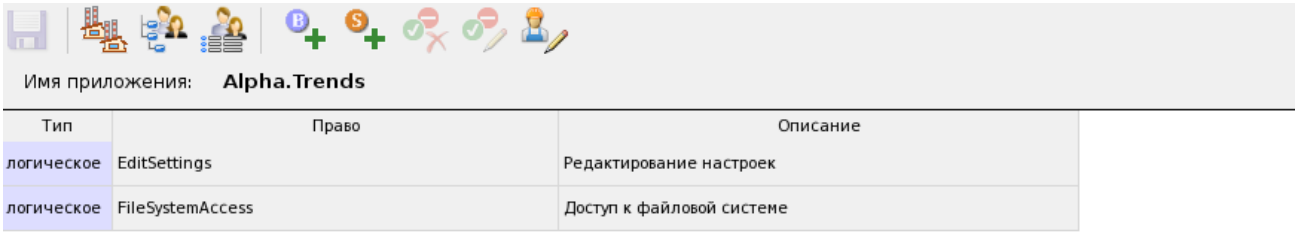


Рисунок 58 – Права приложения

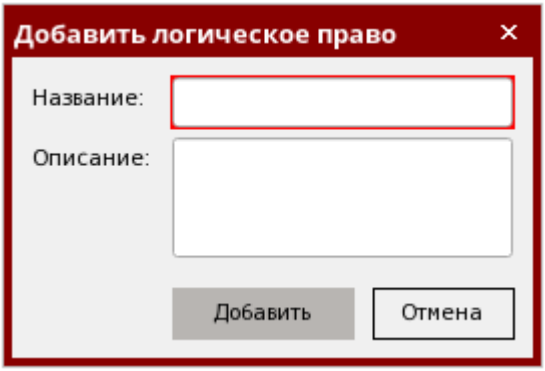


Рисунок 59 – Окно добавления логического права

Строковое право принимает значения:

– разрешить;

– запретить;

Для добавления строкового права следует:

а). Выбрать приложение из списка приложений и нажать кнопку **Редактировать приложение**  . Появится перечень прав, присвоенный данному приложению (см. Рисунок 58).

б). Нажать кнопку **Строковое право**  .

в). В появившемся окне **Добавить строковое право** ввести название и описание строкового права.

Для удаления логического или строкового права следует выбрать право из списка прав и нажать на клавиатуре кнопку **Delete**.

5.3.4 Работа с правами

Область прав позволяет:

– назначить права пользователю или группе пользователей;

– снять права с пользователя или с группы пользователей;

– добавить значение прав.

Для назначения прав следует:

а). Войти в режим редактирования пользователей или групп пользователей.

б). На панели инструментов (группа **Права**) нажать кнопку **Добавить права**  .

в). В окне **Выбор прав** выберите право и нажмите **Добавить** (см. Рисунок 60).

г). Добавленному праву выберите значение **Разрешить** или **Запретить** или в текстовой области введите значение, или напротив нужного значения поставьте флажок.

Для снятия прав пользователя или группы пользователей следует:

а). Перейти в режим редактирования пользователя или группы пользователей.

б). В правой области выбрать право.

в). На панели инструментов (группа **Права**) нажать кнопку **Удалить права**  .

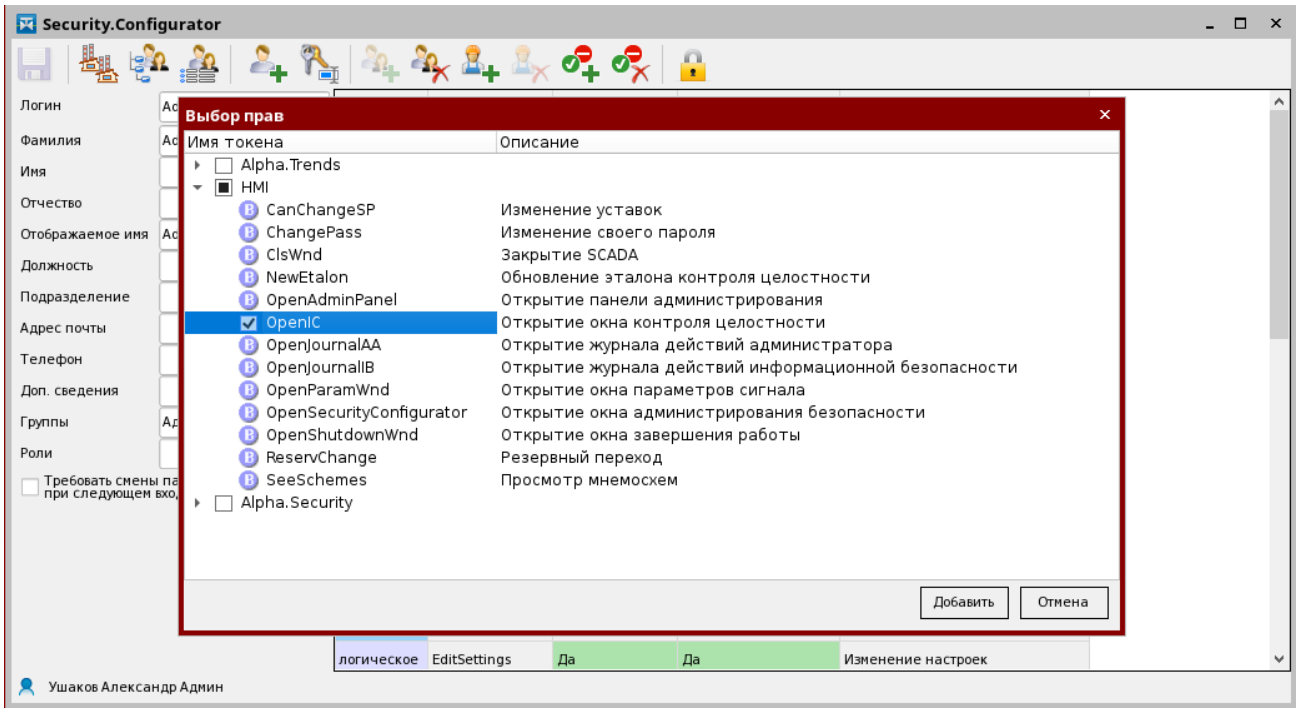


Рисунок 60 – Выбор прав пользователя

Более подробно работа с правами описана в документе «Alpha.Security 1.2. Руководство администратора».

5.4 Контроль целостности компонентов

Для организации контроля целостности файлов приложений Альфа-платформы следует:

1. Нажать кнопку **Проверка целостности** (см. Рисунок 61)
2. Выбрать компьютер, на котором будет выполняться проверка целостности (кнопки АРМ, основной или резервный сервер).
3. Для формирования файла эталонных контрольных сумм нажать кнопку «Создать эталон». Файл эталонных сумм `alpha.security.ic_etalon.xml` создается с помощью алгоритма MD5.
4. Для сравнения вычисленных значений контрольных сумм с эталонными, созданными ранее, нажать кнопку **Проверка**. Положительные результаты проверки отображаются зеленым цветом.

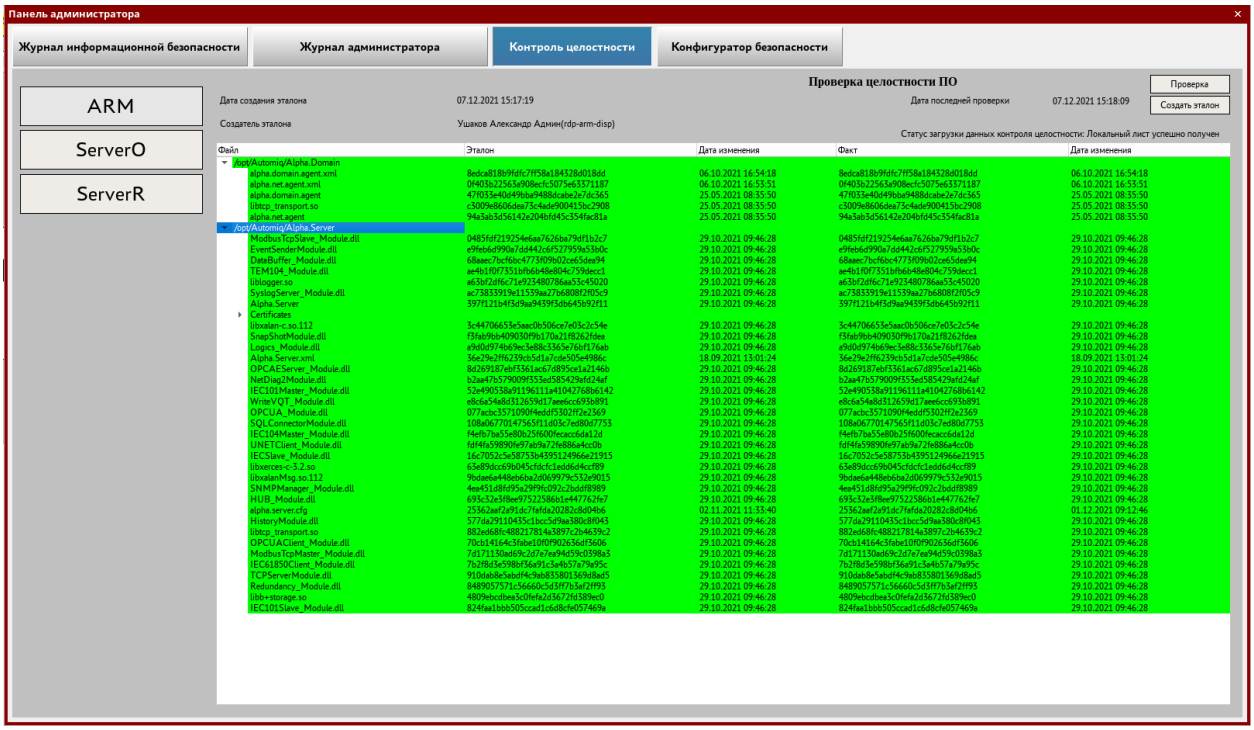


Рисунок 61 – Экран проверки целостности ПО

6 Общие настройки безопасности

6.1 Настройка электропитания для выключения перехода в спящий режим при бездействии

Перейдите в Панели управления в группу «Рабочий стол». Откройте раздел «Оформление Fly» (Рисунок 62).

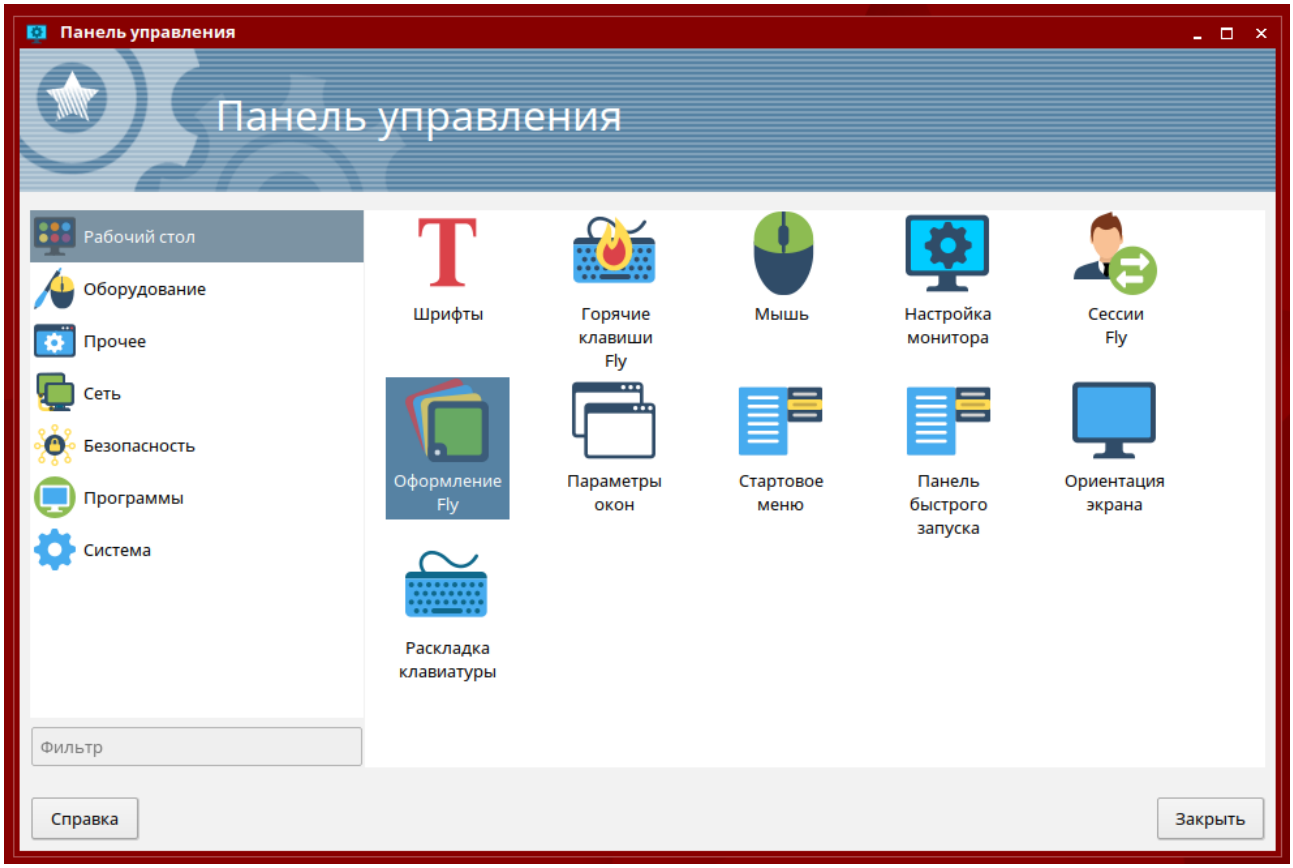


Рисунок 62

Перейдите в группу «Блокировка» и снимите флаг «Блокировать экран» (Рисунок 63).

Нажмите кнопку «Настройка электропитания» и в открывшемся окне снимите флаг «Выключение монитора» (Рисунок 64).

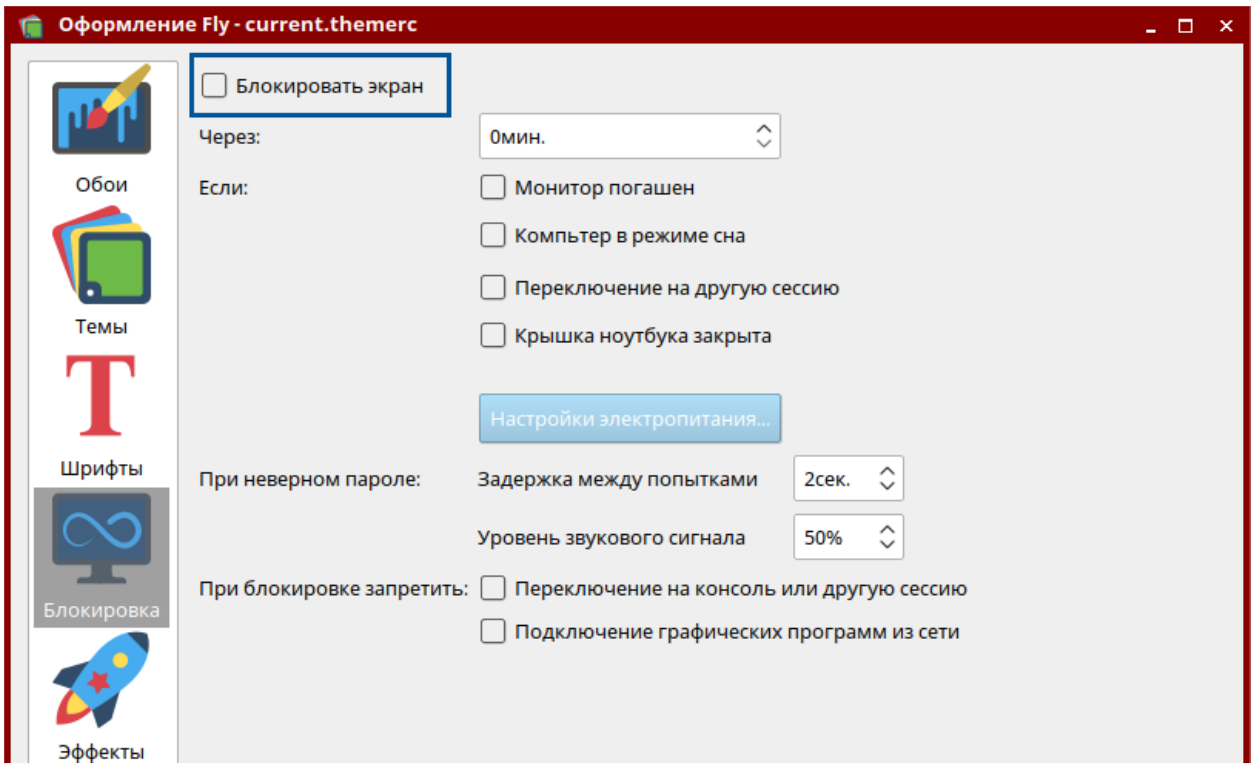


Рисунок 63

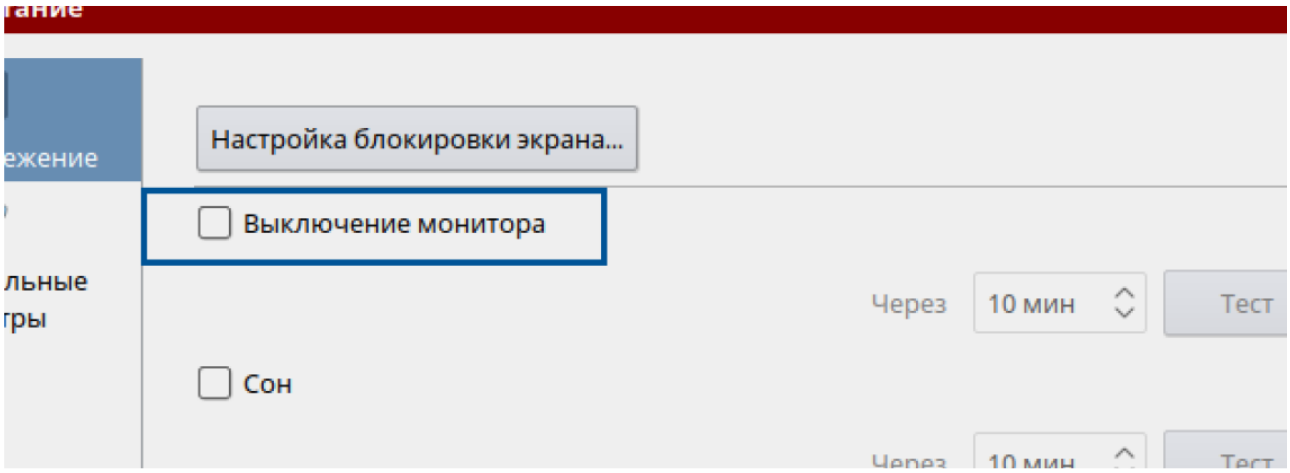


Рисунок 64

6.2 Настройка запрета переключения между виртуальными терминалами

Запустите программу «Терминал Fly», для чего перейдите в меню *Пуск → Системные* и выберите «Терминал Fly».

Перейдите в папку настроек графической среды командой

```
cd /usr/share/X11/xorg.conf.d/
```

Создайте файл конфигурации командой

```
sudo nano 50-novtswitch.conf
```

Запишите в файл флаг запрета переключения между виртуальными терминалами из текущей графической среды:

```
Section "ServerFlags"
Option "DontVTSwitch" "true"
EndSection
```

Сохраните файл и выйдите из редактора Nano, далее перезагрузите ОС Astra Linux командой

```
sudo shutdown -r now
```

6.3 Настройка разрешения переключения между виртуальными терминалами

Запустите программу «Терминал Fly», для чего перейдите в меню *Пуск → Системные* и выберите «Терминал Fly».

Перейдите в папку настроек графической среды командой

```
cd /usr/share/X11/xorg.conf.d/
```

Удалите ранее созданный файл конфигурации с флагом запрета переключения между виртуальными терминалами командой

```
sudo rm 50-novtswitch.conf
```

Чтобы изменения вступили в силу, перезагрузите ОС Astra Linux командой

```
sudo shutdown -r now
```

6.4 Отключение портов USB и устройств CD-ROM

Вариант №1. Для блокировки доступа к USB и CD-ROM можно использовать права доступа файловой системы. Обычно все съемные диски монтируются в раздел /media.

Запустите программу «Терминал Fly», для чего перейдите в меню *Пуск → Системные* и выберите «Терминал Fly». Введите команду:

```
sudo chmod 700 /media
```

Данная команда разрешает монтировать съемные диски только суперпользователю (root).

Для разблокировки доступа используется следующая команда:

```
sudo chmod 755 /media
```

Вариант №2. Использование списка блокировки. Для этого необходимо отредактировать файл blacklist.conf в папке /etc/modprobe.d/.

Запустите программу «Терминал Fly» и введите откройте файл редактором nano:

```
sudo nano /etc/modprobe.d/blacklist.conf
```

Содержимое файла обычно выглядит следующим образом:

```
# This file lists those modules which we don't want to be loaded by
# alias expansion, usually so some other driver will be loaded for the
# device instead.

# evbug is a debug tool that should be loaded explicitly
blacklist evbug

# these drivers are very simple, the HID drivers are usually preferred
blacklist usbmouse
blacklist usbkbd
. . .
```

Добавьте в конец файла следующие две строки:

```
# Block access to USB
blacklist usb_storage
```

Сохраните и закройте файл, затем перезагрузите ОС Astra Linux командой:

```
sudo shutdown -r now
```

Порты USB будут отключены. Для активации портов USB снова откройте данный файл, удалите эти строки (или закомментируйте их).

Для блокировки доступа к устройствам CD-ROM просто удалите пользователя, от имени которого будет работать оператор, из группы cdrom (по умолчанию, это пользователь oper). Запустите программу «Терминал Fly» и введите команду:

```
sudo usermod -G cdrom oper
```

После этого пользователь oper не сможет с ним работать.

Также можно удалить пользователя oper из группы cdrom, отредактировав файл /etc/group с помощью текстового редактора.

6.5 Контроль и анализ защищенности программного обеспечения и программно-аппаратных средств

Контроль и анализ защищенности программного обеспечения и программно-аппаратных средств СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») заключается в проведении мероприятий по анализу защищенности информационной системы и поиску уязвимостей. Контроль и анализ осуществляется Эксплуатирующей организацией или специализированными службами в соответствии с нормативной документацией общества в рамках ТО.

В качестве средств контроля и анализа защищенности программного обеспечения и программно-аппаратных средств СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») возможно использование различных программ, в частности «Сканер ВС», «MaxPatrol», «XSpider» и «ScanOVAL» и т.д..

Для проведения контроля и анализа защищенности используется программа ScanOVAL (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») для автоматизированных проверок наличия уязвимостей программного обеспечения, производящая сравнения состояния системных параметров сканируемого ПО (или его компонентов) с базой уязвимостей, представленной в виде OVAL-описаний, разработанных в соответствии со спецификацией OVAL не ниже версии 5.10.* для ПО для семейства Linux.

Программа позволяет выявлять одиночные и множественные уязвимости, в зависимости от количества поданных ей на вход OVAL-описаний.

Программа предназначена для специалистов в области информационной безопасности прошедших полное обучение по работе с ПО Astra Linux не ниже версии 1.7, для проведения оценки защищенности информационных систем на наличие уязвимостей, сведения о которых содержатся в данных OVAL-описаниях угроз безопасности информации.

6.5.1 Установка ScanOVAL

Для установки программы требуется учетная запись root или другая учетная запись с привилегиями суперпользователя.

Программа функционирует под управлением ОС Astra Linux 1.7 SE. Для обеспечения работы Программы необходимо следующее ПО:

- графический интерфейс пользователя Fly 2.0;
- Xorg версии 7.7;
- qt 5.11;
- libcurl3 (поставляется совместно с дистрибутивом Программы);

– openscap-scanner;

– openscap-common;

– openssl.

Программа представлена в виде архива, содержащего локальный репозиторий scanovalrepo.

Скачать программу ScanOVAL можно с сайта ФСТЭК (https://bdu.fstec.ru/scanovalforlinux).

Архив включает в себя пакет программы, описания уязвимостей в формате OVAL, а также необходимые зависимости для работы Программы.

ВАЖНО! Перед установкой Программы необходимо подключение ОС Astra Linux 1.7.* SE к актуальному репозиторию *base* (требуется наличия подключенных локальных репозиториев общества или подключение к сети интернет).

Для установки Программы необходимо выполнить следующие действия.

1. Скопировать/скачать на компьютер в директорию */mnt* архив локального репозитория (*https://bdu.fstec.ru/files/scanoval-repo-alse17.tar.gz*.)

2. Разархивировать репозиторий путем выполнения следующих команд:

$ cd /mnt

$ sudo tar -C /var/lib -xvf <наименование архива>.tar.gz

3. Установить открытый ключ:

$ sudo apt-key add /var/lib/scanoval/repo/PUBLIC-GPG-KEY-scanoval

4. Создать конфигурационный файл локального репозитория:

$ sudo touch /etc/apt/sources.list.d/scanoval.list

5. Изменить файл ./scanoval.list:

$ sudo nano /etc/apt/sources.list.d/scanoval.list

6. Добавить следующую строку:

deb file:///var/lib/scanoval/repo 1.7_x86-64 main content

Сохранить изменения.

7. Обновить информацию о пакетах и их источниках командой:

$ sudo apt-get update

8. Установить Программу путем выполнения следующей команды:

$ sudo apt-get install openscap-scanner openscap-common openssl scanoval scanoval-content-alse17

Перед запуском Программы должен быть отключен режим Замкнутой программной среды.

6.5.2 Запуск ПО ScanOVAL

Запуск Программы происходит из терминала следующей командой:

Графический интерфейс Программы представляет собой Главное окно, которое разделено на четыре логических зоны:

- строка меню (рисунок 65), расположена в верхней части окна и предназначена для доступа к сервисным функциям Программы, настройке Программы и справке;

Рисунок 65 – Строка меню

- панель быстрого доступа (рисунок 66), расположена ниже строки меню и содержит функциональные кнопки для работы с Программой;

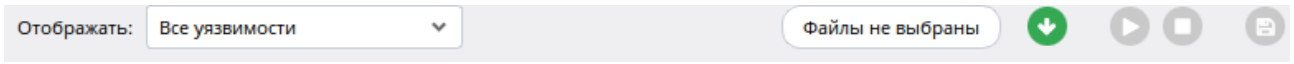
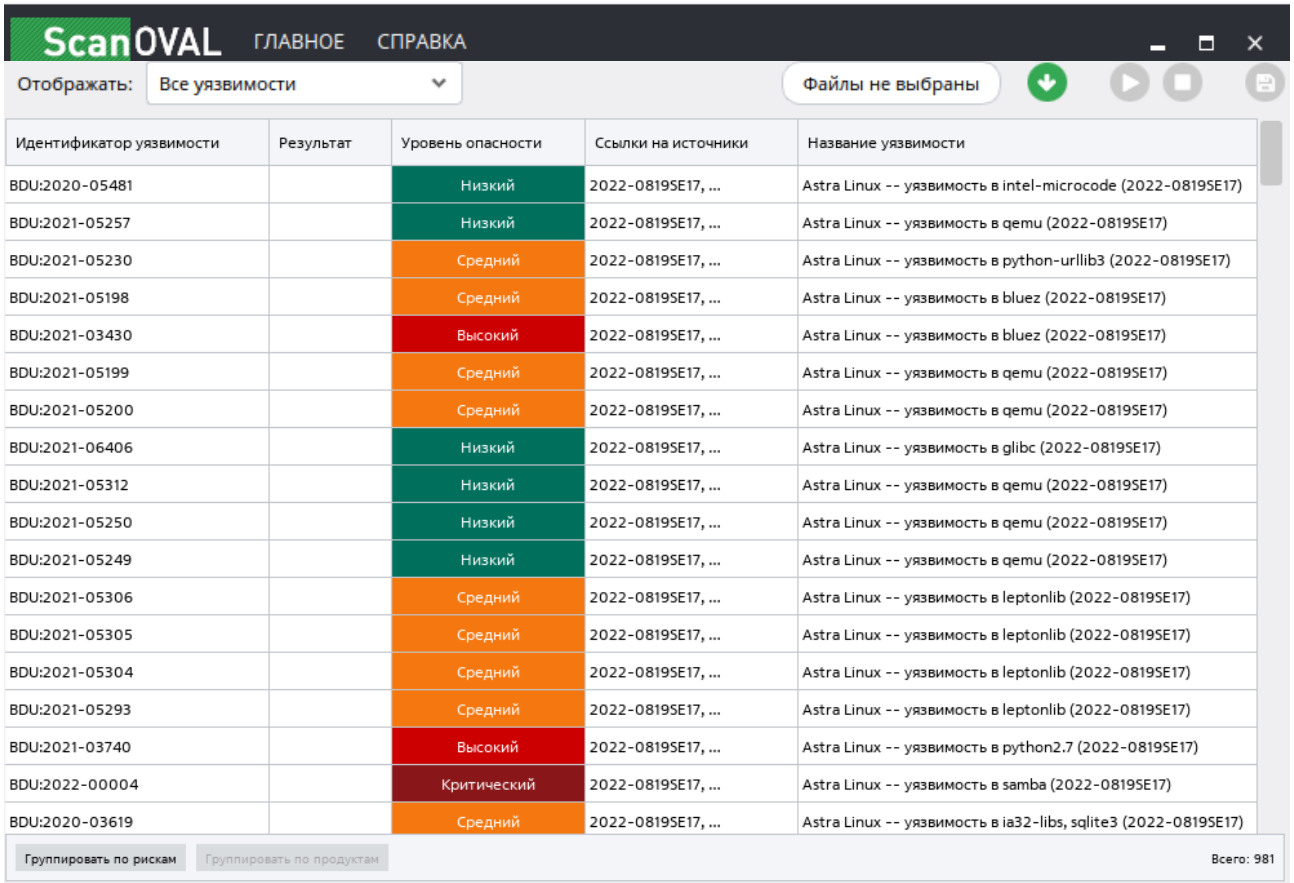


Рисунок 66 – Панель быстрого доступа

- панель «Результаты» (рисунок 67), расположена в центральной части Главного окна, отображает список результатов проверок;

Главного окна, отображает список результатов проверок;



Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2020-05481		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в intel-microcode (2022-0819SE17)
BDU:2021-05257		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05230		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в python-urllib3 (2022-0819SE17)
BDU:2021-05198		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-03430		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-05199		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05200		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-06406		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в glibc (2022-0819SE17)
BDU:2021-05312		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05250		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05249		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05306		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05305		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05304		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05293		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-03740		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в python2.7 (2022-0819SE17)
BDU:2022-00004		Критический	2022-0819SE17, ...	Astra Linux -- уязвимость в samba (2022-0819SE17)
BDU:2020-03619		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в ia32-libs, sqlite3 (2022-0819SE17)

Рисунок 67 – Панель «Результаты»

- панель «Подробности» (рисунок 68), расположена в нижней части окна программы, отображает детализированную информацию об уязвимости.

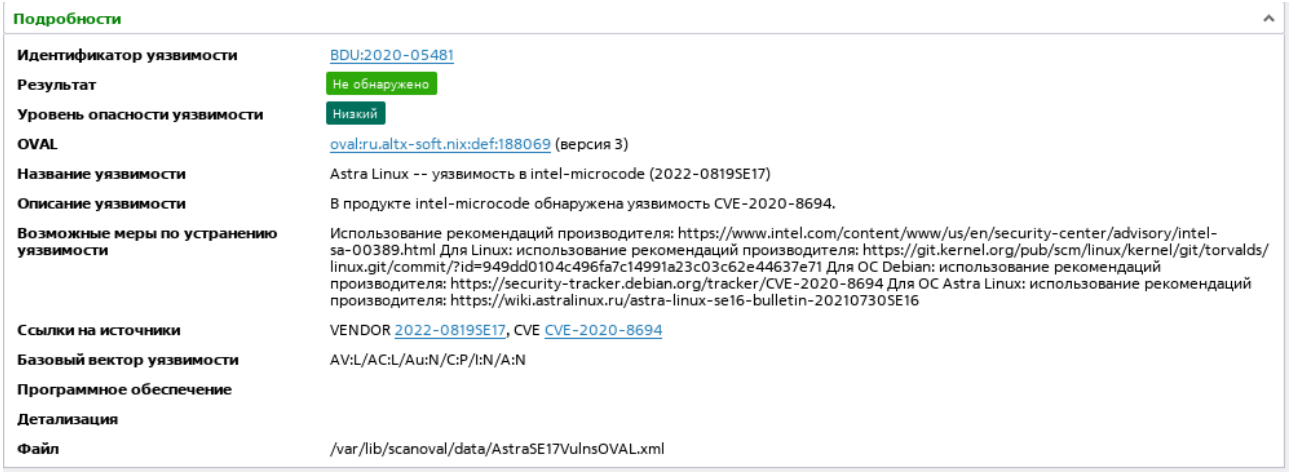


Рисунок 68 – Панель «Подробности»

Для автоматического обнаружения уязвимостей необходимо в программу ScanOVAL загрузить соответствующие XML-файлы, содержащие OVAL-описания уязвимостей.

Программа работает с описаниями уязвимостей, разработанным в соответствии со спецификацией OVAL версии не ниже 5.10.1. OVAL-описания могут быть загружены с сайта банка данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России).

Загружаемый XML-файл с OVAL-описанием может содержать:

- описания одиночных уязвимостей;
- множественные (пакетные) описания, собранные в один файл.

Для загрузки описаний уязвимостей в Главном окне программы необходимо нажать на кнопку «Открыть файл» (рисунок 69). XML-файл может быть загружен с локального диска компьютера, сетевого диска или иного места, доступного пользователю на данном компьютере. XML-файл с OVAL-описаниями уязвимостей, поставляемый вместе с Программой, находится в папке по умолчанию «/var/lib/scanoval/data».

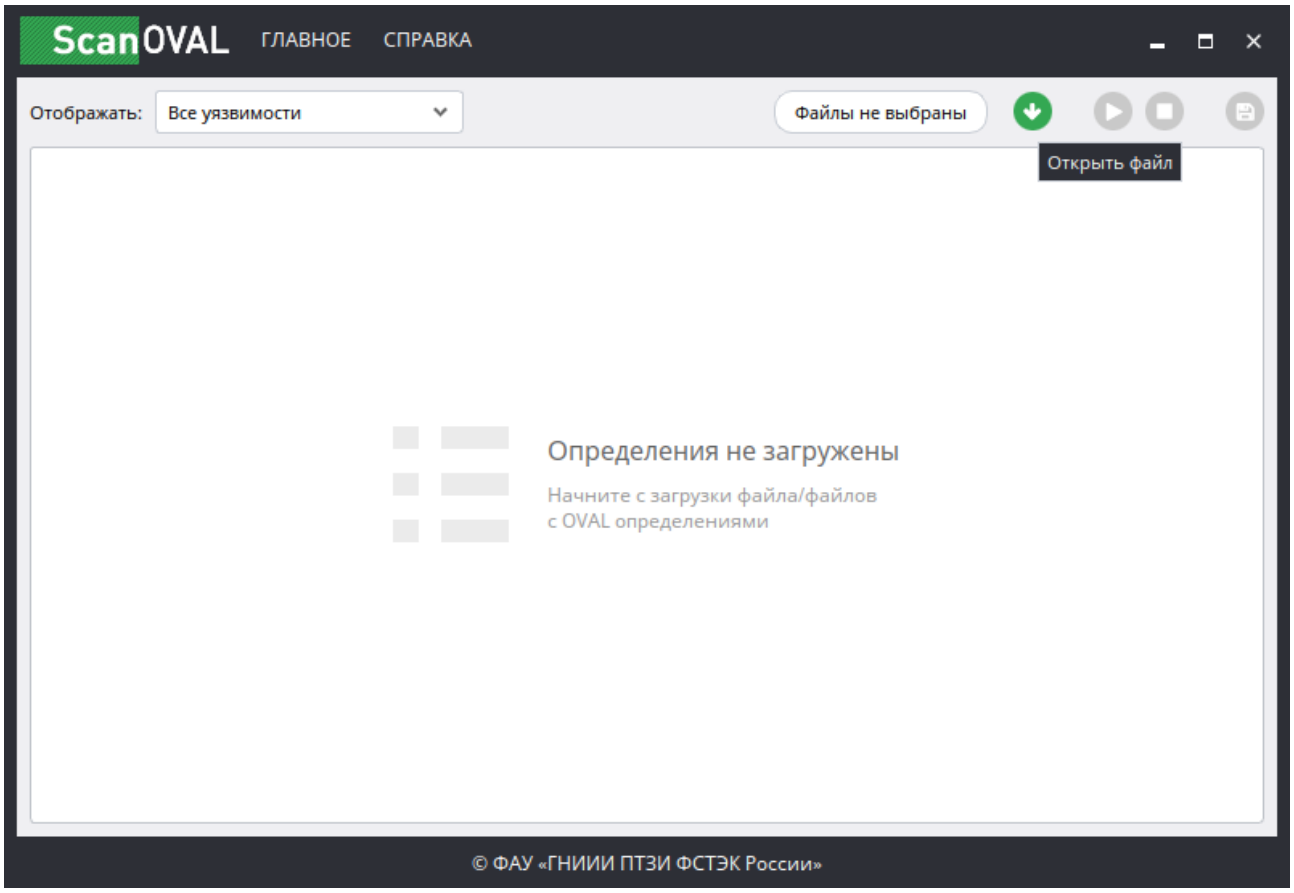
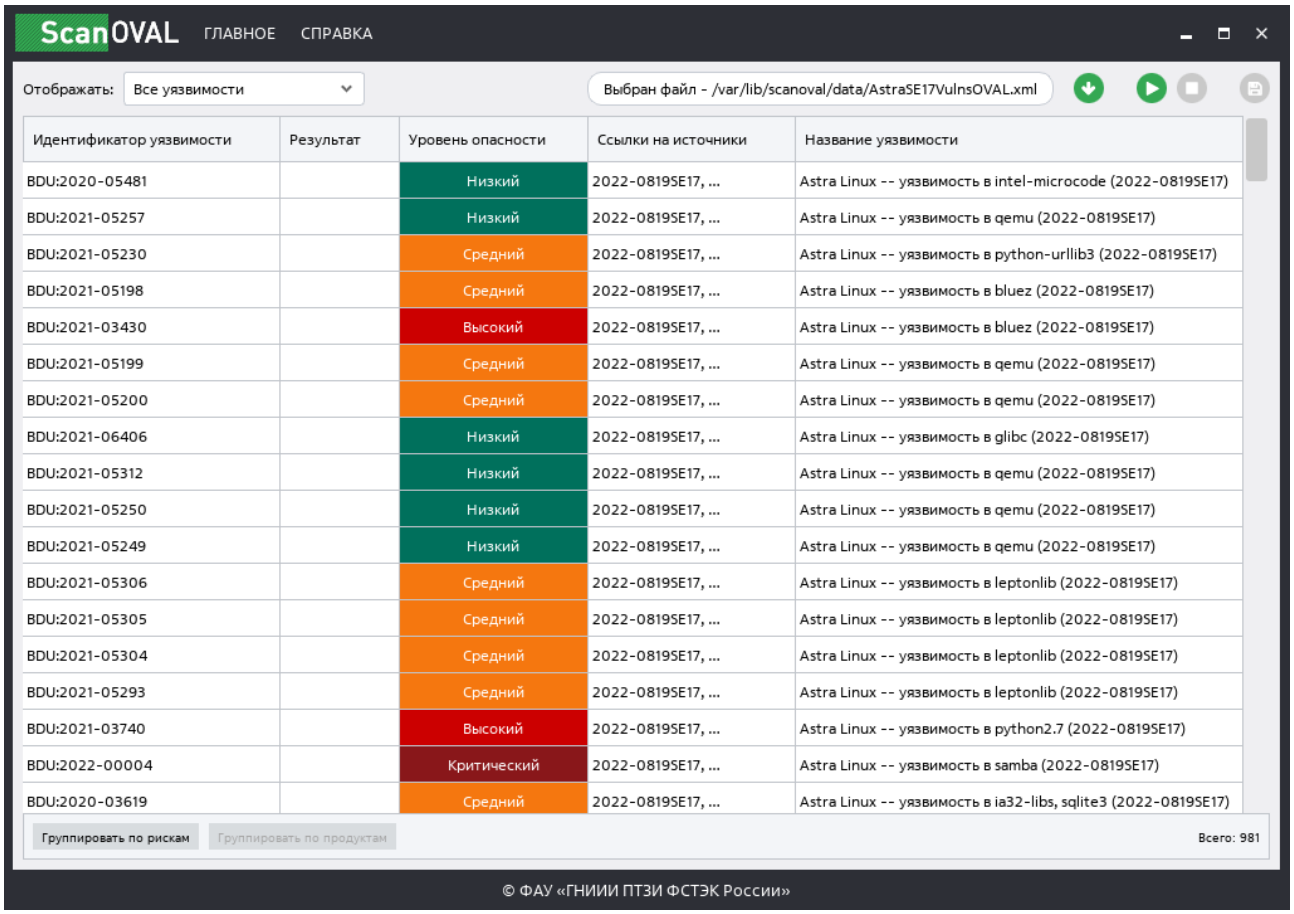


Рисунок 69 – Главное окно программы

В появившемся диалоговом окне выбрать необходимый файл и нажать кнопку «Открыть». В Главном окне программы появится список выбранных описаний уязвимостей (рисунок 70).



Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2020-05481		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в intel-microcode (2022-0819SE17)
BDU:2021-05257		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05230		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в python-urllib3 (2022-0819SE17)
BDU:2021-05198		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-03430		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-05199		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05200		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-06406		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в glibc (2022-0819SE17)
BDU:2021-05312		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05250		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05249		Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05306		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05305		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05304		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05293		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-03740		Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в python2.7 (2022-0819SE17)
BDU:2022-00004		Критический	2022-0819SE17, ...	Astra Linux -- уязвимость в samba (2022-0819SE17)
BDU:2020-03619		Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в ia32-libs, sqlite3 (2022-0819SE17)

Рисунок 70 – Список выбранных описаний уязвимостей

Для добавления или удаления уже загруженных OVAL-описаний необходимо повторно нажать кнопку и в появившемся окне (рисунок 71) выбрать требуемую операцию: «Добавить OVAL файл» или «Удалить все файлы». Добавление осуществляется в диалоговом режиме. Для подтверждения операции необходимо нажать кнопку «Загрузить».

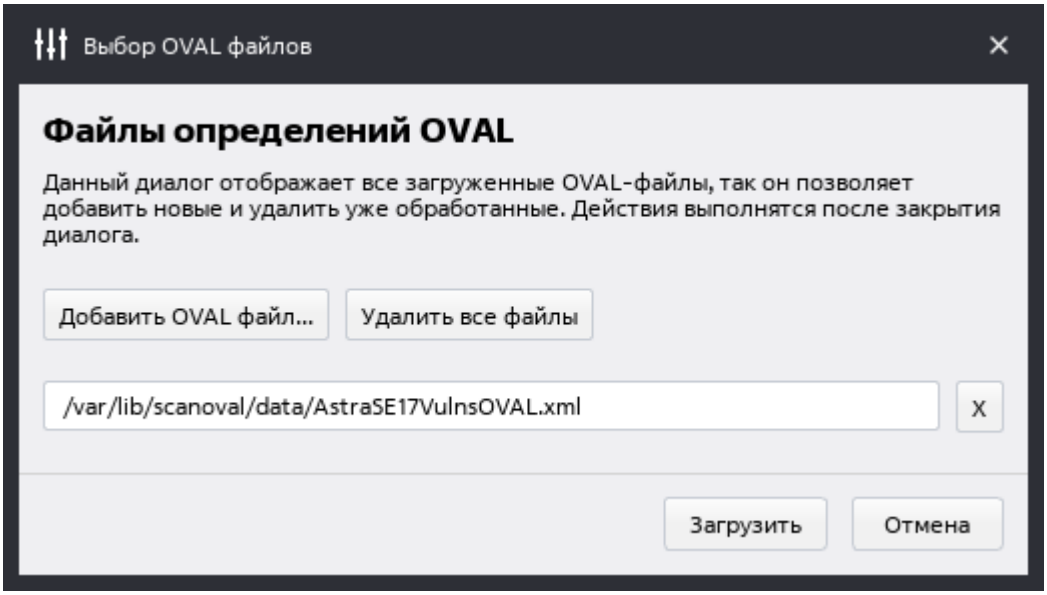
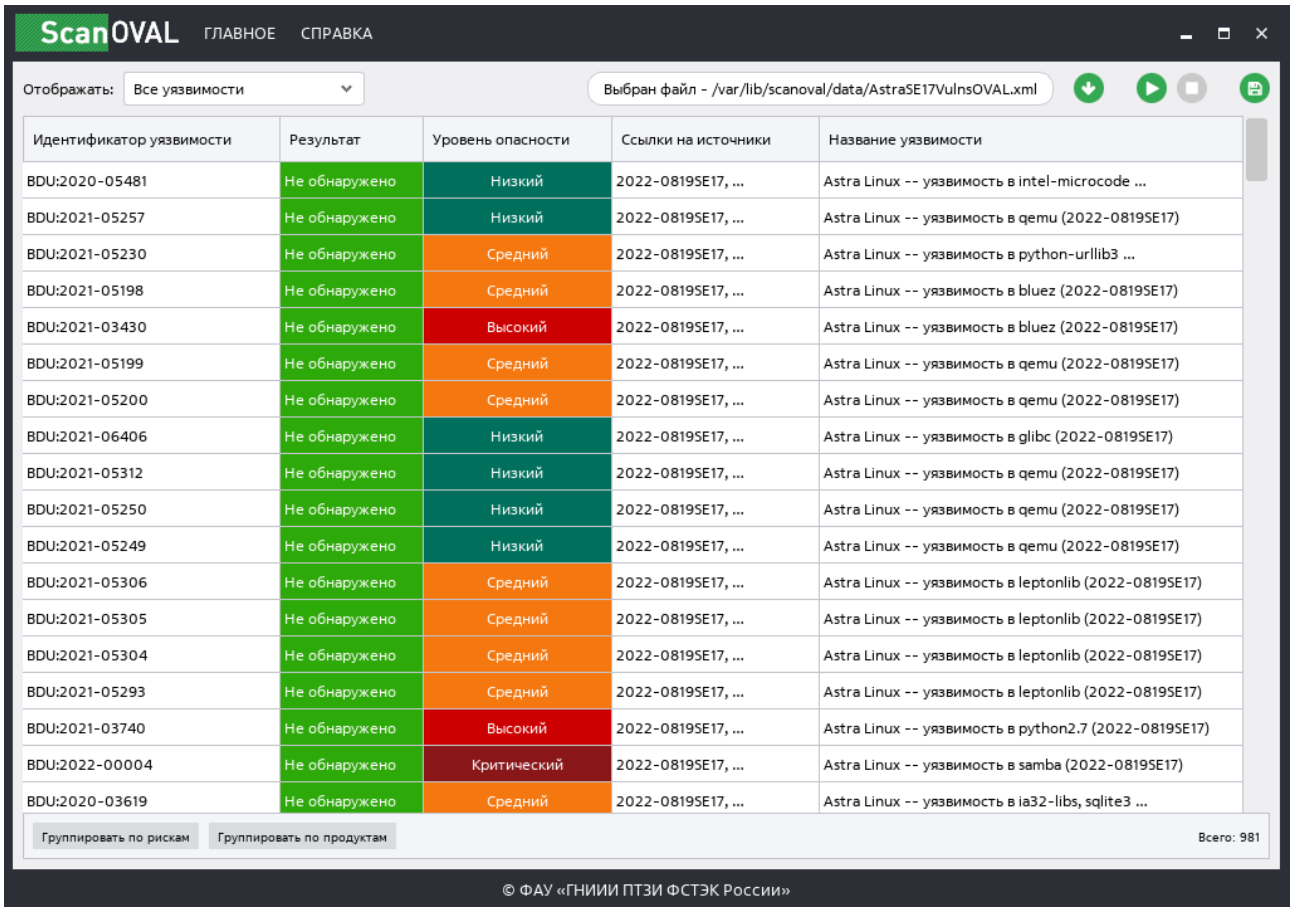


Рисунок 71 – Окно добавления/удаления OVAL-описаний

Для обнаружения уязвимостей необходимо нажать на кнопку «Выполнить аудит», в результате чего в Главном окне появится сообщение «Выполнение…», а на затемненном фоне окна будет наблюдаться динамика выполнения проверок. Время осуществления проверок зависит от количества загруженных OVAL-описаний, а также от аппаратных ресурсов компьютера. Сканирование может занимать от нескольких секунд для одного или нескольких описаний до нескольких минут и более для сотен и тысяч загруженных описаний. По окончании проверок сообщение «Выполнение…» исчезает, при этом в Главном окне появляются результаты проверок с сообщениями «обнаружено» / «не обнаружено» (рисунок 72).



Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2020-05481	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в intel-microcode ...
BDU:2021-05257	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05230	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в python-urllib3 ...
BDU:2021-05198	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-03430	Не обнаружено	Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в bluez (2022-0819SE17)
BDU:2021-05199	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05200	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-06406	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в glibc (2022-0819SE17)
BDU:2021-05312	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05250	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05249	Не обнаружено	Низкий	2022-0819SE17, ...	Astra Linux -- уязвимость в qemu (2022-0819SE17)
BDU:2021-05306	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05305	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05304	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-05293	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в leptonlib (2022-0819SE17)
BDU:2021-03740	Не обнаружено	Высокий	2022-0819SE17, ...	Astra Linux -- уязвимость в python2.7 (2022-0819SE17)
BDU:2022-00004	Не обнаружено	Критический	2022-0819SE17, ...	Astra Linux -- уязвимость в samba (2022-0819SE17)
BDU:2020-03619	Не обнаружено	Средний	2022-0819SE17, ...	Astra Linux -- уязвимость в ia32-libs, sqlite3 ...

Рисунок 72 – Результат выполненной проверки

Результаты проверок отображаются в Главном окне программы в панелях «Результаты» и «Подробности». Панель «Результаты» содержит общую информацию о результатах проверок. В строке результата отображается следующая информация:

- Идентификатор уязвимости – идентификатор уязвимости в БДУ;
- Результат – результат проверки («Обнаружено» / «Не обнаружено»);
- Уровень опасности уязвимости;
- Ссылки на источники описания уязвимости;
- Название уязвимости.

Панель «Подробности» расположена ниже панели «Результаты» и раскрывается кликом мыши по строке результата проверки или нажатием на кнопку «Подробности» (рисунок 73).

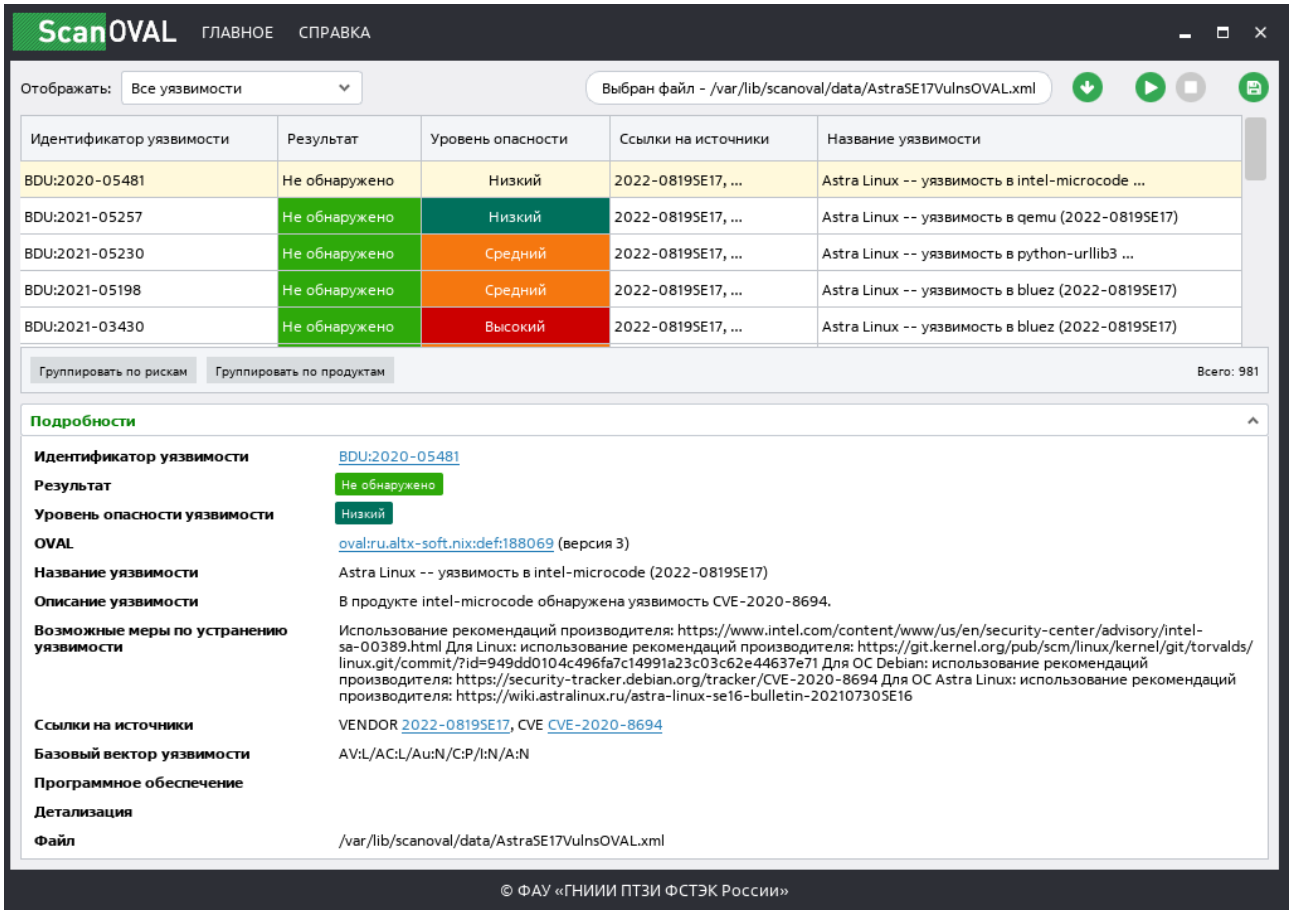


Рисунок 73 – Детализированная информация об уязвимости

В панели представлена детализированная информация об уязвимости:

- Идентификатор уязвимости в БДУ, содержащий гиперссылку на соответствующую страницу сайта БДУ;
- Результат – результат проверки: «Обнаружена» / «Не обнаружена»;
- Уровень опасности уязвимости;
- OVAL – путь к месту загрузки OVAL-описания;
- Название уязвимости;
- Описание уязвимости;
- Возможные меры по устранению уязвимости;
- Ссылки на источники;
- Базовый вектор уязвимости (CVSS);
- Программное обеспечение – обозначение уязвимого программного обеспечения в классификации CPE (Common Platform Enumeration);
- Детализация – объект, для которого осуществлялась проверка;

- Файл – путь к расположению уязвимого ПО (файла). Данная строка появляется только при выявлении уязвимости.

Работа Программы завершается нажатием на кнопку в правом верхнем углу или через строку меню, путем перехода в закладку «Главное» и последующего выбора пункта «Выйти из программы».

ВАЖНО! Если после выполнения сканирования и обнаружения уязвимостей, критичными уязвимостями для корректной работы программного обеспечения и программно-аппаратных средств СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») являются только уровни опасности с маркером «Высокий» и «Критичный».
Маркеры «Низкий» и «Средний» не несут критической уязвимости на систему, и полностью закрываются Антивирусным ПО (установка и настройка Антивирусного ПО осуществляется Эксплуатирующей организацией или специализированными службами).

7 Контроль целостности

7.1 Проверка целостности на уровне ОС

Программа проверки целостности ОС предназначена для проверки соответствия модулей системы модулям, входящим в состав дистрибутива ОС. Проверка выполняется путем подсчета контрольных сумм модулей и их сравнения с эталонными значениями. Запускается в режиме суперпользователя (root). Для работы программы необходим носитель с дистрибутивом ОС, соответствующим версии ОС, установленной в системе.

Для запуска программы проверки целостности следует выбрать в главном меню ОС Astra Linux *Пуск* пункты *Панель управления* и далее *Проверка целостности системы* (см. Рисунок 74).

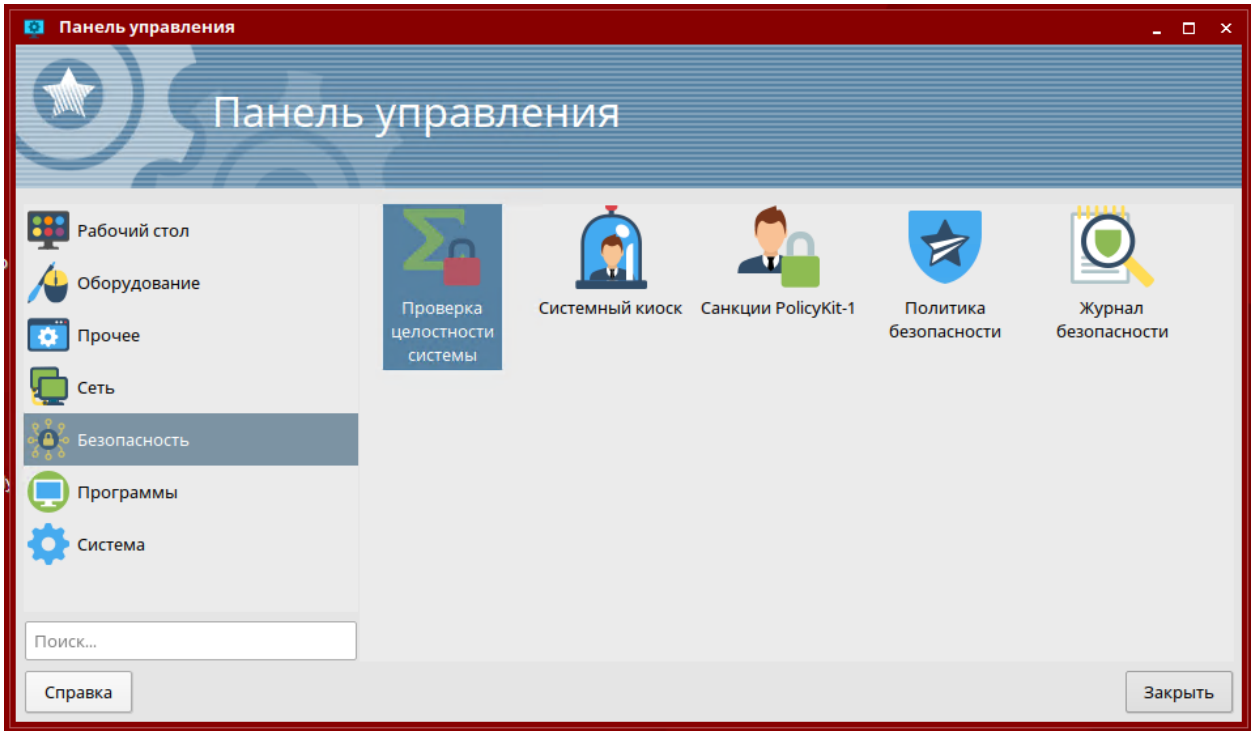


Рисунок 74 – Панель управления

После запуска программы открывается окно на вкладке «Параметры проверки целостности» (см. Рисунок 75). В данной вкладке устанавливаются параметры проверки целостности системы и параметры сохранения отчета в файл.

Во вкладке «Состояние» отображается результат проверки целостности (Рис. 76). Вкладка становится доступной только после начала проверки целостности.

Основное меню программы располагается вверху окна и служит для управления программой, настройки вида отчетов, а также установки фильтров для проверки целостности.

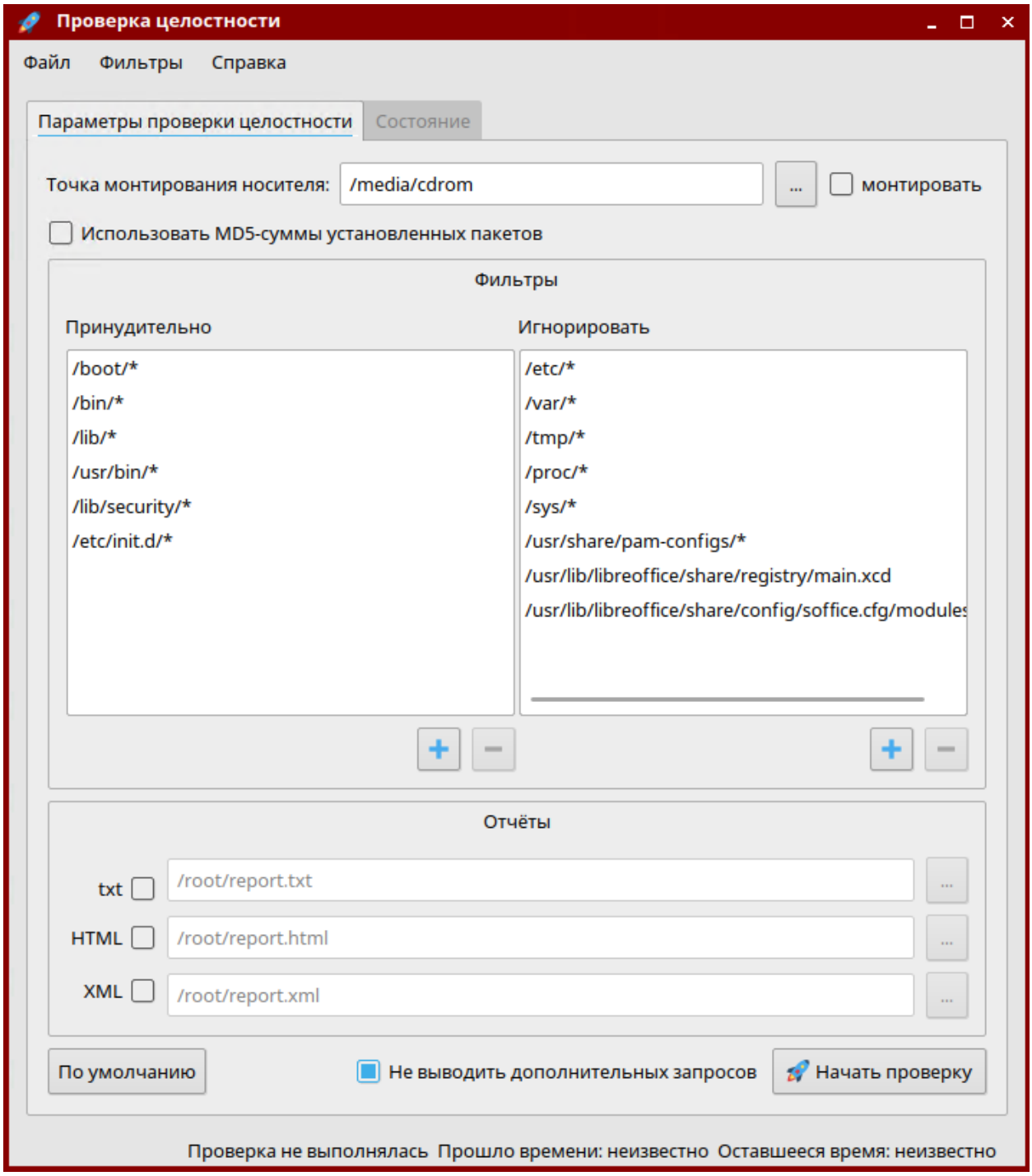


Рисунок 75 – Рабочая панель программы проверки целостности

Меню программы содержит следующие пункты:

– «Файл»:

– «Начать проверку» - выполняется проверка целостности системы;

– «Выход» - работа программы завершается;

– «Фильтры» - добавляется новый элемент в список файлов во вкладке «Параметры проверки целостности» (Вкладка «Параметры проверки целостности») или выделенный в списке элемент удаляется (элемент списка выделяется щелчком

любой кнопки мыши на нем). При установке имени файла разрешается использование групповых операций:

– «Добавить в принудительные...» - открывается окно с строкой ввода для установки имени нового элемента в списке «Принудительно». После подтверждения или отмены окно закрывается и новый элемент, соответственно, отображается или не отображается в списке;

– «Удалить из принудительных...» - из списка «Принудительно» удаляется выделенный элемент;

– «Добавить в игнорируемые...» - открывается окно с строкой ввода для установки имени нового элемента в списке «Игнорировать». После подтверждения или отмены окно закрывается и новый элемент, соответственно, отображается или не отображается в списке;

– «Удалить из игнорируемых...» - из списка «Игнорировать» удаляется выделенный элемент.

– «Справка»:

– «Содержание» - вызов окна справки;

– «О программе...» - вызов окна с краткой информацией о программе.

Вкладка «Параметры проверки целостности» содержит следующие управляющие элементы:

– «Точка монтирования носителя» - задается для проверки целостности путем сравнения контрольных сумму файлов с эталонными значениями контрольных сумм, размещенными в файле gostsums.txt, обычно находящемся в корневом разделе дистрибутива ОС Astra Linux. Для выполнения сравнения контрольных сумм файлов с эталонными значениями должен быть снят флаг «**Использовать MD5-суммы установленных пакетов»**. В строке ввода или из диалогового окна устанавливается точка монтирования носителя с дистрибутивом ОС из /etc/fstab (по умолчанию - /cdrom). При нажатии на кнопку [...] (справа) открывается диалоговое окно для установки точки монтирования (каталога). После подтверждения или отмены окно закрывается и установленный каталог, соответственно, отображается или не отображается в строке ввода;

– флаг «Монтировать» - включает монтирование носителя;

– флаг «Использовать MD5-суммы установленных пакетов» - включает проверку у файлов из установленных пакетов контрольных сумм MD5 согласно списка из соответствующих им файлов для проверки /var/lib/dpkg/info/*.md5sums. Если это флаг установлен, то будет выполняться проверка целостности

установленных пакетов с помощью алгоритма MD5, а поле **«Точка монтирования носителя**» будет неактивно.

– поле «Фильтры» - устанавливаются списки исключаемых из проверки файлов: тех, которые могут изменяться в процессе нормального функционирования ОС (файлы, не заданные явно в фильтрах по умолчанию, включаются в список проверки):

– «Принудительно» - список файлов, обязательно включаемых в список проверки;

– «Игнорировать» - список файлов, исключаемых из списка проверки, если они не указаны в списке «Принудительно»;

– поле «Отчеты» - установка в стоках ввода или из диалоговых окон имен файлов с отчетами, формируемыми в процессе проверки. Кнопка [...] (справа от строки ввода) - открывается диалоговое окно для установки имени файла с отчетом. После подтверждения или отмены окно закрывается и установленное имя, соответственно, отображается или не отображается в строке ввода:

– флаг «txt» - устанавливает текстовый формат для отчета;

– флаг «HTML» - устанавливает формат формате HTML для отчета;

– флаг «XML» - устанавливает формат формате XML для отчета;

– флаг «Не выводить дополнительных запросов» включает полностью неинтерактивный режим работы (отсутствие дополнительных предложений типа: «Вставьте диск», «Укажите отчеты» и прочее);

– Кнопка [Начать проверку] — выполняется проверка целостности системы.

– После запуска проверки активируется вкладка «Состояние» (см. Рисунок 76). После выполнения проверки на рабочей панели в табличном виде отображаются результаты.

– Столбцы: «Файл» - полное имя проверенного файла; «Статус» - статус проверяемого файла: «ОК», «Изменен», «Не найден», «Ошибка», «Проверяется», «Не проверен»;

– индикатор ход выполнения проверки в процентах от объема проверяемых файлов;

– флаг «Прокрутка» - включает прокрутку;

– индикатор ход выполнения проверки в процентах от количества проверяемых файлов;

– [Прервать] - проверки целостности системы прерывается.

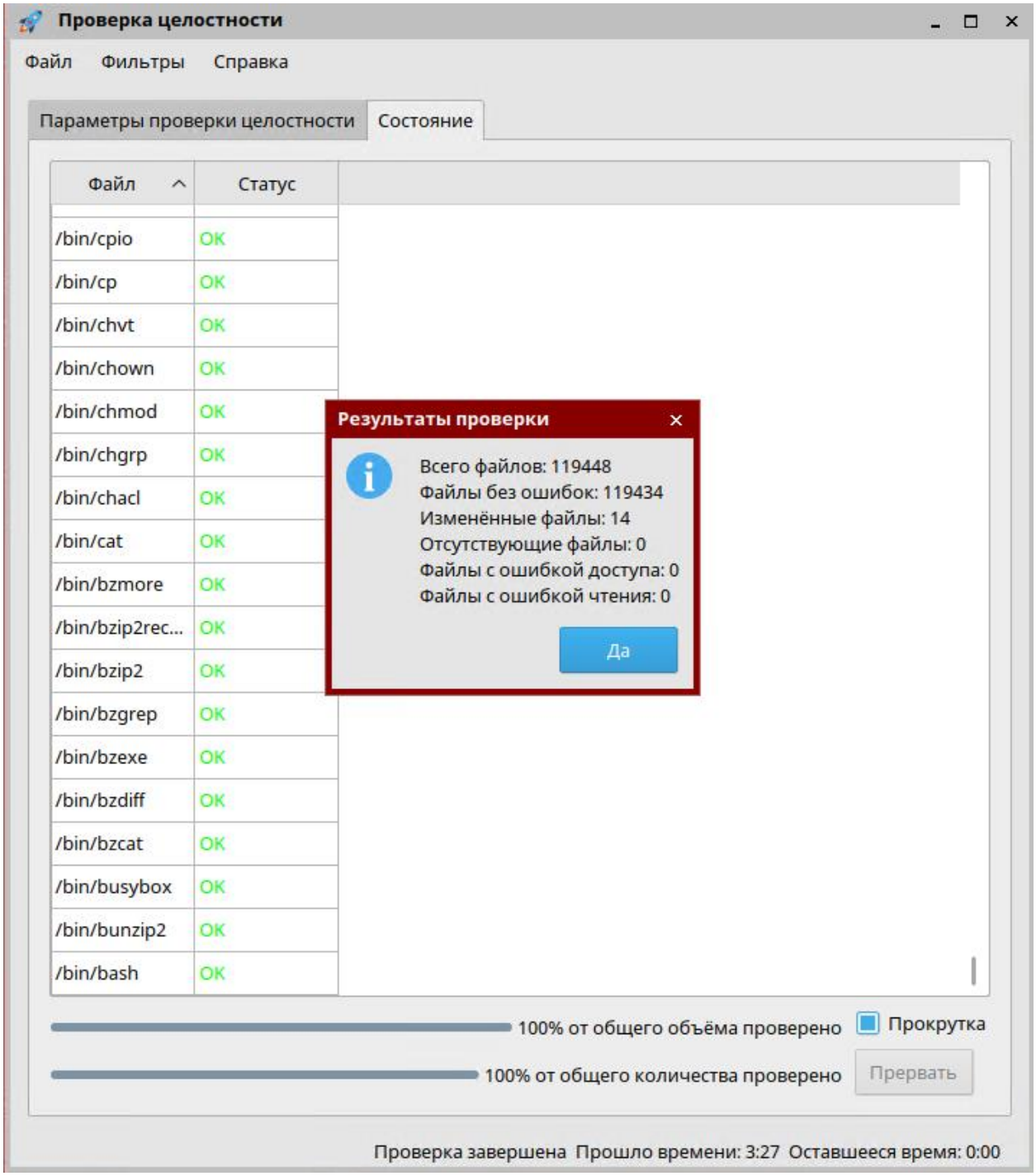


Рисунок 76

7.2 Контроль целостности файловой системы

Для организации регламентного контроля целостности системных файлов ОС Astra Linux и файлов прикладного ПО используется набор программных средств afick (Another File Integrity Checker). В afick реализована возможность проведения периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов

расширенной подсистемы протоколирования) с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотек пакета libgost-astra, обеспечивающей подсчет контрольных сумм по алгоритмам ГОСТ.

Эталонные значения контрольных сумм и атрибутов файлов хранятся в соответствующей БД программы afick, имеющей формат записей dbm (database manager) вида ключ=значение. Если посмотреть ее содержимое, то можно обнаружить набор строк, каждая из которых — имя файла и далее через пробел его атрибуты и сигнатуры. БД защищается системой разграничения доступа ОС Astra Linux.

Для проверки работы механизма, осуществляющего контроль за целостностью объектов файловой системы, необходимо:

1. Войти в систему от имени администратора с высоким уровнем целостности.
2. Запустить программу «Терминал Fly».
3. Выполнить команду

```
sudo afick -i
```

4. Подождать, пока будет сформирована первоначальная БД.

Для настройки параметров работы программы afick используется конфигурационный файл по умолчанию /etc/afick.conf.

Параметр database задает местоположение БД программы (по умолчанию `/var/lib/afick/afick`).

Во время инсталляции программа afick автоматически установит ежедневное задание для системного планировщика заданий cron. Файл с заданием находится в каталоге `/etc/cron.daily/afick_cron`. Результаты работы данного задания вы получите по электронной почте на адрес, указанный в разделе MAILTO файла конфигурации.

Параметр report_url задает местоположение файла-отчета.

В разделе #file section содержатся указания о том, какие файлы/каталоги подвергаются контролю целостности и с какими правилами. Правило означает слежение за правами доступа, количеством ссылок, временем последнего доступа к файлу и другими стандартными атрибутами. Например

```
/boot GOST
/bin GOST
/etc/security PARSEC
```

```
/etc/pam.d PARSEC
/etc/fstab PARSEC
/lib/modules PARSEC
/lib64/security PARSEC
/lib/security PARSEC
/sbin PARSEC
/usr/bin PARSEC
/usr/lib PARSEC
/usr/sbin PARSEC
```

Кроме того, на выбор администратора ИБ представлен ряд дополнительных путей с правилами. Соответствующие строки помечены знаком комментария # и могут быть активированы снятием этого знака.

Правило PARSEC выглядит следующим образом:

PARSEC = p+d+i+n+u+g+s+b+md5+m+e+t где p+d+i+n+u+g+s+b+md5+m означает слежение за всеми стандартными атрибутами файла и использование хэш-функции MD5-Digest для слежения за целостностью содержимого файлов. +e+t означает контроль расширенных атрибутов: мандатной метки и флагов аудита, соответственно. Контроль ACL осуществляется при установке флага +g.

Правило GOST выглядит следующим образом:

GOST = p+d+i+n+u+g+s+b+gost+m+e+t где p+d+i+n+u+g+s+b+gost+m означает слежение за всеми стандартными атрибутами файла и использование хэш-функции ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит для слежения за целостностью содержимого файлов. +e+t означает контроль расширенных атрибутов: мандатной метки и флагов аудита, соответственно. Контроль по спискам управления доступом (Access Control List, ACL) осуществляется при установке флага +g.

Правило для каталогов:

DIR = p+i+n+u+g означает слежение за правами доступа, метаданными, количеством ссылок и другими стандартными атрибутами.

Для вычисления контрольных сумм могут использоваться алгоритмы: MD5-Digest, SHA1 и ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.

Предположим, что нам необходимо, чтобы файлы в домашнем каталоге пользователя administrator проверялись на изменения при монопольном доступе, изменение прав доступа, изменения размера файлов и времени последнего изменения файла. Для начала нужно создать новое правило в файле конфигурации afick.conf, в разделе #alias, как показано ниже:

```
HOME=u+g+p+m+s
```

Затем в разделе #files to scan необходимо добавить следующую строку:

```
/home/administrator HOME
```

При следующем запуске программа afick добавит ваш каталог в свою БД и будет контролировать находящиеся в нем файлы, согласно указанным критериям. Если вы хотите, чтобы ваши изменения были применены немедленно, то можно запустить afick вручную, используя следующую команду:

```
sudo afick -u
```

Результат исполнения команды будет примерно следующим:

```
new directory : /home/administrator
        number of new files             : 29475
changed file : /etc/afick.conf

# detailed changes
new directory : /home/administrator
        inode_date              : Tue Nov  9 15:15:28 2021
        number of new files             : 29475
changed file : /etc/afick.conf
        md5                     : ba+CfW1wyOK+CLgTOLhYaw
W8QlPjRXsyTlUKBMpY5WHg
        filesize                : 5172 5213

# Hash database updated successfully : 43501 files scanned, 29477 changed (new :
29476; delete : 0; changed : 1; dangling : 0; exclude_suffix : 560;
exclude_prefix : 0; exclude_re : 0; degraded : 0)
# ################################################################
# MD5 hash of /var/lib/afick/afick => 6RXrT5qMtQ95vRk7OxCIuw
# user time : 23.34; system time : 4.56; real time : 32
```

В рассматриваемом примере был изменен конфигурационный файл утилиты afick.conf (это можно считать допустимым изменением), а также появился новый каталог /home/administrator.

Изменим с помощью текстового редактора файл php.ini, имеющийся в каталоге /home/administrator, и запустить программу контроля целостности в режиме сравнения с БД:

```
sudo afick -k
```

Результат исполнения команды будет примерно следующим (приведен частично):

```
changed directory : /home/administrator
.
.
.
changed file : /home/administrator/php.ini

# detailed changes
changed directory : /home/administrator
```

```
        mtime                    : Tue Nov  9 15:15:28 2021     Tue Nov  9
15:43:30 2021
.
.
.
changed file : /home/administrator/php.ini
        filesize                 : 73333        73341
        mtime                    : Mon Oct 25 11:51:35 2021     Tue Nov  9
15:43:30 2021

# Hash database : 43501 files scanned, 8 changed (new : 0; delete : 0; changed :
8; dangling : 0; exclude_suffix : 560; exclude_prefix : 0; exclude_re : 0;
degraded : 0)
# ################################################################
# MD5 hash of /var/lib/afick/afick => 6RXrT5qMtQ95vRk7OxCIuw
# user time : 23.01; system time : 3.89; real time : 27
```

Таким образом, получена информация о времени последней модификации и об изменении размера файла php.ini.

Более подробную информацию о средствах регламентного контроля целостности файлов можно получить из справочной системы ОС Astra Linux (с помощью команд man afick и man afick.conf), а также документа РУСБ.10015-01 97 01-1 «Руководство по комплексу средств защиты информации, часть 1», разд. 9.4.

7.3 Контроль целостности компонентов программы Kaspersky Endpoint Security

Программа Kaspersky Endpoint Security содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Один или несколько исполняемых модулей или файлов программы могут быть заменены другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в программе Kaspersky Endpoint Security предусмотрена проверка целостности компонентов программы. Программа проверяет модули и файлы на наличие неавторизованных изменений и повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Программа проверяет целостность файлов, целостность которых важна для корректной работы программы. Список этих файлов программы содержится в файле манифеста integrity_check.xml. Файлы манифеста подписаны цифровой подписью, их целостность также проверяется.

Проверка целостности компонентов программы выполняется с помощью утилиты проверки целостности integrity_check_tool. Эту утилиту требуется запускать под учетной записью суперпользователя (root).

Утилита проверки целостности, устанавливаемая вместе с программой, расположена в каталоге /opt/kaspersky/kesl/bin. Файл манифеста обычно расположен там же.

Чтобы проверить целостность компонентов программы, последовательность действий следующая:

1. Зарегистрируйтесь в системе как суперпользователь (root).
2. Перейдите в нужный каталог командой cd /opt/kaspersky/kesl/bin
3. Выполнить команду

```
./integrity_check_tool -v -m integrity_check.xml
```

4. Результат проверки выглядит следующим образом:

```
=============================================>
Summary( failed / skipped / succeeded ):
        Manifests: 0 / 0 / 1
        Environment: 0 / 0 / 1
        Command: 0 / 0 / 0
        Files: 0 / 0 / 334
        File dirs: 0 / 0 / 1
        Registries: 0 / 0 / 0
        Registry values: 0 / 0 / 0
=============================================>
SUCCEEDED
```

7.4 Передача копии сетевого трафика

Передача копии сетевого трафика, передаваемого в СЛТМ в коммутируемой сети Ethernet, на сервер оперативного мониторинга состояния информационной безопасности осуществляется с помощью порта №22 Ethernet-коммутатора MES2324.

8 Просмотр журналов ОС Astra Linux

Журналирование является основным источником информации о работе системы и ее ошибках. Большинство файлов журналов содержится в разделе /var/log:

- **/var/log/syslog** или **/var/log/messages** содержит глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройствах, сетевых интерфейсов и много другого;
- **/var/log/auth.log** — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации;
- **/var/log/audit/audit.log** — Записи, созданные службой аудита auditd;
- **/var/log/boot.log** — информация, которая пишется при загрузке операционной системы;
- **/var/log/btmp** —журнал записи неудачных попыток входа в систему.
- **/var/log/dpkg.log** — Для программ, установленных с помощью менеджера пакетов dpkg в Debian Linux и всем семействе родственных дистрибутивов.
- **/var/log/faillog** — Неудачные попытки входа в систему. Очень полезно при проверке угроз в системе безопасности, хакерских атаках, попыток взлома методом перебора. Прочитать содержимое можно с помощью команды faillog.
- **var/log/kern.log** — журнал содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок пользовательских модулей, встроенных в ядро.
- **/var/log/lastlog** — Последняя сессия пользователей. Прочитать можно командой last.
- **/var/log/samba/** — журналы файлового сервера Samba, который используется для доступа к общим папкам ОС Windows и предоставления доступа пользователям Windows к общим папкам Linux.
- **/var/log/wtmp** —журнал записи входа пользователей в систему на данный момент. Вывод на экран командой utmpdump. (см. Рисунок)

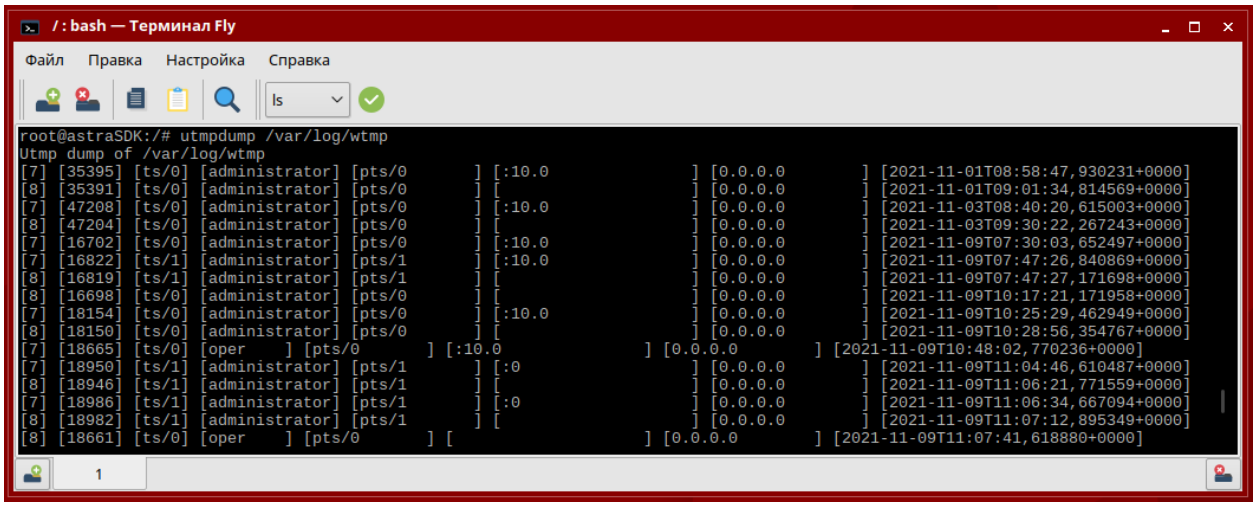


Рисунок 77

Журналы можно открыть любой утилитой для просмотра текста, например, less, cat, tail. Откроем файл журнала /var/log/auth.log (см. Рисунок 78)

```
less /var/log/auth.log
```

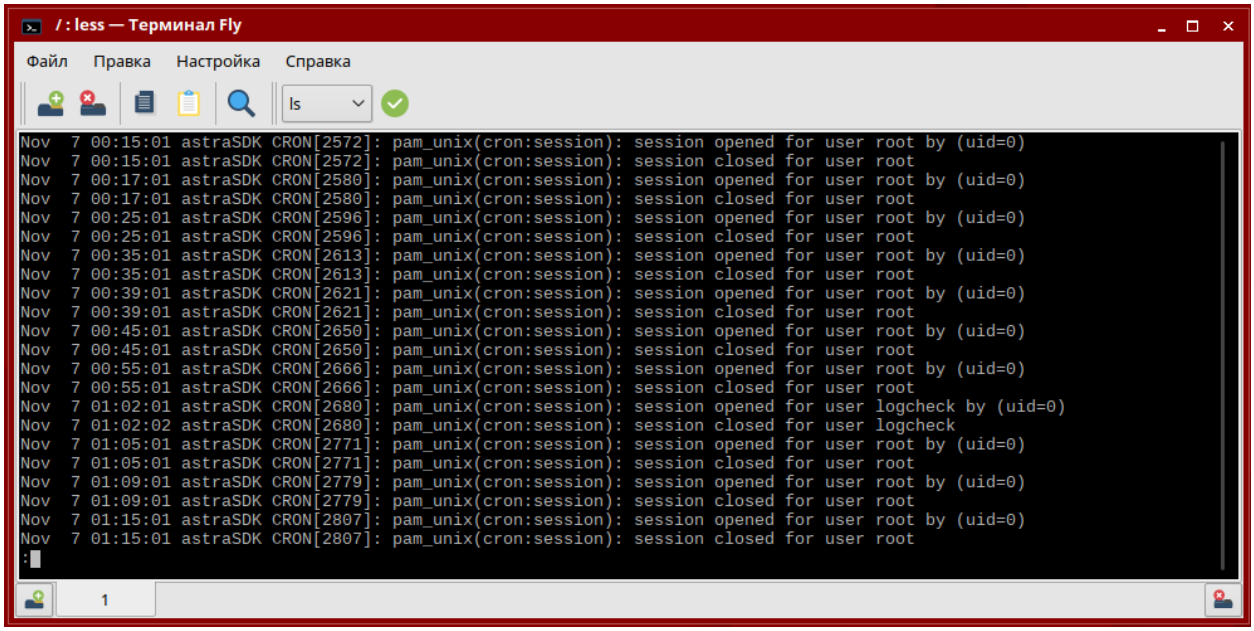


Рисунок 78

9 Руководство по резервному копированию

В СЛТМ «Магистраль-ДУ» (SCADA «Поток-ДУ») обеспечивается возможность взаимодействия со средствами резервного копирования и восстановления данных, конфигурационной информации, а также при необходимости, программного обеспечения.

В качестве средств резервного копирования возможно применение программного обеспечения, входящего в состав ОС Astra Linux, либо стороннего ПО резервного копирования КиберБэкап.

9.1 Создание регулярного сохранения информации

Для резервного копирования конфигурации программного обеспечения и архивных данных (протокол событий, историческая база данных) используется встроенный в ASTRA Linux инструмент Lucky backup.

Программа позволяет создать "копию" данных в другом месте, и безопасно. Резервное копирование любого каталога (исходного) на другой (назначения). Lucky Backup копирует только измененные файлы и папки, то есть те, в которые были внесены изменения.

luckyBackup обеспечивает синхронизацию каталогов, архивацию данных и представляет собой GUI к консольной утилите rsync, имеет возможность удалять архивные файлы, имеется возможность сделать тестовый прогон и просмотреть какие файлы будут архивироваться.

Для создания резервной копии или восстановления необходимой директории (или папок), то запустить luckyBackup.

9.1.1 Создание задания с помощью LuckyBackup

Чтобы запустить LuckyBackup для настройки резервного копирования, выполнить следующие действия:

1. Запустить LuckyBackup Пуск-Системные-LuckyBackup (суперпользователь).

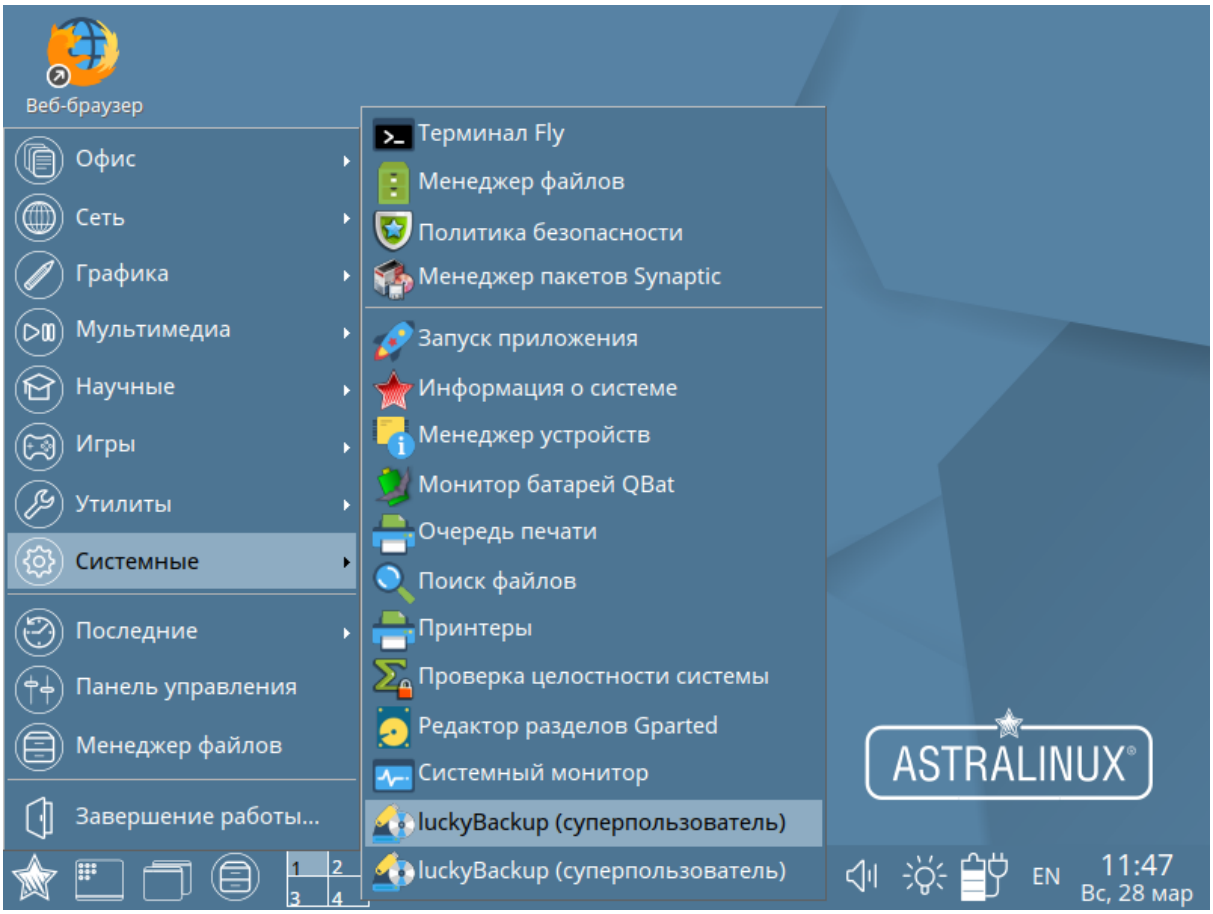


Рисунок 79 – Запуск суперпользователя

2. Создать новый профиль.

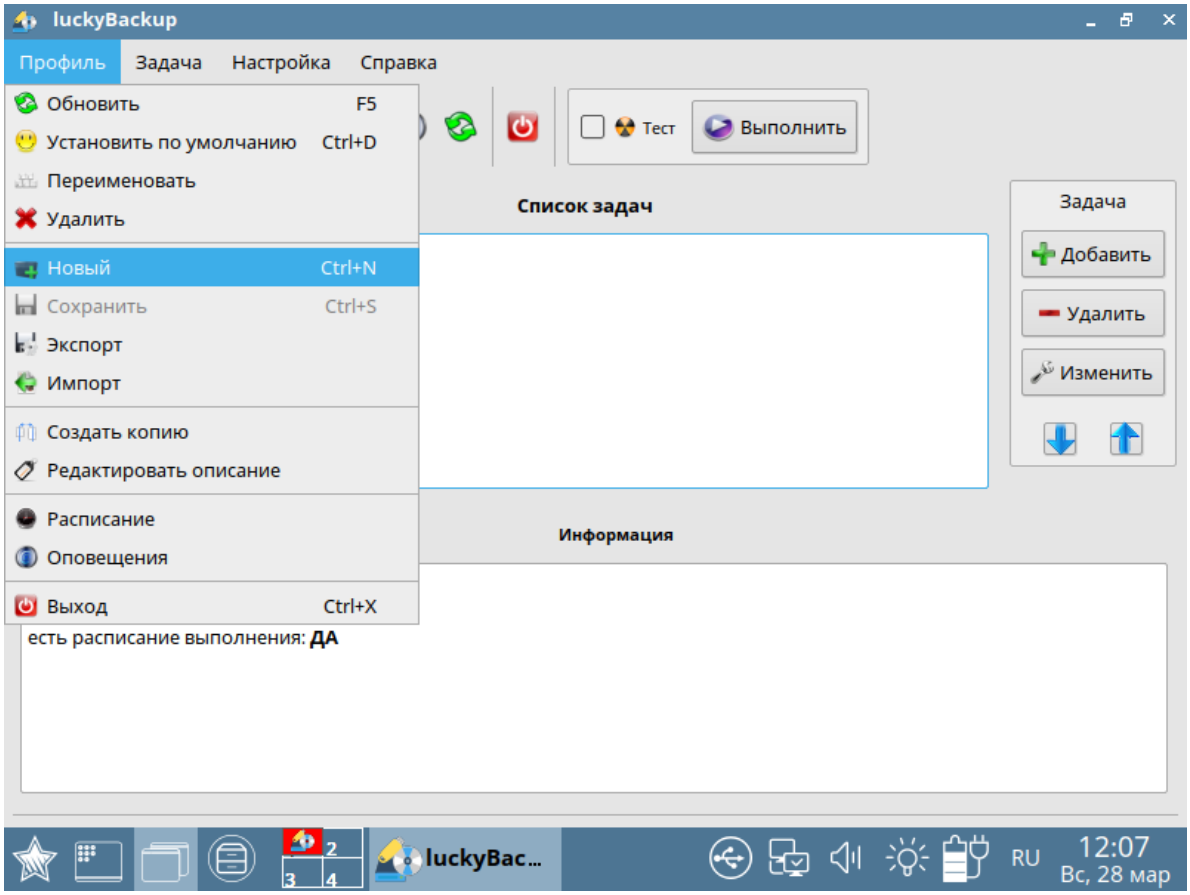


Рисунок 80 – Создание нового профиля

3. Добавить новую задачу для резервного копирования, нажав "Добавить".

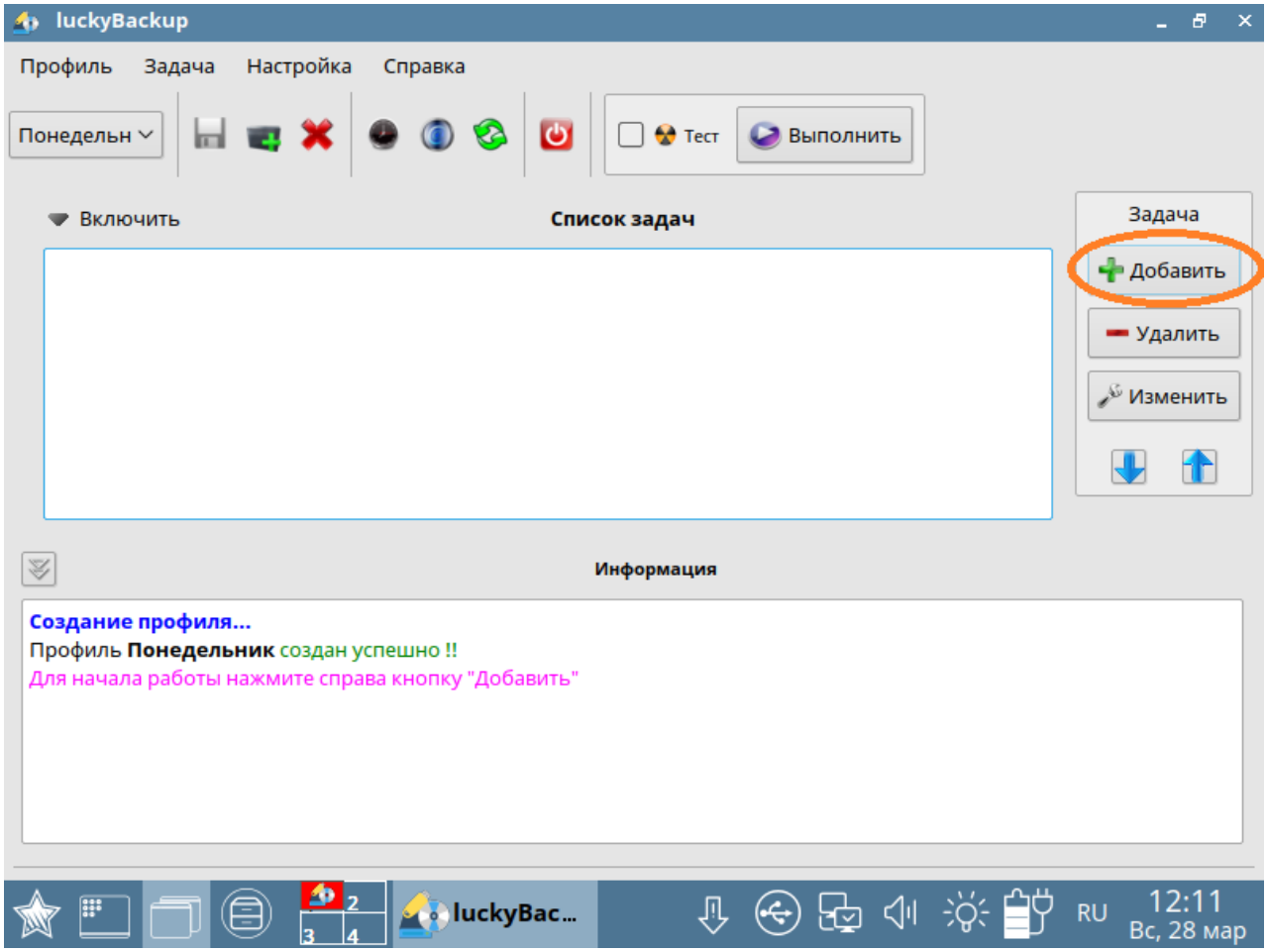


Рисунок 81 – Добавление новой задачи

4. Ввести новое название задачи, например, "Копия1", источник файлов для резервирования, "/opt", и место для резервирования файлов, выбирается место хранения резервной копии. Количество резервных копий вводится в зависимости сколько необходимо резервных копий. Нажимаем «ОК» (также существует опция выбора сетевой папки, обеспечивающая отправку копий на другое сетевое хранилище).

5. (Также можно выбрать папку, находящуюся в сети, тем самым отправлять копии на другое сетевое хранилище!)

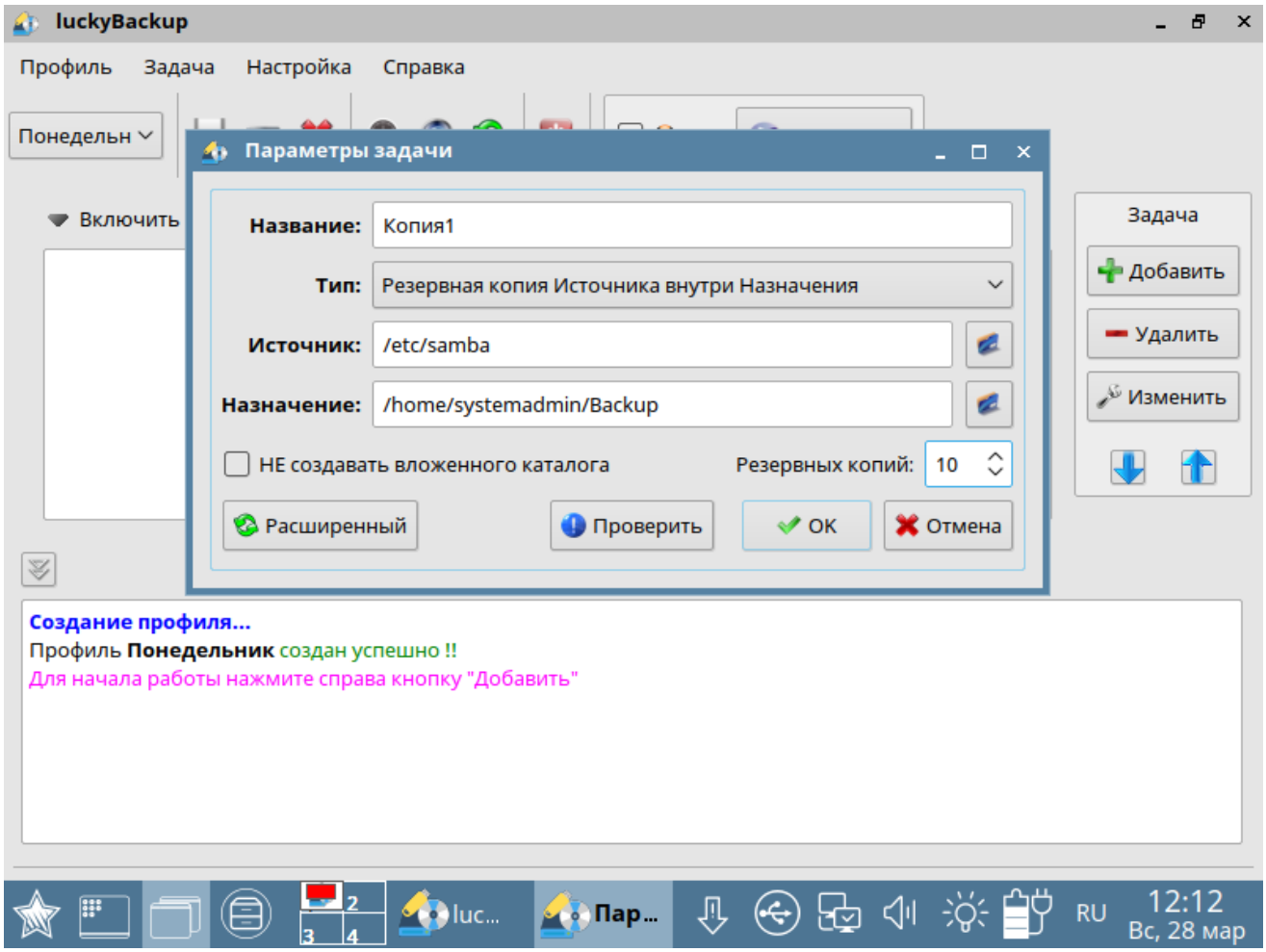


Рисунок 82

6. Проводим проверку резервного копирования, для этого отмечаем созданную задачу и «Тест», а затем нажимаем «Выполнить».

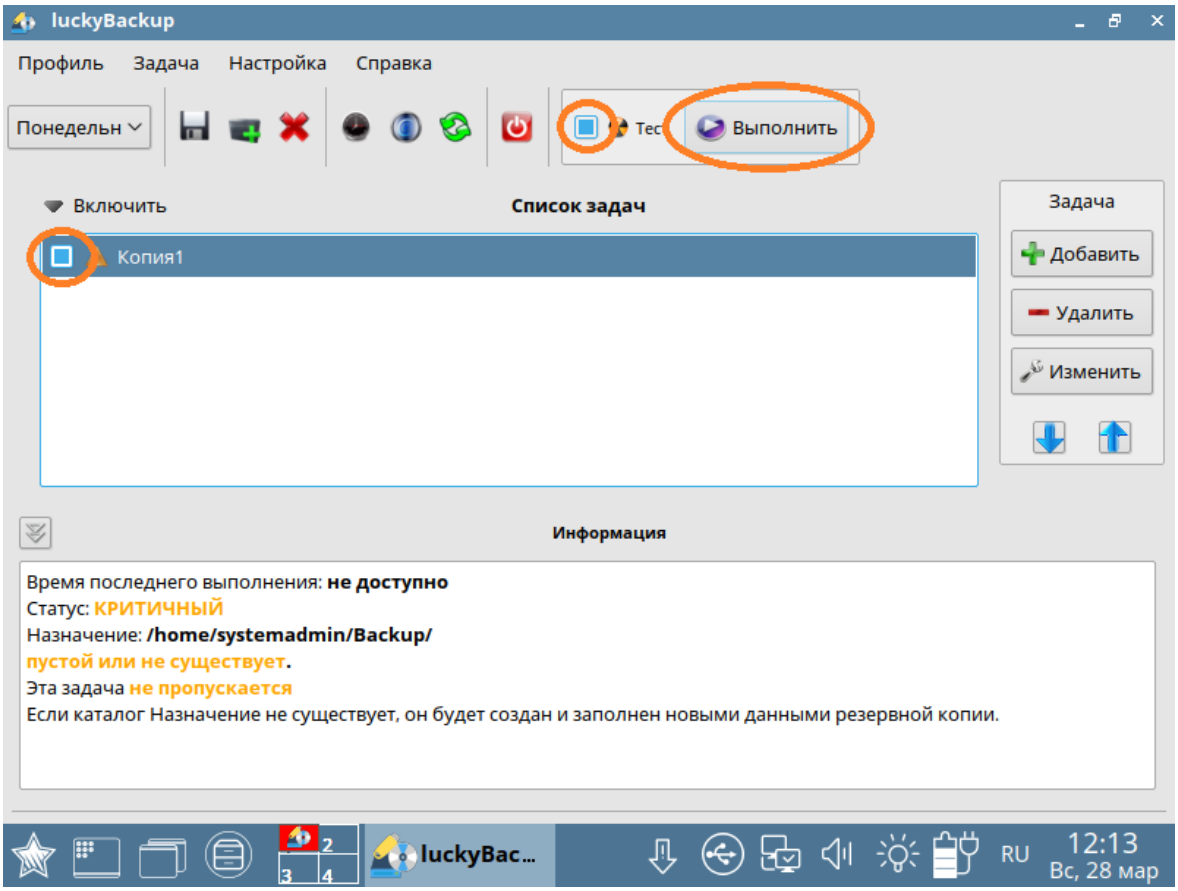


Рисунок 83 – Проверка резервного копирования

7. Если всё правильно сделано, то ошибки будут отсутствовать. Нажимаем «Готово».

8. Далее устанавливаем расписание выполнение задачи: «Профиль» → «Расписание».

9. Нажимаем «Добавить».

10. Выбираем профиль, в нашем случае "Понедельник", время для резервного копирование. Если необходимо делать раз неделю, то выбираем день недели, раз в месяц - день месяца, раз в год — день месяца и месяц. Также выбираем консольный режим, чтобы резервное копирование выполнялось в фоновом режиме. Нажимаем «ОК». (Для резервного копирования несколько раз в сутки или дополнительные дни повторите предыдущий шаг!).

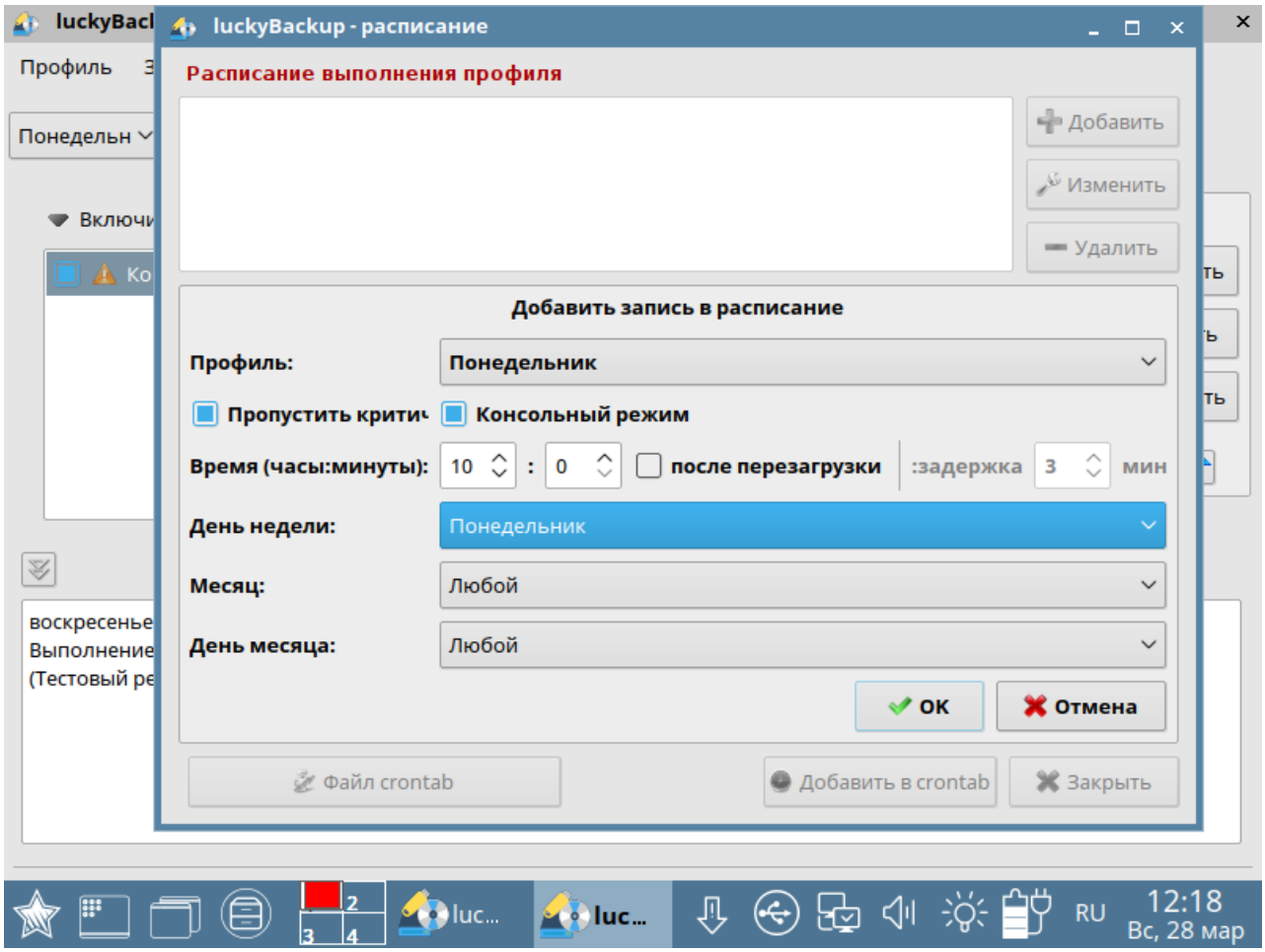


Рисунок 84 – Выбор времени резервного копирования

11. Сохраняем расписание нажав «Добавить в crontab».

12. При сохранении выйдет окно об успешном обновлении файла, нажимаем «ОК».

13. Резервное копирование по расписанию готово, закрываем окно и программу.

9.2 Восстановление данных из резервной копии

9.2.1 Восстановление данных при потере данных

Чтобы выполнить восстановление данных, необходимо выполнить следующие действия:

1. Для восстановления можно просмотреть какие файлы имеются через менеджер файлов, для этого необходимо в менеджере файлов включить отображение скрытых файлов и пройти в каталог, где находится резервная копия. В нашем примере это папка /opt. В данной папке содержится последняя копия.

2. Измененные ранее файлы находятся в папке .luckybackup-snaphost. В скрытой папке находятся папки с названием даты, в которых находятся измененные файлы, в зависимости от даты.

3. Запускаем LuckyBackup (суперпользователь) и выбираем «Задача» → «Список резервных копий»

4. Откроется окно со всеми резервными копиями. При нажатии на «Показать различия» можно просмотреть, когда и какие файлы различались между резервной копией и каталогом источника.

5. Можно посмотреть какие файлы были изменены и когда, нажав "Показать различия".

6. Выбираем дату и нажимаем «Восстановить». В открывшемся окне выбираем куда восстановить файлы (будет выполнено копирование в другое место) или оставить без изменения (будет проведено восстановление) и нажать «Начать».

7. Начнётся восстановление (копирование). По завершению выйдет информация о завершении и ошибках.

8. Восстановление (копирование) выполнено, закрывает окно и программу.

Список используемых сокращений

АРМ	– автоматизированное рабочее место
БД	– база данных
ИБ	– информационная безопасность
МРД	– мандатное разграничение доступа
ОС	– операционная система
ПБ	– политика безопасности
ПО	– программное обеспечение
ПТК	– программно-технический комплекс
ALD	– Astra Linux Directory — система управления доменной сетевой инфраструктурой
FTP	– File Transmission Protocol — протокол передачи файлов по сети
NFS	– Network File System — протокол сетевого доступа, позволяет подключать (монтировать) удалённые файловые системы через сеть
SCADA	– Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных
SMB	– Server Message Block — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам

Лист регистрации изменений

Таблица регистрации изменений								
Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер док.	Подп.	Дата
	измененных	замененных	новых	аннулированных				