ООО «ГА ДИСПЕТЧЕРСКИЕ СИСТЕМЫ»

ПРОГРАМНЫЙ КОМПЛЕКС «ГОРИЗОНТ»

Эксплуатационная документация

Руководство администратора информационной безопасности

___.И13

2022

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
13013				

Содержание

Перв. примен.

Справ. №

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл. 13013

Изм	Лист	№ докум.	Подпись	Дата	Описание алгоритма. Ограничение давления в
Разраб.		Рыбин		12.22	ГАЗОВЫЙ ПРОМЫСЕЛ ГП-2
Пров.		Панкова		12.22	Руководство администратора ИБ
Н.контр.		Колесникова		12.22	
Утв.		Мирошников		12.22	

Лит.	Лист	Листов
	2	93

1 Введение

1.1 Область применения

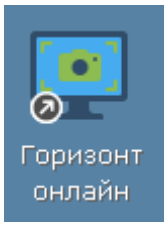
Настоящее руководство администратора по информационной безопасности предназначено для описания обеспечения информационной безопасности системы диспетчерского контроля и управления на базе программного комплекса «Горизонт».

2 Администрирование Системы

Организация работ в системе на основе ПО «Горизонт» с основным меню, панелью инструментов, журналами регистрации оперативной информации, с мнемосхемами и параметрами объектной модели описана в Руководстве диспетчера.

2.1 Запуск системы на базе «Горизонт»

Для запуска «Горизонт» под управление Linux достаточно в терминальном окне (либо putty либо с локальной консоли) набрать команду «ems start», дождаться ее завершения и убедиться что все службы запустились успешно.

Программа интерфейса «Горизонт» запускается двойным нажатием по иконке 

на рабочем столе компьютера.

Далее администратор автоматически окажется в своем личном профиле системы «Горизонт», где будет открыто предварительно сконфигурированное начальное изображение. Пример экрана с активированными пунктами меню показан на рисунке Рисунок 2.**1**.

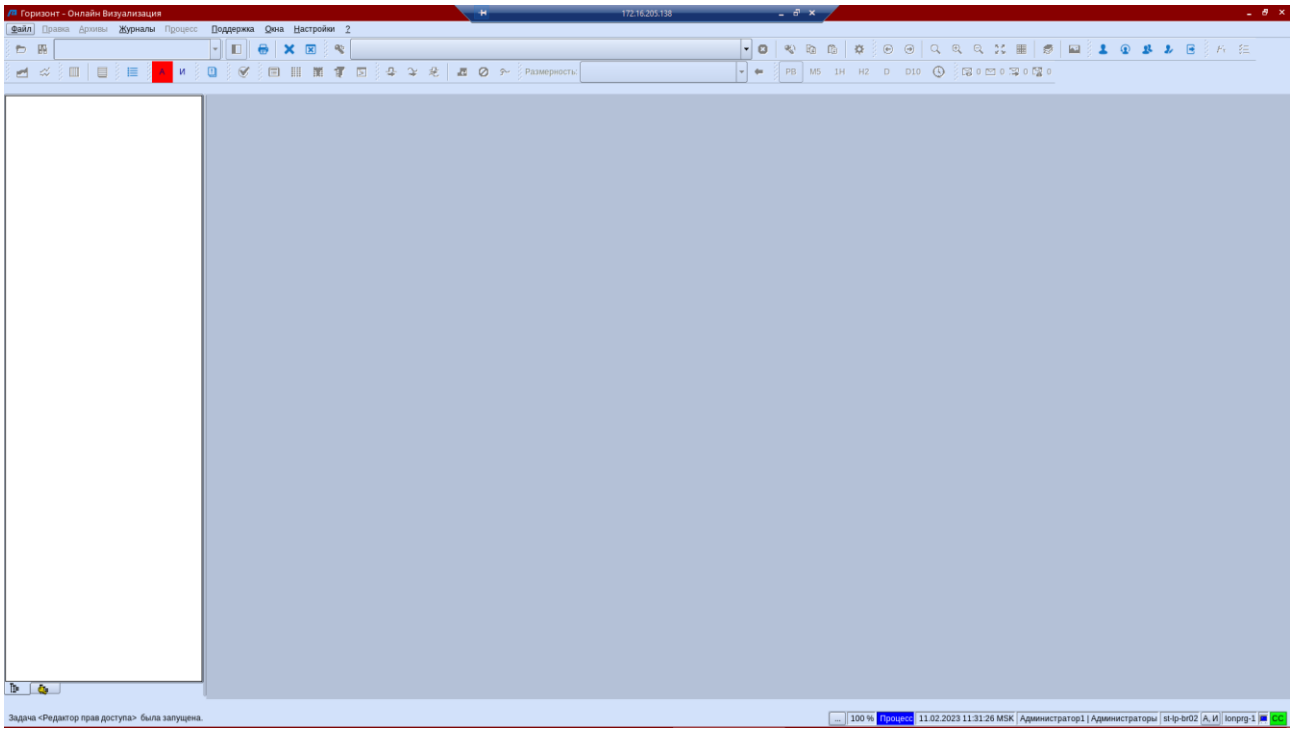


Рисунок 2.1 – Вид стартового окна системы

Структура экрана и его составляющих рассмотрена в руководстве Диспетчера.

С именем администратора и рабочим местом, с которого осуществлен вход в систему, связаны определенные роли и полномочия, которые определяют т.н. «класс доступа». Класс доступа конфигурируется в редакторе прав доступа (см. далее). Для изменения класса доступа необходимо нажать кнопку  на панели инструментов и выбрать из выпадающего меню класс.

2.2 Действия в случае системных ошибок

В случае наличия системной ошибки при запуске системы появится окно с сообщением (рисунке Рисунок 2.**2**).

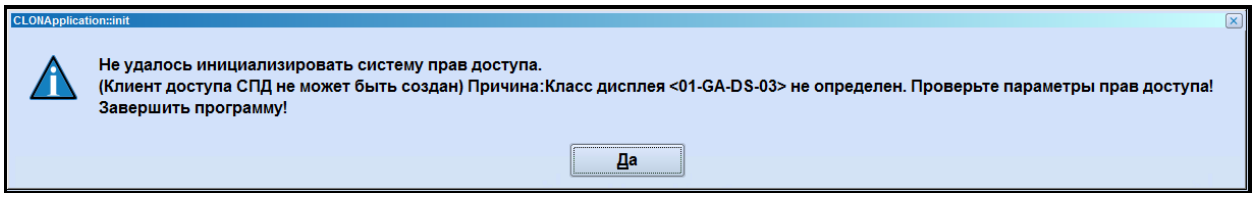


Рисунок 2.2 – Системное сообщение

Это говорит о том, что нет связи с некоторыми (или всеми) службами серверов BR или они остановлены. Необходимо проверить недоступность служб и серверов через PSI Monitor или вызвав команду «ems hosts» (см. далее) и запустить их.

2.3 Проверка состояния служб «Горизонт»

Проверка состояния службы «Горизонт» может выполняться двумя способами:

Запуск утилиты Горизонт-Монитор (команда «ems moni» в командной строке ОС либо ярлык «Монитор» на рабочем столе), при помощи данной утилиты осуществляется визуальный контроль состояния сервисов «Горизонт» в общем случае распределенных по нескольким машинам в локальной сети. Окно монитора является средством быстрой первичной диагностики. На экране утилиты (рисунок**Рисунок** 2.**3**) приведен полный перечень служб «Горизонт», во втором столбце указано имя машины, на которой данный сервис запущен.

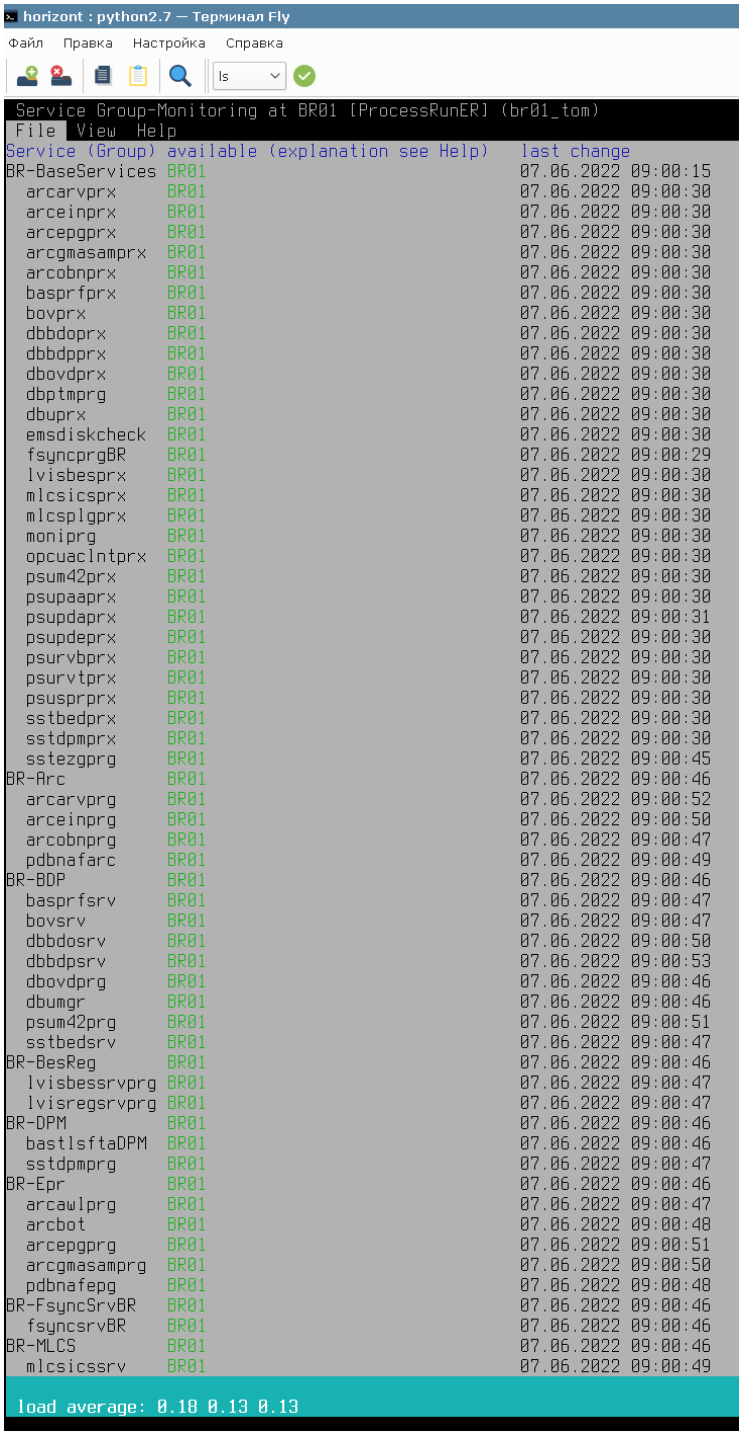


Рисунок 2.3 – Системные службы не доступны

Имя машины может быть указано двумя цветами желтым и зеленым. Желтый цвет говорит о том, что сервис находиться в промежуточном состоянии (останавливается или запускается), зеленый – сервис запущен. Если вместо имени машины указаны символы «-----» это означает, что данный сервис не запущен.

Красные имена машин – это имена резервных машин.

Перемещение по списку осуществляется клавишами Page Up и Page Down.

Команда «ems list» набранная в командной строке. Данная команда показывает состояния служб только на локальной машине. Пример вывода команды «ems list» приведен на рисунке Рисунок 2.**4**:

```
horizont@br01_tom:/usr/PROZESS/horizont$ ems list
Registered PSIControl services
arcarvprg       18389 2022-06-07 09:00:49 AppActive
arcarvprx       16216 2022-06-07 09:00:29 AppActive
arcawlprg       17114 2022-06-07 09:00:46 AppActive
arcbot          18123 2022-06-07 09:00:48 AppActive
arceinprg       18388 2022-06-07 09:00:49 AppActive
arceinprx       16229 2022-06-07 09:00:29 AppActive
arcepgprg       18122 2022-06-07 09:00:48 AppActive
arcepgprx       16214 2022-06-07 09:00:29 AppActive
arcgmasamprg    17113 2022-06-07 09:00:46 AppActive
arcgmasamprx    16228 2022-06-07 09:00:29 AppActive
arcobnprg       17116 2022-06-07 09:00:46 AppActive
arcobnprx       16215 2022-06-07 09:00:29 AppActive
basprfprx       16254 2022-06-07 09:00:29 AppActive
basprfsrv       17105 2022-06-07 09:00:46 AppActive
bastlsftaDPM    17109 2022-06-07 09:00:46 AppActive
bovprx          16232 2022-06-07 09:00:29 AppActive
bovsrv          17104 2022-06-07 09:00:46 AppActive
dbbdoprx        16221 2022-06-07 09:00:29 AppActive
dbbdosrv        17772 2022-06-07 09:00:47 AppActive
dbbdpprx        16220 2022-06-07 09:00:29 AppActive
dbbdpsrv        18868 2022-06-07 09:00:50 AppActive
dbovdprg        17101 2022-06-07 09:00:46 AppActive
dbovdprx        16225 2022-06-07 09:00:29 AppActive
dbptmprg        16222 2022-06-07 09:00:29 AppActive
dbumgr          17102 2022-06-07 09:00:46 AppActive
dbuprx          16233 2022-06-07 09:00:29 AppActive
emsdiskcheck    16226 2022-06-07 09:00:29 AppActive
fsyncprgBR      16213 2022-06-07 09:00:29 AppActive
fsyncsrvBR      17100 2022-06-07 09:00:46 AppActive
lonprg-1        26586 2022-06-07 11:33:02 AppStarted br01_tom
lvisbesprx      16223 2022-06-07 09:00:29 AppActive
lvisbessrvprg   17111 2022-06-07 09:00:46 AppActive
lvisregsrvprg   17110 2022-06-07 09:00:46 AppActive
mlcsicsprx      16255 2022-06-07 09:00:29 AppActive
mlcsicssrv      17117 2022-06-07 09:00:46 AppActive
mlcsplgarc      18407 2022-06-07 09:00:49 AppActive
mlcsplgprx      16256 2022-06-07 09:00:29 AppActive
moniprg         16212 2022-06-07 09:00:29 AppActive
opcuaclntprg    17136 2022-06-07 09:00:46 AppActive
opcuaclntprx    16235 2022-06-07 09:00:29 AppActive
opcuakopprg     18399 2022-06-07 09:00:49 AppActive
pdbnaf          17106 2022-06-07 09:00:46 AppActive
pdbnafarc       17115 2022-06-07 09:00:46 AppActive
pdbnafepg       17112 2022-06-07 09:00:46 AppActive
psuarv          18392 2022-06-07 09:00:49 AppActive
psuevn          18391 2022-06-07 09:00:49 AppActive
psufwaprg       19453 2022-06-07 09:00:52 AppActive
psugrv          18393 2022-06-07 09:00:49 AppActive
psum42prg       18869 2022-06-07 09:00:50 AppActive
psum42prx       16230 2022-06-07 09:00:29 AppActive
psupaaers       18396 2022-06-07 09:00:49 AppActive
psupaaprg       18397 2022-06-07 09:00:49 AppActive
psupaaprx       16219 2022-06-07 09:00:29 AppActive
psupdaprg       18390 2022-06-07 09:00:49 AppActive
psupdaprx       16994 2022-06-07 09:00:30 AppActive
psupdeprg       19264 2022-06-07 09:00:51 AppActive
psupdeprx       16217 2022-06-07 09:00:29 AppActive
psurvbprg       17107 2022-06-07 09:00:46 AppActive
psurvbprx       16231 2022-06-07 09:00:29 AppActive
psurvo          18394 2022-06-07 09:00:49 AppActive
psurvtprg       18395 2022-06-07 09:00:49 AppActive
```

Рисунок 2.4 – Пример ввода команды «es list»

В результате команды «ems list» для анализа доступна информация о том какие сервисы «Горизонт» запущены на локальной машине (статус AppAktiv). Статус AppGestartet говорит о том что запущено какое-то приложение «Горизонт» (например: lonprg-1, lonprg-2, lonprg-3 – три запущенные копии визуализации (LVis)).

2.4 Останов службы «Горизонт»

Останов службы «Горизонт» под управлением операционной системы Linux осуществляется командой «ems stop» с терминального соединения (putty) либо с терминала Linux через консоль (VNC либо локальная консоль).

2.5 Ошибка прав доступа

При запуске может возникнуть следующая ошибка, см. рисунок Рисунок 2**.5**.

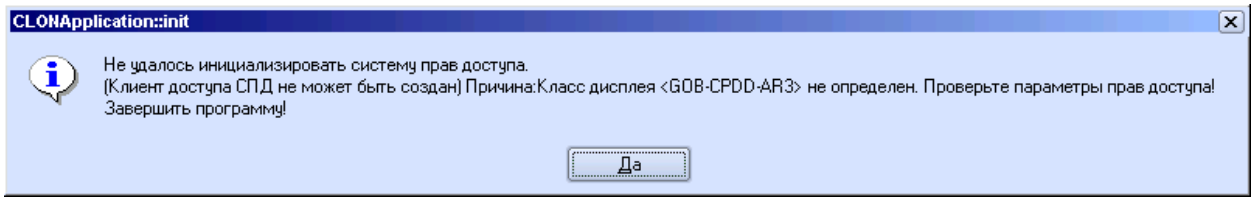


Рисунок 2.5 – Ошибка прав доступа

Чтобы устранить ошибку, необходимо:

– запустить редактор прав доступа из командной строки при помощи команды emsrun sstbedcln.exe

– создать новый дисплей для данного АРМ-а, см. Редактор прав доступа . Определение и конфигурация дисплеев.

– обновить права доступа командой «emsrun sstbedgen».

– редактор прав доступа может быть запущен из командной строки при помощи команды «emsrun sstbedcln.exe».

Для работы с редактором прав доступа необходимо знать пару имя пользователя/ пароль для работы с редактором прав доступа. При внесении изменений в права доступа для их актуализации необходимо выполнить обновление прав доступа.

Работа с редактором прав доступа описаны далее в настоящем документе.

2.6 Каталоги Системы

Для описания путей к директориям будем использовать переменную окружения {PROZ_DIR}. В случае ОС Linux {PROZ_DIR} = /usr/PROZESS.

3 Элементы интерфейса

В данном разделе описаны элементы функционального меню и панели инструментов, которые используются при работе с учетными записями и правами доступа пользователей.

3.1 Элементы функционального меню

Пункт меню «Файл» (рисунок Рисунок 3.**1**) используется при работе с учетными записями и правами доступа пользователей.

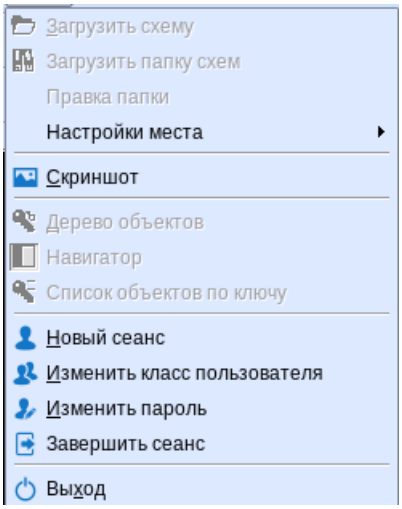


Рисунок 3.1 – Меню «Файл»

Рассмотрим пункты данного меню, которые позволяют работать с учетными записями и правами доступа.

Новый сеанс. При выборе данного пункта в меню «Файл» открывается диалог регистрации пользователя (рисунок Рисунок 3.**2**).

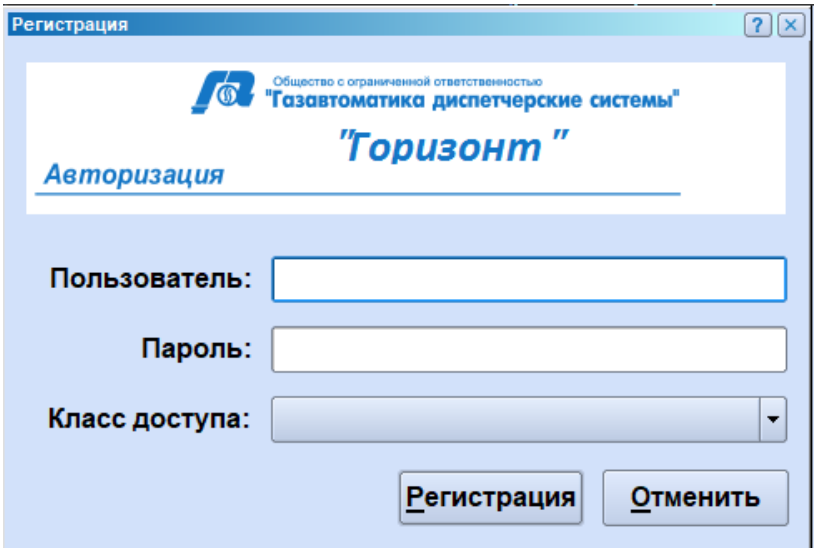


Рисунок 3.2 – Диалог регистрации

При необходимости сменить пользователя и класс доступа в данном диалоге вводится имя пользователя и пароль. Из выпадающего списка выбирается класс доступа. По нажатию кнопки «Регистрация» осуществляется вход в систему под другим пользователем и другим классом доступа, если он выбран.

Изменить класс пользователя. При выборе данного пункта в меню «Файл» открывается диалог изменения класс пользователя (рисунок Рисунок 3**.3**).

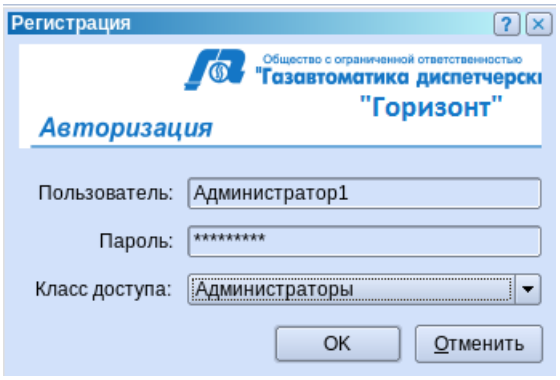


Рисунок 3.3 – Диалог изменения класса пользователя

Данный функционал используется при необходимости изменить класс доступа для данного пользователя. В открывшемся окне в выпадающем списке выбирается класс доступа. По нажатию кнопки «Регистрация» осуществляется вход с систему с другим классом доступа – другими правами.

Изменить пароль. При выборе данного пункта в меню «Файл» открывается диалог изменения пароля пользователя (рисунок**Рисунок** 3.**4**).

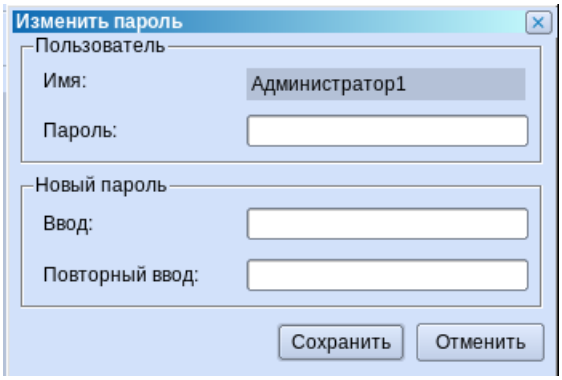


Рисунок 3.4 – Диалог изменения пароля

Завершить сеанс. Выбор данного пункта меню «Файл» завершает сеанс работы пользователя, приложение «Горизонт» остается открытым и можно зарегистрироваться снова, выбрав пункт меню «Файл\Новый сеанс».

Завершить. По данному пункту меню «Файл» завершается работа приложения «Горизонт», оно закрывается.

3.2 Элементы панели инструментов

Элементы панели инструментов (рисунокРисунок 3.**5**) дублирующие функционал пунктов меню «Файл» представлены в таблице 1.

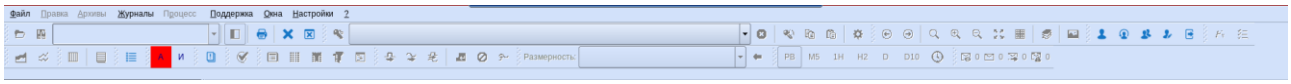


Рисунок 3.5 – Панель инструментов

Все элементы панели инструментов активируются «выбором» с помощью манипулятора «мышь» - наведение курсора «мыши» и однократное нажатие на левую клавишу.

Подведение курсора «мыши» без нажатия на клавишу приводит к появлению всплывающей подсказки с пояснениями к функционалу данного инструмента.

Таблица 1 – Элементы панели инструментов

Иконка	Название	Функция
	Регистрация	Открывает окно регистрации
	Сменить пользователя	Выйти из данного пользователя и зайти с другого
	Изменить класс доступа	Изменить класс доступа
	Изменить пароль	Изменить пароль
	Завершить сеанс	Завершить сеанс

4 Настройки рабочего места

Описания интерфейса и представления данных в Системе даны в документе «Руководство диспетчера».

4.1 Настройки рабочего места

Рабочее место может быть настроено как пользователем, так и администратором Системы. Настройка производится с помощью пункта меню «Файл», подпункт «Настройки места».

Для того чтобы сохранить сконфигурированные настройки рабочего места необходимо выполнить следующие действия:

– открыть меню Файл/Настройки места/Сохранить

– в открывшемся окне (рисунок Рисунок 4.**1**) ввести имя рабочего места (латиницей) и нажать «Сохранить».

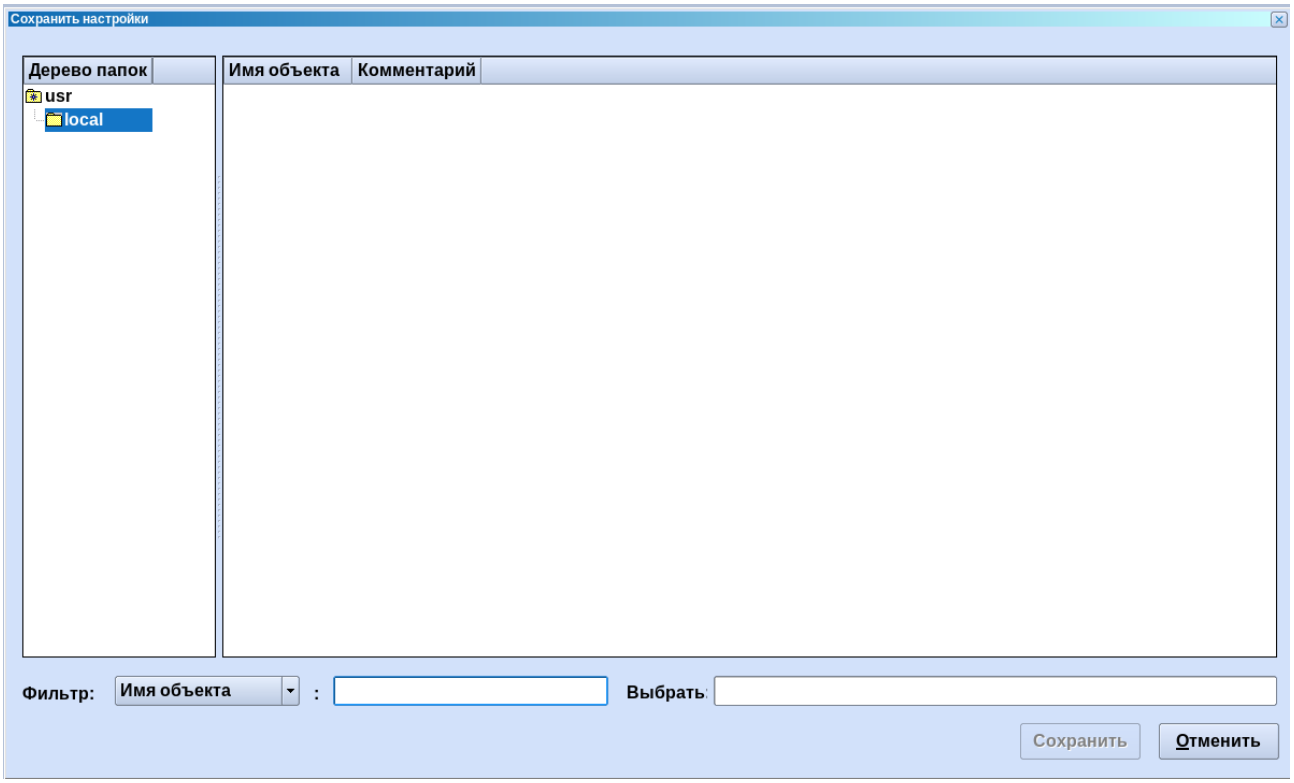


Рисунок 4.1 – Сохранение настроек рабочего стола

– в следующем диалоге (рисунок Рисунок 4.**2**) ввести комментарий (допускается использование кириллицы). Комментарий является необязательным атрибутом – поле может остаться пустым.

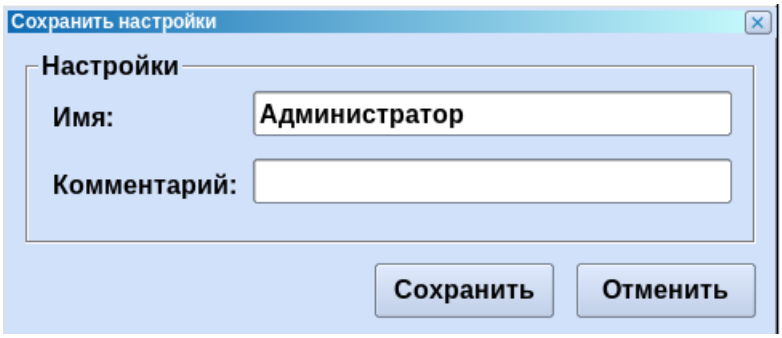


Рисунок 4.2 – Сохранение настроек рабочего стола. Комментарий

Для того чтобы данная конфигурация рабочего стола запускалась автоматически при запуске «Горизонта», необходимо дать ей имя учетной записи пользователя. Имя учетной записи пользователя можно увидеть в правом нижнем углу экрана. В данном поле указано имя учетной записи (рисунок Рисунок 4**.3**), а также класс доступа пользователя.

Рисунок 4.3 – Имя учетной записи пользователя

Пользователь может сохранить несколько конфигураций рабочего места под разными именами. Чтобы загрузить необходимую конфигурацию рабочего места, необходимо:

– открыть меню Файл/Настройки места/Загрузить

– в открывшемся окне (рисунок Рисунок 4**.4**) выбрать конфигурацию рабочего места и нажать «Загрузить».

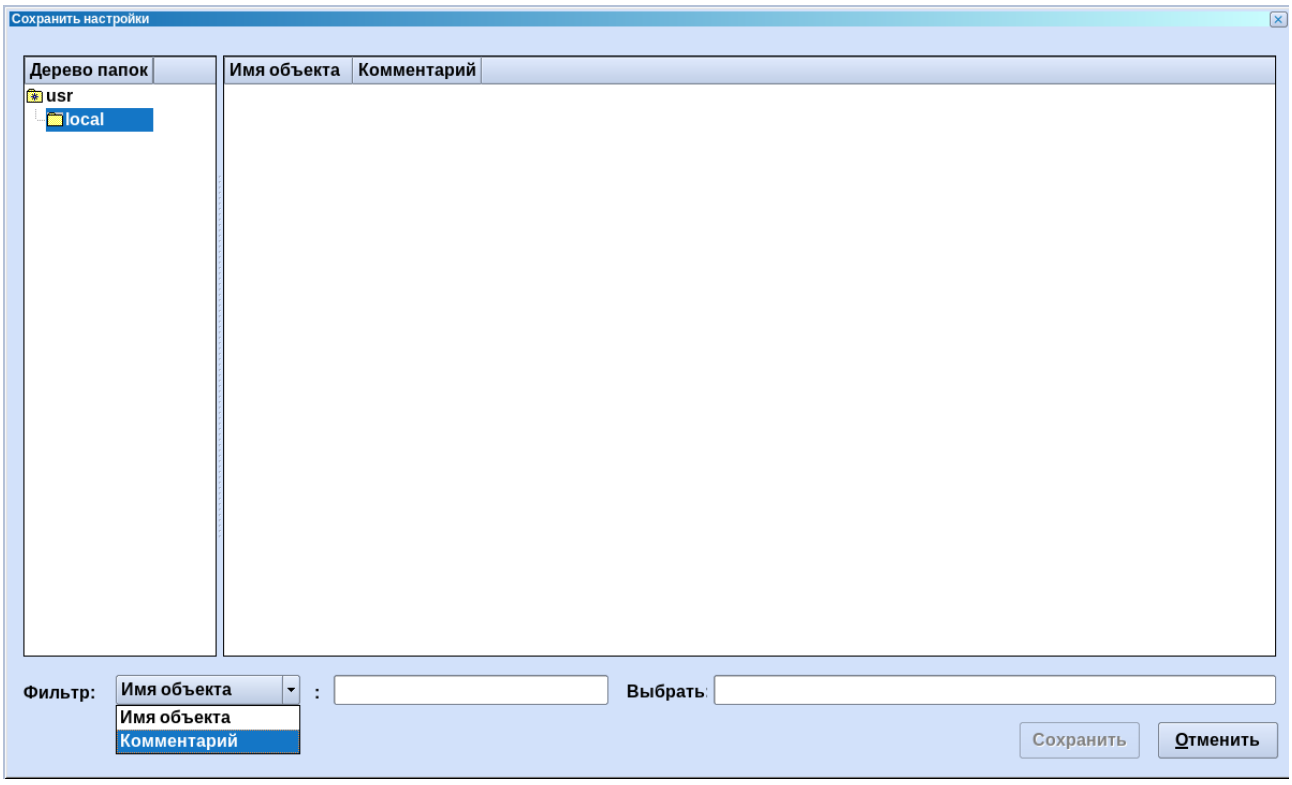


Рисунок 4.4 – Открыть сохраненные настройки рабочего места

– для поиска необходимого рабочего места предусмотрена фильтрация по имени рабочего места и комментарию. Часть имени или комментария вводится в пустое поле через *. Например: *мое рабочее место*.

Для того, чтобы отредактировать ранее сохраненное рабочее место необходимо либо открыть данное рабочее место, выбрать другие схемы\табличные формы и сохранить его, либо:

– открыть меню Файл/Настройки места/Правка

– в открывшемся окне выбрать конфигурацию рабочего места и нажать «Редактировать».

– откроется окно «Правка настроек» (рисунок Рисунок 4.**5**). В нем по кнопке с тремя точками открывается окно поиска запускаемого при открытии рабочего места приложения.

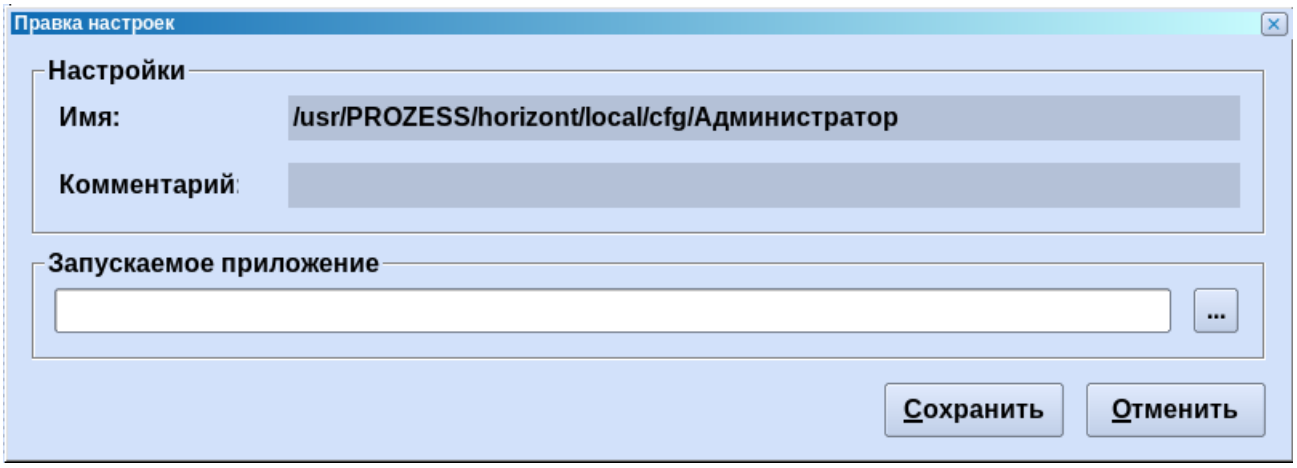


Рисунок 4.5 – Правка настроек

Для того чтобы удалить ранее сохраненное рабочее место, необходимо:

– открыть меню Файл/Настройки места/Удалить

– в открывшемся окне выбрать конфигурацию рабочего места и нажать «Удалить».

– откроется окно с предупреждением, в котором необходимо нажать ОК.

4.2 Настройки принтера

Настройки принтера. При выборе пункта скриншот в меню «Файл» появляется окно настроек печати (рисунок Рисунок 4.**6**).

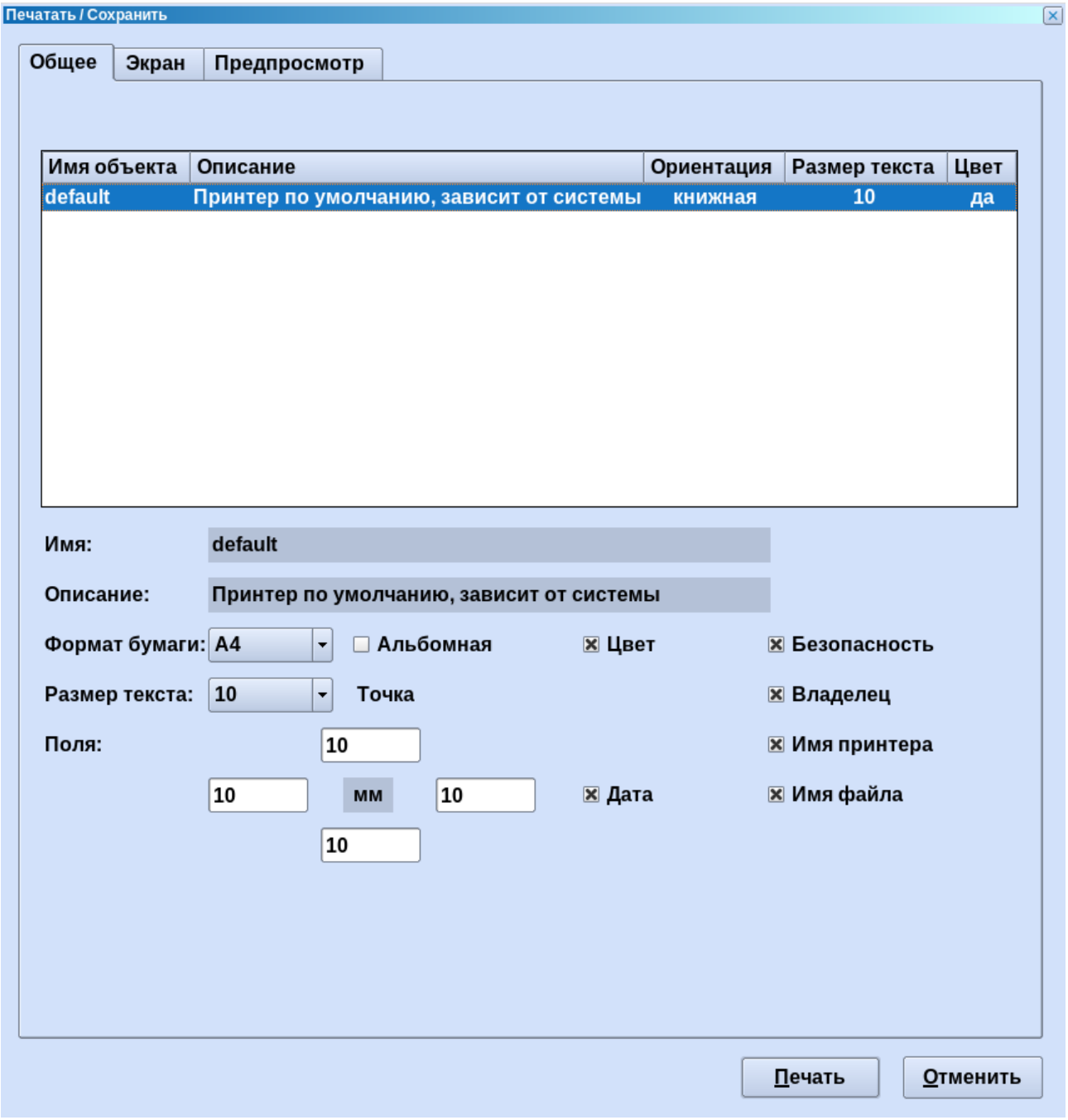


Рисунок 4.6 – Печать

В данном окне представлены все виды печати. По кнопке «Настройки» открывается окно с выбором предсохраненных настроек печати.

5 Поддержка системы

Дана информация о работе администратора по поддержке Системы.

5.1 Меню «Поддержка»

Пункт меню «Поддержка» (рисунок Рисунок 5.**1**) позволяет обновлять права доступа, а также изменять другие настройки Системы на базе ПО «Горизонт».

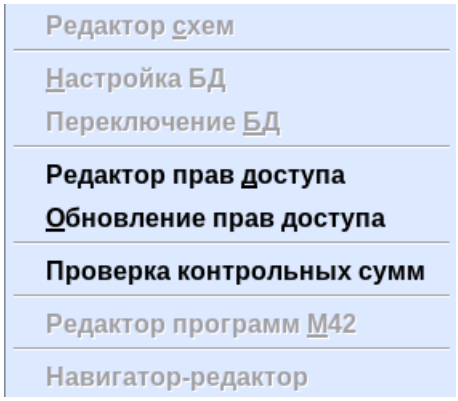


Рисунок 5.1 – Меню «Поддержка»

– редактор схем. При выборе данного пункта меню открывается редактор, позволяющий создавать и редактировать схемы;

– настройка БД. При выборе данного пункта меню открывается редактор, позволяющий создавать и редактировать объекты модели данных;

– переключение БД. При выборе данного пункта меню открывается диалог переключения БД. После проведения переключения БД становятся видны онлайн все изменения, внесенные в модель данных в редакторе БД;

– редактор прав доступа. При выборе данного пункта меню открывается редактор прав доступа. Работа с ним описана ниже;

– обновление прав доступа. Запускает обновление прав доступа, которые необходимо обновлять после создания новых таблиц или схем, а также после внесения изменений в редакторе прав доступа. После завершения обновления прав доступа внизу экрана появится сообщение (рисунок Рисунок 5.**2**). Необходимо нажать кнопку Enter.

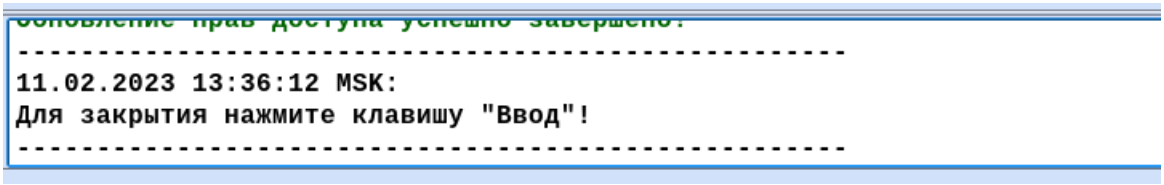


Рисунок 5.2 – Обновление прав доступа

– редактор программ M42. При выборе данного пункта меню открывается редактор, позволяющий создавать и редактировать программы на языке M42.

6 Описание редактора прав доступа

Следующая схема показывает механизм формирования прав доступа в ПК «Горизонт» (рисунок Рисунок 6.**1**).

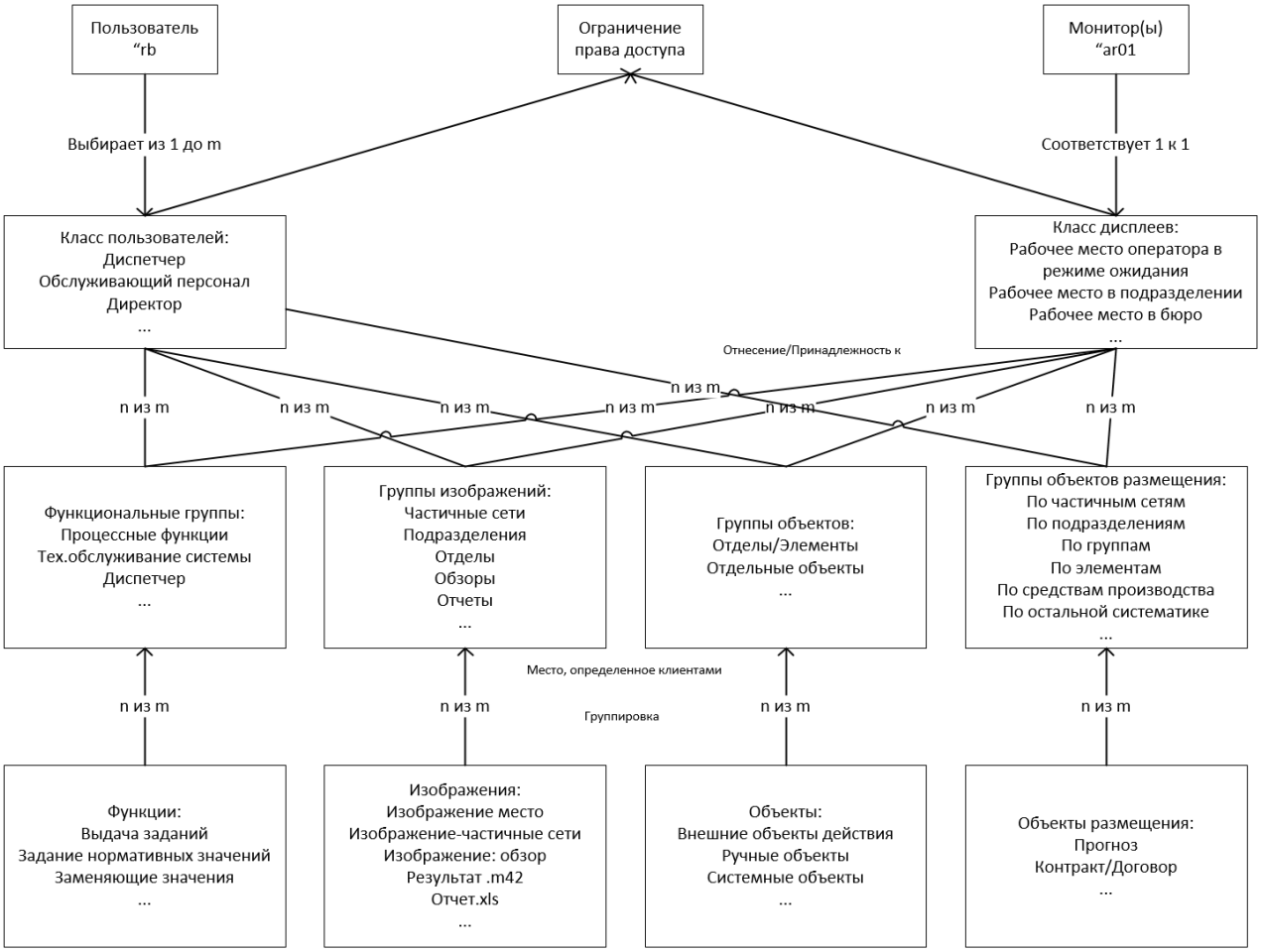


Рисунок 6.1 – Диалог регистрации

Сначала из отдельных функций (перечень функций приведен в разделе 5 Перечень функций), схем, правил вычисления и объектов БД (процесса) формируются группы функций, группы схем и группы объектов. Эти группы получают от администратора прав доступа специальные имена. При этом функциям, мнемосхемам могут быть задано до 128 названий групп. Каждая функция, каждая мнемосхема может относиться сразу к нескольким группам.

В качестве первого обобщающего понятия для прав доступа служит «класс пользователя». Каждому классу пользователя назначаются доступные группы функций, группы схем и группы объектов. Назначение классу пользователя групп функций, групп объектов и групп схем определяет, какие мнемосхемы и правила вычисления может просматривать пользователь, относящийся к этому классу, какие функции он может выполнять и т.д. Таким образом, определяемый класс

пользователя получает профиль доступных функций, мнемосхем, правил вычисления, объектов БД и т.д.

В качестве второго обобщающего понятия для прав доступа служит класс дисплея (рабочего места). В определении класса дисплея (рабочего места) указываются доступные на АРМ этого класса группы схем, группы объектов и группы функций. Таким образом, класс дисплея (рабочего места) получает профиль доступных объектов и функций.

Пользователь всегда привязан к одному из классов пользователя, от которого он наследует права доступа. Пользователь может осуществлять вход в систему с любого рабочего места, зарегистрированного в системе прав доступа. Права пользователя, вошедшего в систему, определяются исходя из прав доступа класса пользователя и прав доступа класса дисплея (рабочего места) с которого осуществлен вход в систему. Права доступа пользователя формируются путем пересечения множества прав класса пользователя и множества прав класса дисплея (рабочего места). Например, если классу пользователя доступна какая-либо мнемосхема, а классу дисплея (рабочего места), с которого пользователь вошел в систему, данная мнемосхема недоступна, то в результате пересечения множества прав доступа класса пользователя и класса дисплея (рабочего места) пользователю данная мнемосхема будет недоступна.

6.1 Общее описание

Редактор прав доступа запускается через пункт меню Поддержка\Редактор прав доступа. После запуска редактора прав доступа необходимо зарегистрироваться. Регистрация осуществляется через пункт «Новый сеанс» меню «Файл» (рисунок Рисунок 6**.2**).

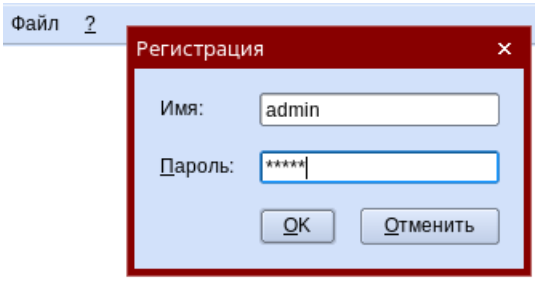


Рисунок 6.2 – Регистрация

После успешной регистрации появляется главное окно редактора прав доступа (рисунок Рисунок 6**.3**).

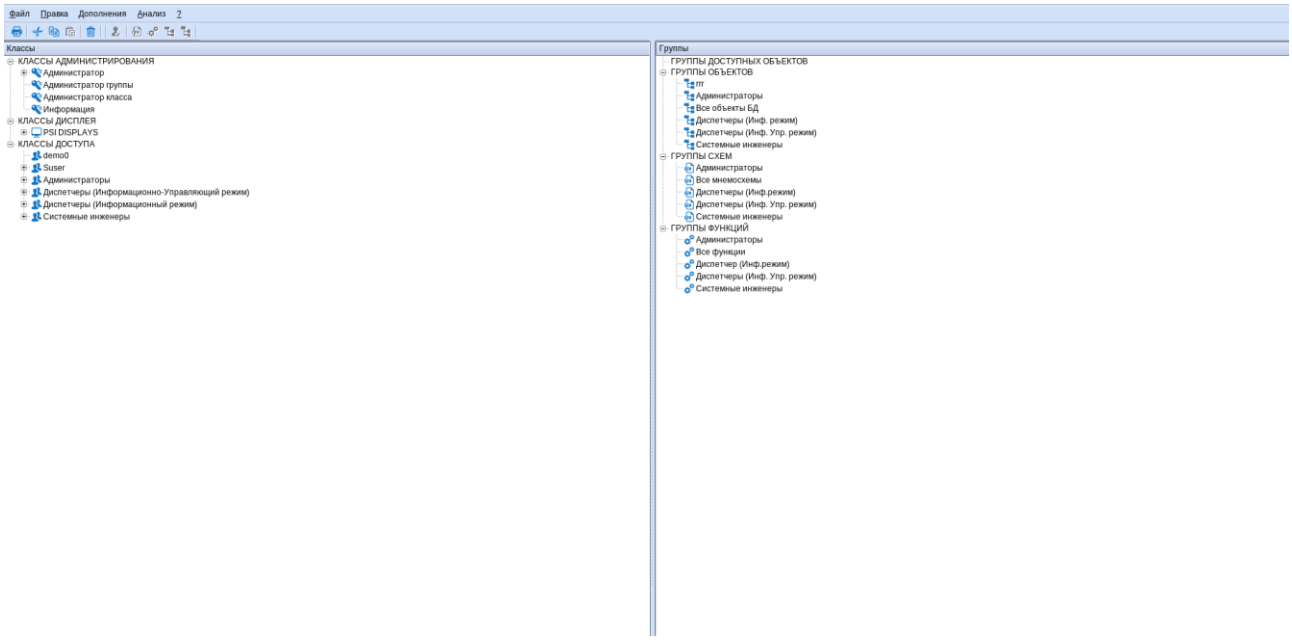


Рисунок 6.3 – Окно редактора прав доступа

В левой части главного окна отображаются, определенные в системе классы пользователей, классы дисплея (рабочего места) и классы администрирования. В правой части находятся все группы (группы схем, группы функций, группы объектов и группы доступных объектов). Как правило, по умолчанию активна функция «Упорядочить по классам» в меню «Дополнительно». В таком режиме просмотра отображаются классы и под ними принадлежащие им пользователи, дисплеи (рабочие места) или администраторы. Через функцию «Упорядочить по пользователям» меню «Дополнительно» режим отображения может быть переключен в режим просмотра, когда видны все пользователи, дисплеи и администраторы и под ними классы, к которым они принадлежат.

6.2 Работа с классами доступа

В режиме просмотра «Упорядочить по классам» к классам могут быть применены следующие операции:

- создать новый класс;
- удалить класс;
- копировать, вырезать, вставить;
- редактировать свойства класса.

Операции над классами доступны в меню «Правка» или через контекстное меню типов классов или классов (рисунок Рисунок 6**.4**).

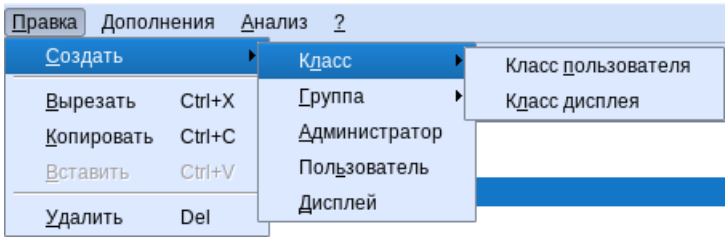


Рисунок 6.4 – Функции классов

При создании нового класса, появится диалоговое окно «Определение классов» (рисунок Рисунок 6.**5**).

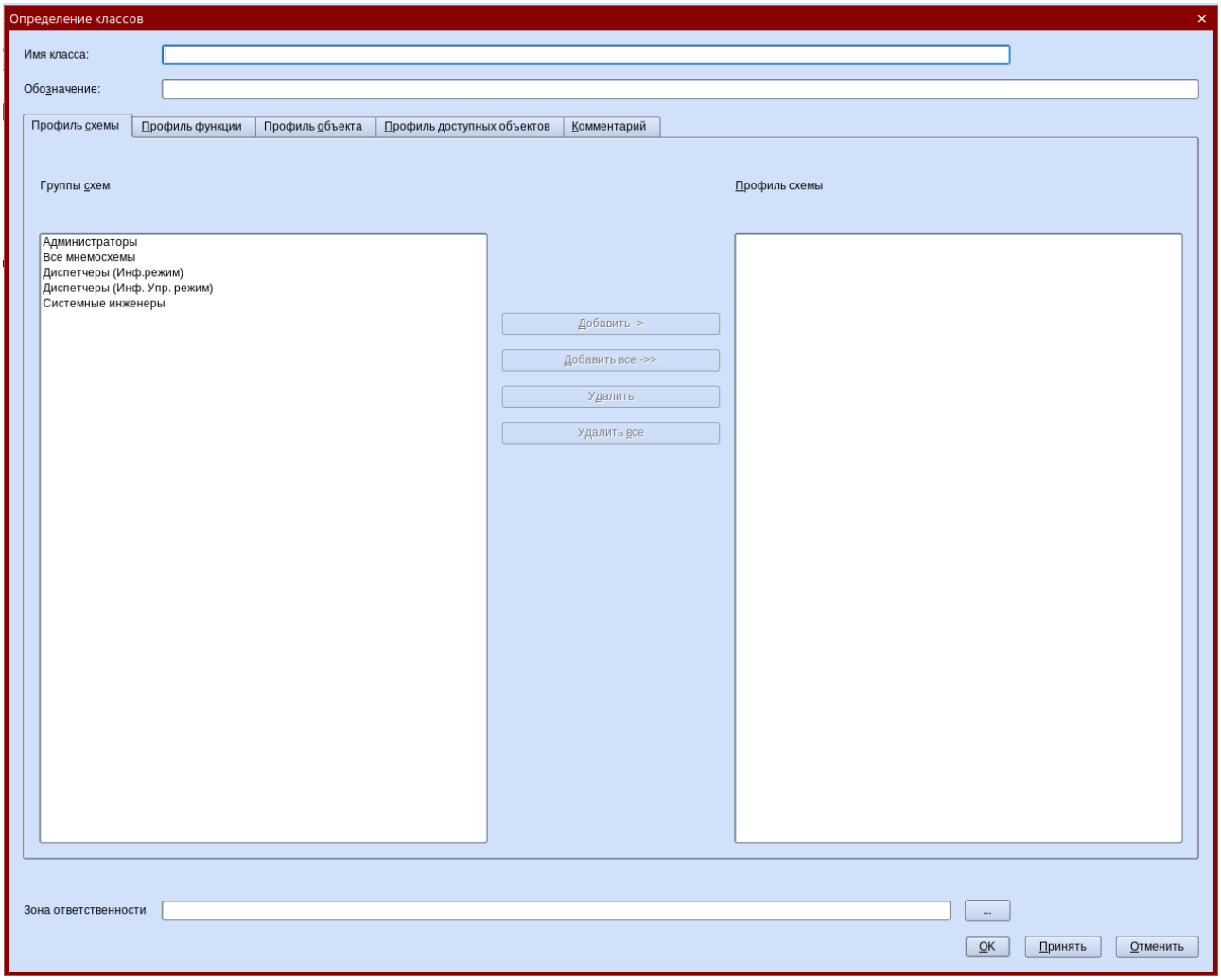


Рисунок 6.5 – Определение классов

В этом окне сначала вводится имя класса и обозначение.

В каждом профиле выбирается одна или несколько групп. С левой стороны находятся имеющиеся группы одного типа, справа – группы, отнесенные к этому профилю. Посредством выбора и нажатием клавиши «Добавить», «Добавить все», «Удалить» и «Удалить все» параметры можно изменить.

Во вкладке «Комментарий» может быть внесена любая информация (описание) о классе.

По кнопке с тремя точками выбирается зона ответственности, которые задаются в редакторе модели данных.

В больших системах с большим количеством различных заданий имеет смысл объединять частичные области по их принадлежности. Одна группа обработчиков может тогда, например, отвечать за одно определенное количество событий, другая же группа обработчиков – за другие события.

ПК «Горизонт» включает концепцию распределения зон ответственности. Зона ответственности означает по существу обязанность квитировать события. Для каждой области ответственности в системе предусмотрено отдельное окно Журнала аварийных сообщений. При параметрировании объектов БД предусмотрена возможность указать, в какой области ответственности должны быть квитированы события по объектам, где они должны быть приняты к сведению, а где собраны и занесены в протокол.

В редакторе доступа области ответственности могут быть отнесены к определенным классам. Отнесенные к одному классу пользователей области ответственности образуют рабочую область этого класса пользователей. В случае если один пользователь авторизуется на одном рабочем месте, он получает доступ к этим определенным областям ответственности в рабочей области своего класса пользователей. При этом нужно различать собственные и сторонние области ответственности. Собственные области ответственности определяются исходя из рабочей области класса пользователей и из областей ответственности класса дисплеев. Сторонние области ответственности – это оставшиеся области ответственности рабочей области. В своей собственной области ответственности один пользователь может квитировать события, напротив, в сторонних областях ответственности не может.

Удаление выбранного класса осуществляется выбором функции «Удалить» из меню «Правка» или контекстного меню. При удалении класса система запросит подтверждение.

Копирование выбранного класса осуществляется с помощью кнопки «Копировать». Выбрав тип класса, и нажав кнопку «Вставить» можно вставить скопированный класс. Свойства исходного класса будут унаследованы скопированным классом. Для однозначности имен, при копировании должно быть указано новое имя для класса.

Копирование классов возможно исключительно только в пределах одного типа классов, например, только в пределах классов доступа.

6.3 Работа с пользователями

В режиме просмотра «Упорядочить по классам» к пользователям могут быть применены следующие операции:

- создание нового пользователя;
- удаление пользователя из класса пользователей;
- удаление пользователя;
- копирование и вставка;
- перемещение;
- редактирование свойств.

Операции над пользователями доступны в меню «Правка» или через контекстное меню (рисунок Рисунок 6.**6**).

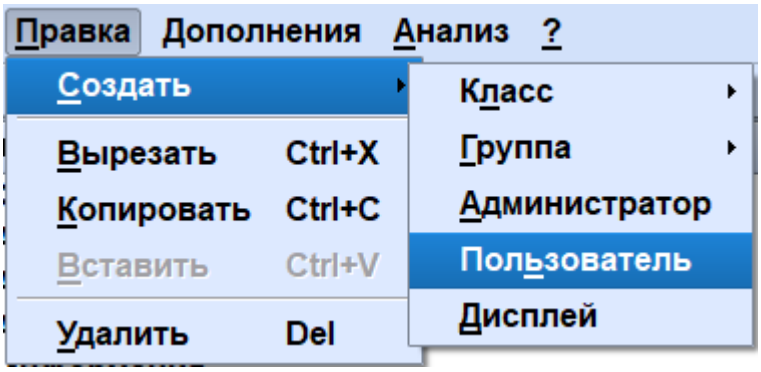


Рисунок 6.6 – Операции с пользователями

При выборе операции создания пользователя появляется диалоговое окно «Учетная запись пользователя» (рисунок Рисунок 6.**7**).

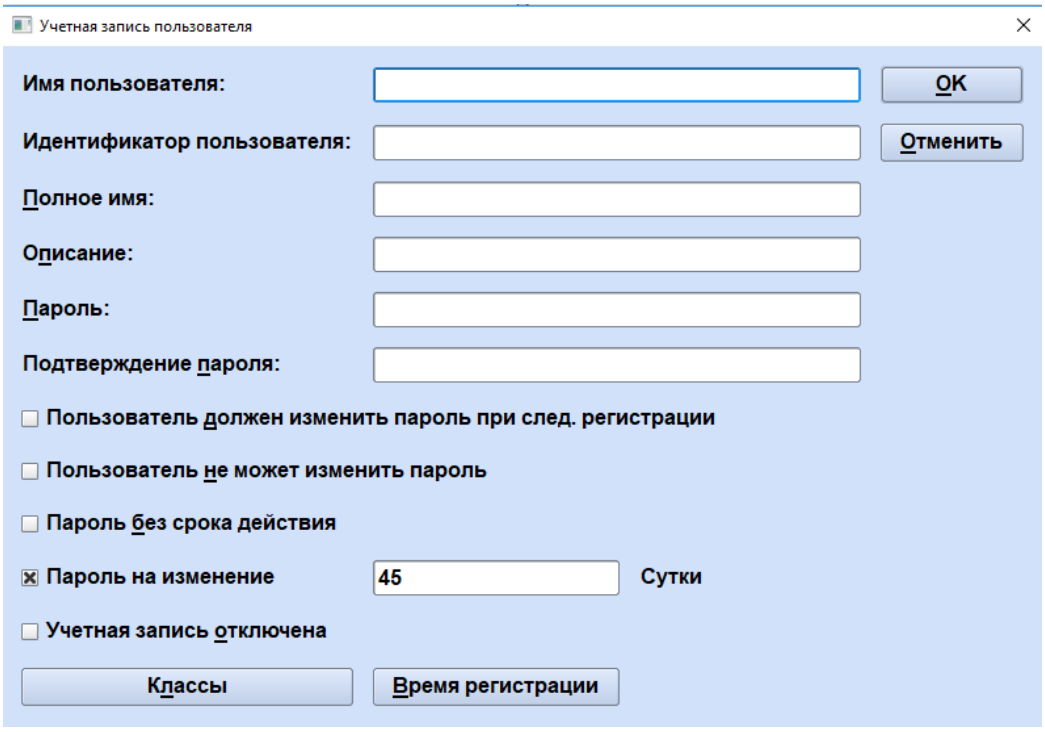


Рисунок 6.7 – Учетная запись пользователя

Окно «Определение пользователя» содержит следующие поля:

– имя пользователя;

– идентификатор (ID) пользователя;

– полное имя пользователя;

– описание, которое пользователь может составить сам (эта запись необязательная);

– пароль данного пользователя;

– подтверждение пароля.

Если поставлен флажок «Пользователь обязан сменить пароль при след. регистрации», то пользователь обязан при своей следующей регистрации задать новый пароль. Пользователю будет сообщено об этом в специальном окне при запуске программы.

Если поставлен флажок «Пользователь не может изменить пароль», то у пользователя нет возможности изменить свой пароль.

Если поставлен флажок «Пароль без срока действия», то пароль не теряет силу до следующего изменения. Если пароль просрочен, то пользователь больше не сможет зарегистрироваться. В этом случае появляется соответствующее сообщение, и пользователь обязан обратиться к администратору системы. Чтобы своевременно уведомить пользователя о необходимости смены пароля, Online-система в процессе регистрации выдает предупредительные сообщения-указания. Это происходит, когда паролю остается действовать не более 4 недель.

Для составления допустимого пароля служат следующие правила:

– минимальная длина 10 символов;

– наличие символов в нижнем регистре;

– наличие символов в верхнем регистре;

– наличие цифровых символов;

– наличие спецсимволов;

– количество паролей в истории 5.

Так как пользователь может перемещаться между различными разрешенными классами, то для одного пользователя может быть задано несколько классов пользователей. После нажатия кнопки «Классы» отображается окно членства в классах (рисунок Рисунок 6**.8**).

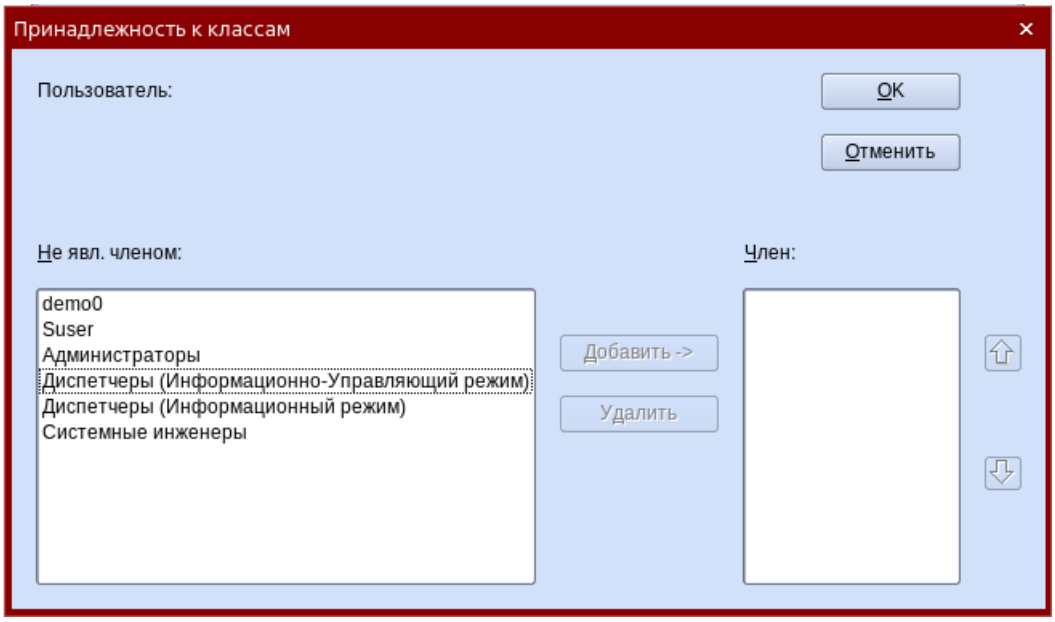


Рисунок 6.8 – Определение классов пользователя

Здесь может быть задано несколько классов пользователей. Если задан более чем один класс пользователей, то пользователь при регистрации в Online-системе обязан выбрать один из предусмотренных для него классов. Это позволяет реализовать, например, функции замещения на случай отпуска или болезни пользователя.

После нажатия кнопки «Время регистрации» появляется диалоговое окно «Время регистрации» (рисунок Рисунок 6.**9**).

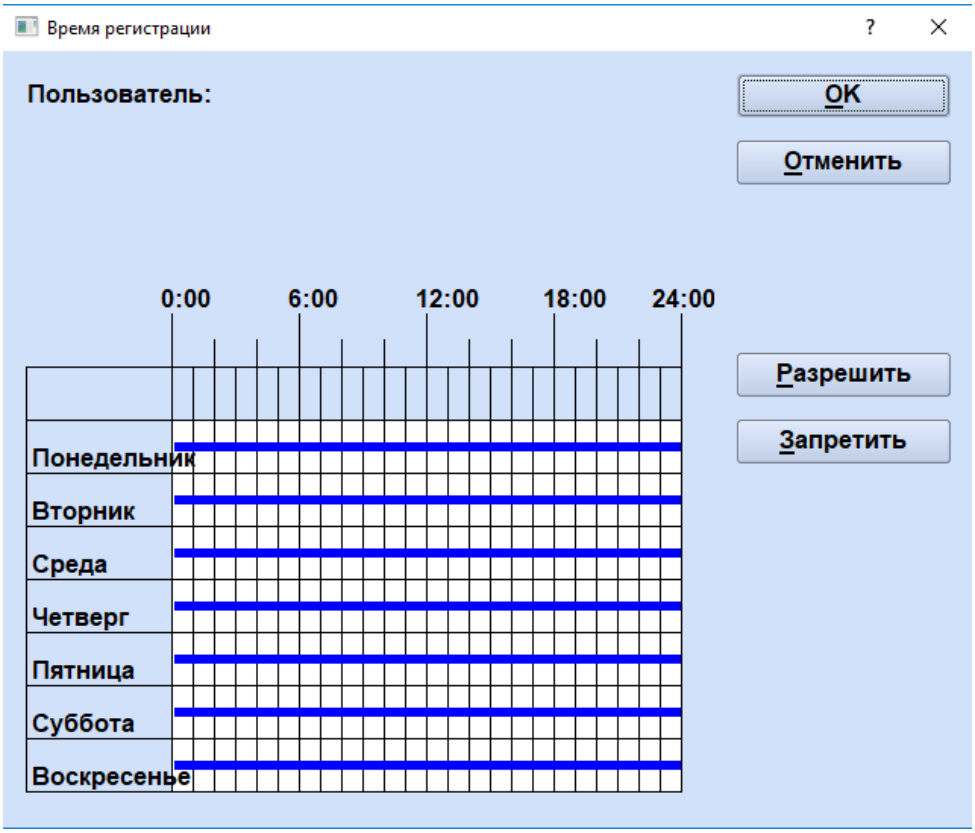


Рисунок 6.9 – «Время регистрации»

В диалоговом окне «Время регистрации» могут быть внесены следующие изменения:

– у каждого пользователя может быть удалено или разрешено время регистрации;

– после нажатия кнопки «Извлечение» с помощью нажатия на левую клавишу мышки можно перемещением слева направо задавать соответствующее время, которое сразу же выделяется красным цветом;

– после нажатия кнопки «Разрешить» можно также с помощью нажатия на левую клавишу мыши передвигать слева направо и тем самым задавать соответствующее время. Здесь помеченное красным цветом время удаляется;

– выделение соответствующей области является возможным с помощью нажатия на левую клавишу мыши и перемещением слева направо или нажатием желаемого отрезка времени.

После выбора пункта меню «Администратор» появляется диалоговое окно «Учетная запись администратора» (рисунок Рисунок 6.**10**).

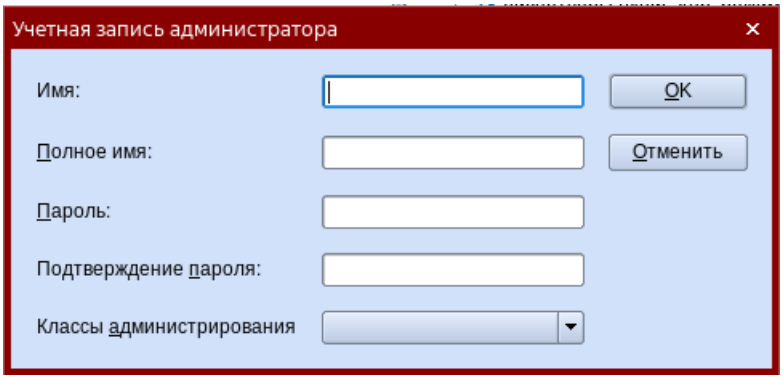


Рисунок 6.10 – Учетная запись администратора

Для каждого администратора создается профиль. Для определения профиля администратора необходимо определить следующие свойства:

– имя администратора как сокращенное имя;

– полное имя, фамилия администратора;

– пароль администратора;

– подтверждение пароля;

– соответствующий класс администраторов.

Все функции редактора-доступа могут быть отнесены следующим классам администраторов:

– Информация («доступ чтения» ко всем данным кроме персональных параметров);

– Администратор группы («доступ правки» только ко всем функциям, относящимся к этой группе, «доступ чтения» ко всем остальным данным кроме персональных параметров);

– Администратор классов («доступ правки» только к функциям, относящимся к этому классу или группе, никакого доступа к персональным параметрам);

– Администратор (никакого ограничения к доступу, без ограничений);

– Пользователи, которые получают доступ к данным системы доступа, должны принадлежать одному из вышеназванных классов.

Удалить пользователя можно через контекстное меню или через основное меню по кнопке «Удалить».

В случае копирования пользователя и вставки его в другой класс пользователей этот класс пользователей будет дополнительно приписан к пользователю. Если он будет вставлен в этот же класс пользователей, то будет создан новый пользователь, и будет запрошено новое имя и новый идентификатор пользователя.

6.4 Работа с дисплеями (рабочими местами)

В режиме просмотра «Упорядочить по классам» к дисплеями могут быть применены следующие операции:

– создание дисплея (рабочего места);

– удаление дисплея из класса дисплеев;

– удаление дисплея;

– копирование и вставка;

– перемещение;

– редактирование свойств.

Операции над дисплеями доступны в меню «Правка» или через контекстное меню (рисунок Рисунок 6.**11**).

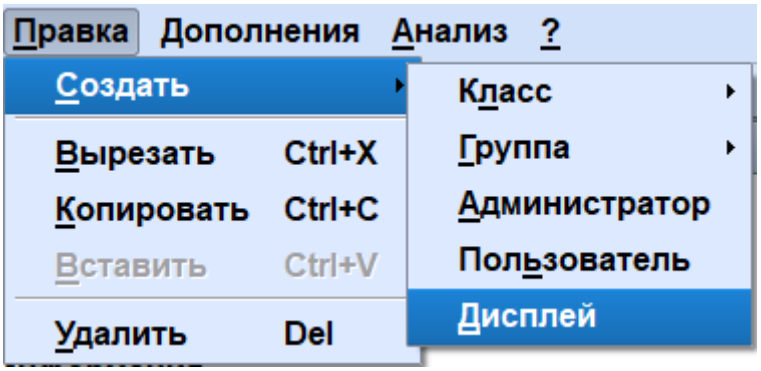


Рисунок 6.11 – Операции с дисплеями

При создании нового дисплея появляется диалоговое окно «Определение дисплея» (рисунок Рисунок 6.**12**).

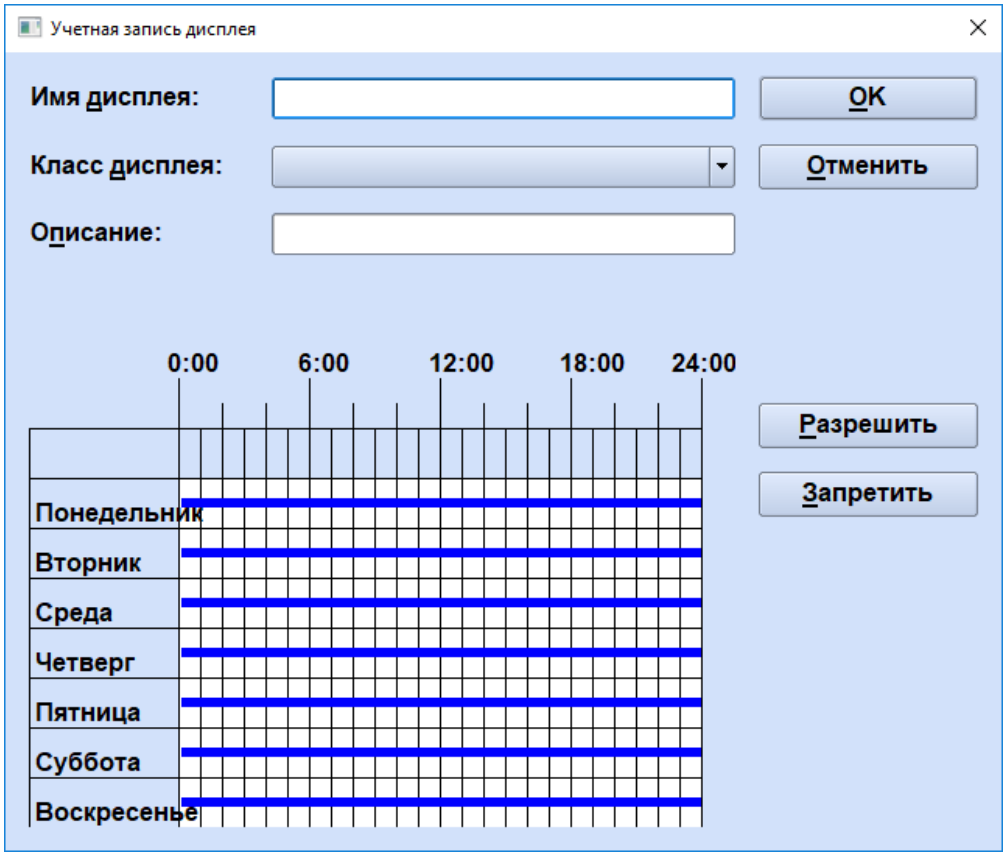


Рисунок 6.12 – Учетная запись дисплея

В диалоговом окне «Определение дисплея» могут быть выполнены следующие операции:

– разрешить, изменить или удалить время регистрации;

– после нажатия кнопки «Извлечение» с помощью нажатия на левую клавишу мышки можно перемещением слева направо задавать соответствующее время, которое сразу же выделяется красным цветом;

– после нажатия кнопки «Разрешить» можно также с помощью нажатия на левую клавишу

– мышки передвигать слева направо и тем самым задавать соответствующее время. Здесь помеченное красным цветом время удаляется;

– выделение соответствующей области является возможным с помощью нажатия на левую клавишу мышки и перемещением слева направо или нажатием желаемого отрезка времени.

Имеются и следующие функции:

– запись имени дисплея в поле «Имя дисплея»

– выбор соответствующего класса дисплеев

– ввод в поле «Описание» любого комментарии для пользователя. Эта запись является необязательной.

6.5 Работа с группами

В режиме просмотра «Упорядочить по классам» к группам могут быть применены следующие операции:

– создание новой группы

– удаление группы

– копирование группы

– вставка группы в соответствующий профиль классов

– редактирование свойств группы.

Операции над группами могут быть выбраны в меню «Правка» или через контекстное меню типов групп или группы (рисунок Рисунок 6**.13**).

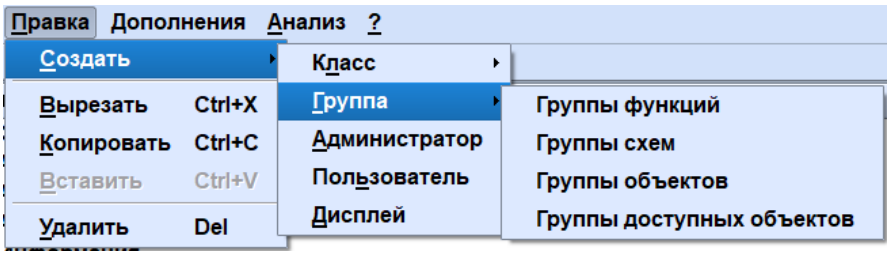


Рисунок 6.13 – Функции групп

После двойного щелчка на группе или выбора соответствующей функции в меню, будет загружено окно «Группы объектов» (рисунок Рисунок 6**.14**).

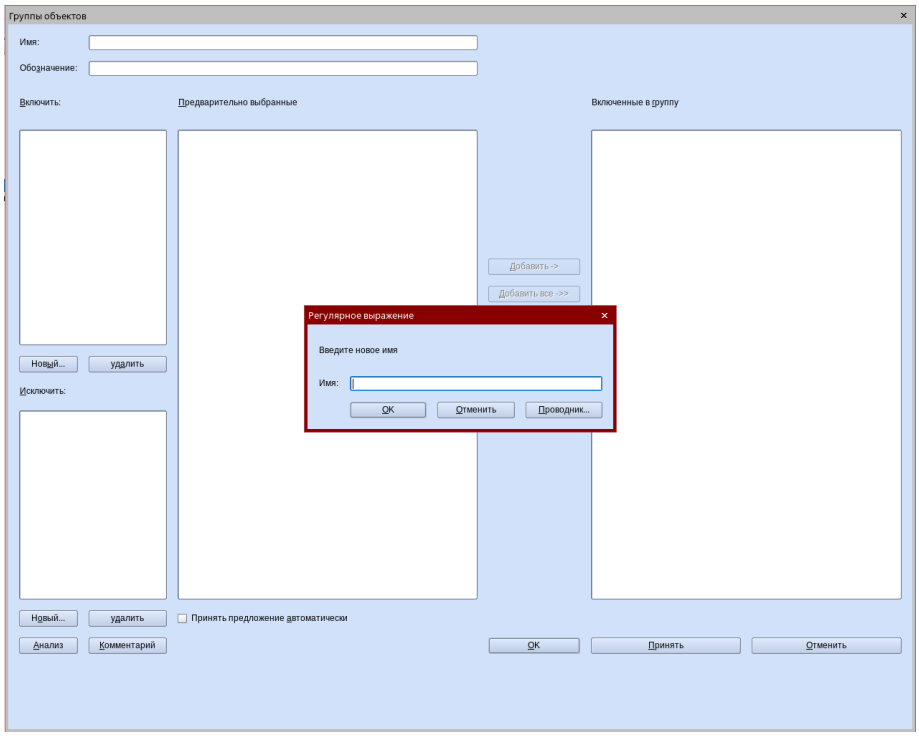


Рисунок 6.14 – Группа объектов/новый

В окне заполняются поля «Имя» и при необходимости «Обозначение». С помощью фильтров «Включить» и «Исключить» возможно совершить выборку из объектов.

После нажатия на кнопку «Новый…» в поле «Включить» или «Исключить» будет открыто окно «Регулярное выражение», где можно вводить следующие знаки:

– ? – «знак вопроса» стоит для любого знака, т.е. когда, например, задано выражение «?p», то будет проведен поиск выражения, где в начале стоит любой знак, а на конце – «p»;

– * – «звезда» стоит для любого количества любых знаков, т.е. когда, например, задано;

– выражение «*p», то будет проведен поиск выражения, где в начале стоит любое количество знаков, а на конце – «p».

После нажатия на кнопку «Проводник» (рисунок Рисунок 6**.15**) будет запущен браузер для соответствующего типа элементов. При запуске фильтр автоматически устанавливается на «*». Одновременно можно выбрать одну или несколько записей, затем они разделяются запятыми в поле ввода окне «Регулярное выражение».

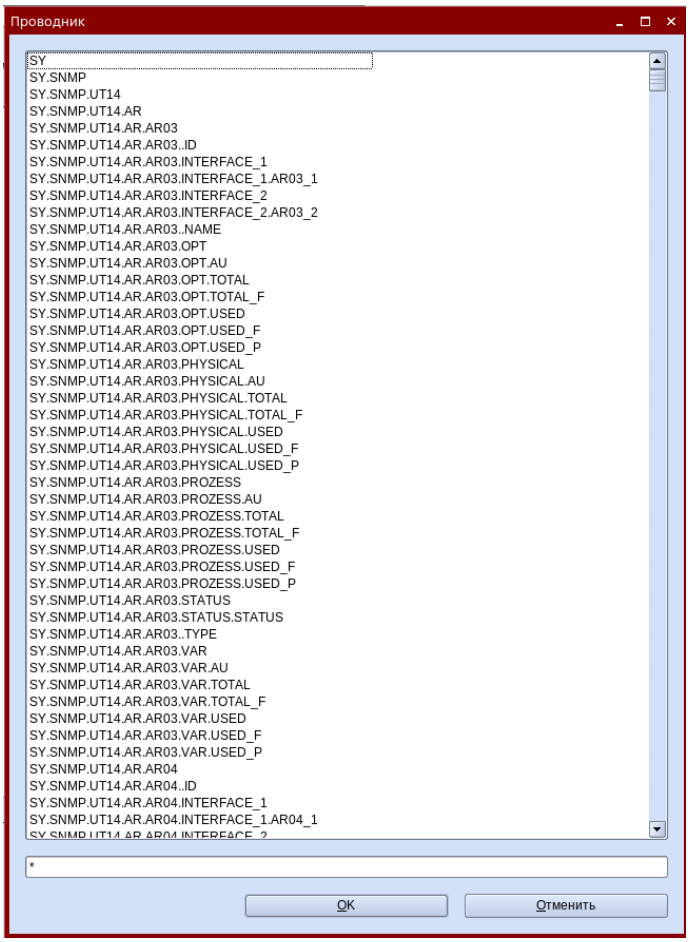


Рисунок 6.15 – Проводник

Если после выбора требуемого выражения в поле «Включить» будет нажата кнопка «удалить», то соответствующее выражение будет удалено.

В списке «Исключить» вышеназванные знаки и функции «новый» и «удалить» работают так же, как и в списке «Включить».

При не выбранном «Принять предложение автоматически» выражения имеют только один выбор. После нажатия кнопки «рецензировать/оценка» (Анализ) отображаются все элементы, которые выполняют критерии фильтра в списке «Предложенный выбор». Предложенные в этом списке элементы могут быть добавлены с помощью отдельного выбора определения групп.

При снятой галочке в поле «Принять предложение автоматически» и нажатии кнопки «Анализ» в списке «Предложение» автоматически будут показаны все функции, имеющиеся в базе данных.

При выбранном поле «Принять предложение автоматически» и нажатии кнопки «Анализ» в списке «Определение групп» будут показаны все имеющиеся в базе данных функции.

После нажатия кнопки «Комментарий» появится окно, в котором можно ввести комментарий о группе.

Клавиша «ОК» сохраняет измененные данные и одновременно закрывает диалоговое окно «Определение групп».

Кнопка «Применить» сохраняет измененные данные в базе данных. Диалоговое окно «Определение групп» остается, однако открытым и может быть дальше исправлено.

Кнопка «Отмена» не сохраняет измененные данные в базе данных. Диалоговое окно «Определение групп» закрывается.

6.6 Меню «Поиск»

После выбора пункта меню Дополнения\Поиск появляется окно поиска (рис. Рисунок 6.**16**).

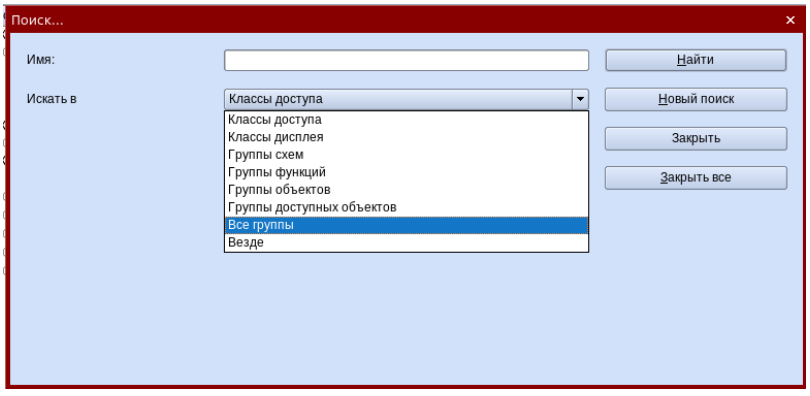


Рисунок 6.16 – Поиск

С помощью этой функции могут быть найдены один или несколько элементов. одного класса или группы в классах доступа, классах дисплеев, группах схем, группах изображений, группах функций, группах объектов, группах доступных объектов и во всех группах и везде.

В диалоговом окне «Поиск» может быть задано любое слово для поиска. Результаты отображаются в поле результата.

В качестве области поиска могут быть заданы:

– отдельные группы (в зависимости от типа)
– все группы
– классы дисплеев
– классы пользователей
– везде

При нажатии кнопки «Найти» результаты будут отображены в этом диалоговом окне (рисунок Рисунок 6**.17**).

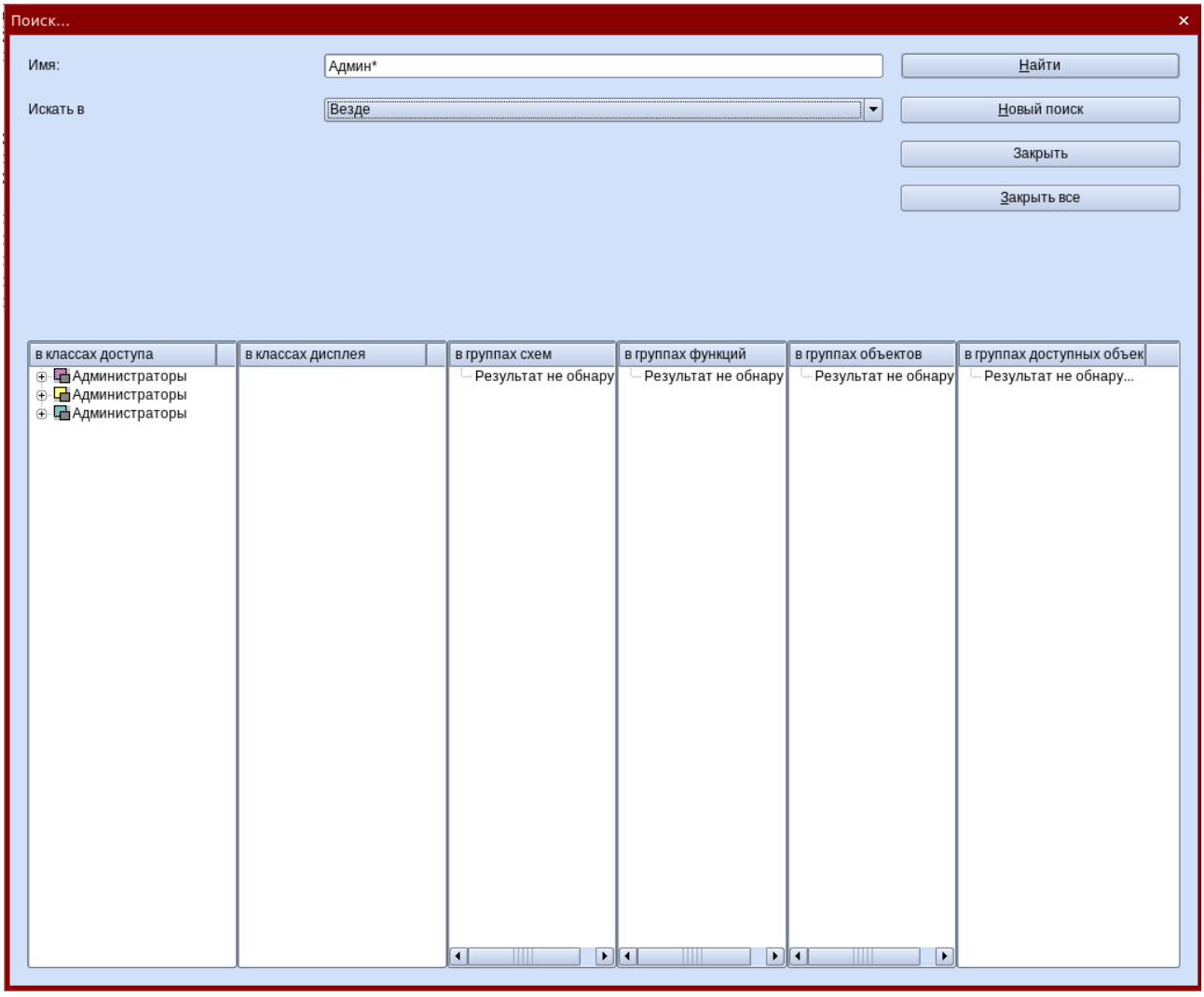


Рисунок 6.17 – Результат поиска

Для последующего поиска в этом же диалоговом окне может быть введено новое поисковое слово. После нажатия кнопки «Новый поиск» откроется новое окно поиска (максимально 5 окон). Кнопка «Закрыть» закрывает текущее диалоговое окно поиск. Нажатие кнопки «Закрыть все» закрывает одновременно все диалоговые окна поиска.

В поле ввода «Имя» вводится поисковое слово. Если имя известно не полностью, то можно использовать специальные символы (*, ?).

В поле «Поиск в» выбирается соответствующий тип класса или группы, в котором нужно искать. Если тип класса или группы неизвестен, можно выбрать в качестве диапазона поиска «Все классы» или «Везде».

6.7 Меню «Анализ»

С помощью пункта меню «Вид» возможно переключение главного окна в режим анализа (рисунок Рисунок 6**.18**).

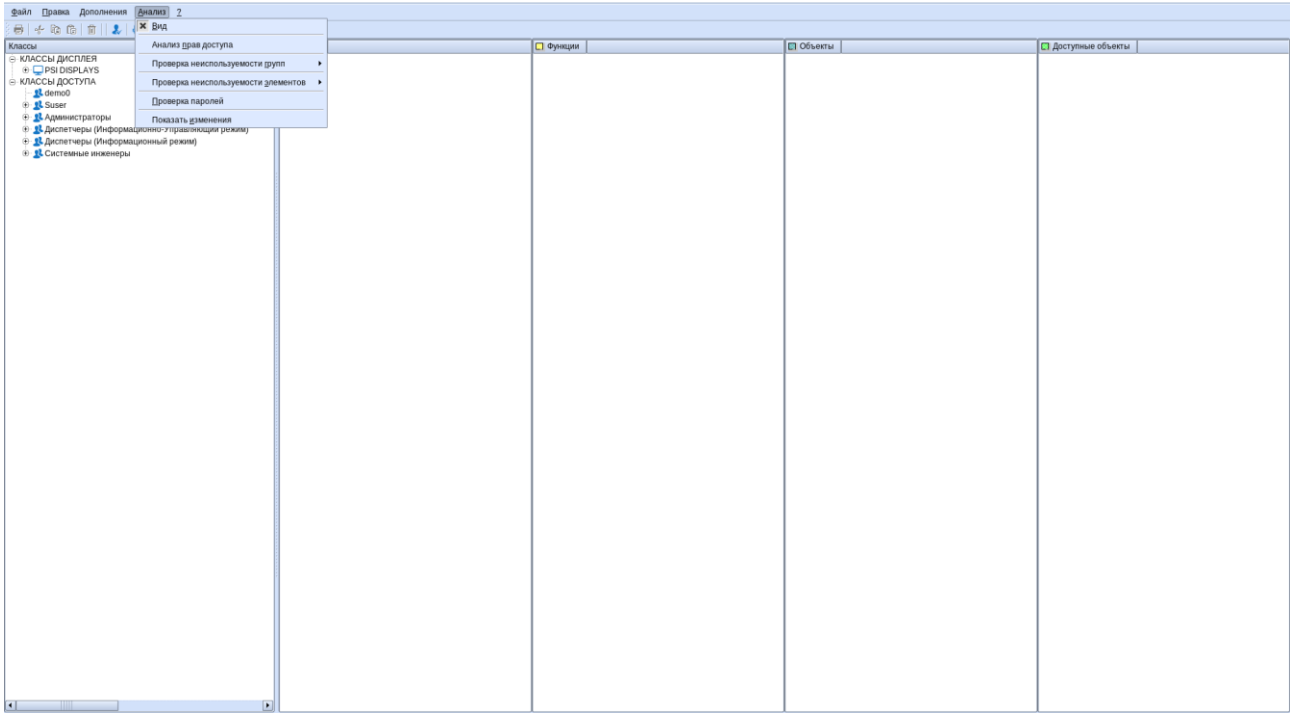


Рисунок 6.18 – Режим анализа

Анализ прав доступа - необходимо выбрать класс пользователей (или пользователя) и класс дисплеев (или дисплей). После обработки будут показаны все четыре колонки с соответствующими мнемосхемами, функциями и объектами, которые данному классу пользователей разрешено обрабатывать или использовать внутри этого класса дисплеев.

Пункт меню «Проверка консистенции группы» показывает, к каким группам не отнесены ни одни классы пользователей или дисплеев. Проверка консистентности

может осуществляться для групп функций, групп схем, групп объектов и групп доступных объектов.

Пункт меню «Проверка консистентности элемента» показывает, какой элемент не отнесен ни к одной группе.

7 Перечень функций

В таблице 2 приведен перечень функций, каждая из которых определяет доступность пользователю определенного функционала – пункта меню, запускающего данный функционал.

Таблица 2 – Перечень функций

Название	Описание
ARCSIMDIA_CD-диалог_Местонахождение_Загрузка	Включает пункт меню Архивы/Вдольтрассовые графики/Открыть вдольтрассовый график
ARCSIMDIA_CD-диалог_Местонахождение_Удалить	Включает пункт меню Архивы/Вдольтрассовые графики/Удалить вдольтрассовый график
ARCSIMDIA_CD-диалог_Местонахождение_Сохранить	Включает пункт меню Архивы/Вдольтрассовые графики/Открыть вдольтрассовый график/Выбрать файл/сохранить график
ARCSIMDIA_CD-диалог_Местонахождение_Показать	Включает пункт меню Архивы/Вдольтрассовые графики/Открыть вдольтрассовый график/Выбрать файл из списка
LONARC_Показать_архив_таблица_10часовой_газовый_день	Включает пункт меню Архивы\Правка архивных значений\Газовые сутки (10ч)
LONARC_ПоказатьАрхивТаблицу_2Часа	Включает пункт меню Архивы\Правка архивных значений\2 Часа
LONARC_ПоказатьАрхивТаблицу_5Минут	Включает пункт меню Архивы\Правка архивных значений\5 минут
LONARC_Выписка_из_Журнала_Событий_показать	Включает пункт меню Журналы\Выписка из журнал событий\Зона собственной ответственности
LONARC_Выписка_из_Журнала_Событий_чужая_ответственность_показать	Включает пункт меню Журналы\Выписка из журнал событий\Зона сторонней ответственности
LONARC_Журнал_Событий_показать	Включает пункт меню Журналы\Журнал событий\Зона собственной ответственности
LONARC_Журнал_Событий_чужая_ответственно	Включает пункт меню Журналы\Журнал событий\Зона

Название	Описание
сть_показать	сторонней ответственности
LONARC_Экстремум_Таблица	Включает пункт меню Архивы\Правка архивных значений\График по объекту
LONARC_ЖАС_показать	Включает пункт меню Журналы\Журнал аварийных сообщений\Зона собственной ответственности
LONARC_ЖАС_дистанционное_управление	Включает пункт меню Журналы\Журнал аварийных сообщений\Дистанционное управление
LONARC_ЖАС_чужая_ответственность_показать	Включает пункт меню Журналы\Журнал аварийных сообщений\Зона сторонней ответственности
LONARC_ЖАС_Удалить	Включает в журнале аварийных сообщений в контекстном меню объекта пункт "Удалить"
LONARC_ЖАС_Квитировать	Включает в журнале аварийных сообщений в контекстном меню объекта пункт "Квитировать"
LONARC_ЖАС_Квитировать_Постранично	Включает в журнале аварийных сообщений кнопку "Квитировать"
LONARC_ЖАС_Перенаправить	Включает в журнале аварийных сообщений в контекстном меню объекта пункт "Передача данных"
LONARC_Меню_Архив	Включает пункт меню Архивы
LONARC_Меню_Журналы	Включает пункт меню Журналы
LONARC_Пересчет	Включает пункт меню Архивы\Пересчет и Пересчет скриптов проверки
LONARC_Пересчет_скрипт	Включает пункт меню Архивы\Пересчет правила вычисления
LONARC_Подменю_Журнал_Событий	Включает пункт меню Журналы\Журнал событий
LONARC_Подменю_Выписка_из_Журнала_Событий	Включает пункт меню Журналы\Выписка из журнал событий
LONARC_Подменю_ЖАС	Включает пункт меню Журналы\Журнал аварийных сообщений
LONARC_Подменю Объект	Включает пункт меню Журналы/Заметки по объекту
LONARC_Подменю_Тре	Включает пункт контекстного меню объекта График

Название	Описание
нд	архивных значений
LONARC_Тренд_10ЧасовГазДень	Включает пункт меню Архивы\График архивных значений\Диалоговое окно\Газовые сутки (10ч) или Рабочая область\Газовые сутки (10ч) и те же пункты в контекстном меню объекта
Включает пункт меню Архивы\График архивных значений\Диалоговое окно\2 Часа или Рабочая область\2 Часа и те же пункты в контекстном меню объекта	Включает пункт меню Архивы\График архивных значений\Диалоговое окно\2 Часа или Рабочая область\2 Часа и те же пункты в контекстном меню объекта
Включает пункт меню Архивы\График архивных значений\Диалоговое окно\5 минут или Рабочая область\5 минут и те же пункты в контекстном меню объекта	Включает пункт меню Архивы\График архивных значений\Диалоговое окно\5 минут или Рабочая область\5 минут и те же пункты в контекстном меню объекта
LONPSU_Команды	Выдача команд
LONPSU_Проводник_по_индикаторам	Включает пункт меню Процесс\Проводник по индикаторам и Проводник по индикаторам с фильтром
LONPSU_Информационный_список	Включает пункт меню Процесс\Фильтр по объектам
LONPSU_Меню_Процесс	Включает пункт меню Процесс
LONPSU_Ручная_корректировка	Включает пункт меню Процесс\Ручная корректировка
LONPSU_Онлайн_трассировка	Включает пункт меню Процесс\Трассировка скриптов М42
LONPSU_Информация_о_процессе	Включает пункт меню Процесс\Состояние о процессе
LONPSU_Быстрая команда	Включает пункт меню процесс/блокировка

Название	Описание
LONPSU_Имитация телеграммы	Включает пункт меню процесс/имитация телеграммы
LONVI_Завершить_сеанс	Включает пункт меню Файл\Завершить сеанс
LONVI_Регистрация	Включает пункт меню Файл\Регистрация
LONVI_Настройка_БД_запустить	Включает пункт меню Поддержка\Настройка БД
LONVI_Завершить	Включает пункт меню Файл\Завершить
LONVI_Редактор_прав_доступа_запустить	Включает пункт меню Поддержка\Редактор прав доступа
LONVI_Обновление_прав_доступа_запустить	Включает пункт меню Поддержка\Обновление прав доступа
LONVI_Редактор_схем_запустить	Включает пункт меню Поддержка\Графический редактор
LONVI_Список_папок_схем	Включает пункт меню Файл\Открыть папку схем и Правка папок схем
LONVI_Список_схем	Включает пункт меню Файл\Открыть схему
LONVI_Контрольная сумма_проверки	Включает пункт меню Поддержка/Проверка контрольных сумм
LONVI_Переключение_БД	Включает пункт меню Поддержка\Переключение БД
LONVI_Окна_расположить	Включает пункт меню Окно\Упорядочить
LONVI_Окна_закрыть	Включает пункт меню Окно\Закрыть все
LONVI_Окна_перекрывающиеся	Включает пункт меню Окно\Каскад
LONVI_Схема_привязки	Включает пункт меню Схема привязка в контекстном меню объекта
LONVI_Печатная_копия	Включает пункт меню Файл\Печать окна
LONVI_Информация	Включает пункт Свойства в контекстном меню объекта
LONVI_Конфигурация_редактировать	Включает пункт меню Файл\Настройка рабочего места\Редактировать

Название	Описание
LONVI_Конфигурация_загрузить	Включает пункт меню Файл\Настройка рабочего места\Загрузить
LONVI_Конфигурация_удалить	Включает пункт меню Файл\Настройка рабочего места\Удалить
LONVI_Конфигурация_сохранить	Включает пункт меню Файл\Настройка рабочего места\Сохранить
LONVI_копировать_ключ	Включает пункт меню Правка\Копировать ключ объекта
LONVI_копировать_объект	Включает пункт меню Правка\Копировать
LONVI_Меню_Обработать	Включает пункт меню Правка
LONVI_Меню_Файл	Включает пункт меню Файл
LONVI_Меню_Вставить	Включает пункт меню Правка\Вставить
LONVI_Меню_Дополнительно	Включает пункт меню Поддержка
LONVI_Меню_Окно	Включает пункт меню Окно
LONVI_Меню_Помощь	Включает пункт меню ?
LONVI_Меню_Опции	Включает пункт меню Настройки
LONVI_Объект_поиск	Включает пункт меню Правка\Найти объект
LONVI_Использование_объекта	Включает пункт Использование объекта в контекстном меню объекта
LONVI_Список_объектов	Включает пункт меню Файл\Дерево объектов и Список объектов по ключу
LONVI_Изменить_пароль	Включает пункт меню Файл\Изменить пароль
LONVI_просмотр ситуации	Включает меню процесс/просмотр ситауции
LONVI_Подменю_конфигурация_рабочего_места	Включает пункт меню Файл\Настройка рабочего места
M42_Просмотр	Редактор M42
M42_Редактирование	Редактор M43

Название	Описание
M42_Воздействие на процесс	Редактор M44
M42_Процесс распознования	Редактор M45
M42_Изменеие порядка	Редактор M46

8 Программное обеспечение Kaspersky Endpoint Security

8.1 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 8.1).

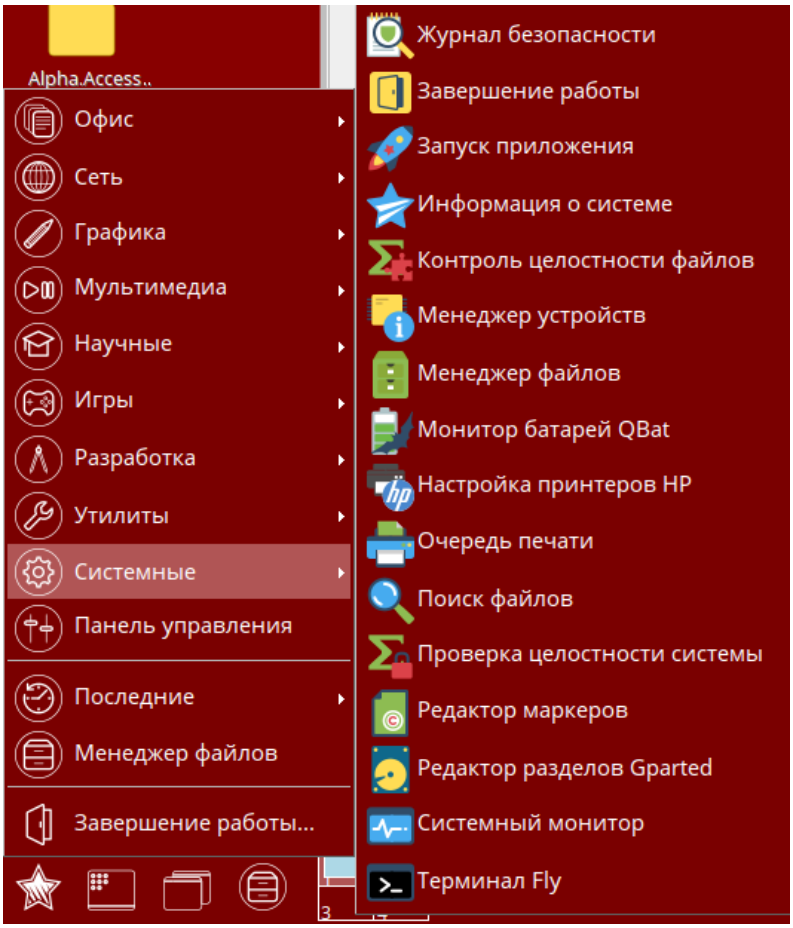


Рисунок 8.1 – Запуск «Терминал Fly»

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 8.2) `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 8.2 – Установка антивируса Kaspersky Endpoint Security

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 8.3 **– Начальная настройка Kaspersky Endpoint Security**

).

```
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 8.3 – Начальная настройка Kaspersky Endpoint Security

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 8.4). 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 8.4 – Ознакомление с лицензионным соглашением и политикой конфиденциальности

Примите лицензионное соглашение, для этого нажмите клавиши «y» и Enter (Рисунок 8.5).

```
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 8.5 – Принятие лицензионного соглашения

Повторно подтвердите, что принимаете лицензионное соглашение, для этого нажмите клавиши «y» и Enter (Рисунок 8.6).

```
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 8.6 – Повторное принятие лицензионного соглашения

Примите политику конфиденциальности, для этого нажмите клавиши «y» и Enter (Рисунок 8.7).

```
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 8.7 – Принятие политики конфиденциальности

Ознакомьтесь и примите заявление KASPERSKY SECURITY NETWORK (KSN Statement), для этого нажмите клавиши «y» и Enter (Рисунок 8.8).

```
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 8.8 – Принятие заявления KSN Statement

Установите графический интерфейс пользователя (GUI), для этого нажмите клавиши «y» и Enter (Рисунок 8.9).

Рисунок 8.9 – Установка графичеческого интерфейса пользователя

Введите логин для учетной записи администратора – administrator, и нажмите клавишу Enter (Рисунок 8.10).

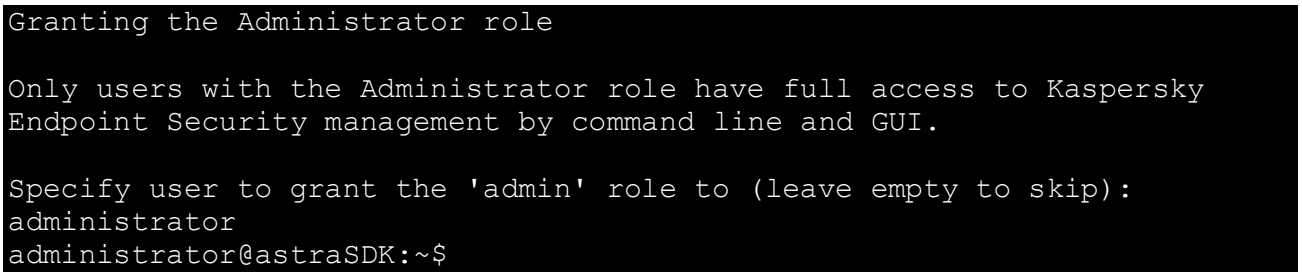


Рисунок 8.10 – Вход в учетную запис администратора

Укажите источник обновлений баз и модулей антивируса (Рисунок 8.11) 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.

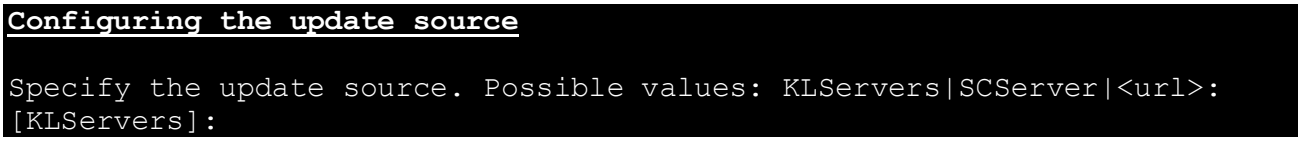


Рисунок 8.11 – Источник обновения баз и модулей антивируса

Далее предлагается ввести настройки прокси-сервера — откажитесь, нажав клавиши «n» и **Enter** (Рисунок 8.12).

Рисунок 8.12 – Настройка прокси-сервера

На следующем этапе предлагается обновить базы данных антивируса, нажмите клавиши «y» (согласиться на обновление) или «n» (отказаться от обновления) и Enter (Рисунок 8.13).

```
Updated databases are an essential part of your server protection.
Please note that the application may be restarted during the update
process.
Do you want to download the latest databases now? [y]: n
```

Рисунок 8.13 – 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 8.14).

```
Enabling automatic updates of the application databases

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

Рисунок 8.14 – 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 8.15).

```
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 8.15 – Запрос активации антивируса

8.2 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).

8.3 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:

– Укажите нужное значение параметра

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

– Убедитесь, что значение параметра изменено в конфигурационном файле задачи

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

8.4 Управление задачами путем изменения конфигурационного файла

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

– Сохраните параметры задачи в конфигурационный файл:

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

– Откройте созданный конфигурационный файл для редактирования.

– Измените нужный параметр в конфигурационном файле.

– Сохраните изменения в конфигурационном файле.

– Импортируйте в задачу параметры из конфигурационного файла:

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

8.5 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 .

Таблица 3 – Параметры задачи «Обновление»

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

Параметр	Описание	Значение
		SCServer — с установленного в 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

Параметр	Описание	Значение
		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 обновлений в локальной сети или в сети Интернет	Значение по умолчанию: Не задано Содержит адрес HTTP-сервера, на котором расположен раздел с обновлениями или каталог на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS
Enabled	Включение	Значение по умолчанию: Не

Параметр	Описание	Значение
	использования источника обновлений, указанного в параметре URL. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.	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
```

8.6 Настройка расписания задачи «Обновление»

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

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

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

– Откройте созданный конфигурационный файл для редактирования.

– Задайте параметры расписания.

– Сохраните изменения в конфигурационном файле.

– 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
```

9 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.

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 9.1).

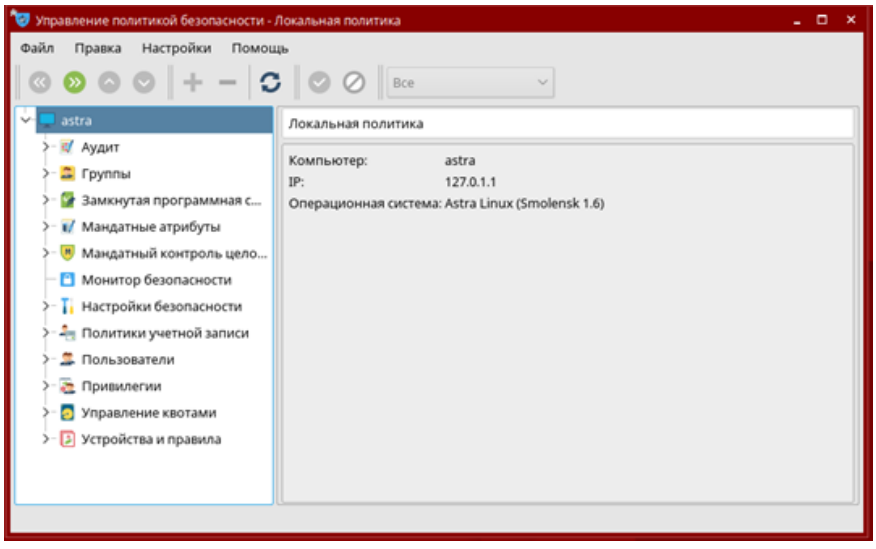


Рисунок 9.1 – Панель управления политикой безопасности

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.

9.1 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:

– если указана специальная запись для пользователя, то используется эта запись;

– 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;

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

– 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 .

Таблица 4 – Перечень протоколируемых событий ОС Astra Linux

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

Разряд	Ключ	Событие	Описание события	Успех	Отказ
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:

– «По умолчанию» (см. Рисунок 9.2) - 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.

– «Группы» (Рисунок 9.3) - список групп с персональными настройками аудита. Двойным щелчком левой кнопки мыши на элементе списка на рабочей панели отображаются настройки аудита соответствующей группы;

– «Пользователи» (см. Рисунок 9.4) - список пользователей с персональными настройками аудита. Двойным щелчком левой кнопки мыши на элементе списка на рабочей панели отображаются настройки аудита соответствующего пользователя.

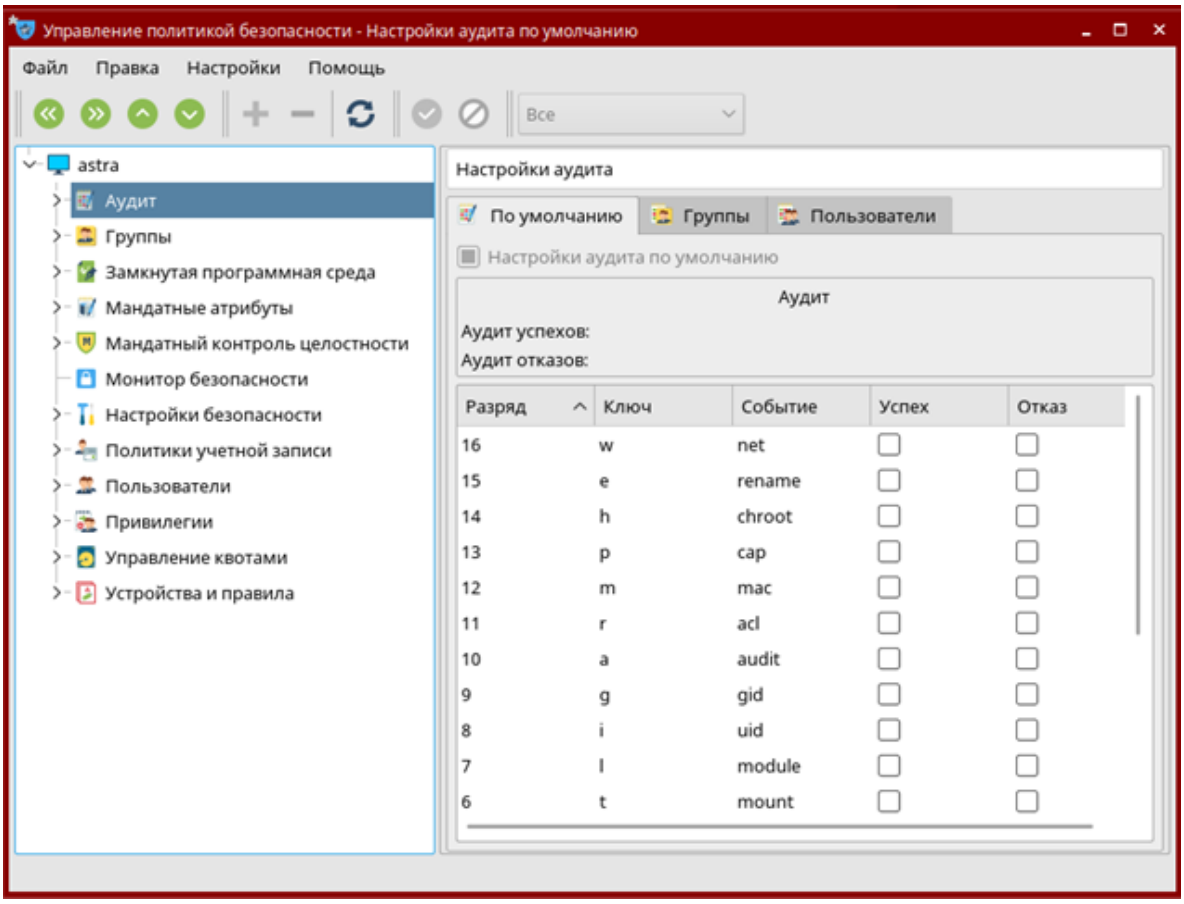


Рисунок 9.2 – Настройка аудита

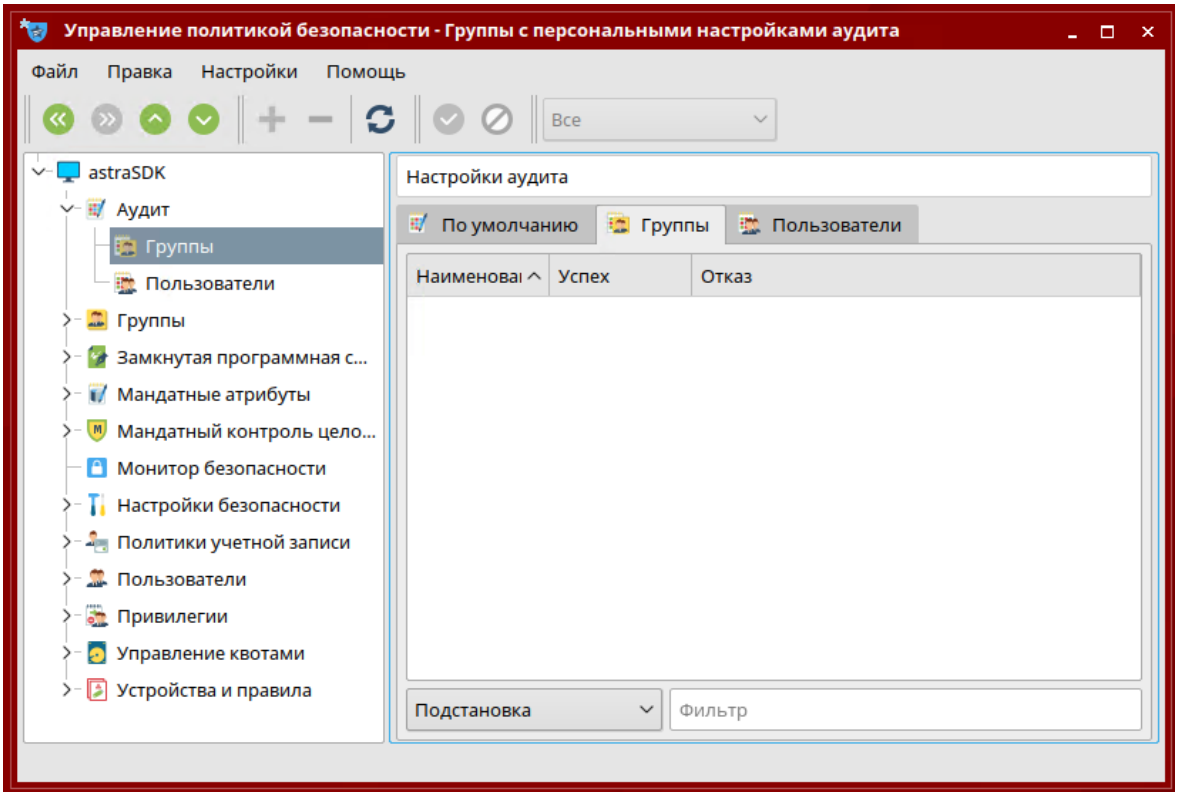


Рисунок 9.3 – Настройка аудита групп

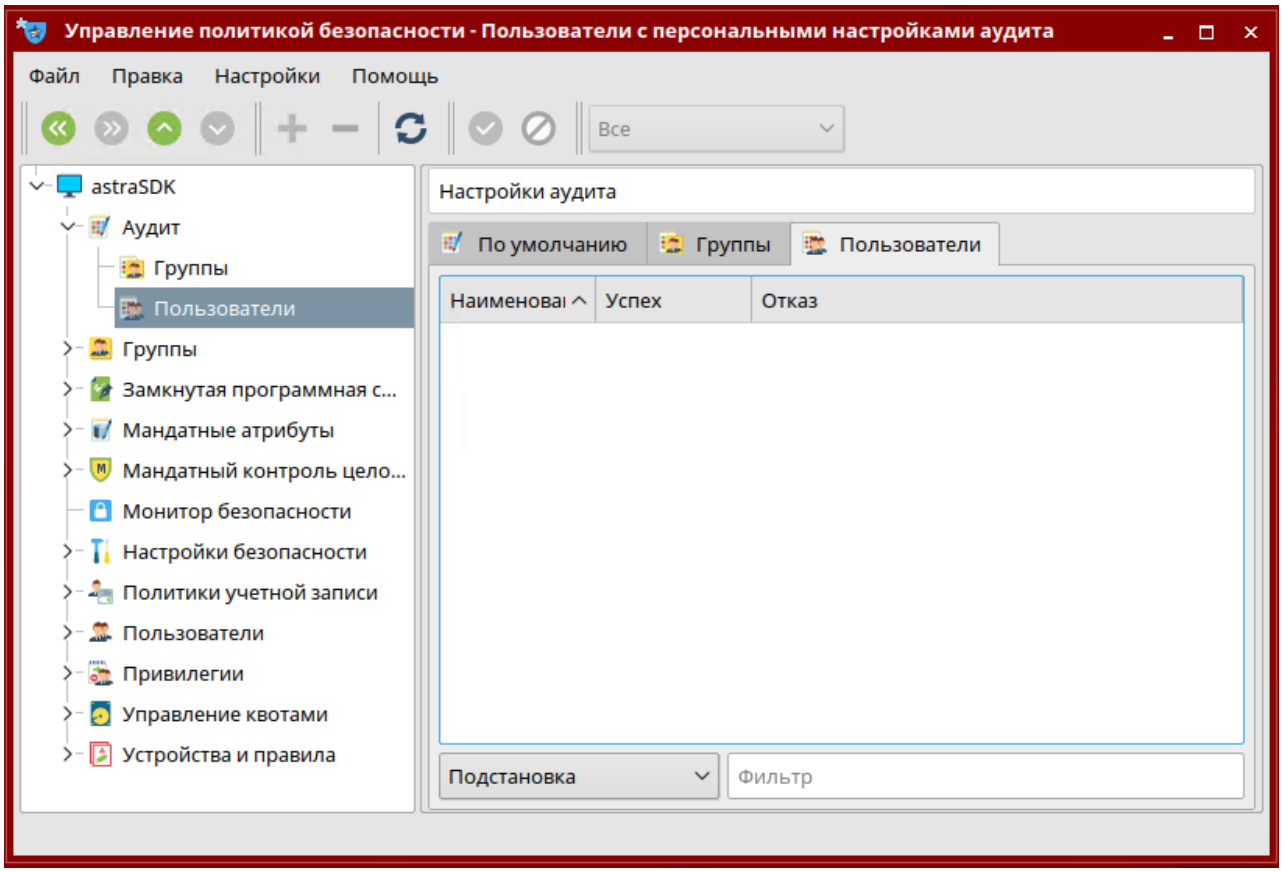


Рисунок 9.4 – Настройка аудита пользователей

9.2 Группы

На рабочей панели (см. Рисунок 9.5) 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 9.6):

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 9.7):

– 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.

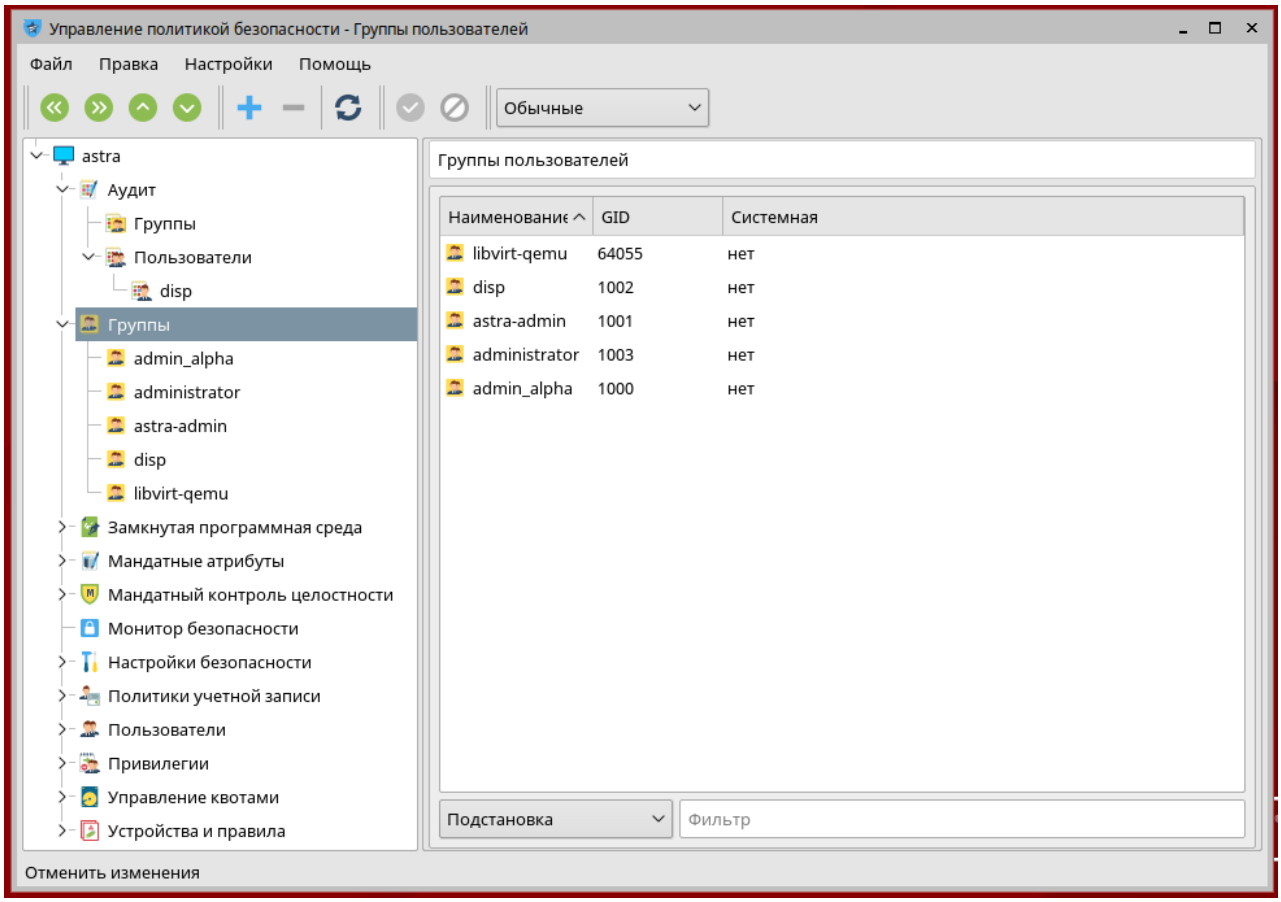


Рисунок 9.5 – Группы пользователей

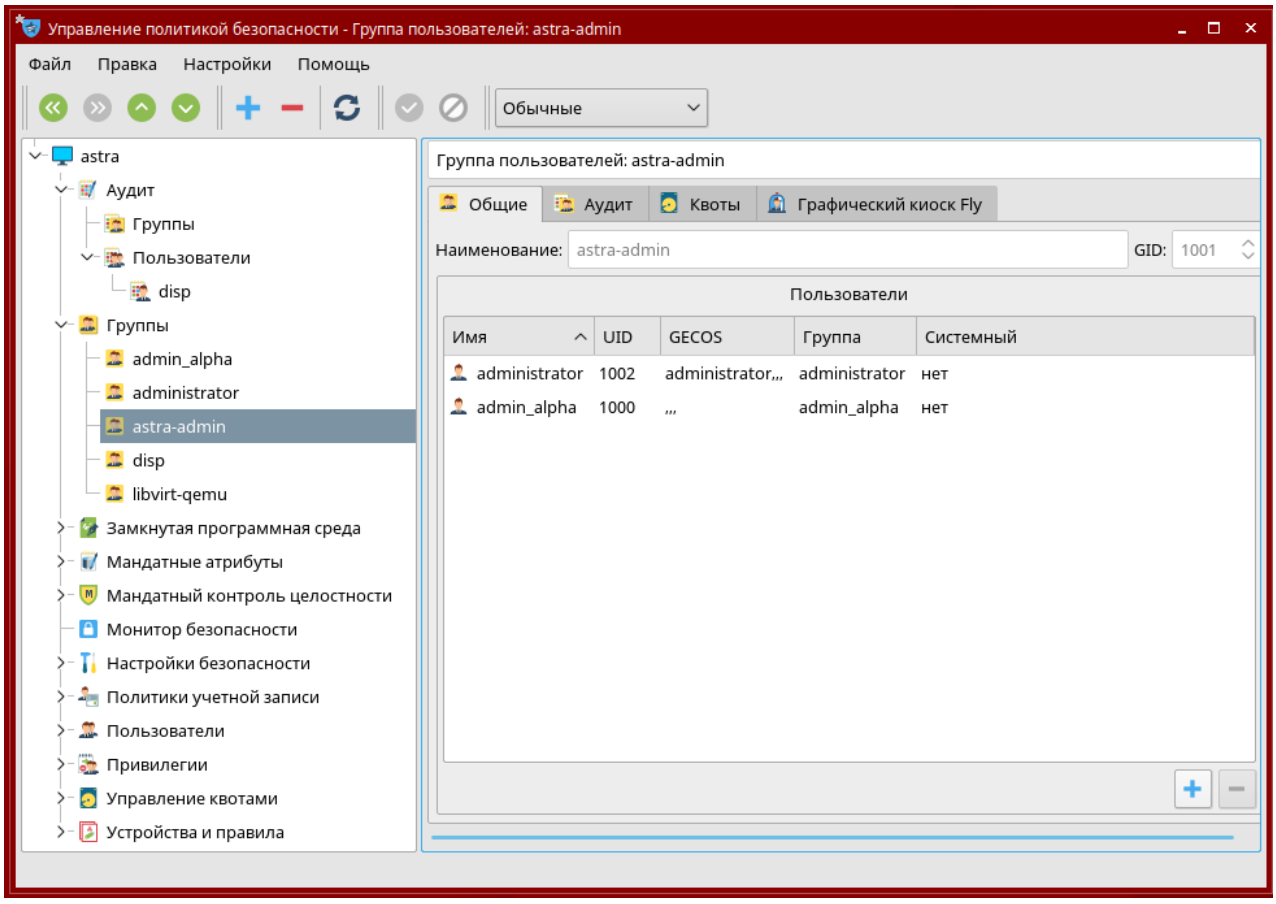


Рисунок 9.6 – Общие настройки группы ползователей

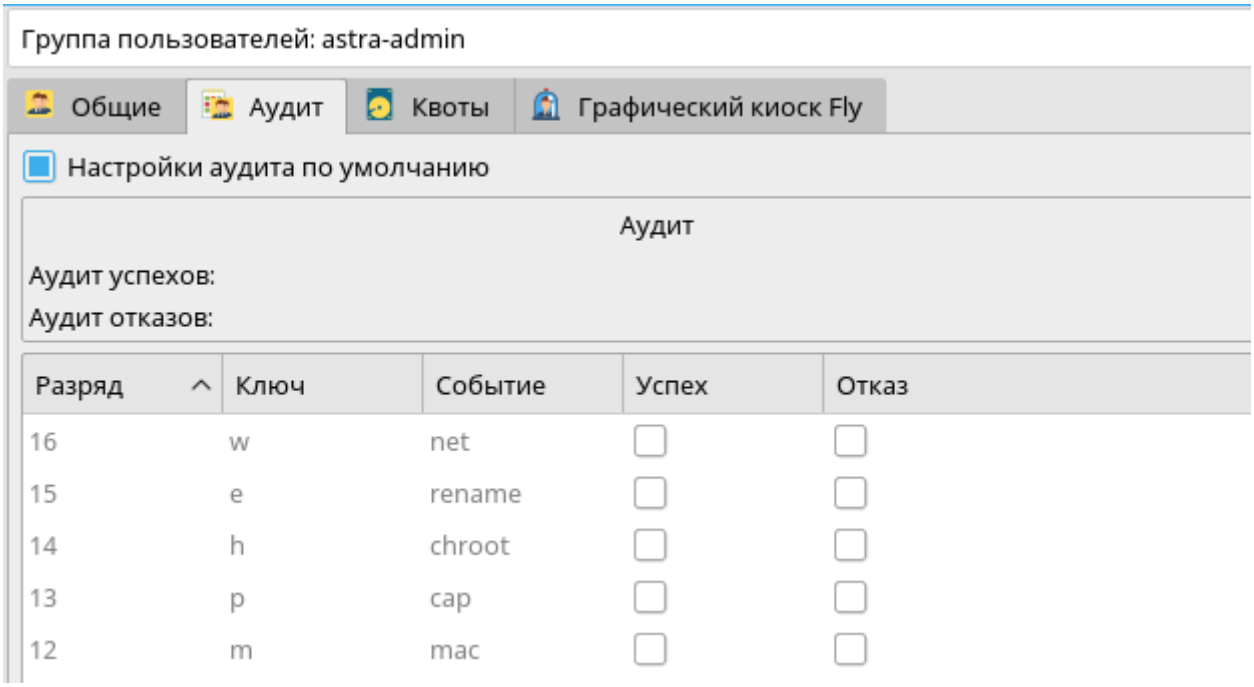


Рисунок 9.7 – Настройки аудита группы пользователей

3) вкладка «Квоты» (см. Рисунок 9.8) - 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»).

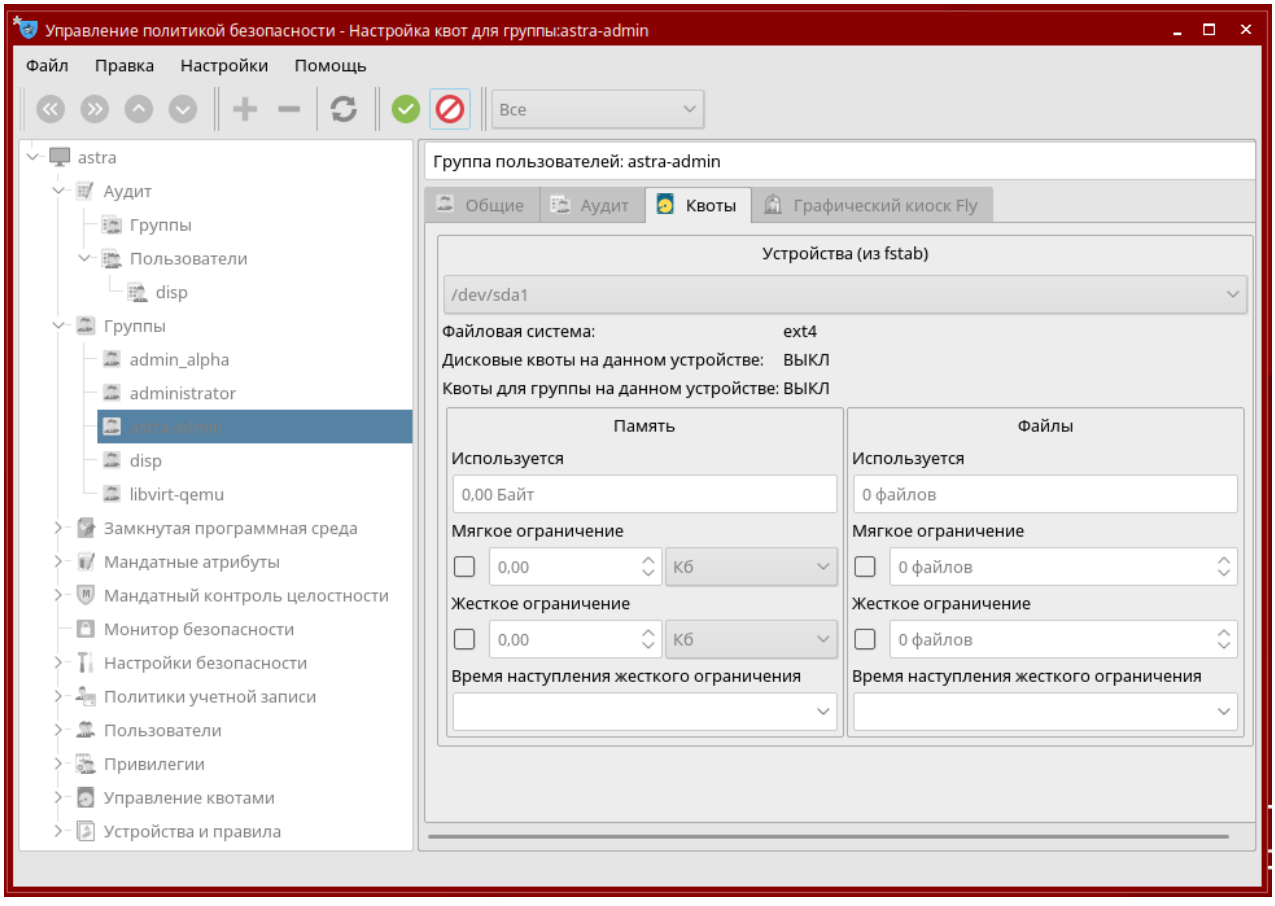


Рисунок 9.8 – Настройка квот групп пользователей

9.3 Пользователи

Войдите в систему как суперпользователь (root), откройте Панель управления (меню «Пуск»). Перейдите в группу «Безопасность» и откройте раздел «Политика безопасности» (см. Рисунок 9.9). Перейдите на узел «Пользователи».

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.

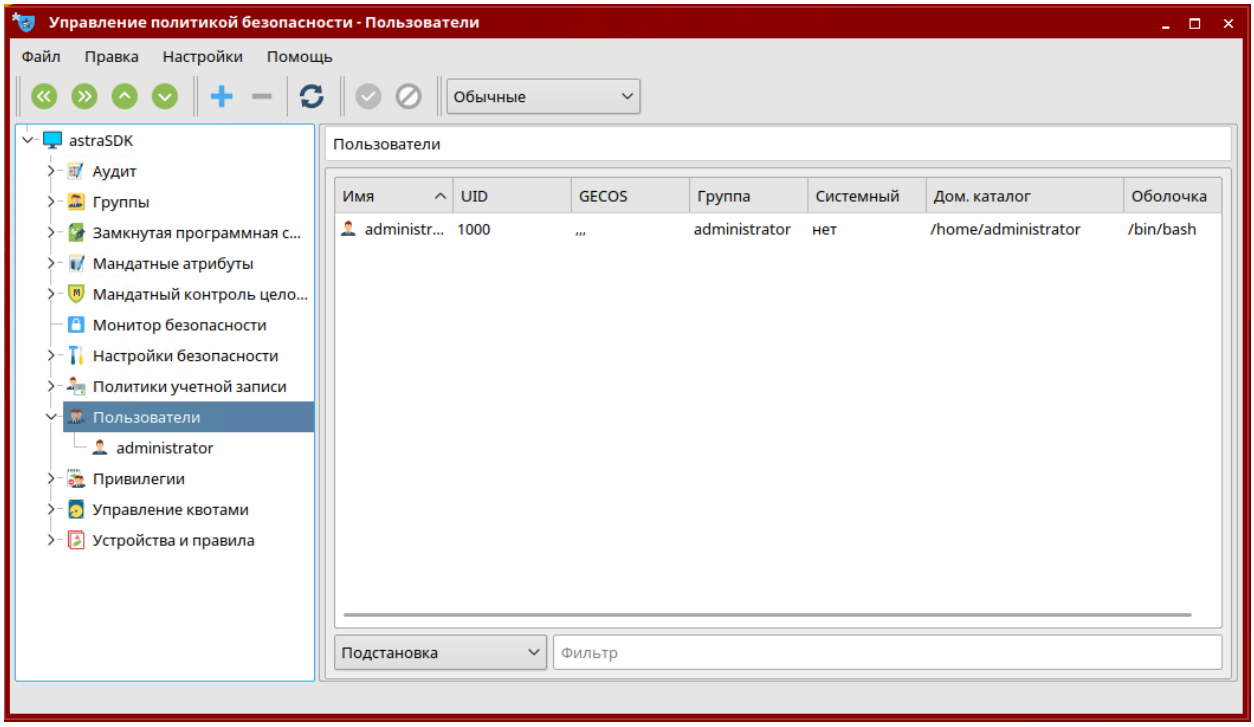


Рисунок 9.9 – Рабочая панель «Пользователи»

Двойным щелчком левой кнопки мыши на имени пользователя на рабочей панели появляются вкладки со значениями настроек политики безопасности для пользователя этой группы (см. Рисунок 9.10):

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.

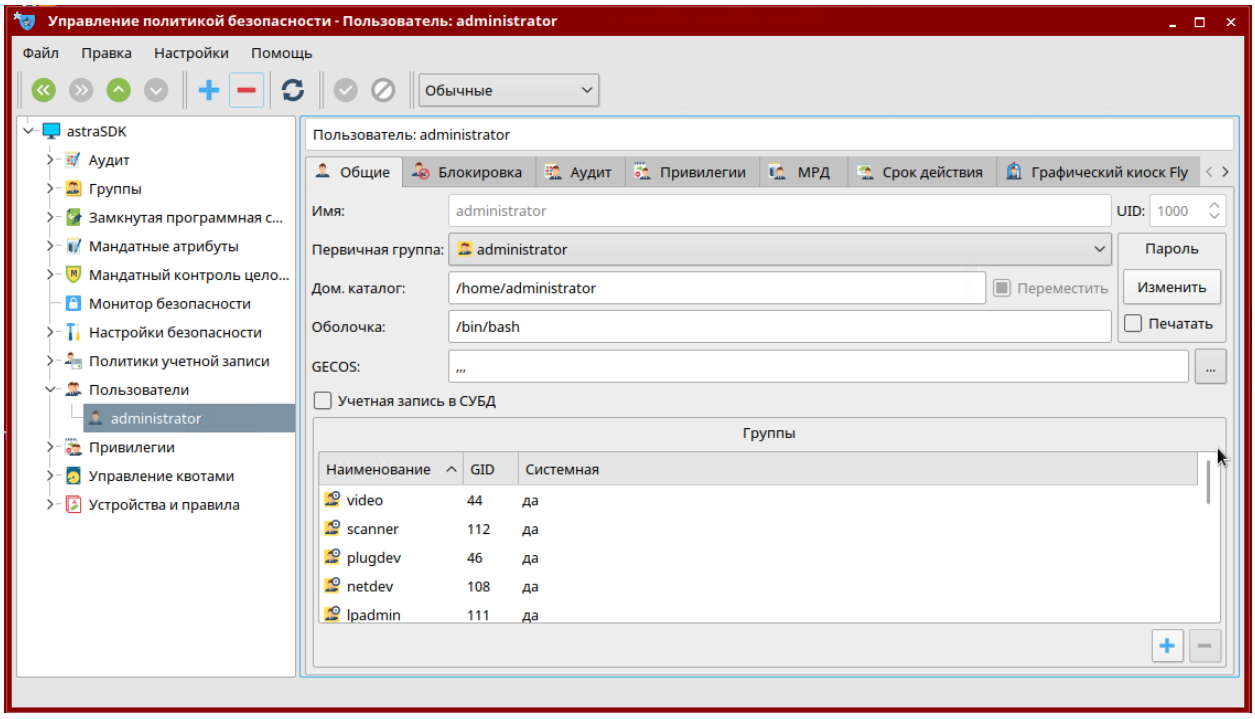


Рисунок 9.10 – Общие свойства пользователя

2) вкладка «Блокировка» (см. Рисунок 9.11)

– «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;

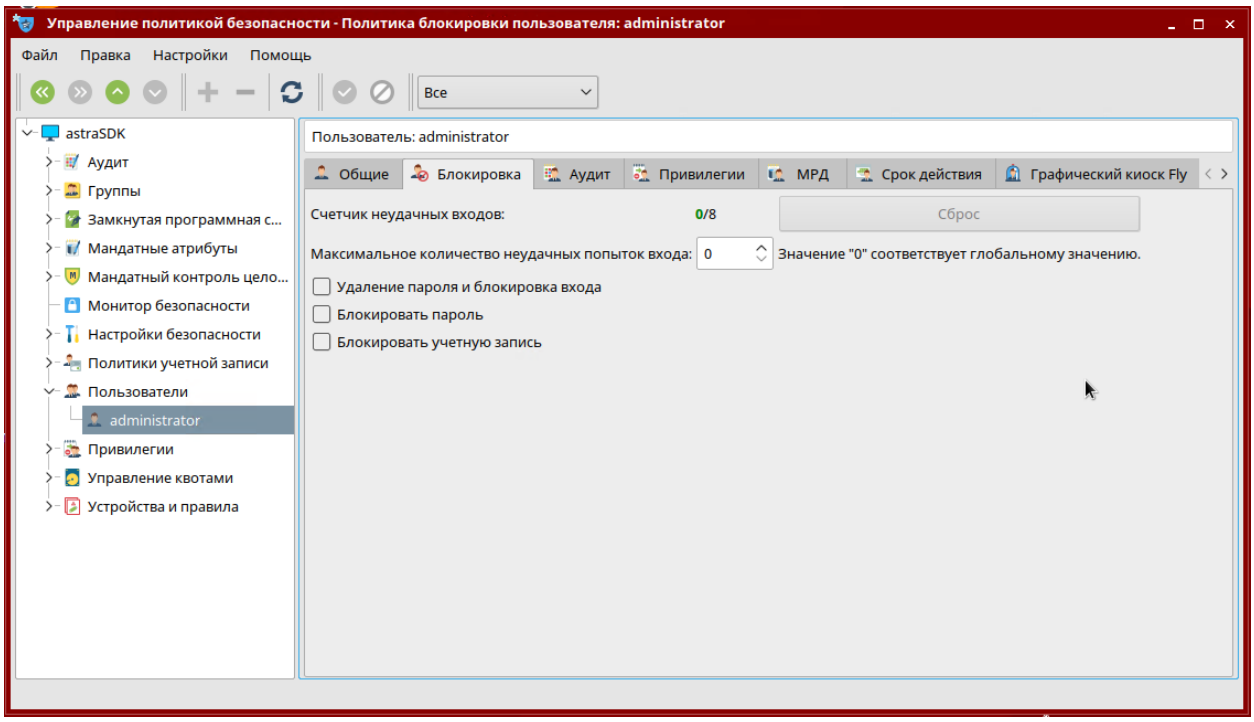


Рисунок 9.11 – Вкладка «Блокировка»

3) вкладка «Аудит» - настройки аудита пользователя (см. Рисунок 9.12):

– 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 9.13). 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.

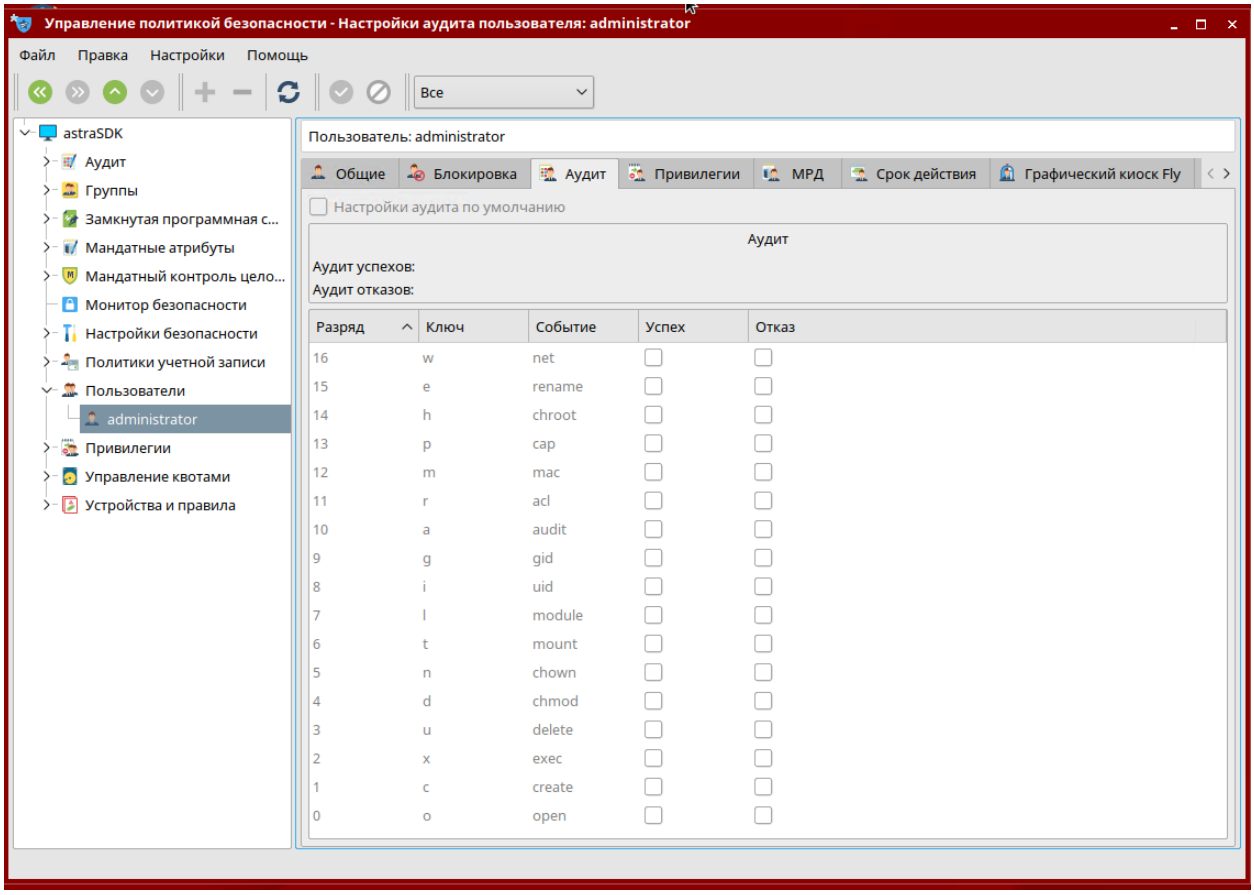


Рисунок 9.12 – Настройки аудит пользователя

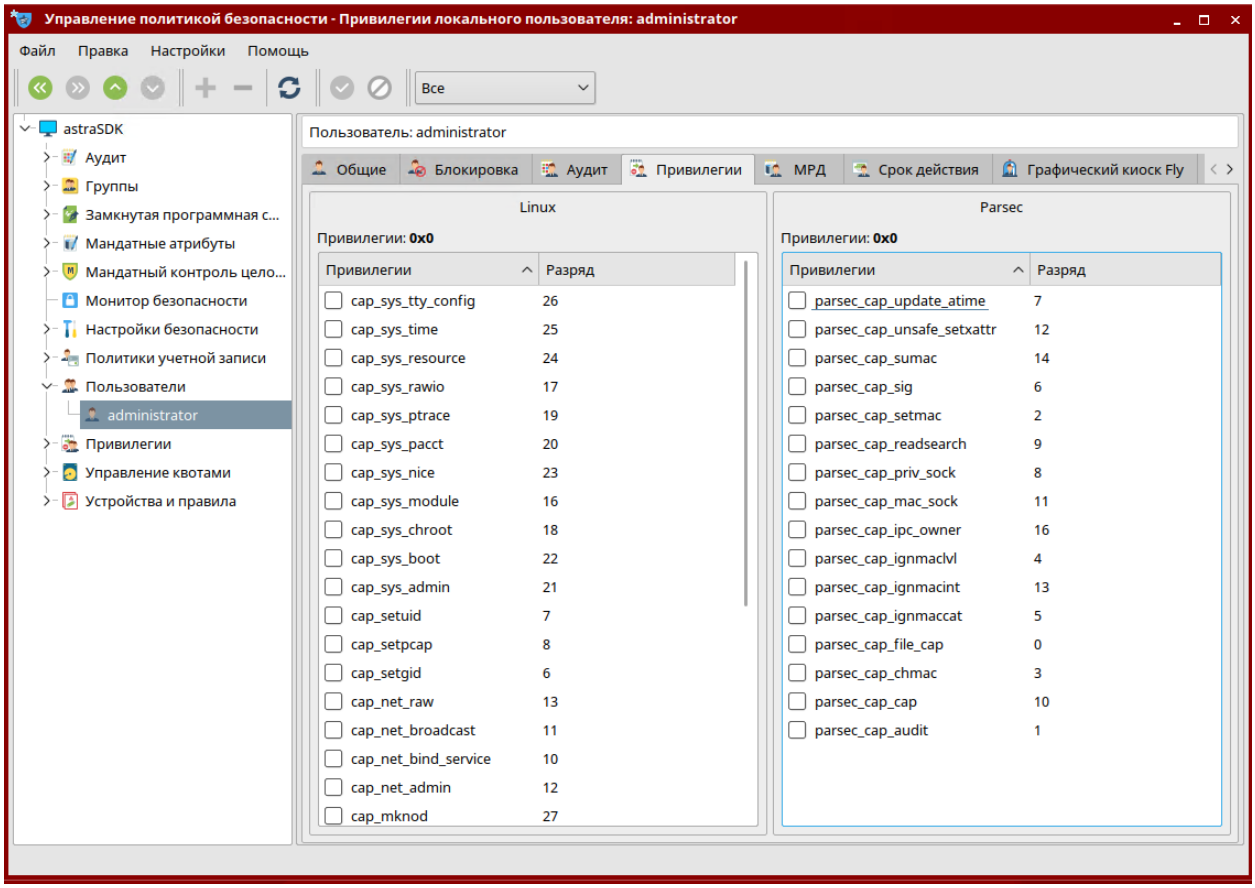


Рисунок 9.13 – Настройки Linux- и Parsec-привелегий ползователя

5) Вкладка «МРД» (мандатное разграничение доступа) (см. Рисунок 9.14). 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 9.15). 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.

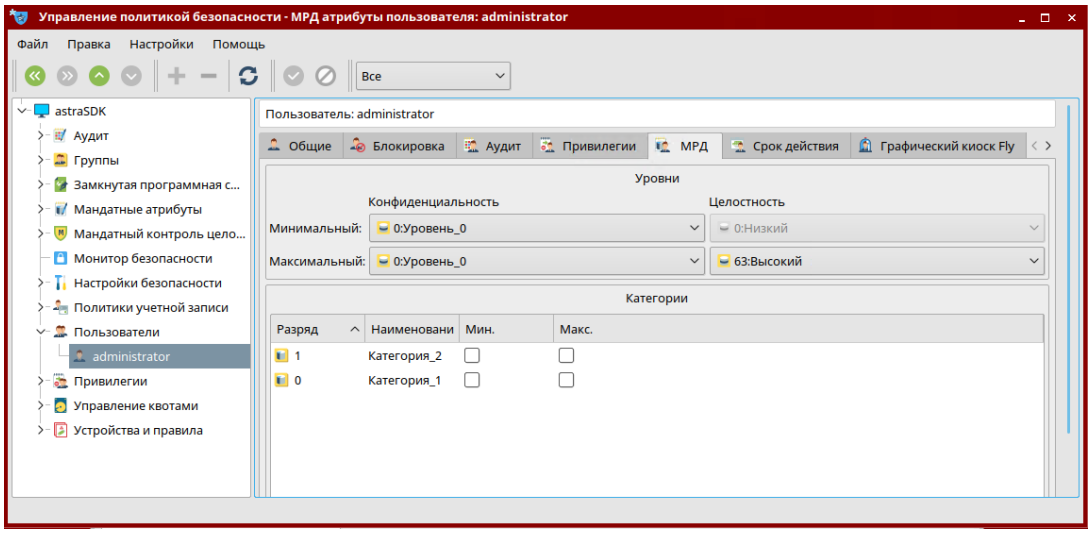


Рисунок 9.14 – Мандатное разграничение доступа для пользователя

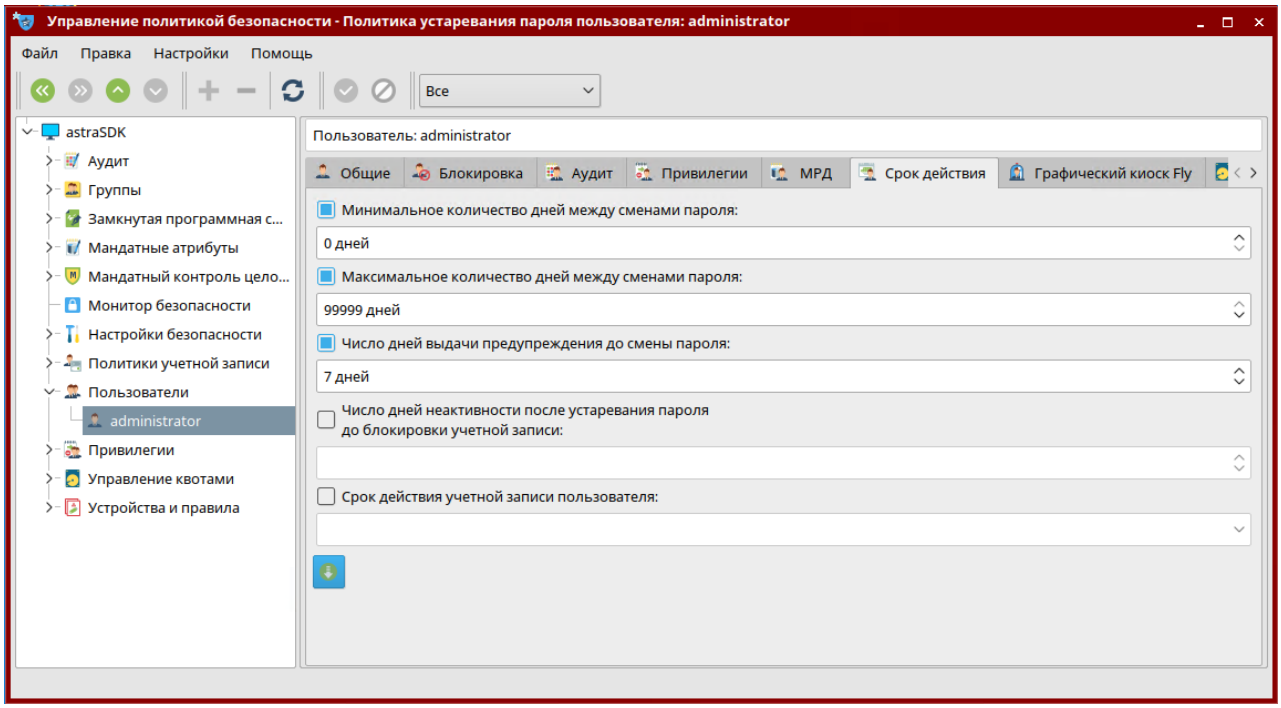


Рисунок 9.15 – Срок действия пароля пользователя

7) Вкладка «Графический киоск Fly» (см. Рисунок 9.16) 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 9.17). 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).

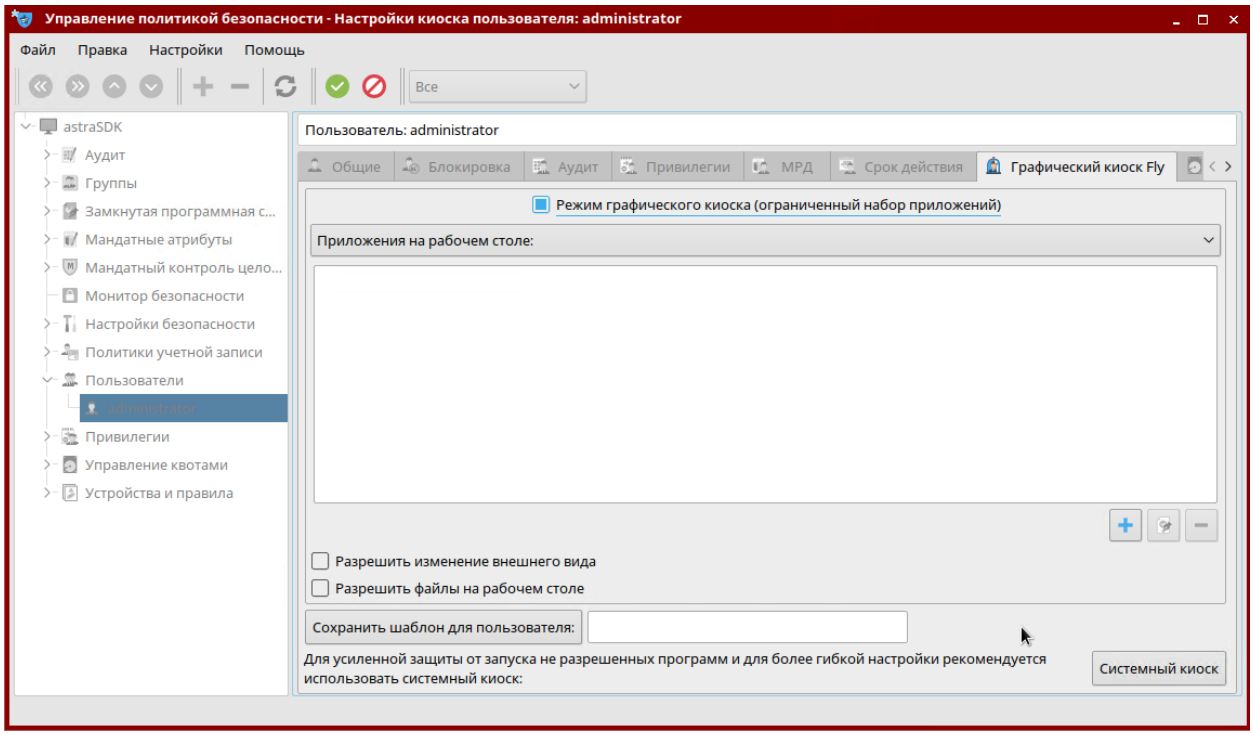


Рисунок 9.16 – Настройка графического киоска

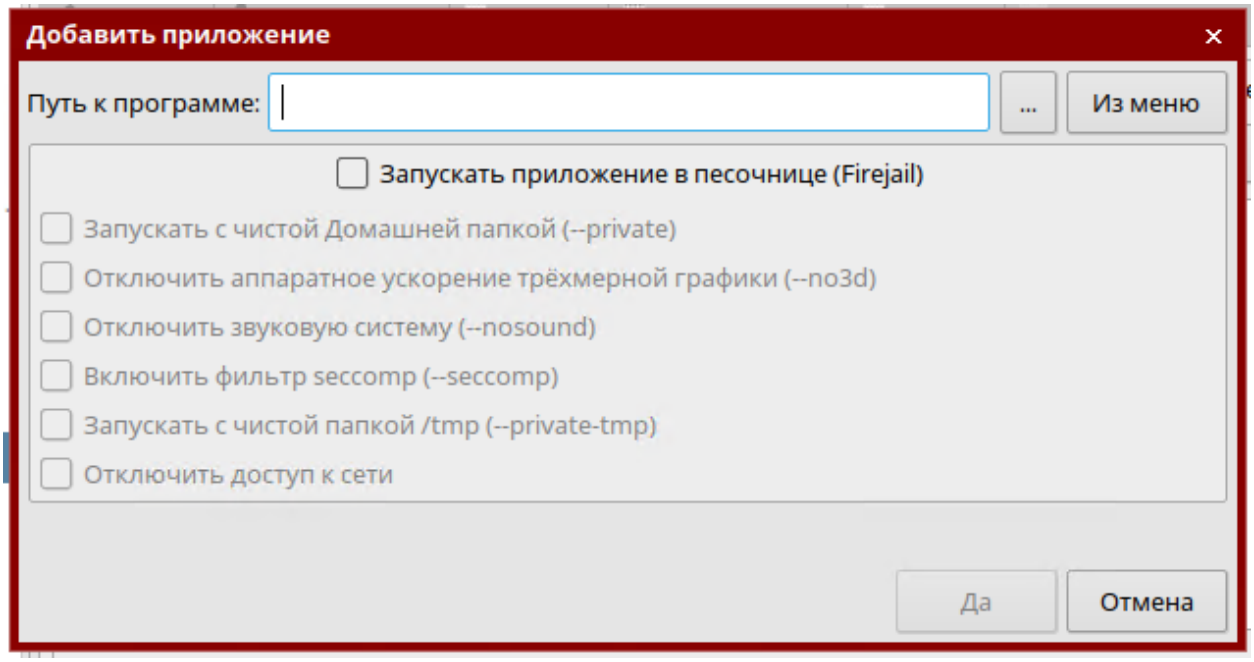


Рисунок 9.17 – Окно для установки имени программы

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».

9.4 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  RMSIZEROTYPE MOUNTPOINT

sda    8:0    0 20G  0 disk
```

```
├─sda2 8:2    0 1K0 part
├─sda5 8:5    0 1022M  0 part [SWAP]
├─sda3 8:3    0 7.9G0 part
└─sda1 8:1    0 9G0 part /
sr0    11:0   1 1024M  0 rom
sdb    8:32   1 14.9G  0 disk
├─sdb2 8:34   1 2.3M0 part
└─sdb1 8:33   1 1.7G0 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 9.18).

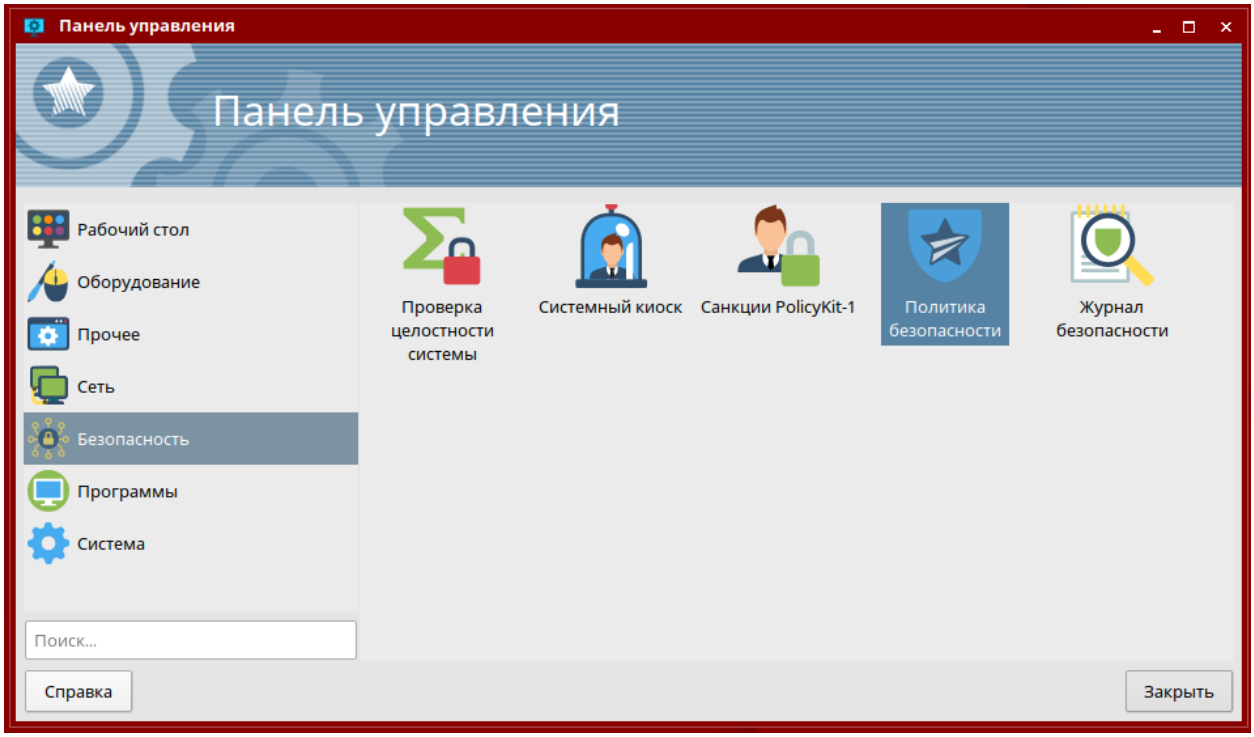


Рисунок 9.18 – Панель управления

Далее следует выбрать в дереве настроек политики безопасности, которое отображается на боковой панели навигации, пункты Устройства и правила → Устройства (см. Рисунок 9.19).

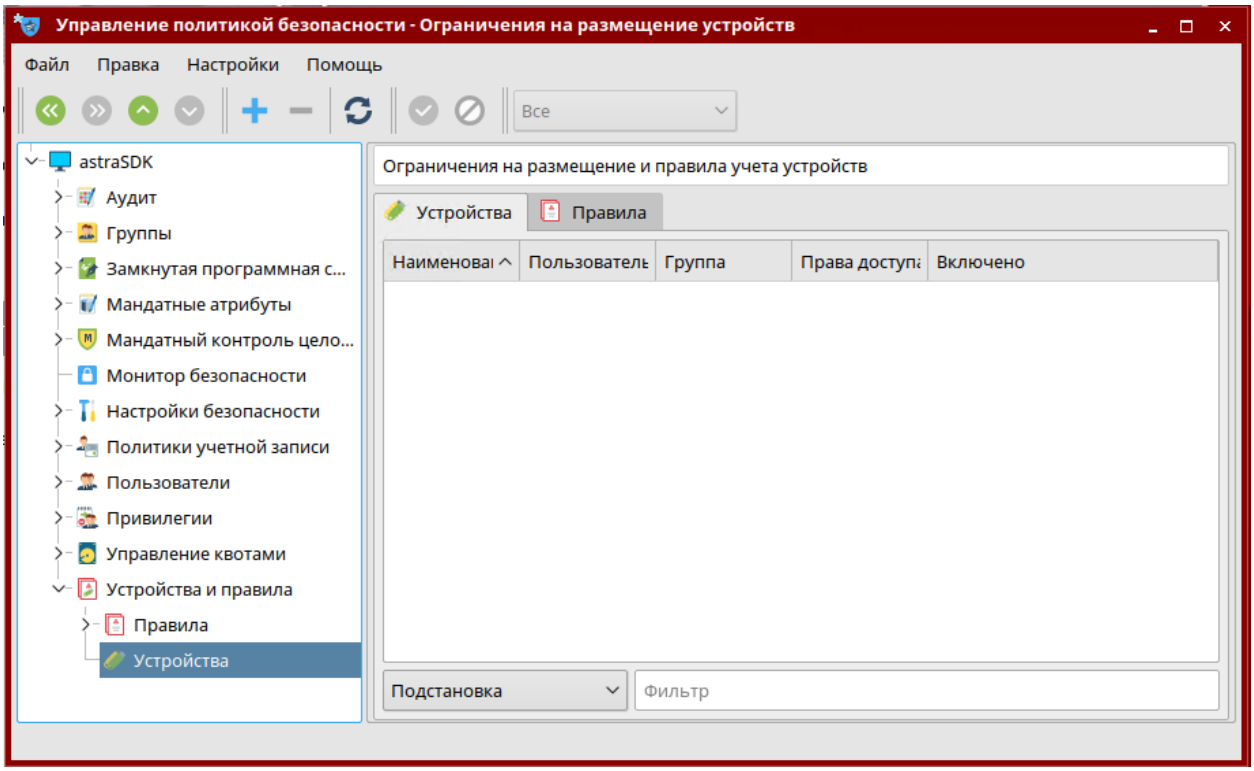


Рисунок 9.19 – Рабочая панель «Устройства»

Нажмите на панели инструментов кнопку  [Создать новый элемент]. Дождитесь появления графического окна «Добавить устройство» (см. Рисунок 9.20) и подключите USB-накопитель к USB-порту компьютера.

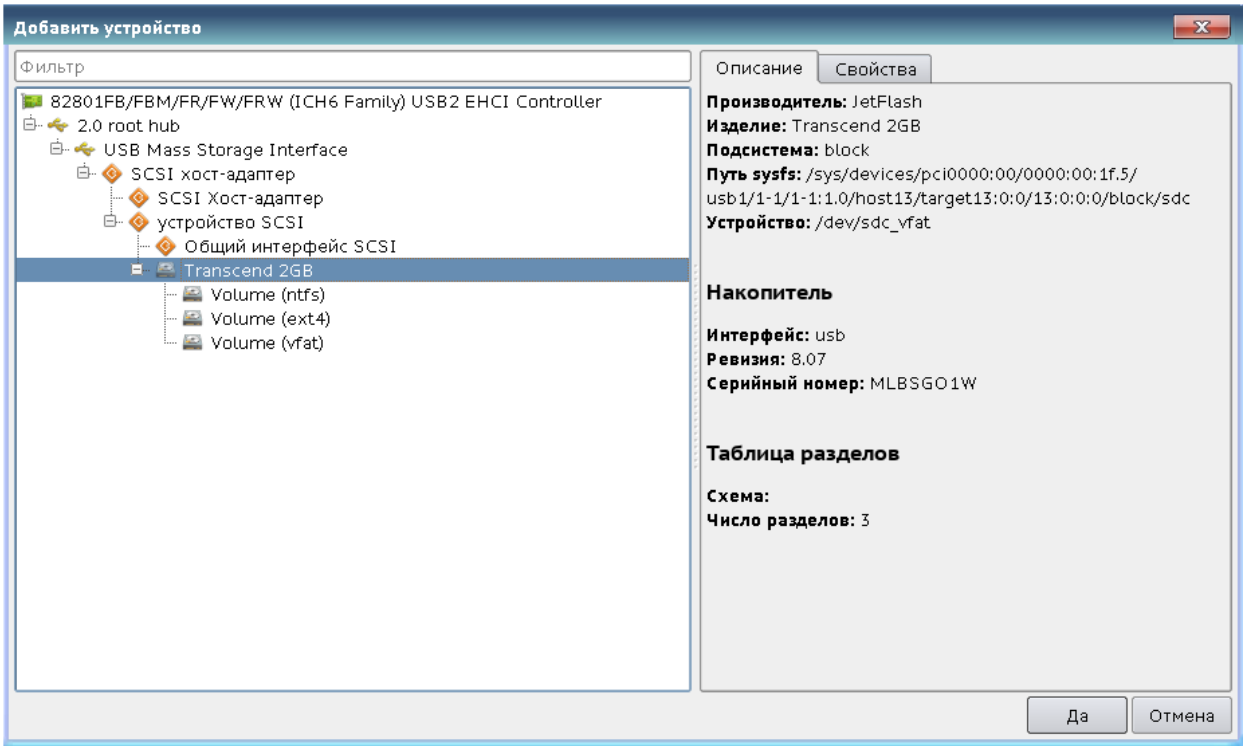


Рисунок 9.20 – Окно регистрации нового устройства

Перейти к вкладке «Общие» (Рисунок 9.21). 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.

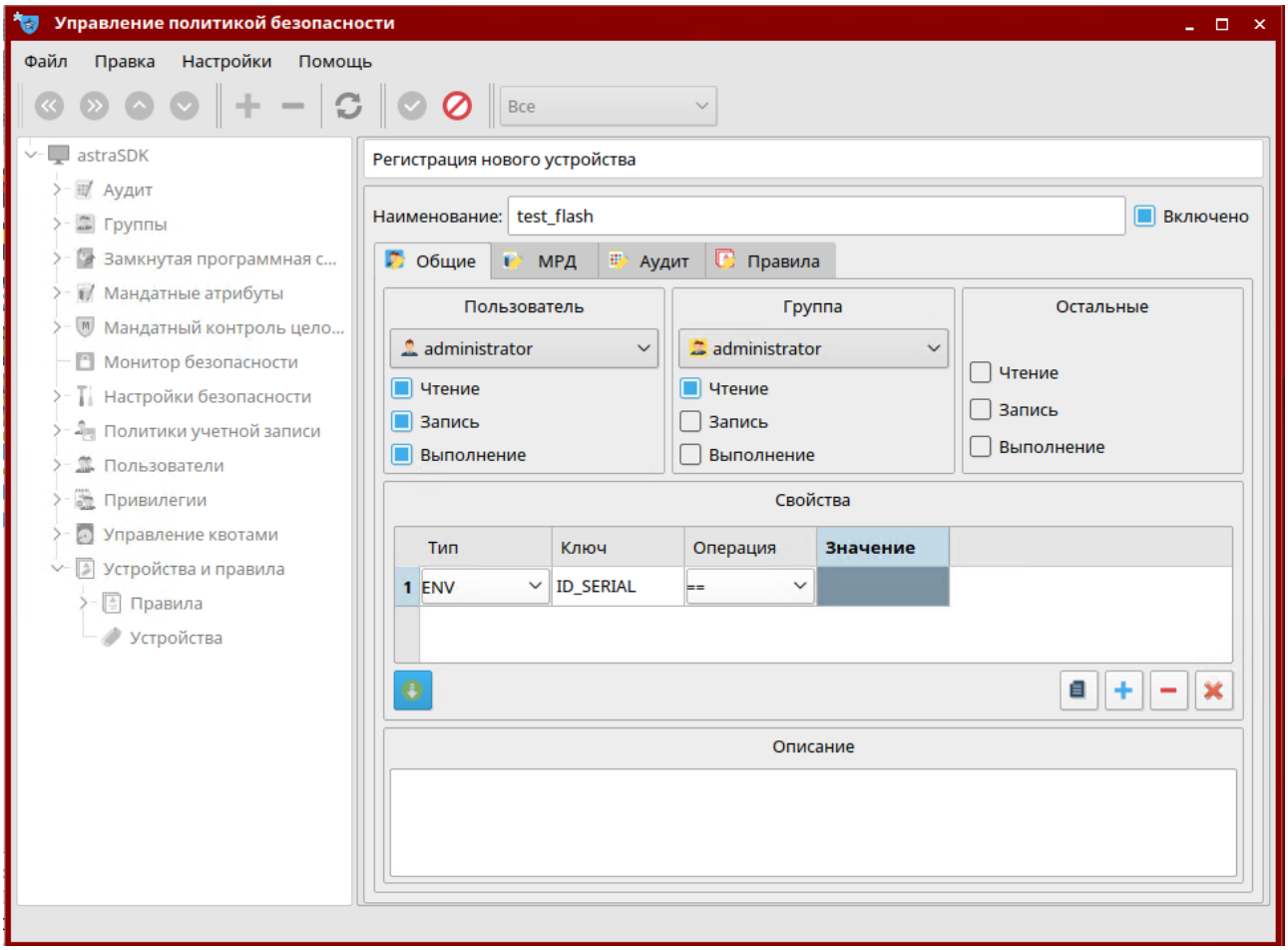


Рисунок 9.21 – Общие свойства нового устройства

Далее следует перейти к вкладке «МРД», выбрать мандатный уровень из выпадающего списка, далее указать набор мандатных категорий (Рисунок 9.22).

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"
```

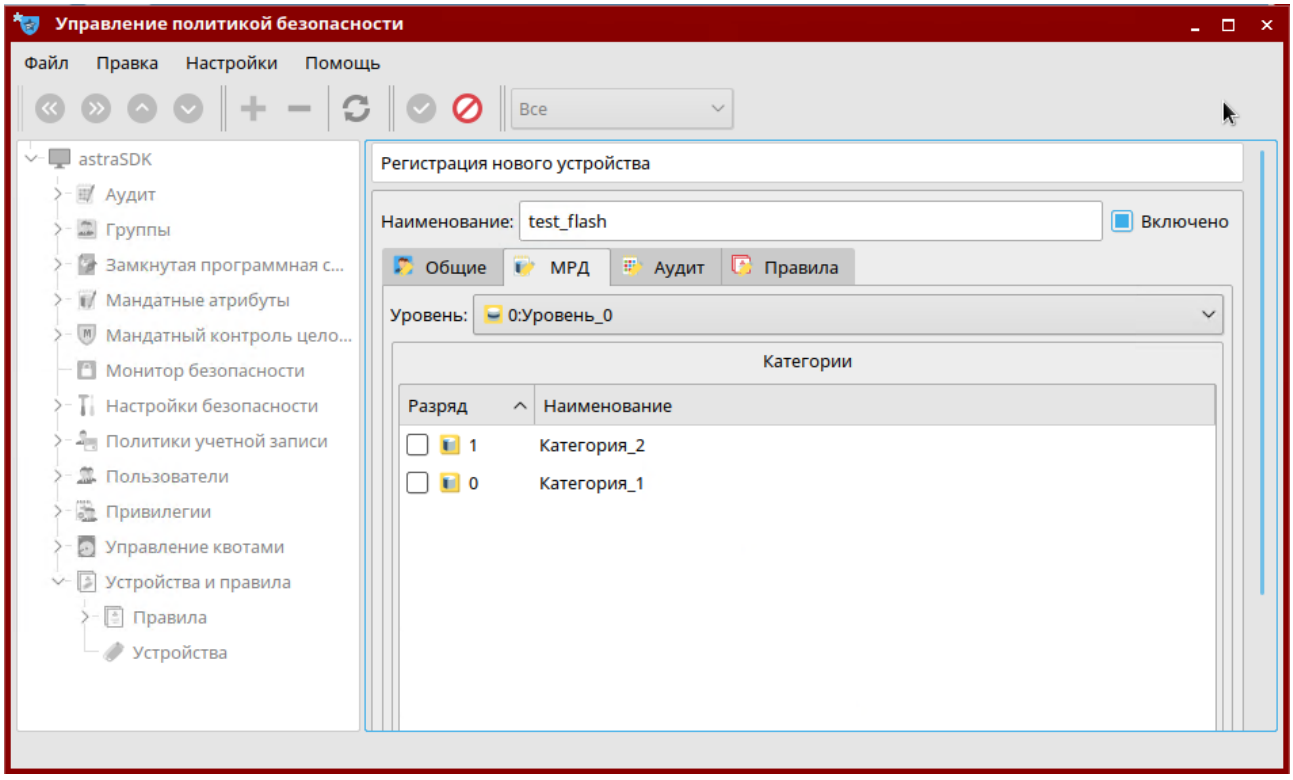


Рисунок 9.22 – Мандатый доступ

Далее следует назначить параметры регистрации событий, связанных с устройством, для этого во вкладке «Аудит» необходимо выбрать событие и результат (успех, отказ), подлежащие регистрации (Рисунок 9.23).

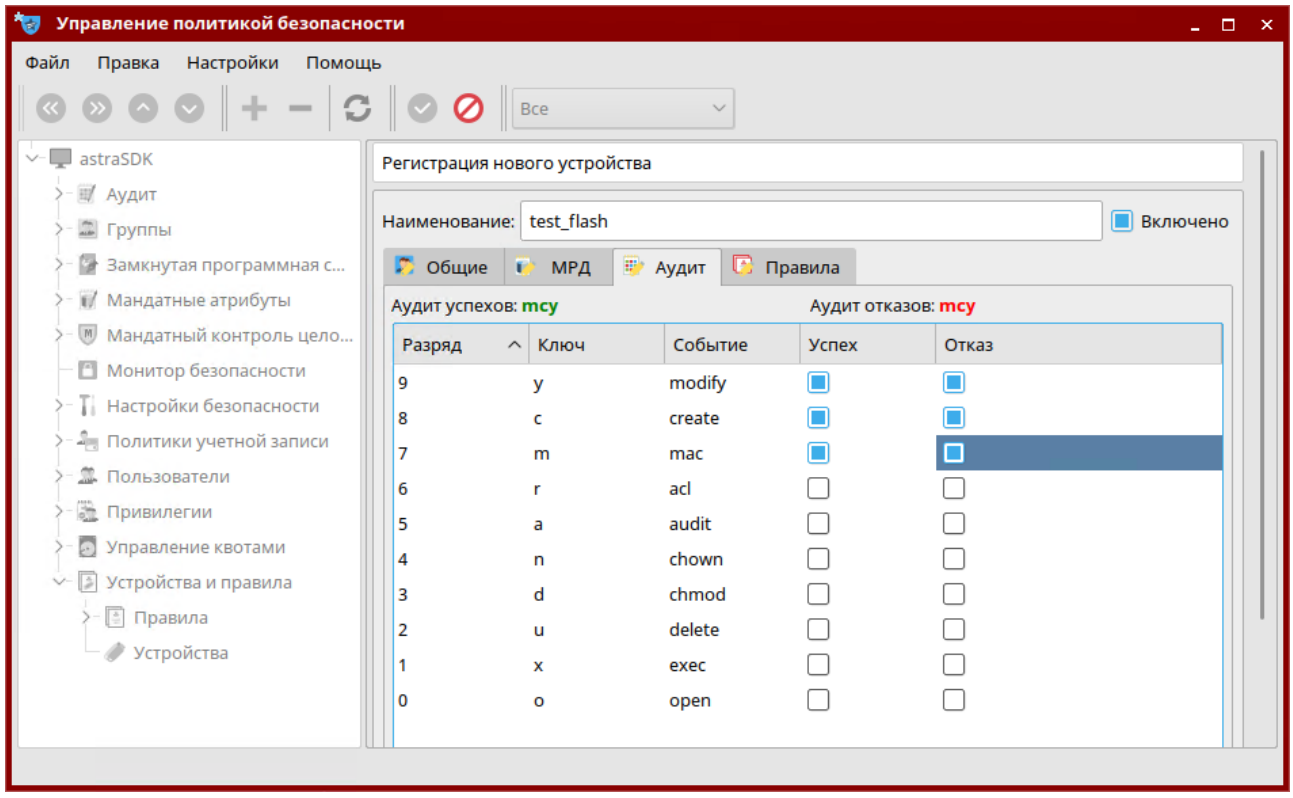


Рисунок 9.23 – Параметры аудита сообщений, связанных с USB-накопителем

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.

10 Общие настройки безопасности

10.1 Настройка электропитания для выключения перехода в спящий режим при бездействии

Перейдите в Панели управления в группу «Рабочий стол». Откройте раздел «Оформление Fly» и перейдите в группу «Блокировка» и снимите флаг «Блокировать экран» (Рисунок 10.1).

Нажмите кнопку «Настройка электропитания» и в открывшемся окне снимите флаг «Выключение монитора» (Рисунок 10.2).

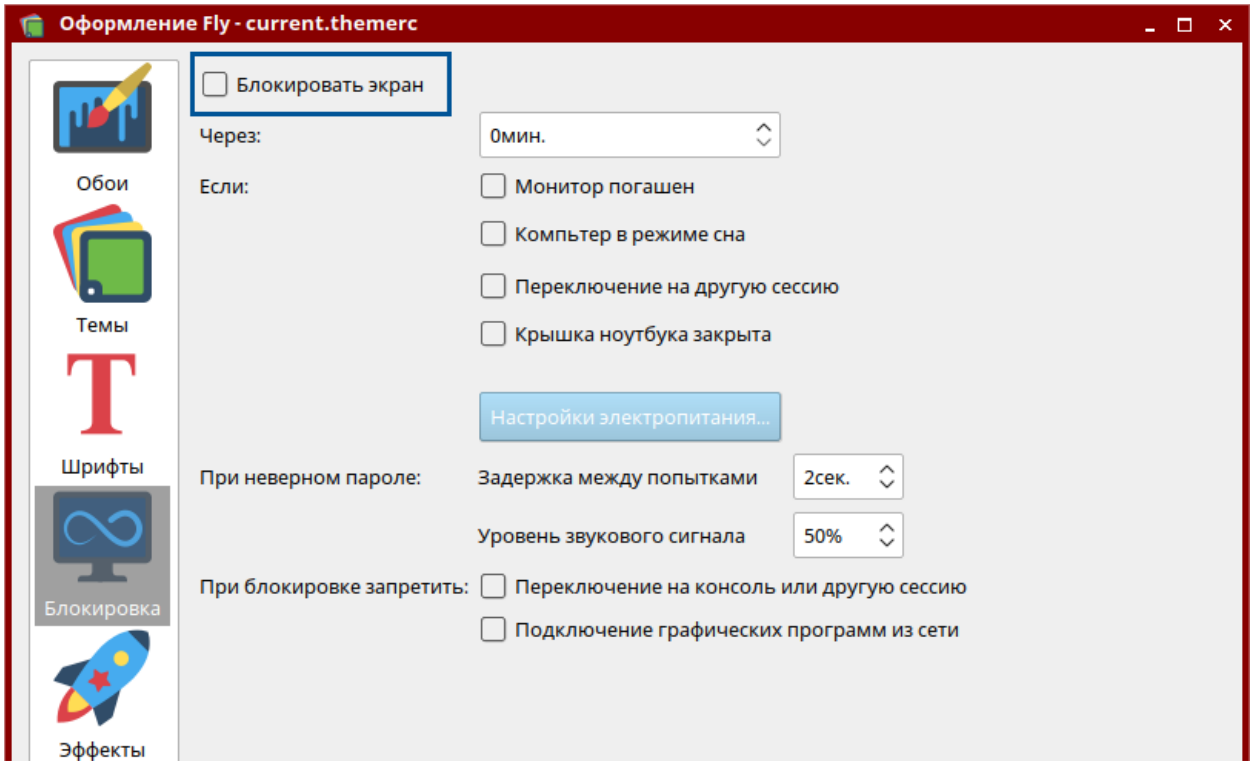


Рисунок 10.1 – Раздел «Оформление Fly». Блокировка экрана

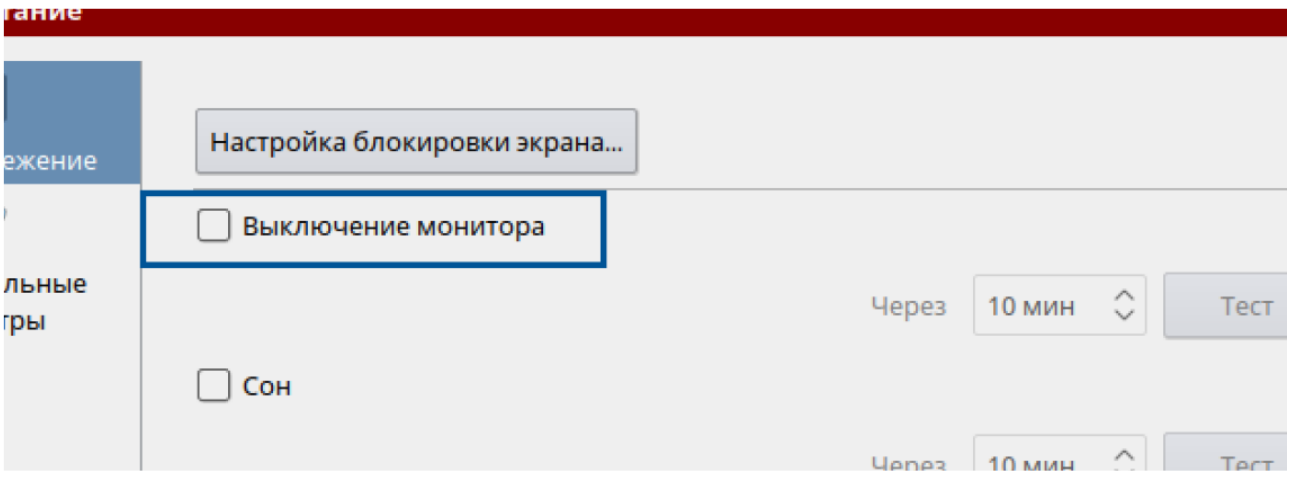


Рисунок 10.2 – Раздел «Оформление Fly». Настройки электропитания. Выключение монитора

10.2 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
```

10.3 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
```

10.4 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.

11 Контроль целостности

11.1 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 11.1).

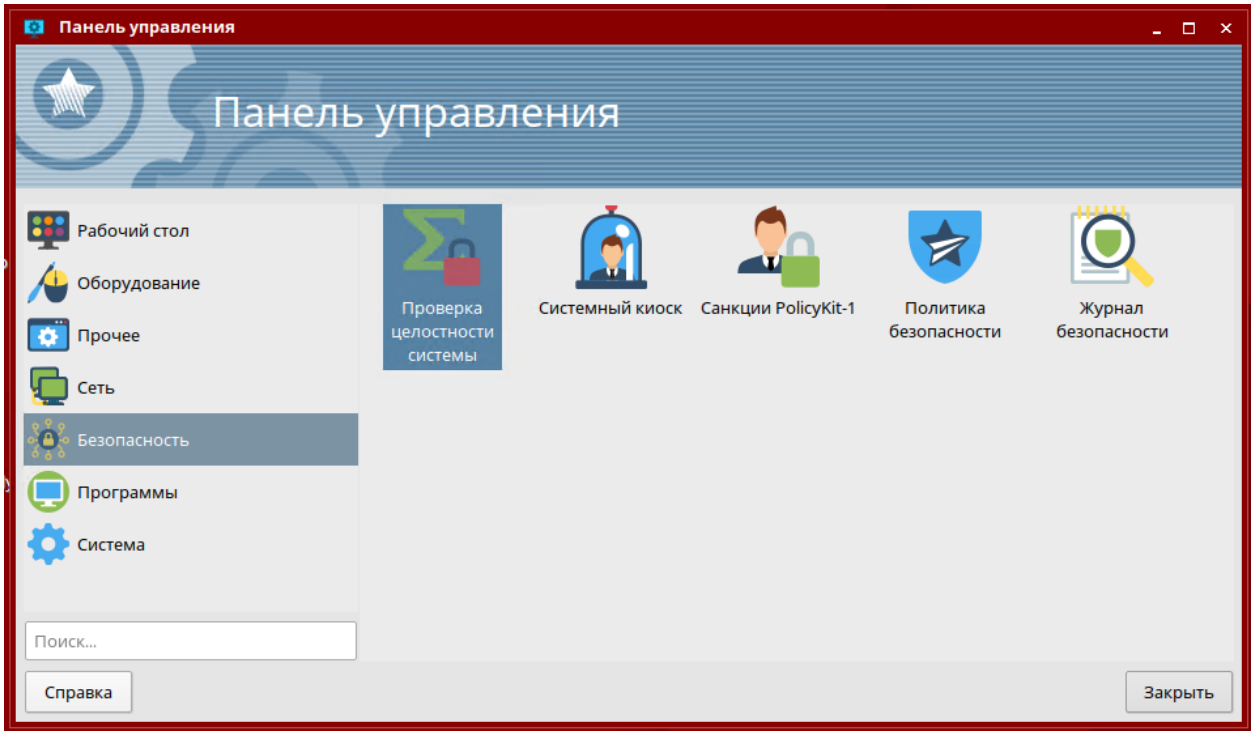


Рисунок 11.1 – Панель управления

После запуска программы открывается окно на вкладке «Параметры проверки целостности» (см. Рисунок 11.2). В данной вкладке устанавливаются параметры проверки целостности системы и параметры сохранения отчета в файл.

Во вкладке «Состояние» отображается результат проверки целостности (Рис. 2). 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.

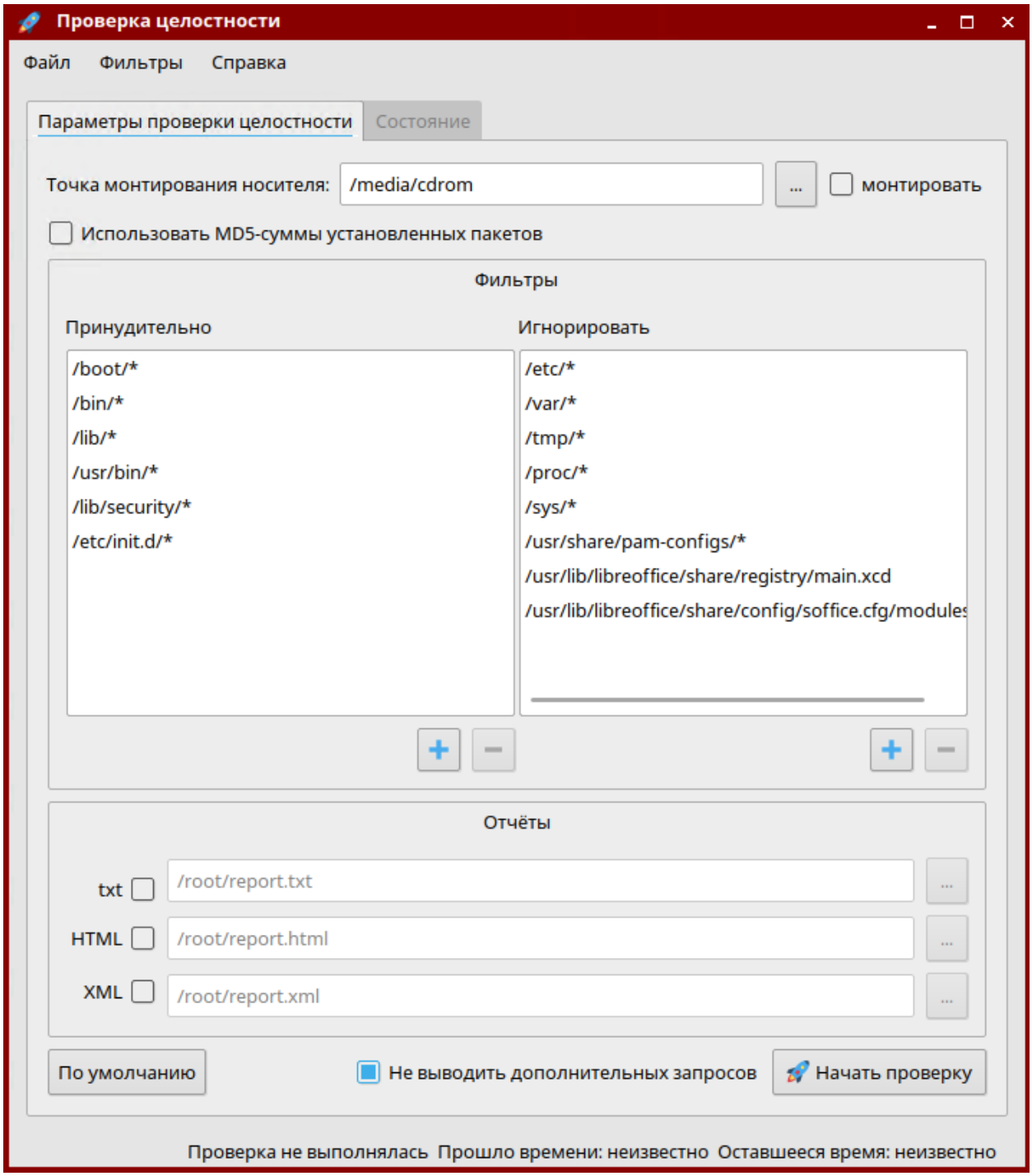


Рисунок 11.2 – Рабочая панель программы проверки целостности

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 11.3). 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.

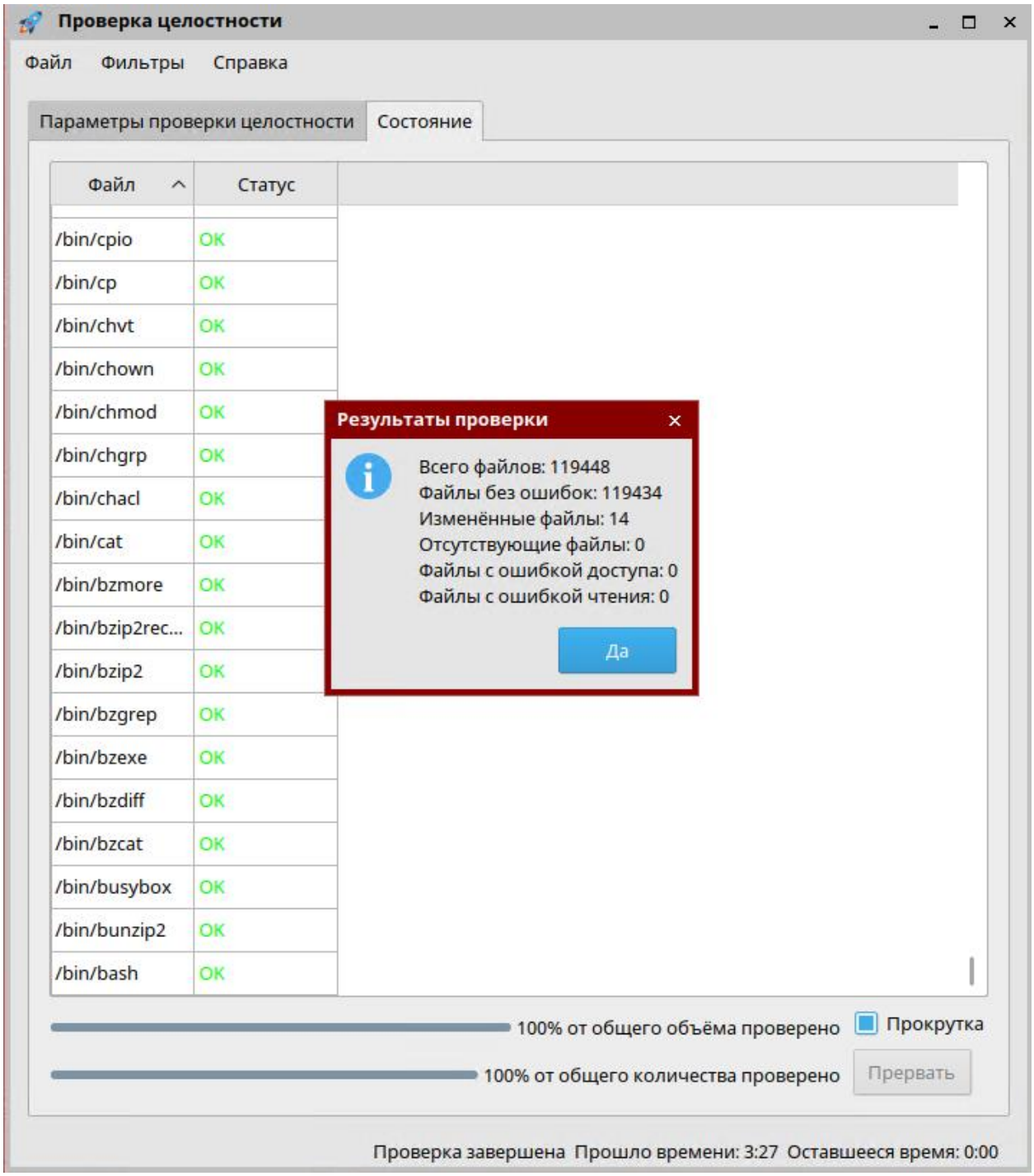


Рисунок 11.3 – Вкладка «Состояние»

11.2 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:

– войти в систему от имени администратора с высоким уровнем целостности;

– запустить программу «Терминал Fly»;

– выполнить команду;

```
sudo afick -i
```

– 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.

```
/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.

11.3 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:

- зарегистрируйтесь в системе как суперпользователь (root);
- перейдите в нужный каталог командой cd /opt/kaspersky/kesl/bin;
- выполнить команду.

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

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
```

12 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 12.1)

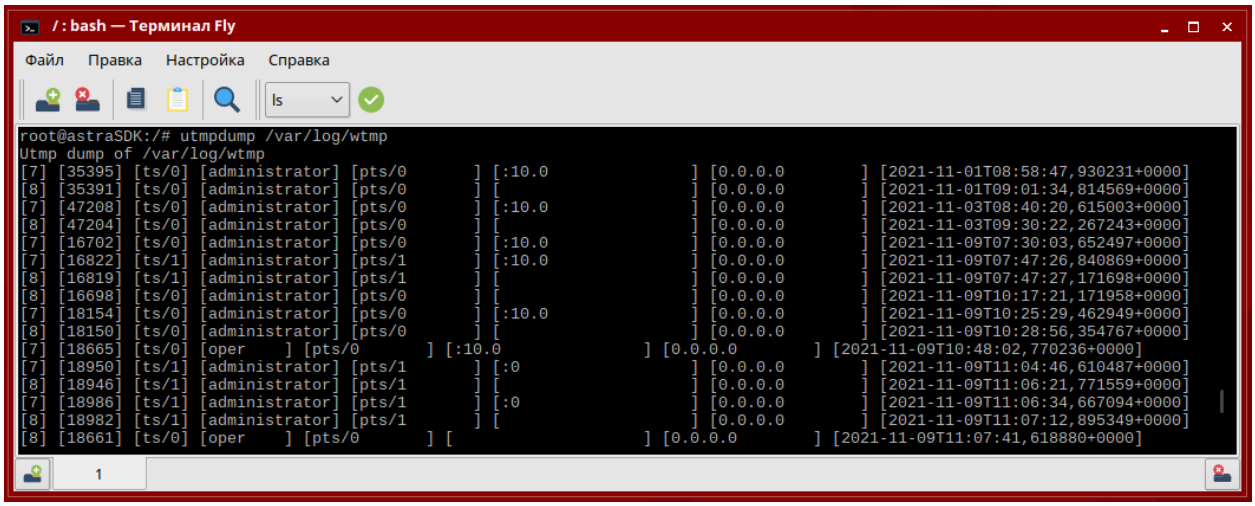


Рисунок 12.1 – Журнал записи входа в систему

Журналы можно открыть любой утилитой для просмотра текста, например, less, cat, tail. Откроем файл журнала /var/log/auth.log (см. Рисунок 12.)

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

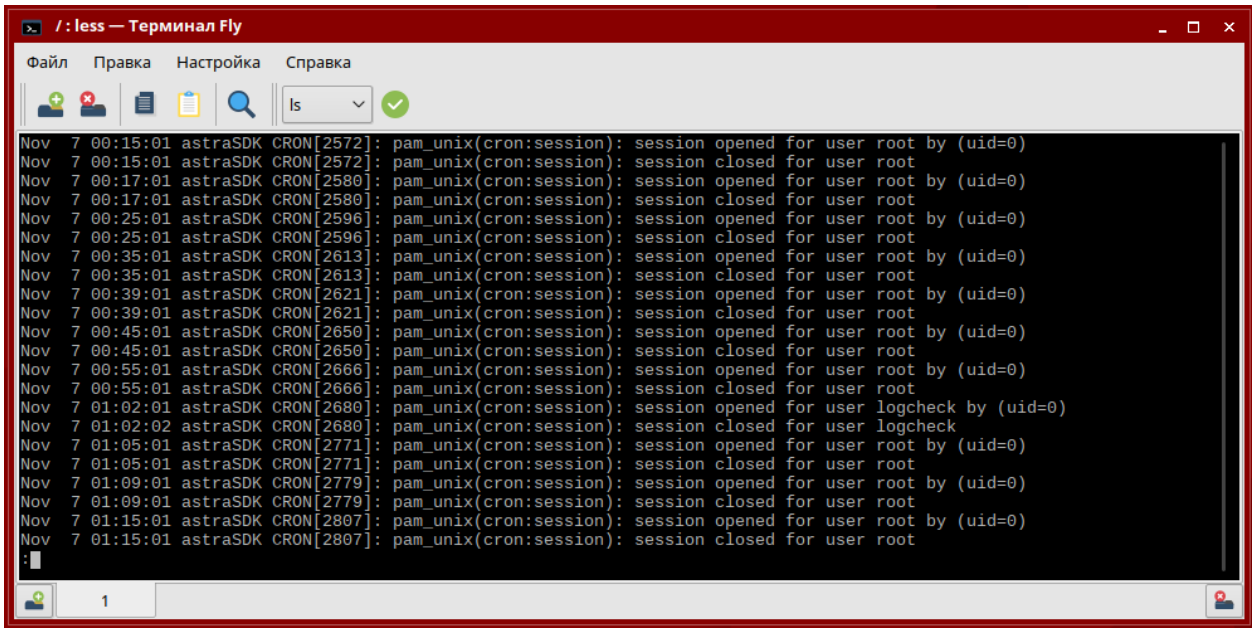


Рисунок 12.2 – Журнал информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации

13 Перечень принятых обозначений и сокращений

АРМ - Автоматизированное рабочее место

БД - База данных

МРД - Мандатное разграничение доступа

ПК - Программный комплекс

ПО - Программное обеспечение

СЛТМ - Система линейно телемеханики