Утвержден

РУСБ.30488-04 ЛУ

ПС АРМ АБИ

Руководство оператора

РУСБ.30488-04 34 01

Листов 96

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2022

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является Руководством оператора Программного средства автоматизированного рабочего места администратора безопасности информации (ПС АРМ АБИ).

Руководство содержит назначение, условия выполнения программы, описание последовательности действий оператора и сообщения оператору при запуске, выполнении операций и завершении работы с программой.

Руководство предназначено должностным лицам, осуществляющим и обеспечивающим эксплуатацию программы.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

ПС АРМ АБИ (далее – программа) предназначено для автоматизации повседневной деятельности администраторов безопасности информации при выполнении работ на серверах и рабочих станциях, функционирующих под управлением операционной системы специального назначения «Astra Linux Special Edition» очередное обновление 1.6 (без обновлений или установленными оперативными обновлениями 6, 10, 12) и очередное обновление 1.7 (без обновлений или установленными оперативными обновлениями 1.7.1, 1.7.3) с версиями ядра 4.15, 5.4, 5.10, 5.15.

Программа обеспечивает решение следующих основных задач:

1) построение списка доменов и реестра управляемых устройств, и контроль состояния управляемых устройств;

2) управление разграничением доступа к ресурсам управляемых устройств;

3) получение списка процессов, запущенных на управляемом устройстве;

4) генерация, установка и смена паролей учетных записей пользователей с использованием программы генерации паролей;

5) получение списка пользователей, выполнивших вход на управляемое устройство;

6) управление доступом пользователей к устройствам домена;

7) стирание защищаемой информации на управляемых устройствах по команде администратора безопасности информации;

8) создание/редактирование учётных записей пользователей;

9) блокировка/разблокировка учетных записей пользователей администратором безопасности информации;

10) проведение регламентного контроля целостности на управляемых устройствах с возможностью отображения и документирования результатов;

11) управление работой и контроль состояния средств антивирусной защиты на управляемых устройствах;

12) тестирование работоспособности средств защиты информации на управляемых устройствах с возможностью отображения и документирования результатов;

13) формирование и просмотр журналов событий информационной безопасности;

14) архивирование, восстановление и очистка журналов событий информационной безопасности;

15) прием и передача событий НСД соответственно с АРМ АБИ нижнего уровня на АРМ АБИ верхнего уровня.

16) автоблокировка пользователя при возникновении заданных событий НСД;

17) резервное копирование данных (конфигурации) управляемых доменов;

18) резервное копирование и восстановление базы данных программы;

19) возможность передачи на АРМ АБИ экстренного сообщения о возникновении внештатной ситуации («Работа под принуждением») с любого управляемого устройства;

20) оповещение администратора безопасности о фактах или попытках НСД к защищаемым ресурсам;

21) тиражирование правил доступа к отчуждаемым носителям информации.

22) ведение таблицы разграничения доступа пользователей к защищаемым ресурсам;

23) проведение контроля соответствия действующих дискреционных, мандатных прав доступа и политики аудита требуемым значениям таблицы разграничения доступа к защищаемым ресурсам.

Для решения вышеуказанных задач программа предоставляет пользователю эргономичный графический интерфейс.

Реализация функционального назначения программы осуществляется путем сбора, обработки, представления в удобном для пользователя виде необходимой для просмотра информации.

Для обеспечения выполнения функциональной задачи, приведенной в перечислении 4), необходимо наличие установленного на АРМ АБИ изделия «Комплекс программ «Специализированный генератор паролей» (КП СГП) РУСБ.30563-01.

Для обеспечения выполнения функциональной задачи, приведенной в перечислении 11), необходимо наличие установленного на управляемых устройствах средства антивирусной защиты.

2. УСЛОВИЕ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Минимальный состав аппаратных средств

2.1.1. Условием работы программы является наличие технических (аппаратных) средств с параметрами, удовлетворяющими следующим требованиям:

1) серверная часть:

- процессор с тактовой частотой не ниже 2 ГГц;
- ОЗУ – не менее 2 Гбайт;
- объем свободного дискового пространства на НЖМД – не менее 100 Гбайт;
- монитор с разрешением не менее 1024x768;

2) клиентская часть:

- процессор с тактовой частотой не ниже 1 ГГц;
- ОЗУ – не менее 1 Гбайт;
- объем свободного дискового пространства на НЖМД – не менее 1 Гбайт;
- монитор с разрешением не менее 1024x768.

2.1.2. Для представления результатов работы программы в виде выходных документов в печатной форме необходимо наличие печатающего устройства.

2.1.3. Технические (аппаратные) средства объединяются в локальную вычислительную сеть со скоростью передачи данных не менее 100 Мбит/с.

2.2. Минимальный состав программных средств

Программа предназначена для функционирования в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту – ОС СН), включающей в свой состав нижеприведенное общее программное обеспечение:

- средства организации единого пространства пользователей (ЕПП) на основе служб организации домена ALD или FreeIPA;
- защищенную СУБД PostgreSQL.

Для реализации функционального назначения программы необходимо наличие установленного программного обеспечения:

- средства антивирусной защиты (на управляемых устройствах);
- изделия «Комплекс программ «Специализированный генератор паролей» (КП СГП) РУСБ.30563 01 (на АРМ АБИ).

2.3. Требования к персоналу (пользователю)

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Запуск программы

Для запуска программы необходимо дважды кликнуть по расположенному на рабочем столе администратора безопасности информации ярлыку «ПС АРМ АБИ»  .

После запуска программы открывается форма аутентификации (рис. 1), в которой требуется указать значения параметров соединения с базой данных (имя или ip-адрес компьютера с БД, порт соединения с БД, наименование БД, имя и пароль пользователя БД), а также имя и пароль администратора домена (при работе с ALD имя и пароль администратора, по умолчанию единые для всех доменов).

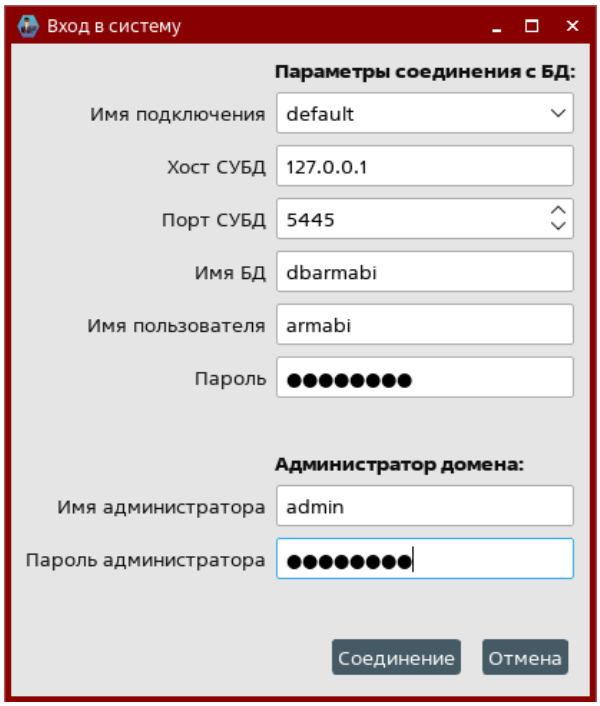


Рис. 1 – Окно аутентификации в БД

При успешном прохождении процедуры аутентификации пользователя открывается основное окно программы.

В верхней части основного окна располагается меню, включающее в себя пункты «Файл», «Настройки» и «Справка».

В левой части основного окна находятся элементы меню с логически сгруппированной по функционалу информаций об управляемых устройствах, образующие соответствующие разделы программы (рис. 2):

- «Устройства»;
- «Пользователи»;
- «Тестирование СЗИ»;

- «Контроль целостности»;
- «Антивирусная проверка»;
- «События ИБ»;
- «Внешние события ИБ».

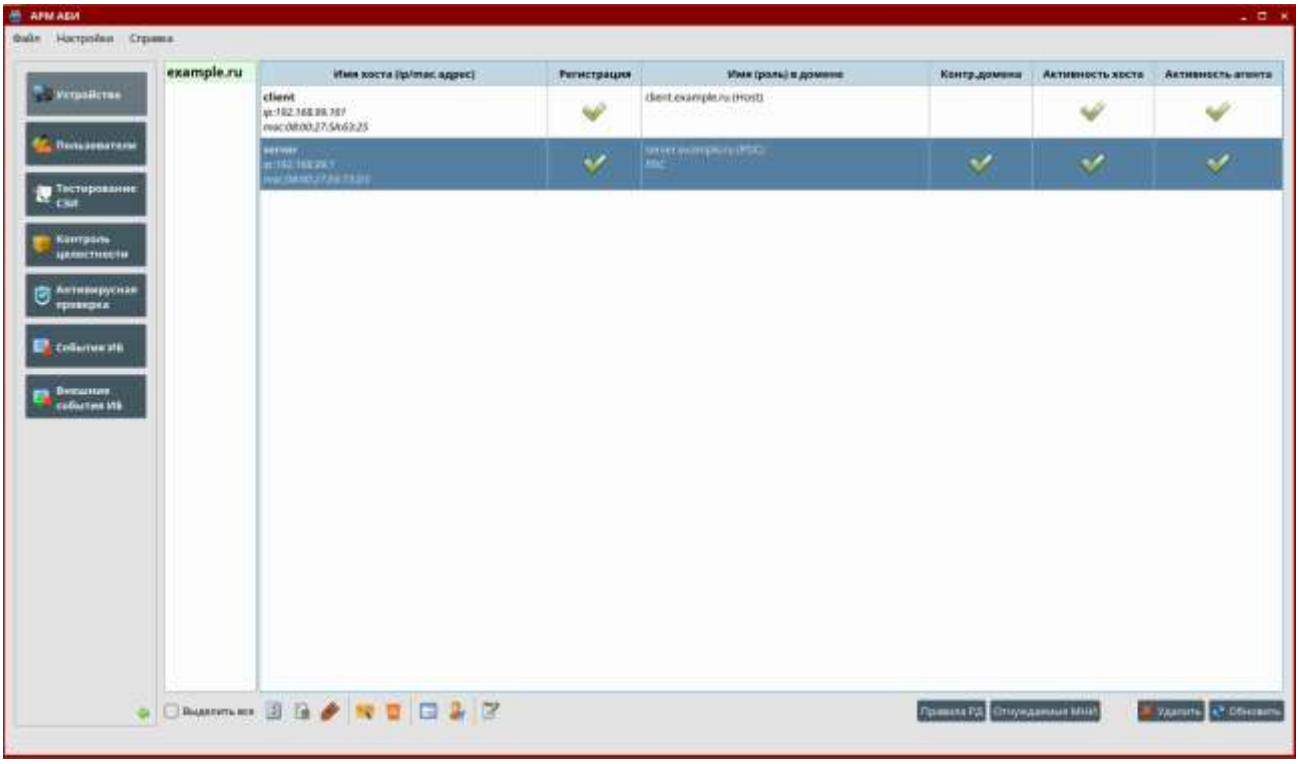


Рис. 2 – Основное окно программы

Переход между разделами программы осуществляется при выборе соответствующего элемента меню. При этом в правой части основного окна программы отображается соответствующая выбранному разделу информация.

В каждом разделе программы, кроме раздела «Внешние события ИБ», присутствует столбец со списком контролируемых доменов. При этом наименование домена подсвечивается зеленым цветом в случае успешного прохождения авторизации с (общим или индивидуальным) именем и паролем администратора домена, красным цветом в случае ошибки авторизации администратора домена и желтым цветом в случае наличия проблем в работоспособности домена или недоступности контроллера домена.

По умолчанию в правой части основного окна программы отображается соответствующая выбранному разделу информация по всем доменам из списка. При выборе определенного домена происходит фильтрация информации в правой части окна программы. Для возврата к отображению информации по всем контролируемым доменам необходимо установить флажок «Выделить все».

3.2. Настройка параметров программы

Для настройки параметров программы требуется выбрать пункт меню «Настройки». Окно «Настройка параметров» содержит две вкладки: «Общие» и «Ресурсы».

На вкладке «Общие» можно просмотреть и в случае необходимости изменить значения параметров (рис. 3):

- «Работа в среде» – используемая для организации единого пространства пользователей служба организации домена (ALD или FreeIPA);

- «ИД АС» – идентификатор системы, используемый при передаче информации о событиях информационной безопасности на вышестоящий уровень;

- «Порт АРМ АБИ» – порт сервера безопасности, используемый для обмена информации с агентами безопасности;

- «Название группы пользователей АРМ АБИ» – название группы, в которую включаются администраторы АРМ АБИ;

- «Минимальный уровень события для сигнализирования» – уровень событий, при возникновении которых выводится всплывающее окно, содержащее информацию о событии информационной безопасности;

- «Автоматическая регистрация новых устройств». Если сбросить флажок, то при регистрации каждого устройства будет выводиться запрос на регистрацию устройства.

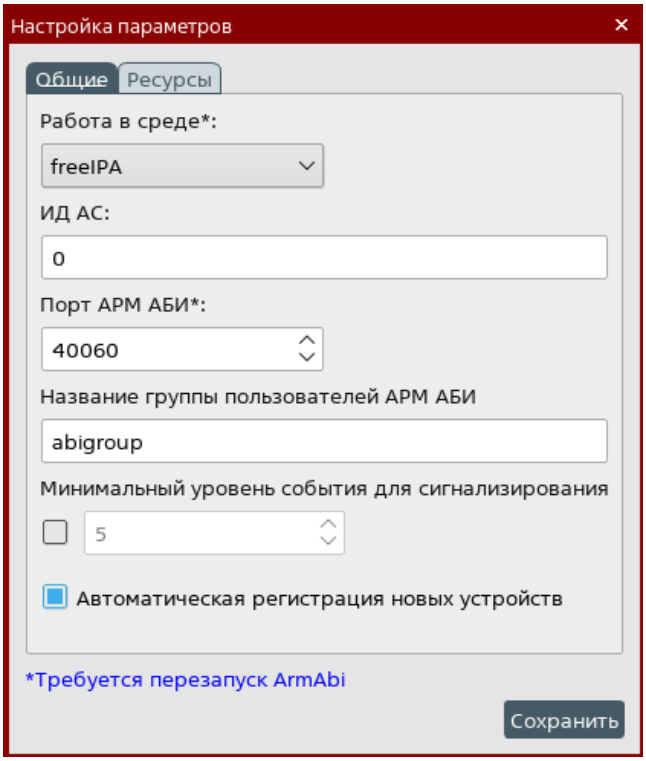


Рис. 3 – Вкладка «Общие»

На вкладке «Ресурсы» можно просмотреть и в случае необходимости изменить значения параметров (рис. 4):

- «Каталог для log-файлов тестирования» – каталог для хранения протоколов проведения КЦ, антивирусной проверки и тестирования СЗИ устройств;

- «Каталог для backup-файлов» – каталог для хранения резервных копий БД ПС АРМ АБИ и для локального сохранения резервных копий домена.

- «Каталог для шаблонов файлов конфигураций» – каталог для хранения шаблонов файлов конфигураций САВЗ и КЦ, а также для хранения настроек автоблокировки и настроек передачи событий на верхний уровень;

- «Каталог для архивов событий» – каталог для хранения архивированных файлов, содержащих информацию о событиях информационной безопасности, удаленных из журнала при нажатии на кнопку **[Очистка журнала]**.

ВНИМАНИЕ! При изменении каталогов во вкладке «Ресурсы» нужно убедиться, что на них установлены требуемые дискреционные права доступа:

- владельцем каталога является АБИ, указанный при установке ПС АРМ АБИ;

- в качестве группы должна указана группа пользователей ПС АРМ АБИ (по умолчанию – группа «abigroup»);

- владелец и члены группы имеют права на чтение/запись в каталог.

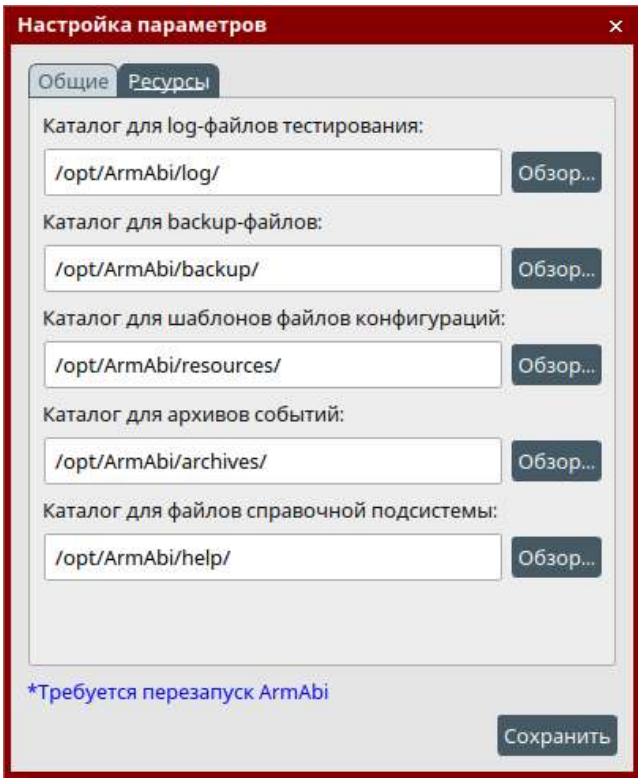


Рис. 4 – Вкладка «Ресурсы»

После установки требуемых значений параметров программы необходимо нажать кнопку **[Сохранить]**.

3.3. Настройка авторизации администратора для доменов ALD

Данная настройка доступна только при работе в среде ALD, т.к. в домене FreeIPA используется единый домен, для которого существует единственный администратор по умолчанию (admin).

ПС АРМ АБИ может контролировать управляемые устройства в различных доменах ALD. В этом случае возможна ситуация, когда для администратора (admin/admin) одного домена указан пароль, отличный от пароля для администратора другого домена.

Для решения этой проблемы в ПС АРМ АБИ предусмотрена функция установки индивидуального пароля, имеющего приоритет над паролем администратора домена, указанным при входе в программу. Для этого требуется нажать правой кнопкой «мыши» на названии домена и в открывшемся меню выбрать пункт « Установить пароль» (рис. 5) и задать пароль администратора домена. При выполнении действий в домене, для которого указан индивидуальный пароль, будет использоваться именно этот пароль.

Для удаления (индивидуального) пароля администратора выбранного домена требуется нажать на правую кнопку «мыши» и выбрать пункт « Удалить пароль» (рис. 5).

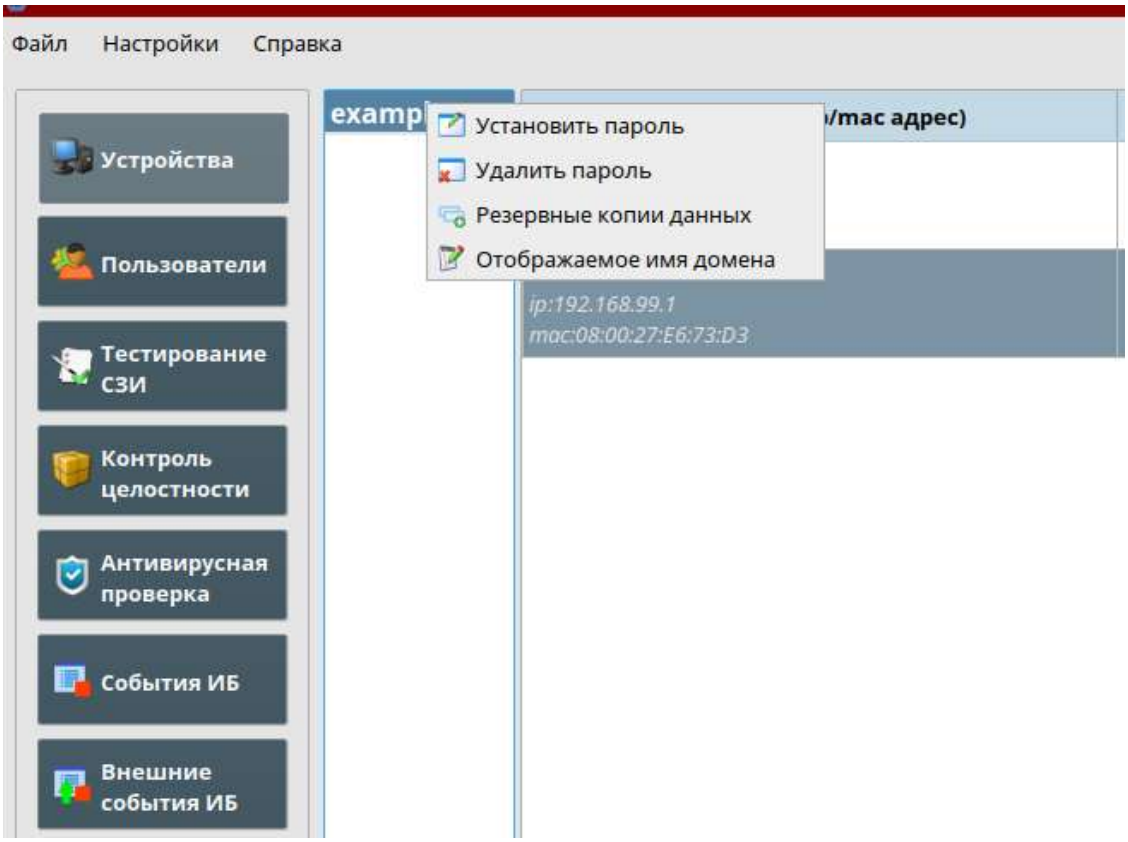


Рис. 5 – Настройка авторизации в контролируемых доменах ALD

3.4. Раздел «Устройства»

Раздел программы «Устройства» предназначен для управления правами доступа (дискреционными и мандатными) к информационным ресурсам на управляемых устройствах, а также аудитом информационных ресурсов.

При выборе раздела в правой части окна программы отображается список управляемых устройств, содержащий следующую информацию (рис. 6):

- имя, ip-адрес и mac-адрес устройства;
- наличие регистрации агента безопасности на сервере безопасности;
- доменное имя устройства;
- информацию о наличии роли контроллера домена;
- информацию об активности устройства;
- информацию об активности агента безопасности.

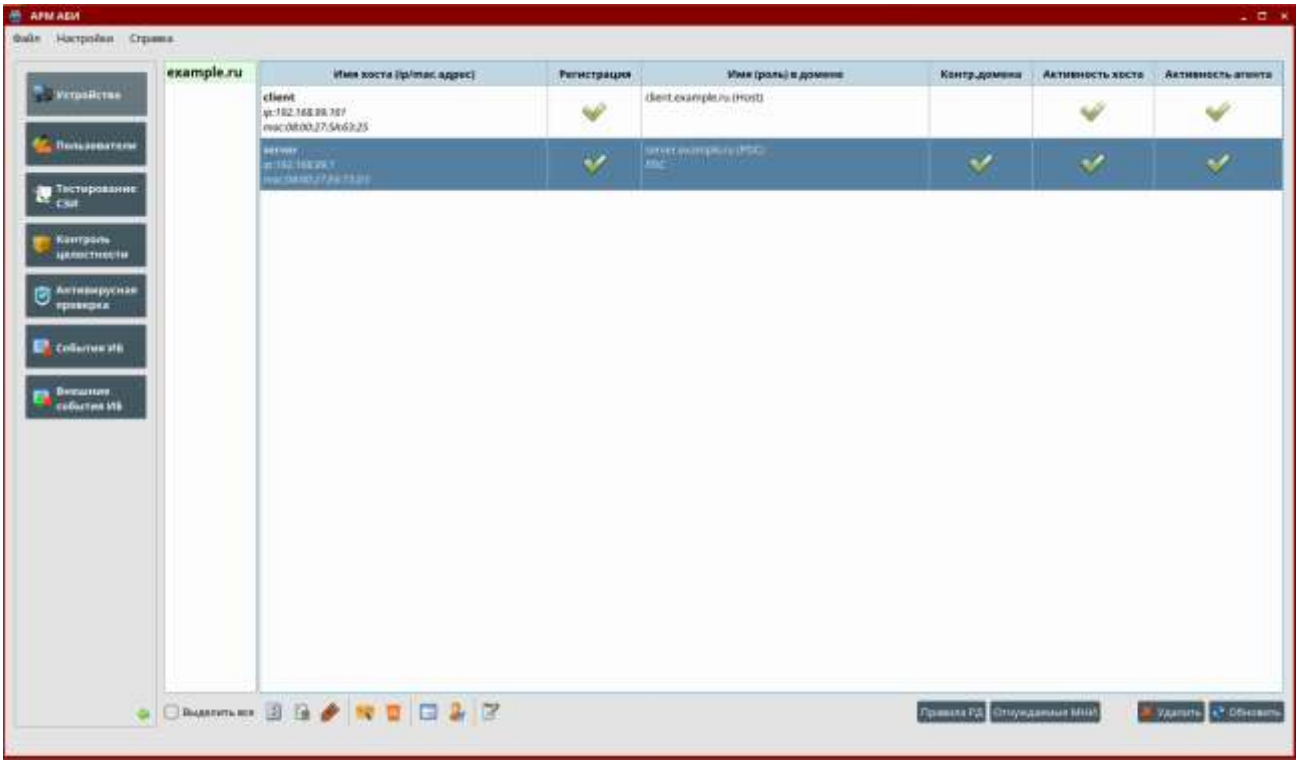


Рис. 6 – Раздел «Устройства»

В нижней части окна программы отображаются кнопки, предназначенные для выполнения следующих действий:

- настройка дискреционных и мандатных прав доступа;
- настройка аудита доступа к информационным ресурсам на управляемых устройствах;

- выбор объектов для гарантированного удаления и выполнения операции гарантированного удаления защищаемой информации (объектов) по команде администратора безопасности информации;

- просмотр запущенных процессов и активных пользователей;

- редактирование отображаемого имени устройства;

- сохранение полных настроек домена (только для FreeIPA);

Также в нижней части окна программы отображаются кнопки **[Удалить]** и **[Обновить]**.

Регистрация новых устройств происходит в автоматическом режиме. Если устройство было уже зарегистрирован и происходит повторная регистрация, тогда появляется запрос на подтверждение регистрации устройства (рис. 7).

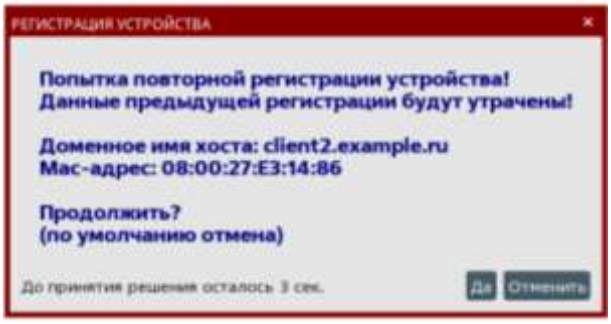


Рис. 7 – Запрос на повторную регистрацию устройства

При регистрации контроллера домена выводится запрос на подтверждение регистрации. В диалоговом окне «Регистрация устройства» подтвердить регистрацию устройства (рис. 8).

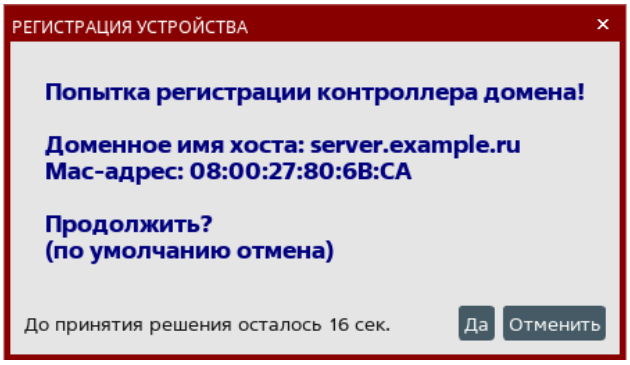


Рис. 8 – Запрос на регистрацию контроллера домена

3.4.1. Управление дискреционными правами доступа к информационным ресурсам

Для настройки дискреционных прав доступа к информационным ресурсам необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Управление политиками» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части на вкладке «Дискреционные атрибуты» – соответствующие дискреционные атрибуты разграничения доступа (рис. 9).

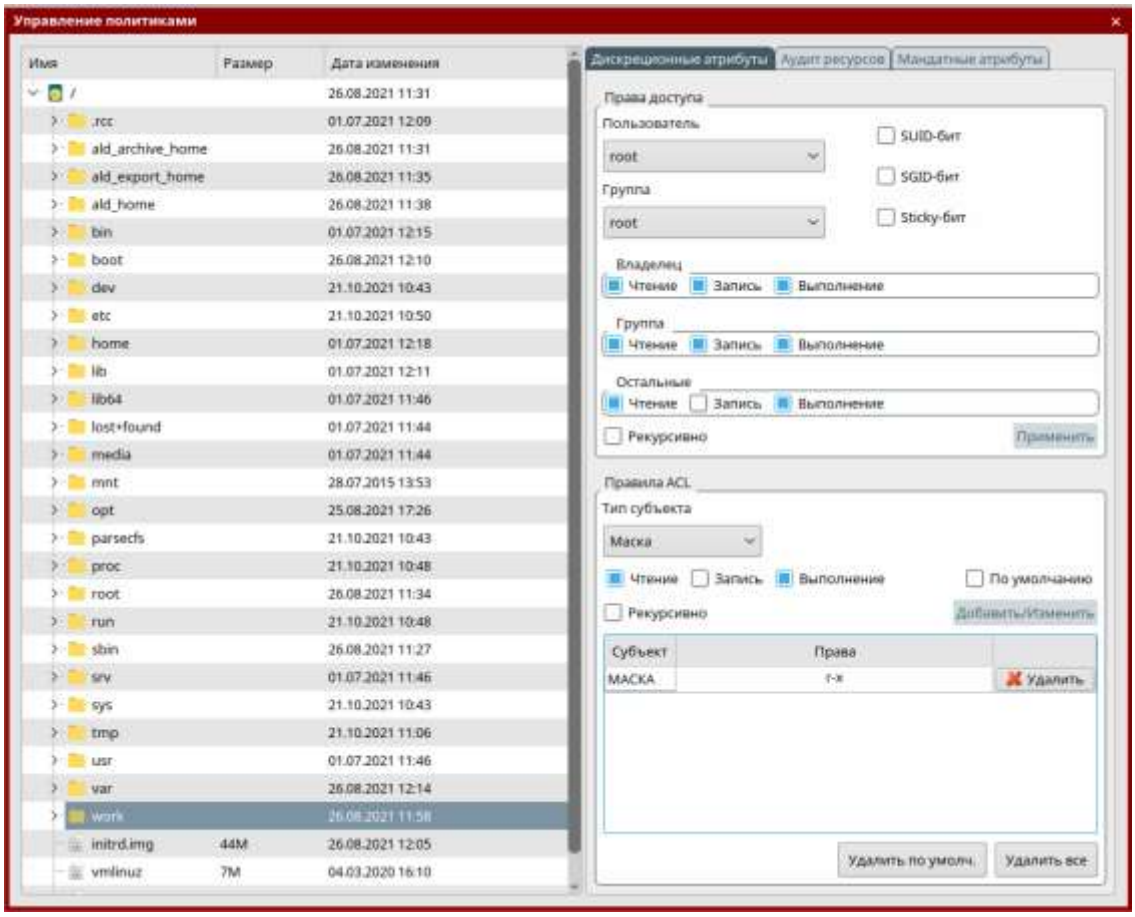


Рис. 9 – Настройка дискреционных прав доступа

Для настройки дискреционных прав доступа к информационному ресурсу необходимо, выбрав его в левой части окна, установить требуемые значения дискреционных атрибутов в блоке «Права доступа» и нажать на кнопку **[Применить]**.

Настройка правил ACL (списков контроля доступа) информационного ресурса выполняется в блоке «Правила ACL».

В данном блоке необходимо выбрать тип субъекта и права, после чего нажать на кнопку **[Добавить/Изменить]**.

Если необходимо выполнить настройку дискреционных прав доступа и/или правил ACL не только для выбранного информационного ресурса, но и для всех информационных ресурсов, содержащихся в нем (рекурсивно), то при редактировании прав доступа требуется установить флажок **«Рекурсивно»** в соответствующем блоке.

Если необходимо установить правила по умолчанию нужно установить флажок **[По умолчанию]**. Для удаления правил по умолчанию необходимо нажать на кнопку

[Удалить по умолч.]. Для удаления всех правил необходимо нажать на кнопку **[Удалить все]**.

По окончании настройки дискреционных прав доступа к информационным ресурсам управляемого устройства необходимо нажать кнопку закрытия в верхнем правом углу окна.

Подробные сведения о дискреционном разграничении доступа приведены в «Операционная система специального назначения «Astra Linux Special Edition» Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

3.4.2. Управление мандатными правами доступа к информационным ресурсам

Для настройки мандатных прав доступа к информационным ресурсам необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Управление политиками» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части на вкладке «Мандатные атрибуты» – соответствующие мандатные атрибуты разграничения доступа (рис. 10).

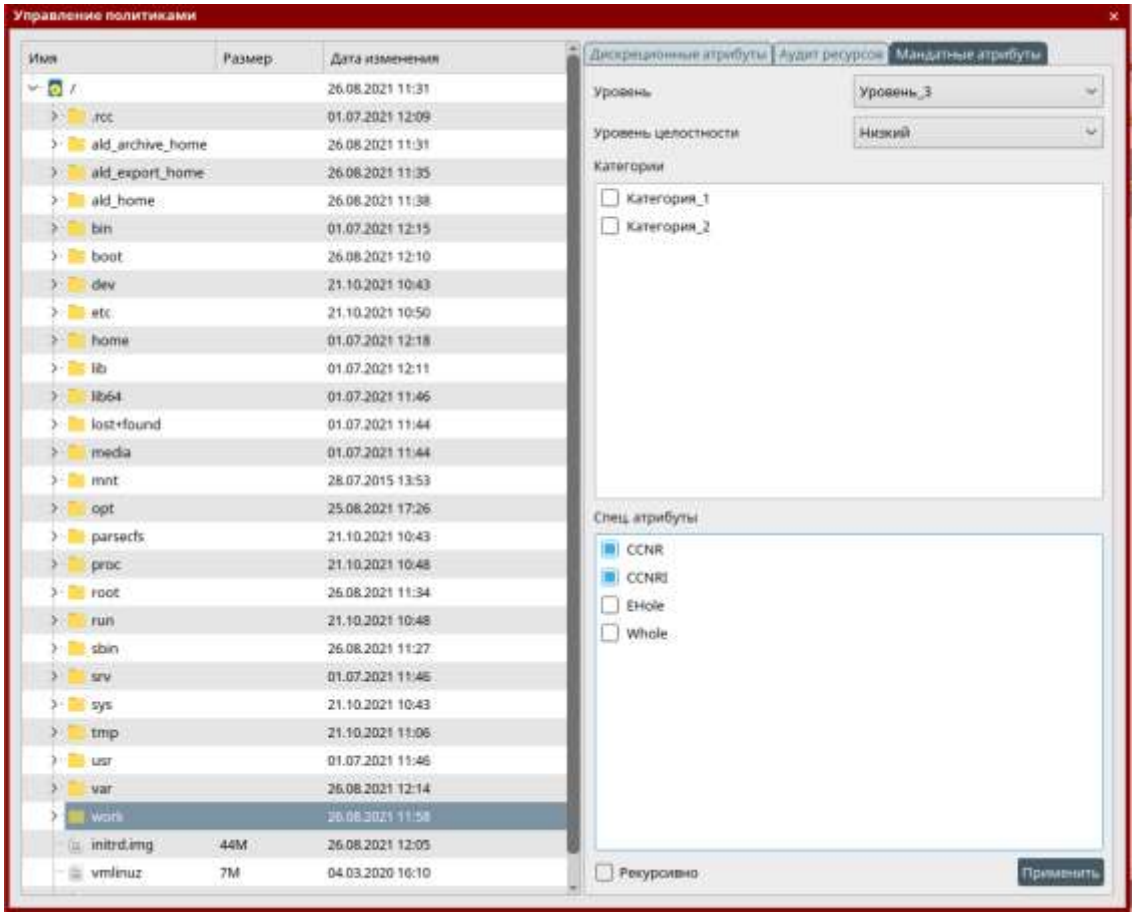


Рис. 10 – Настройка мандатных прав доступа

Для настройки мандатных прав доступа к информационному ресурсу необходимо, выбрав его в левой части окна, установить требуемые значения мандатных атрибутов и нажать на кнопку **[Применить]**.

Если необходимо выполнить настройку мандатных прав доступа не только для выбранного информационного ресурса, но и для всех информационных ресурсов, содержащихся в нем (рекурсивно), то при редактировании прав доступа требуется установить флажок **«Рекурсивно»**.

По окончании настройки мандатных прав доступа к информационным ресурсам управляемого устройства необходимо нажать на кнопку закрытия в верхнем правом углу окна.

Подробные сведения о мандатном разграничении доступа приведены в «Операционная система специального назначения «Astra Linux Special Edition» Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

3.4.3. Управление параметрами аудита информационных ресурсов

Для настройки параметров аудита информационных ресурсам необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Управление политиками» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части на вкладке «Аудит ресурсов» – соответствующие настройки параметров аудита (рис. 11).

Для настройки параметров аудита информационного ресурса необходимо, выбрав его в левой части окна, установить требуемые значения параметров аудита и нажать на кнопку **[Добавить/Изменить]**.

Если необходимо выполнить настройку параметров аудита не только для выбранного информационного ресурса, но и для всех информационных ресурсов, содержащихся в нем (рекурсивно), то при редактировании политики аудита ресурса требуется установить флажок **«Рекурсивно»**.

По окончании настройки параметров доступа к информационным ресурсам управляемого устройства необходимо нажать на кнопку закрытия в верхнем правом углу окна.

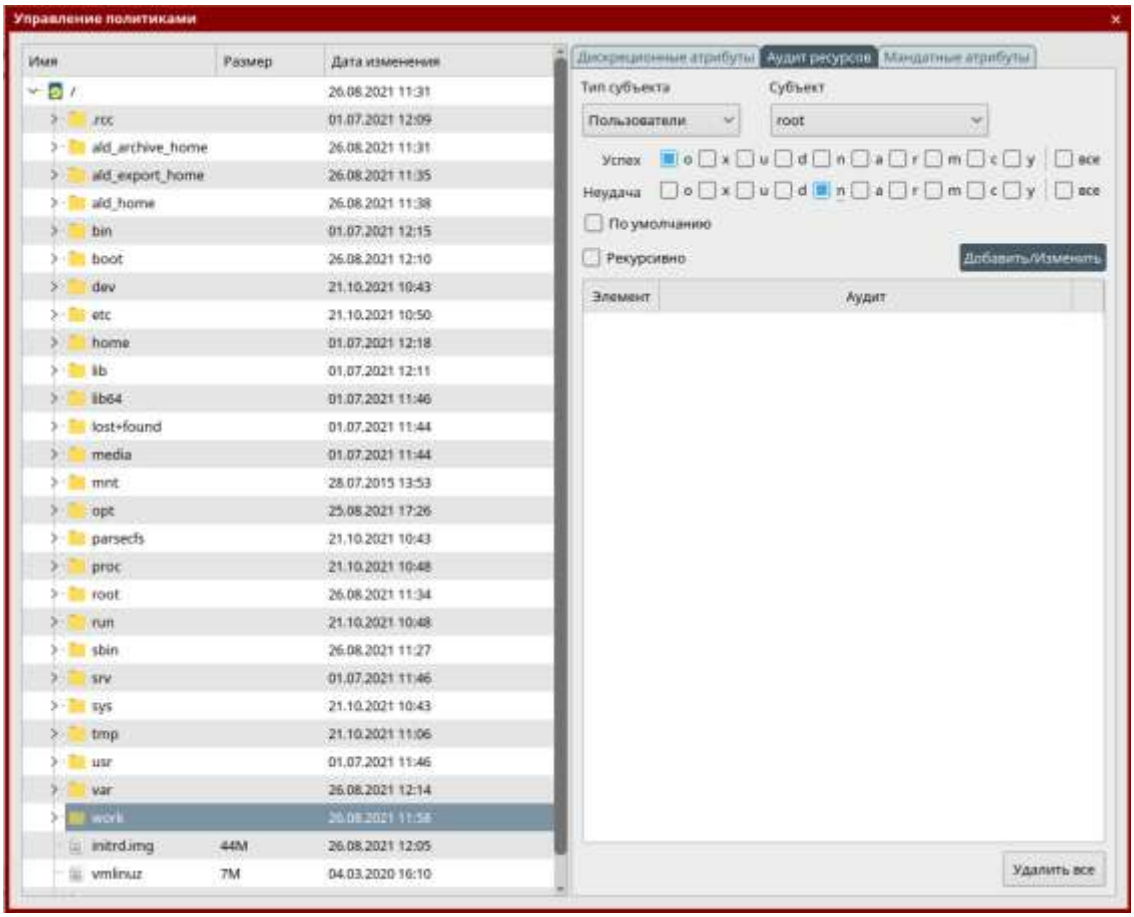


Рис. 11 –Настройка аудита ресурсов

Подробные сведения об аудите информационных ресурсов приведены в «Операционная система специального назначения «Astra Linux Special Edition» Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

3.4.4. Стирание защищаемой информации

Для настройки перечня ресурсов для гарантированного удаления необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Перечень объектов для гарантированного удаления» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части – список компонент, подлежащих стиранию по команде администратора безопасности информации (рис. 12).

Для добавления в перечень нового объекта необходимо выбрать соответствующий файл или директорию в левой части окна и нажать на кнопку  .

Для удаления объекта из перечня необходимо выбрать соответствующий файл или директорию в правой части окна и нажать на кнопку  .

Перечень объектов, подлежащих стиранию по команде администратора безопасности информации, можно загрузить из ранее созданного шаблона конфигурации перечня объектов гарантированного удаления, нажав на кнопку **[Загрузить из шаблона]**.

Нажав на кнопку **[Сохранить шаблон]** можно сохранить текущий перечень объектов, подлежащих стиранию по команде администратора безопасности информации. По окончании редактирования перечня объектов гарантированного удаления необходимо нажать на кнопку **[Сохранить]**.

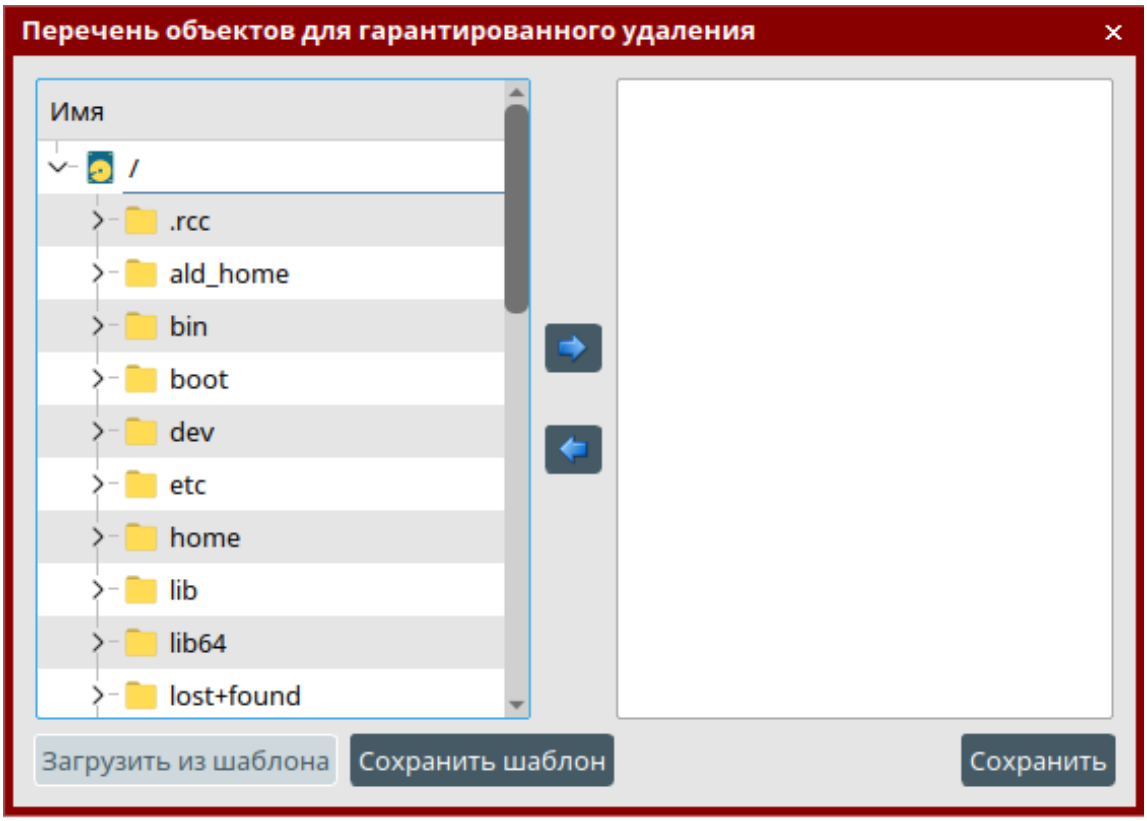


Рис. 12 – Выбор перечня объектов (ресурсов) устройства, подлежащих стиранию по команде администратора безопасности информации

При нажатии на кнопку  после подтверждения операции администратором безопасности информации (рис. 13) происходит удаление всех компонент, заданных в конфигурации устройства.

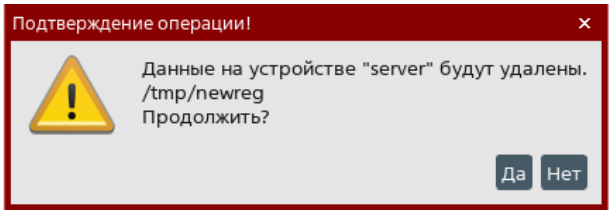


Рис. 13 – Подтверждение операции стирания защищаемой информации

3.4.5. Просмотр списка запущенных процессов

Для просмотра списка запущенных процессов необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

В открывшемся окне «Запущенные процессы» отобразится список запущенных процессов (рис. 14).

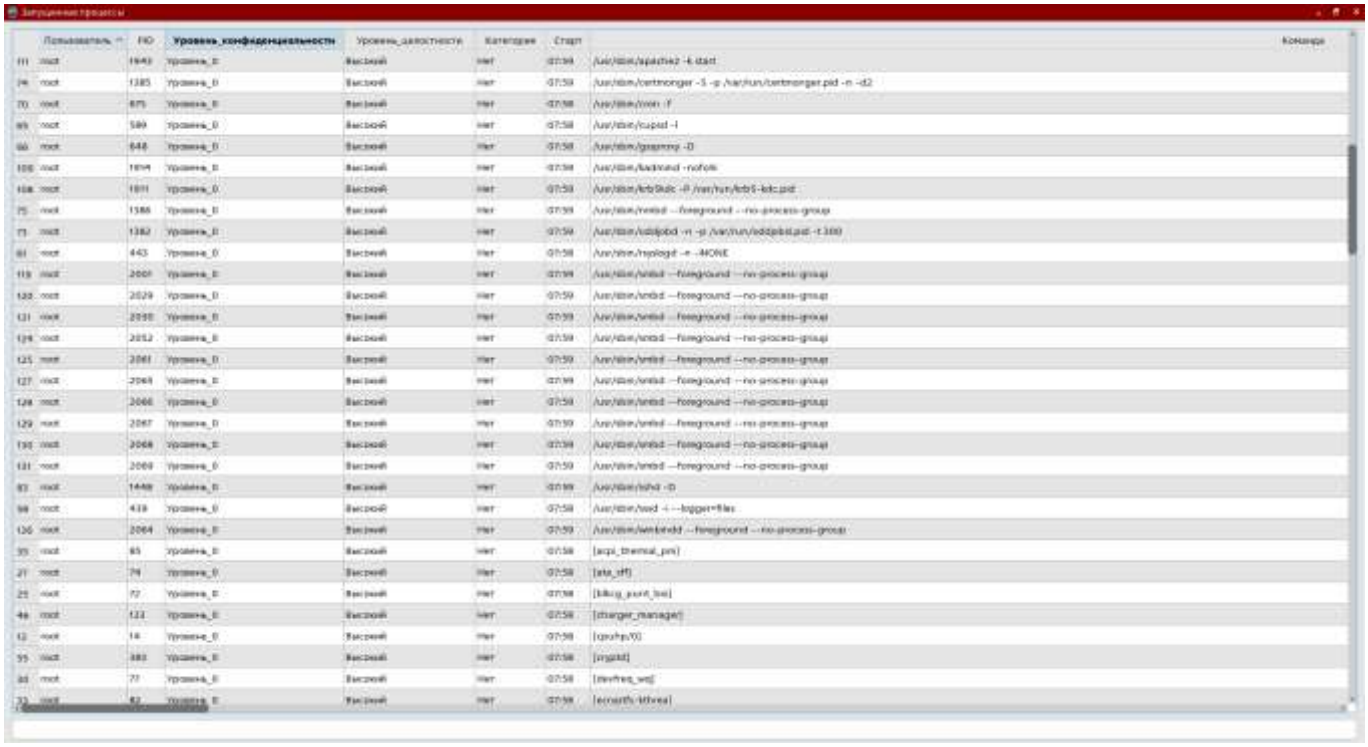


Рис. 14 – Просмотр списка запущенных процессов

Для каждого процесса отображаются следующие параметры:

- имя пользователя, запустившего процесс;
- идентификатор процесса (PID);
- мандатные атрибуты запущенного процесса;
- время запуска процесса;
- программа, для которой выполняется данный процесс.

В нижней части окна «Запущенные процессы» предусмотрено поле ввода для поиска процессов. Поиск производится по столбцу «Команда».

Примечание. В связи с обработкой большого количества запущенных процессов окно открывается не сразу. Требуется подождать 5-10 секунд.

3.4.6. Просмотр списка активных пользователей

Для просмотра списка активных пользователей необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

В открывшемся окне «Активные пользователи» отобразится список активных пользователей (рис. 15).

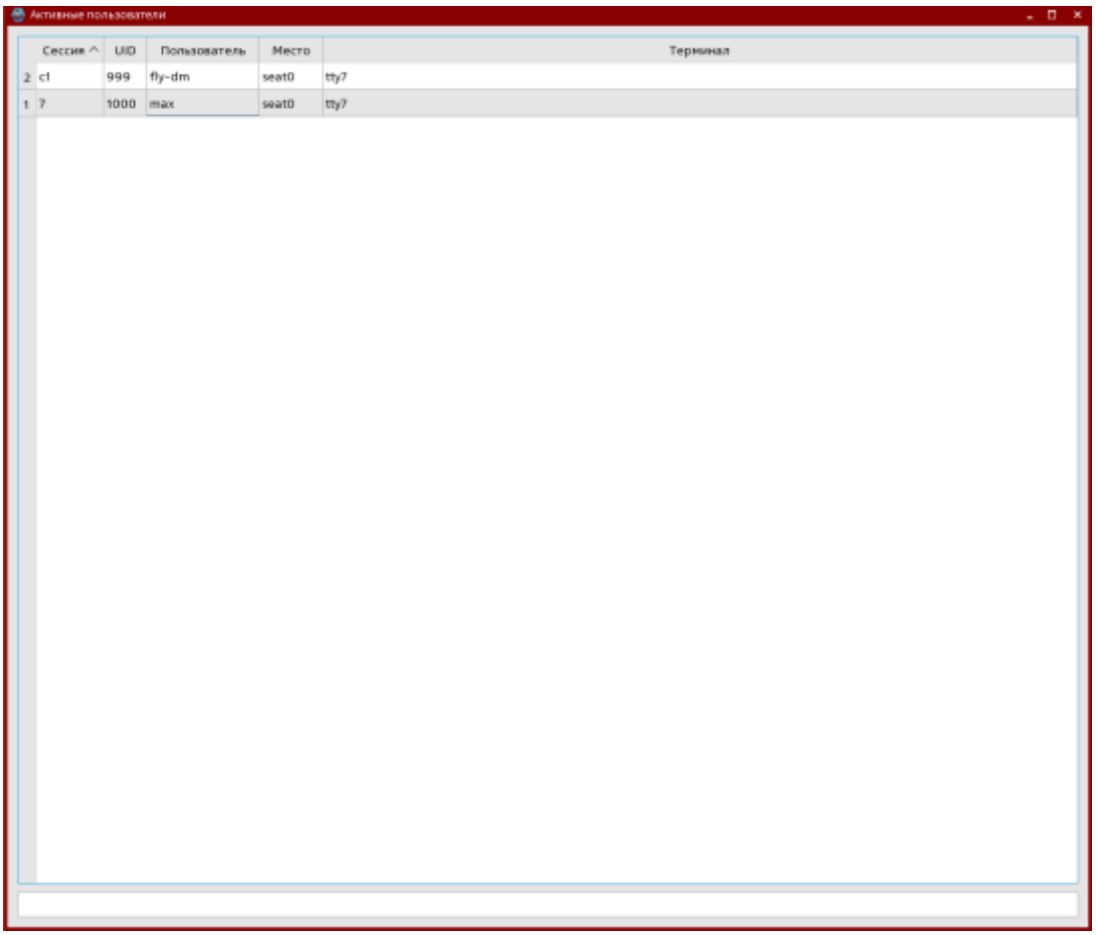


Рис. 15 – Просмотр списка активных пользователей

Для каждого пользователя отображаются следующие параметры:

- сессия пользователя;
- UID – уникальный идентификатор пользователя;
- наименование пользователя;
- место;
- название терминала.

В нижней части окна «Активные пользователи» предусмотрено поле ввода для поиска. Поиск производится по столбцу «Процесс».

3.4.7. Редактирование отображаемого имени устройства

Для редактирования отображаемого имени устройства необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

В открывшемся окне «Переименовать АРМ» необходимо ввести отображаемое имя (по умолчанию оно совпадает с действительным именем) и нажать на кнопку **[Сохранить]** (рис. 16).

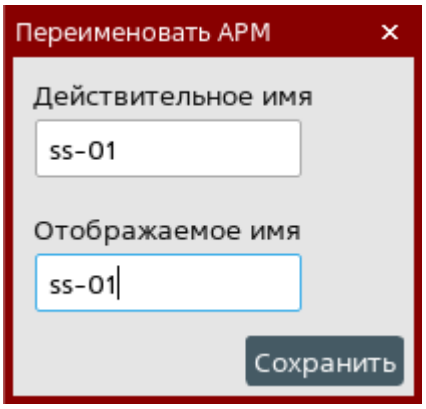


Рис. 16 – Редактирование имени устройства

3.4.8. Удаление устройства

Для удаления устройства необходимо выбрать из списка управляемое устройство и нажать на кнопку **[Удалить]**. На экране появится предупреждение (рис. 17).

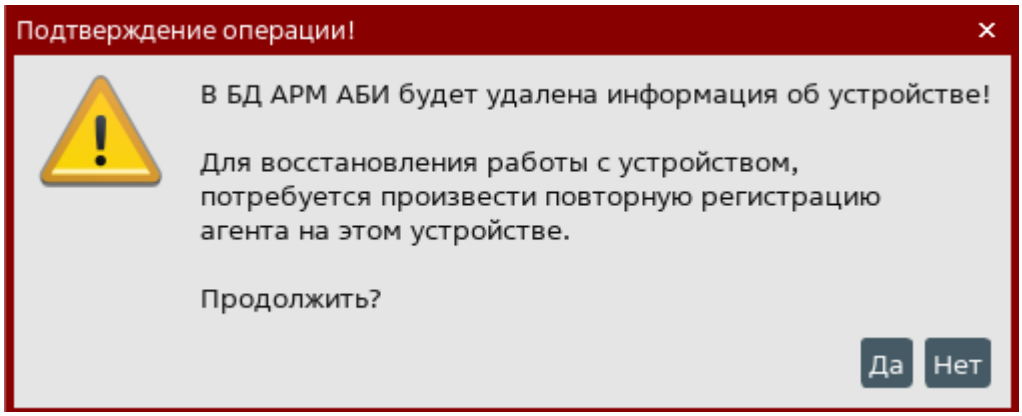


Рис. 17 – Предупреждение при удалении устройства

В окне «Подтверждение операции» необходимо нажать на кнопку **[Да]**.

Примечание. При удалении устройства из списка, агенту данного устройства посылается команда на обнуление параметра `idDev` в файле `/etc/armdl.conf`. При следующем старте агент сам инициирует регистрацию в программе. Данная особенность добавлена для исключения ситуации, когда на удаленном устройстве агент ничего не «знает» об удалении и продолжает пытаться устанавливать соединение с программой со старыми регистрационными данными.

3.5. Раздел «Пользователи»

Раздел программы «Пользователи» предназначен для создания, редактирования учетных записей пользователей, блокировки/разблокировки учетных записей пользователей и их текущих сессий, установки и смены паролей пользователей, настройки доступа к ресурсам на основе ролевой модели. При работе в среде ALD в

данном разделе дополнительно можно выполнить настройку мандатных атрибутов и доменных привилегий пользователей и их доступа к устройствам домена.

Внешний вид раздела отличается в зависимости от используемого домена (ALD, FreeIPA). На рис. 18 приведен вид раздела при работе с доменом FreeIPA.

В разделе «Пользователи» отображается следующая информация:

- UID пользователя;
- логин пользователя;
- полное имя пользователя;
- статус пользователя (активен/блокирован);
- имя домена (только для ALD);
- статус АБИ (состоит ли пользователь в группе пользователей АРМ АБИ).

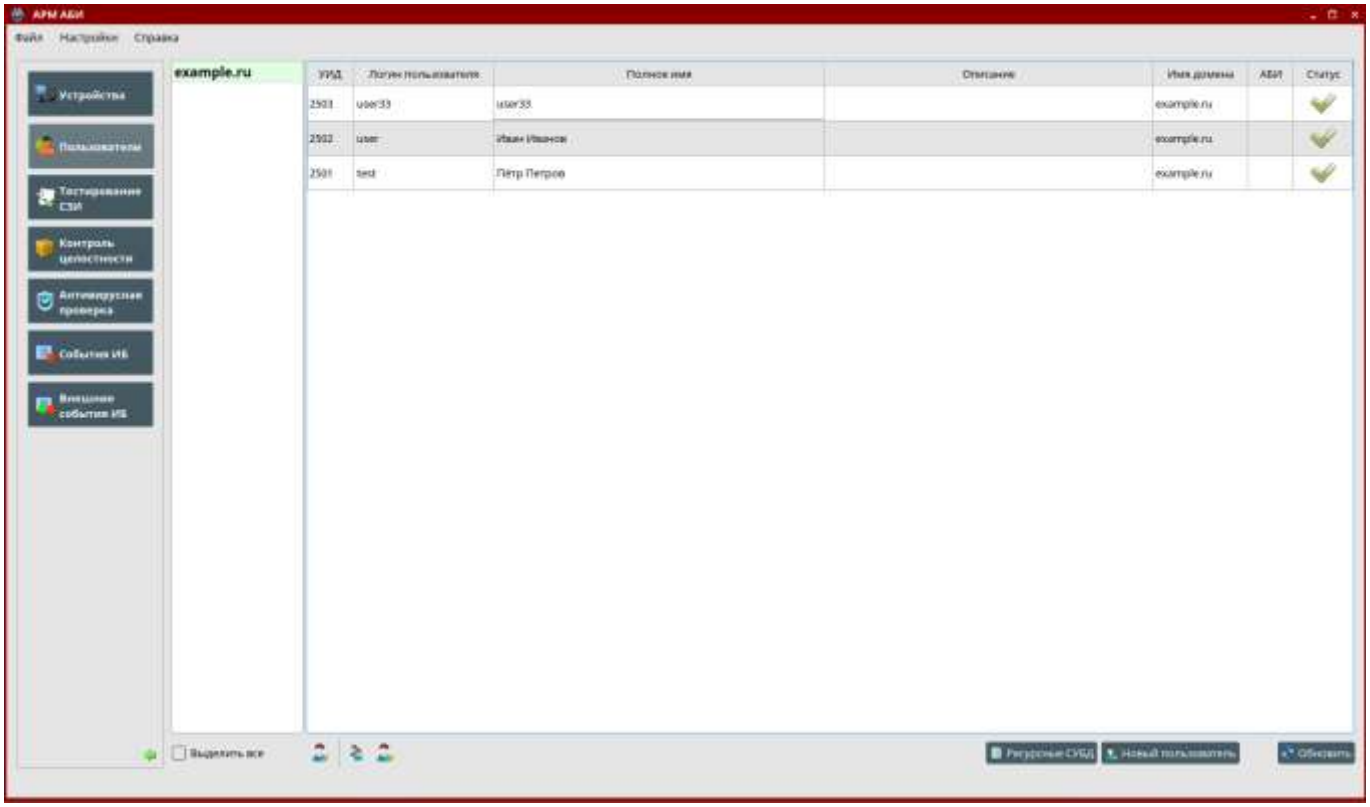


Рис. 18 – Раздел «Пользователи»

В нижней части окна программы отображаются кнопки, предназначенные для выполнения следующих действий:

- редактирования настроек существующей учетной записи;
- создания новой учетной записи;
- добавления пользователя в группу АБИ и исключения из неё;
- удаления пользователя (только для домена FreeIPA);
- настройки ресурсных СУБД для обеспечения настройки доступа пользователей к ресурсам на основе ролевой модели.

Также в нижней части окна программы отображается кнопка **[Обновить]** для обновления информации о пользователях.

3.5.1. Создание/редактирование учетной записи пользователя (домен FreeIPA)

Для создания новой учетной записи пользователя необходимо нажать на кнопку **[Новый пользователь].** Для изменения настроек существующей необходимо выбрать учетную запись и нажать на кнопку  **.**

Вид открывшегося окна «Настройки пользователя» зависит от используемой для организации единого пространства пользователей службы организации домена. В случае использования службы FreeIPA окно «Настройки пользователя» содержит вкладки «Общие», «Ролевая политика» (рис. 19).

Для создания/редактирования учетной записи требуется перейти на вкладку «Общие» и установить значения полей:

- «Пользователь» (обязательное);
- «UID» (обязательное, формируется автоматически в случае отсутствия);
- «GECOS» (необязательное, заполняется с использованием всплывающего диалогового окна);
- «Домашний каталог» (обязательное, используется значение «по умолчанию»);
- «Имя» (обязательное);
- «Фамилия» (обязательное);
- «Оболочка» (обязательное, по умолчанию используется значение «./bin/bash»).

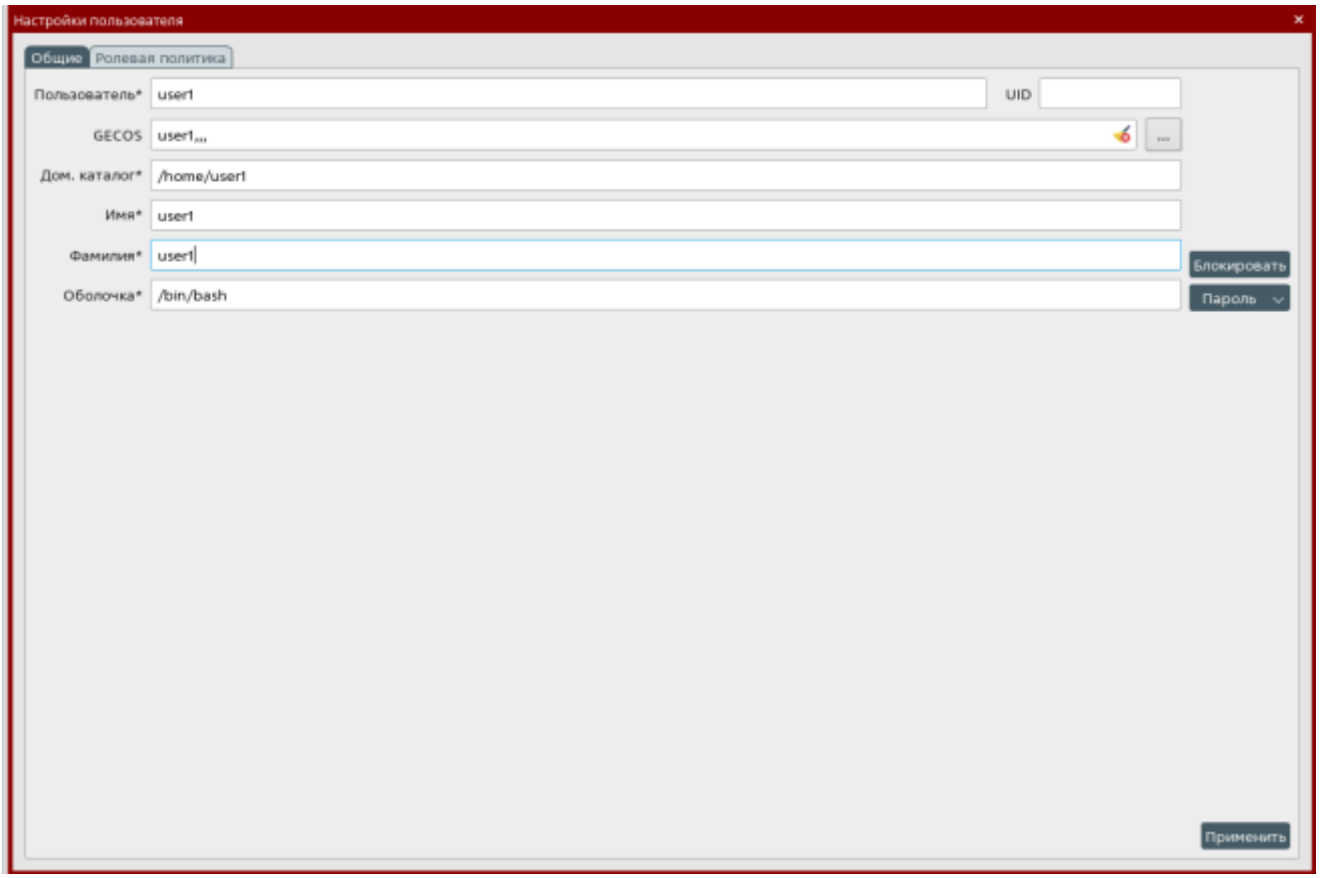


Рис. 19 – Создание/редактирование учетной записи пользователя в домене FreeIPA

Для установки пароля пользователя необходимо нажать на кнопку [**Пароль**] и выбрать один из способов: «Генерировать пароль» или «Задать пароль». При выборе первого варианта генерация и установка пароля пользователю выполняется с использованием программы генерации пароля, при выборе второго вариант пароль задается вручную.

Для сохранения изменений необходимо нажать на кнопку **[Применить]**.

3.5.2. Создание/редактирование учетной записи пользователя (домен ALD)

Для создания новой учетной записи пользователя необходимо нажать на кнопку **[Новый пользователь].** Для изменения настроек существующей необходимо выбрать учетную запись и нажать на кнопку  **.**

Вид открывшегося окна «Настройки пользователя» зависит от используемой для организации единого пространства пользователей службы организации домена. В случае использования службы ALD окно «Настройки пользователя» содержит вкладки «Общие», «Ролевая политика», «МРД» и «Привилегии домена» (рис. 20).

Для создания/редактирования учетной записи требуется перейти на вкладку «Общие» и установить значения полей:

- «Пользователь» (обязательное);

- «UID» (обязательное, формируется автоматически в случае отсутствия);

- «GECOS» (необязательное, заполняется с использованием всплывающего диалогового окна);

- «Домашний каталог» (обязательное, используется значение «по умолчанию»);

- «Полное имя» (обязательное);

- «Описание» (необязательное);

- «Тип файловой системы» (обязательное, используется значение «по умолчанию»);

- «Домашний сервер» (обязательное, используется значение «по умолчанию»);

- «Оболочка» (обязательное, по умолчанию используется значение «./bin/bash»);

- «Первичная группа» (обязательное, по умолчанию используется первичная группа пользователя);

- «Политика паролей» (обязательное, по умолчанию используется значение «default»).

Кроме того, из списка доступных доменов с использованием кнопок  и  необходимо задать домены, в которых будет создана учетная запись пользователя.

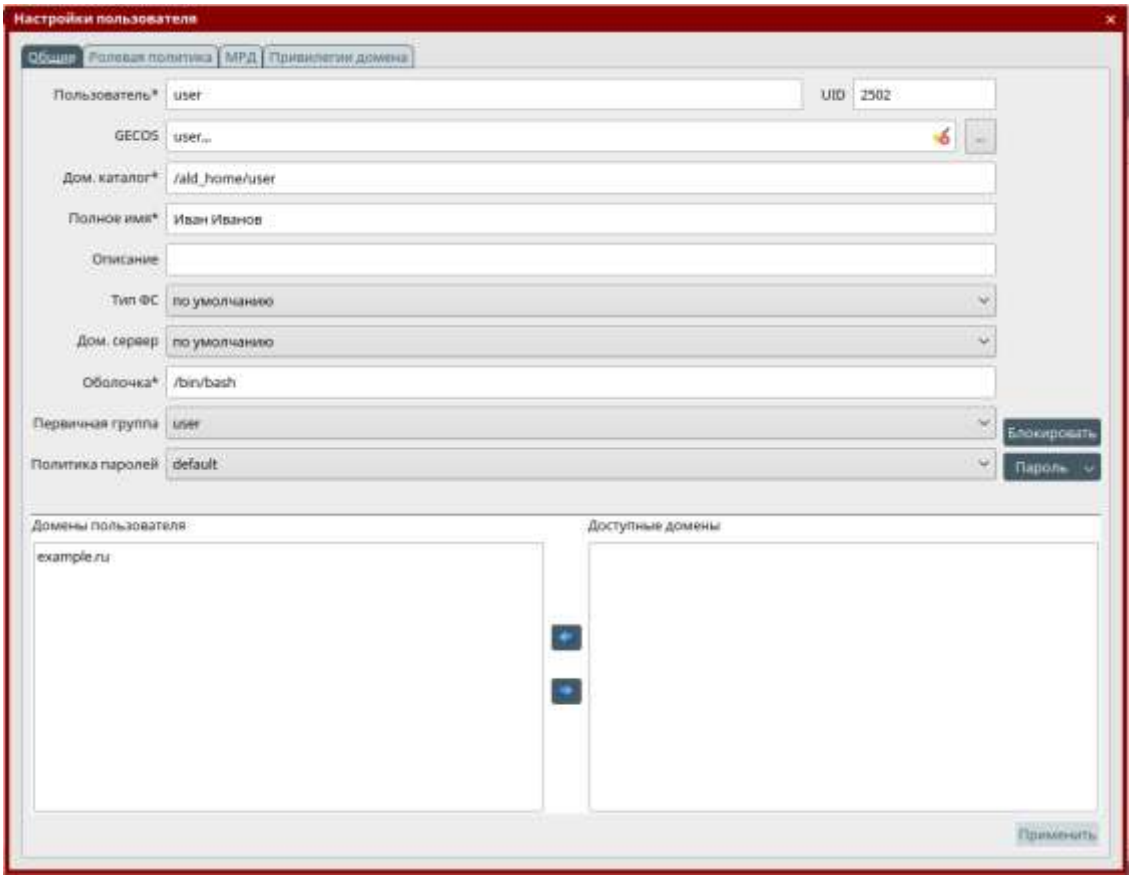


Рис. 20 – Создание/редактирование учетной записи пользователя в домене ALD

Для установки пароля пользователя необходимо нажать на кнопку **[Пароль]** и выбрать один из способов: «Генерировать пароль» или «Задать пароль». При выборе первого варианта генерация и установка пароля пользователю выполняется с использованием программы генерации пароля, при выборе второго вариант пароль задается вручную.

Для сохранения изменений необходимо нажать на кнопку **[Применить]**.

3.5.3. Настройка мандатных атрибутов пользователя (домен ALD)

Для настройки мандатных атрибутов пользователя необходимо перейти в окне «Настройки пользователя» на вкладку «МРД» (рис. 21).

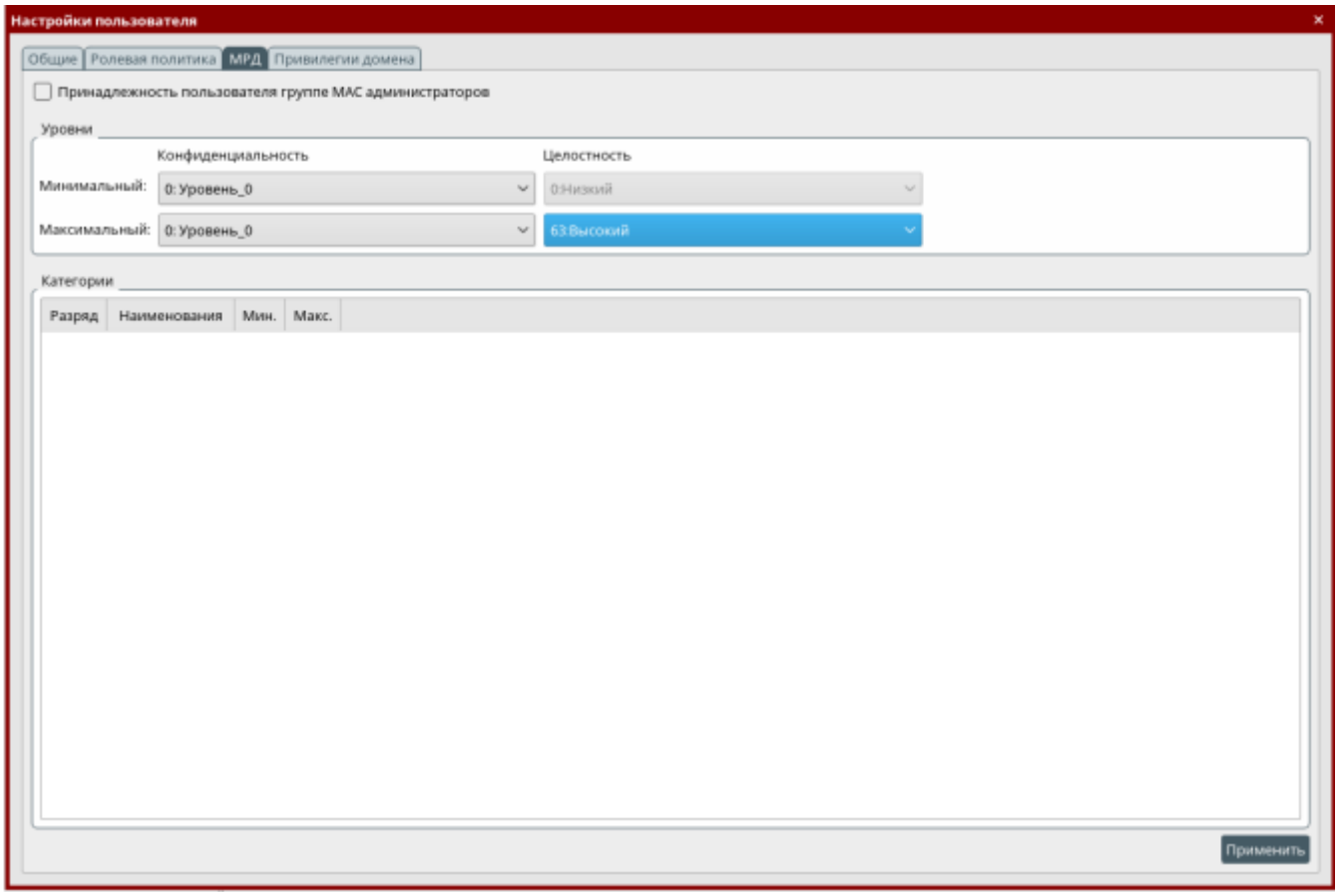


Рис. 21 – Настройка мандатных атрибутов пользователя

Для выбранного пользователя требуется установить из списков «Уровень конфиденциальности» и «Уровень целостности» минимальный и максимальный уровни доступа, а также задать требуемые категории.

Для сохранения изменений необходимо нажать на кнопку **[Применить]**.

3.5.4. Настройка доменных привилегий пользователя (домен ALD)

Для настройки доменных привилегий пользователя необходимо перейти в окне «Настройки пользователя» на вкладку «Привилегии домена» (рис. 22).

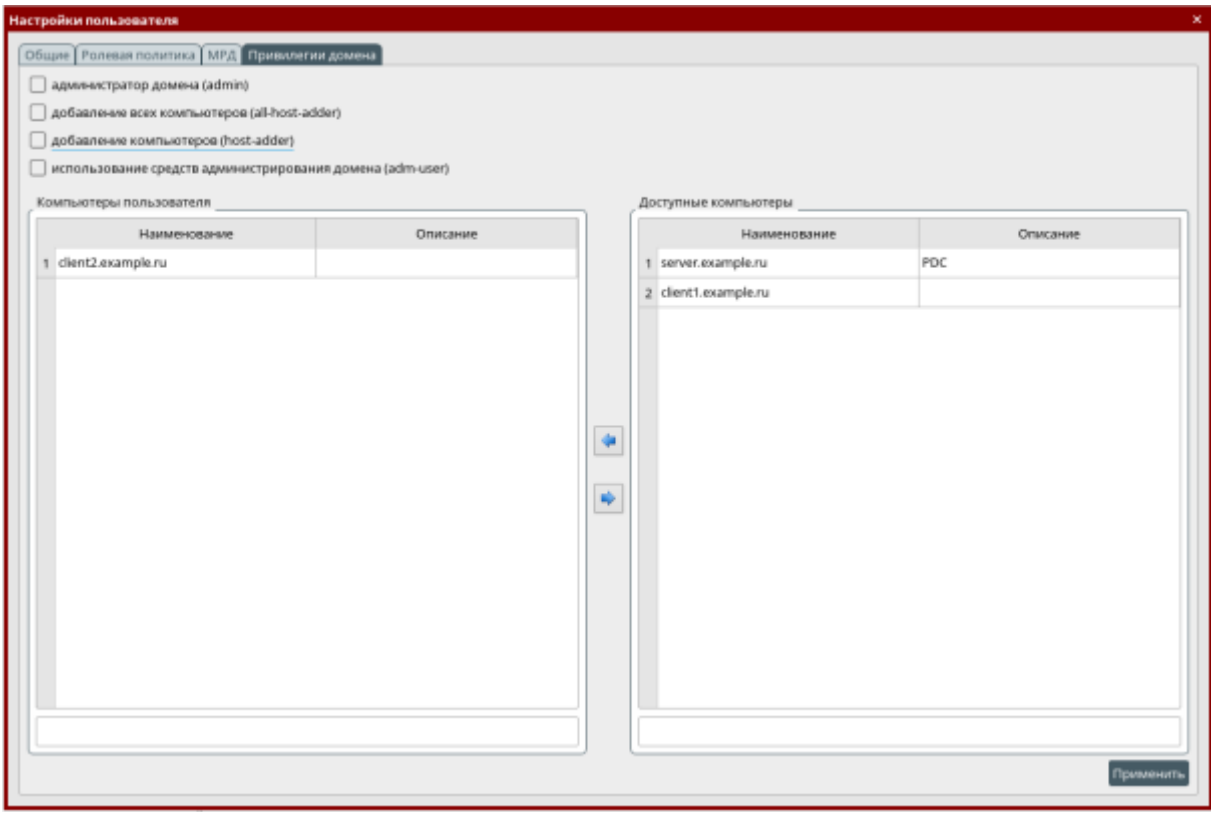


Рис. 22 – Настройка доменных привилегий пользователя

В случае необходимости, отметив соответствующие флажки, пользователю можно установить одну или несколько доменных привилегий:

- администратор домена;
- добавление всех компьютеров в домен;
- добавление компьютера в домен;
- использование средств администрирования домена.

Из расположенных в правой части окна списка доступных устройств (во всех доменах пользователя, отобранных на вкладке «Общие» в списке «Домены пользователя») с использованием кнопок  и  необходимо выбрать устройства, на которые пользователю разрешен вход в систему.

Для сохранения изменений необходимо нажать на кнопку **[Сохранить]**.

3.5.5. Ролевая модель доступа пользователей к информационным ресурсам

Для обеспечения разграничения доступа пользователю к ресурсам файловой системы и СУБД применяется ролевая модель, предусматривающая делегирование прав доступа на основе его принадлежности (или не принадлежности) к определенной специализированной группе пользователей и роли СУБД.

Ролевая модель, обеспечивающая разграничение администратором безопасности информации доступа пользователей к ресурсам файловой системы и СУБД,

предусматривает делегирование прав доступа на основе принадлежности (или не принадлежности) учетной записи (роли в СУБД) пользователя к определенной специализированной группе пользователей (роли в СУБД).

Механизм сквозной авторизации ОС СН обеспечивает возможность получить пользователю доступ только к тем ресурсам, которые необходимы ему для выполнения своих функциональных обязанностей.

Первоначальное формирование специализированных групп пользователей и ролей СУБД, а также первоначальная установка разграничений доступа к ресурсам системы, выполняется средствами СПО, при этом каждой роли в СУБД однозначно соответствует группа пользователей с идентичным наименованием.

Предусматривается использование следующих типов специализированных групп (ролей):

- функциональных, соответствующих решению определённых (конкретных) задач;

- должностных, предназначенных для агрегирования функциональных групп (ролей).

Совокупность специализированных функциональных групп пользователей (и соответствующих им ролей СУБД), образованных посредством включения их в должностную группу (роль СУБД), образуют профиль пользователя.

При назначении пользователю определенного профиля происходит автоматическое включение данного пользователя во все специализированные функциональные группы домена и назначение должностных ролей СУБД. Соответственно, при исключении пользователя из профиля, он автоматически исключается из всех специализированных функциональных групп домена, а также с него снимаются должностные роли СУБД.

Аналогичным образом, при включении в профиль новой функциональной группы (назначении функциональной роли) автоматически происходит включение всех пользователей, входящих в данный профиль, в соответствующую функциональную группу домена, а также включение функциональной роли СУБД в должностную. При исключении из профиля функциональной группы (снятии функциональной роли) все пользователи, входящие в данный профиль, исключаются из соответствующей функциональной группы домена, а также исключение функциональной роли СУБД из должностной.

Для выполнения настройки должностных и функциональных ролей для обеспечения доступа пользователей к информационным ресурсам на основе ролевой

модели необходимо нажать на кнопку **[Ресурсные СУБД]** в основном окне программы раздела «Пользователи».

В открывшимся окне «Ресурсы/Роли» требуется:

- задать местонахождение и параметры соединения с ресурсными СУБД, в которых хранятся системные наименования должностных и функциональных ролей;

- выбрать файл со справочниками ролей нажав кнопку **[Обзор],** в которых хранятся соответствия между системными наименованиями должностных и функциональных ролей и их полными наименованиями;

- нажать на кнопку **[Обновить список ролей]** и указать пароли пользователей для доступа к ресурсным базам данных и базам данных, содержащих справочники ролей;

- сформировать с использованием кнопок  и  должностные роли из списка функциональных ролей и нажать на кнопку **[Применить]** (рис. 23);

- в открывшемся окне «Подтверждение изменений» для сохранения изменений нажать на кнопку **[Подтвердить]** или **[Отменить]** для их отмены.

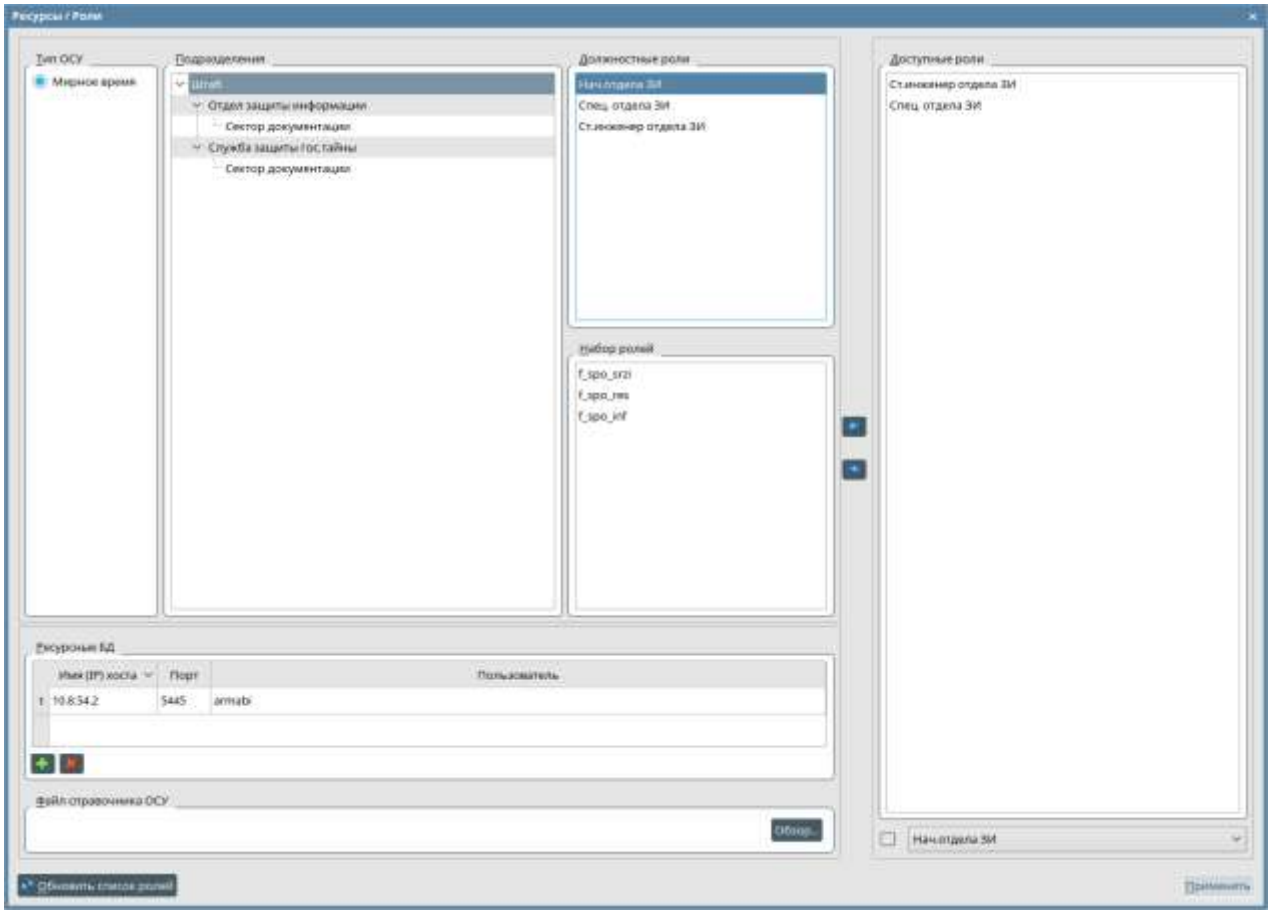


Рис. 23 – Настройка должностных и функциональных ролей

Справочник ролей может загружаться из файлов формата XML или JSON.

3.5.5.1. Описание файла справочника ролей в формателXML

Файл справочника ролей в формате XML состоит из заголовка, тегов подразделений и тегов должностных ролей.

Описание заголовка документа:

- <address:imod xmlns:addresstypes="imod:address:types" xmlns:types="imod:types" xmlns:address="imod:address" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:schemaLocation="imod:address file:../address/imod_address.xsd"> – тег должен содержать все параметры по умолчанию и должен быть закрыт в конце документа </address:imod>;

- <id> – идентификатор сообщения указанный по стандарту UUID;

- <xsdVersion> – версия схемы ИМОД "Адресная книга" должна быть по умолчанию 16.3.0.0;

- <time> – дата и время формирования сообщения в UTC представлении.

Описание тегов подразделений:

- <department> – указывается перечень подразделений ОСУ;

- <id> – идентификатор подразделения указанный по стандарту UUID;

- <classRef> – тип ОСУ, к которому относится подразделение;

- <name> - наименование подразделения, не может быть пустой и длина не более 256 символов;

- <parentDepartmentRef> – ссылка на вышестоящее подразделение, в формате идентификации UUID.

Описание тегов должностных ролей:

- <post> – перечень должностей ОСУ;

- <id> – идентификатор должности указанный по стандарту UUID;

- <classRef> – уникальный код должности, не допускается пустая строка длиной не менее 5 и не более 32 символов. Строка должна соответствовать формату «d_{тип АСУ}_{имя роли}»;

- <name> – краткое (сокращенное), уникальное наименование должности, непустая строка длиной не более 32 символов;

- <fullName> – полное наименование должности, непустая строка длиной не более 256 символов;

- <departmentRef> – ссылка на подразделение указанная по стандарту UUID.

Ниже приведен пример справочника ролей в формате XML.

```
<?xml version="1.0" encoding="UTF-8" ?>
    <address:imod xmlns:addresstypes="imod:address:types"
    xmlns:types="imod:types" xmlns:address="imod:address"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="imod:address
    file:../address/imod_address.xsd">
    <id>8804C663-3227-497E-835D-48D574B7AD58</id>
    <xsdVersion>16.3.0.0</xsdVersion>
    <time>2021-06-06T01:01:05Z</time>
<department>
    <id>0577f1be-e3b6-4713-ba9d-12bd0adc4a91</id>
    <classRef>PEACE</classRef>
    <name>Штаб</name>
</department>
<department>
    <id>80b9b711-dc74-49ab-9e93-8f0df82e2a37</id>
    <classRef>PEACE</classRef>
    <name>Отдел защиты информации</name>
    <parentDepartmentRef>0577f1be-e3b6-4713-ba9d-
    12bd0adc4a91</parentDepartmentRef>
</department>
<post>
    <id>5e42df2d-d7c4-4ae4-a092-48f699f9744d</id>
    <classRef>d_p_nachotd</classRef>
    <name>Нач.отдела ЗИ</name>
    <fullName>Начальник отдела защиты информации</fullName>
    <departmentRef>80b9b711-dc74-49ab-9e93-
    8f0df82e2a37</departmentRef>
</post>
<post>
    <id>e6f8e06b-74f0-427c-b105-aa7ab623ef6b</id>
    <classRef>d_p_stinzh</classRef>
    <name>Ст. Инженер отдела ЗИ</name>
    <fullName>Старший инженер отдела защиты информации</fullName>
    <departmentRef>80b9b711-dc74-49ab-9e93-
    8f0df82e2a37</departmentRef>
```

```
</post>
</address:imod>
```

3.5.5.2. Описание файла справочника ролей в формате JSON

Файл справочника ролей в формате JSON состоит из массивов подразделений и тегов должностных ролей и массивов должностных лиц.

Описание массива подразделений:

- "department": [блоки подразделений] – указывается перечень подразделений ОСУ;
- "id" – идентификатор подразделения указанный по стандарту UUID;
- "typeOsu" – тип ОСУ, к которому относится подразделение;
- "name" – наименование подразделения, не может быть пустой и длина не более 256 символов;
- "memberOfIds" – ссылка на вышестоящее подразделение указанная по стандарту UUID, может содержать несколько подразделений перечисленных через запятую, если нет вышестоящих подразделений, указывается значение null.

Описание массива должностных ролей:

- "posts": [блоки должностных ролей] – перечень должностей ОСУ;
- "id" – идентификатор должности, указанный по стандарту UUID;
- "roleCode" – уникальный код должности, не допускается пустая строка длиной не менее 5 и не более 32 символов. Строка должна соответствовать формату «d_{тип АСУ}_{имя роли}»;
- "name" – краткое (сокращенное), уникальное наименование должности, непустая строка и не более 32 символов;
- "fullName" – полное наименование должности, непустая строка и не более 256 символов;
- "memberOfIds" – ссылка на подразделение, указанная по стандарту UUID, может содержать несколько ссылок на подразделения перечисленных через запятую.

Ниже приведен пример справочника ролей в формате JSON.

```
{
  "departments": [
    {
      "id": "0577f1be-e3b6-4713-ba9d-12bd0adc4a91",
      "typeOsu": "PEACE",
      "name": "Штаб",
      "memberOfIds": null
```

```
    },
    {
      "id": "80b9b711-dc74-49ab-9e93-8f0df82e2a37",
      "typeOsu": "PEACE",
      "name": "Отдел защиты информации",
      "memberOfIds": [
        "0577f1be-e3b6-4713-ba9d-12bd0adc4a91"
      ]
    },
]
  "posts": [
    {
      "id": "5e42df2d-d7c4-4ae4-a092-48f699f9744d",
      "roleCode": "d_p_ nachotd",
      "name": "Нач. отдела ЗИ",
      "fullName": "Начальник отдела защиты информации",
      "memberOfIds": [
        "80b9b711-dc74-49ab-9e93-8f0df82e2a37",
        "0577f1be-e3b6-4713-ba9d-12bd0adc4a91"
      ]
    },
    {
      "id": "e6f8e06b-74f0-427c-b105-aa7ab623ef6b",
      "roleCode": "d_p_stinzh",
      "name": "Ст. инженер отдела ЗИ",
      "fullName": "Старший инженер отдела защиты информации",
      "memberOfIds": [
        "80b9b711-dc74-49ab-9e93-8f0df82e2a37",
      ]
    },
]
}
```

3.5.6. Настройка доступа пользователей к ресурсам на основе ролевой модели

Перед выполнением настройки доступа пользователя на основе ролевой модели необходимо настроить аутентификацию пользователей в базе данных в соответствии с документом «Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 2» РУСБ.10015-01 95 01-2.

При использовании для организации единого пространства пользователей службы организации домена ALD для обеспечения доступа пользователей одного домена к ресурсам другого домена между ними должны быть настроены доверительные отношения в соответствии с документом «Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 1» РУСБ.10015-01 95 01-1.

Для выполнения настройки доступа пользователя к ресурсам на основе ролевой модели необходимо перейти на вкладку «Ролевая политика» в окне «Настройки пользователя» (рис. 24).

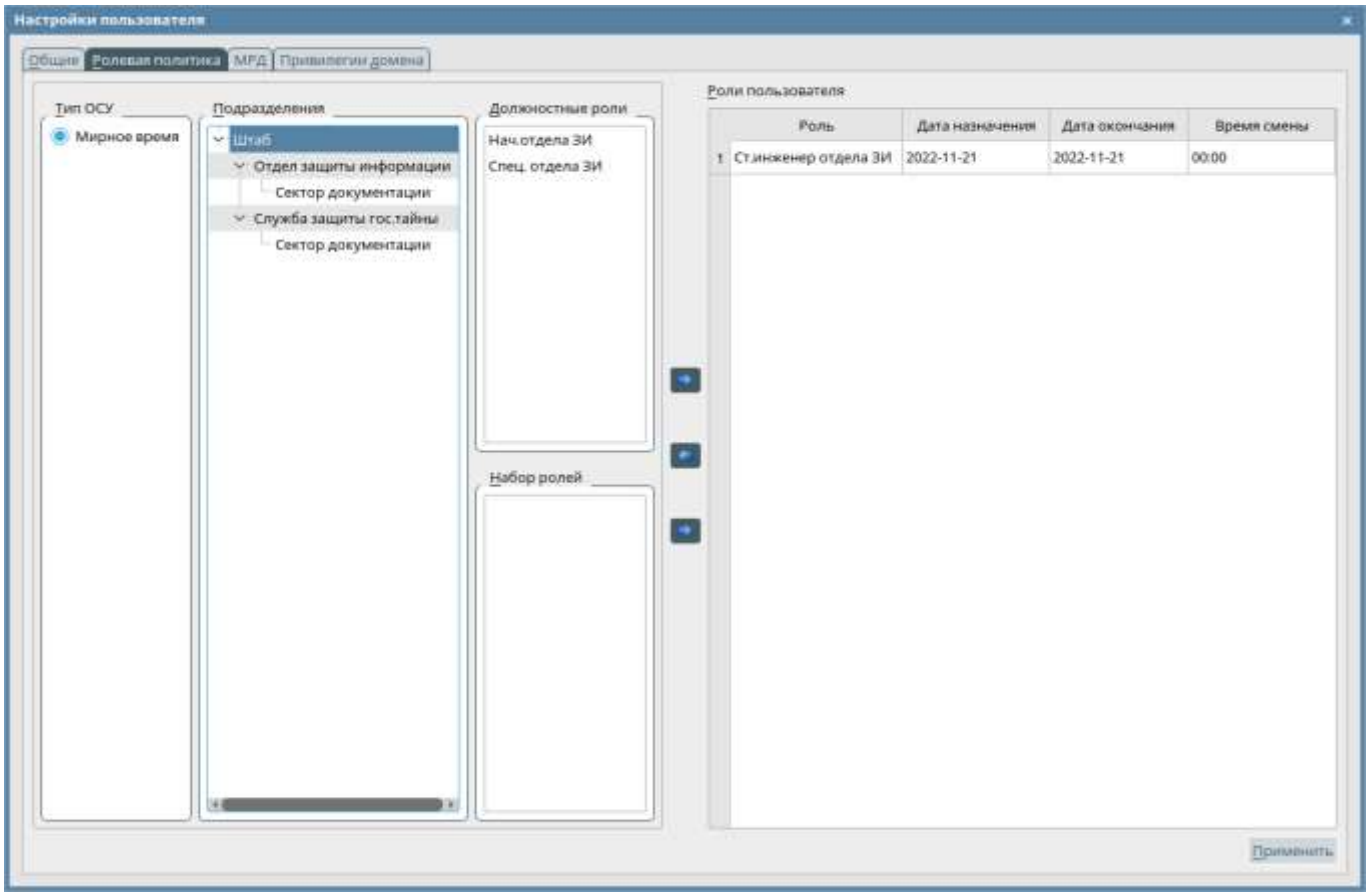


Рис. 24 – Настройка доступа пользователя к ресурсам на основе ролевой модели

В окне «Должностные роли» список доступных должностных и функциональных ролей с использованием кнопок  и  пользователю необходимо назначить роли, обеспечивающие доступ учетной записи к требуемым информационным ресурсам.

Для сохранения изменений необходимо нажать на кнопку **[Применить].**

3.5.7. Блокировка/разблокировка учетной записи пользователя

Для выполнения блокировки/разблокировки учетной записи пользователя необходимо перейти на вкладку «Общие» в окне «Настройки пользователя».

Блокировка/разблокировка учетной записи пользователя выполняется одновременно во всех доменах из списка «Домены пользователя».

В случае, если текущий статус учетной записи пользователя «Активен», при нажатии на кнопку **[Блокировать]** статус учетной записи пользователя меняется на «Блокирован» (рис. 25), текущие сессии пользователя на АРМ прерываются и на экран выводится экран приветствия ОС СН «Astra Linux Special Edition» (запущенные процессы не будут остановлены). Войти в систему повторно пользователь не сможет до тех пор, пока его учетная запись не будет разблокирована.

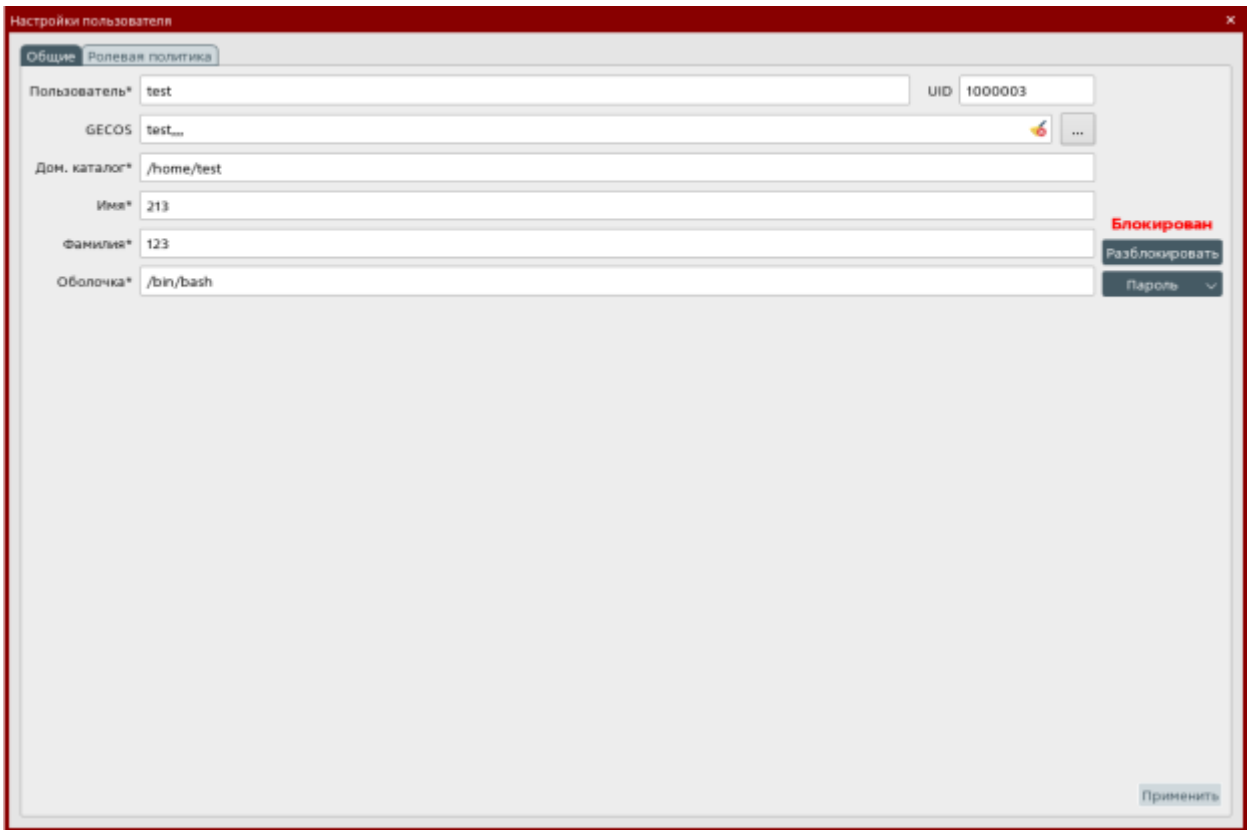


Рис. 25 – Учетная запись пользователя блокирована

В случае если текущий статус учетной записи пользователя «Блокирован» при нажатии на кнопку **[Разблокировать]** учётная запись будет разблокирована и статус «Блокирован» перестанет отображаться.

3.5.8. Установка/смена пароля учетной записи пользователя

Для установки/смены пароля учетной записи пользователя необходимо перейти на вкладку «Общие» в окне «Настройки пользователя».

Установка/смена пароля учетной записи пользователя выполняется одновременно во всех доменах из списка «Домены пользователя». Устанавливаемый для учетной записи пользователя пароль при этом должен соответствовать применяемой политике паролей домена.

Для установки пароля учетной записи пользователя необходимо нажать на кнопку **[Пароль]** и выбрать один из способов: «Генерировать пароль» или «Задать пароль» (рис. 26).

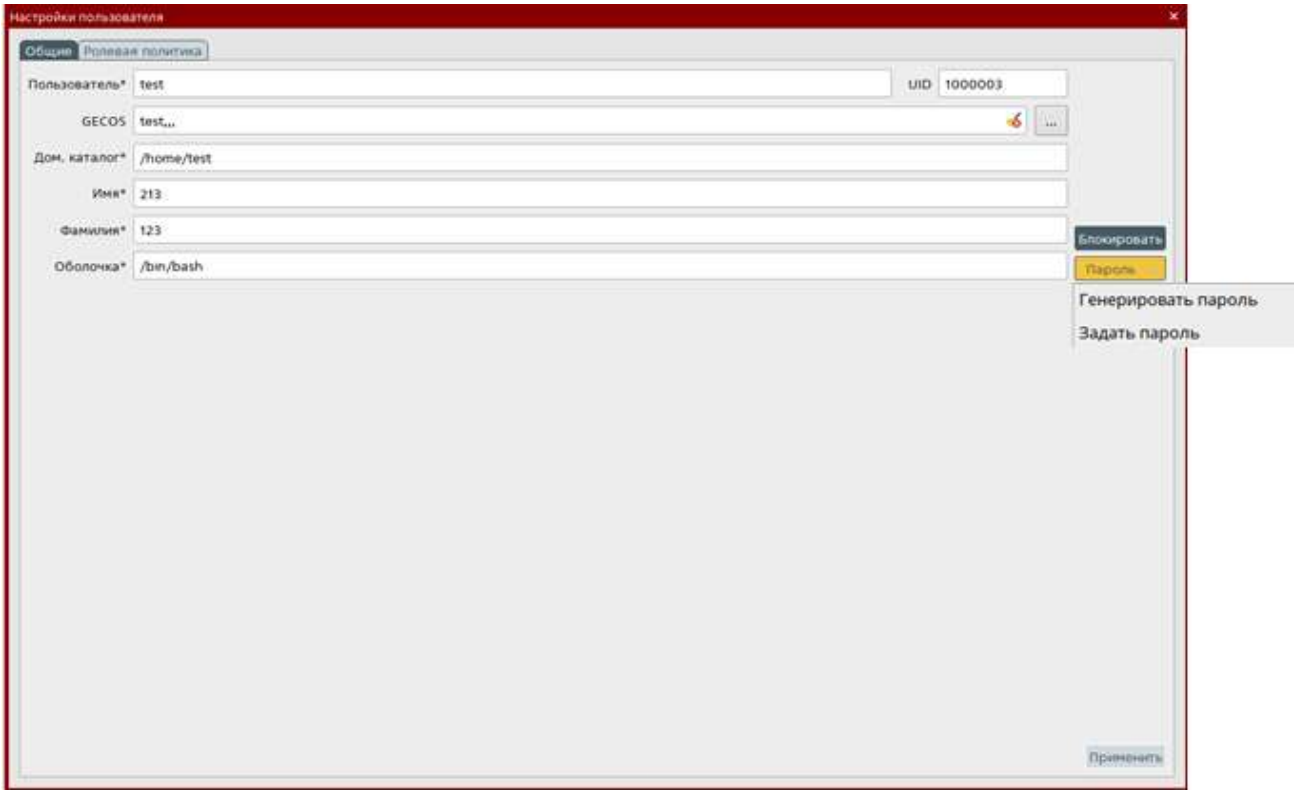


Рис. 26 – Выбор способа генерации пароля

При выборе первого варианта генерация и установка пароля учетной записи пользователя выполняется посредством использования компонента «Динамические программные библиотеки» РУСБ.51122-01 из состава изделия КП СГП РУСБ.30563-01. При этом открывается диалоговое окно, в котором требуется установить значения

параметров вновь создаваемого пароля (длина, алфавит) и нажать на кнопку **[Создать пароль]** (рис. 27).

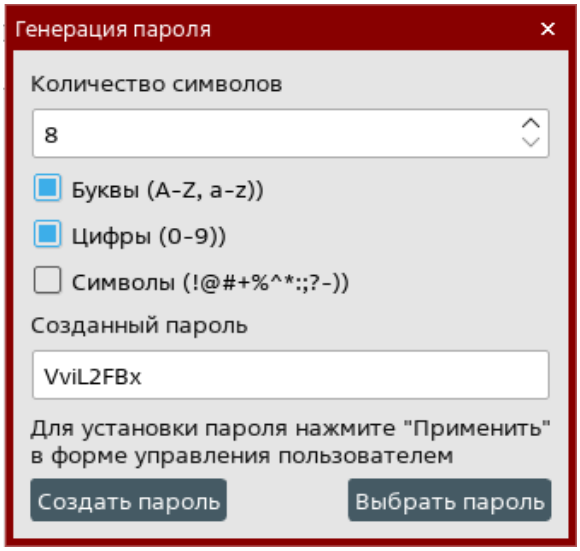


Рис. 27 – Генерация пароля учетной записи пользователя

По завершении генерации пароля, который отобразится в строке «Созданный пароль» необходимо нажать на кнопку **[Выбрать пароль]**.

При выборе второго варианта пароль задается вручную администратором безопасности информации в открывающемся диалоговом окне. Вновь устанавливаемый пароль для учетной записи пользователя требуется ввести в полях «Пароль» и «Подтверждение пароля» и нажать на кнопку **[Подтвердить]** (рис. 28).

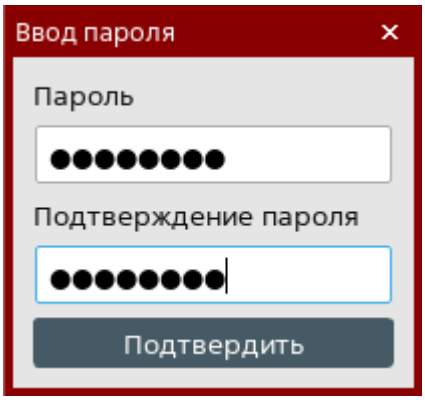


Рис. 28 – Ручной ввод пароля учетной записи пользователя

Для установки пароля учетной записи пользователя требуется нажать на кнопку **[Применить]** в окне «Настройки пользователя».

После установки/смены пароля пользователя будет выведена карточка пользователя со следующими параметрами (рис. 29):

- идентификатор системы;

- номер карточки;

- логин пользователя;
- пароль пользователя;
- место для подписи «Карточку выдал»;
- место для подписи «Карточку получил».

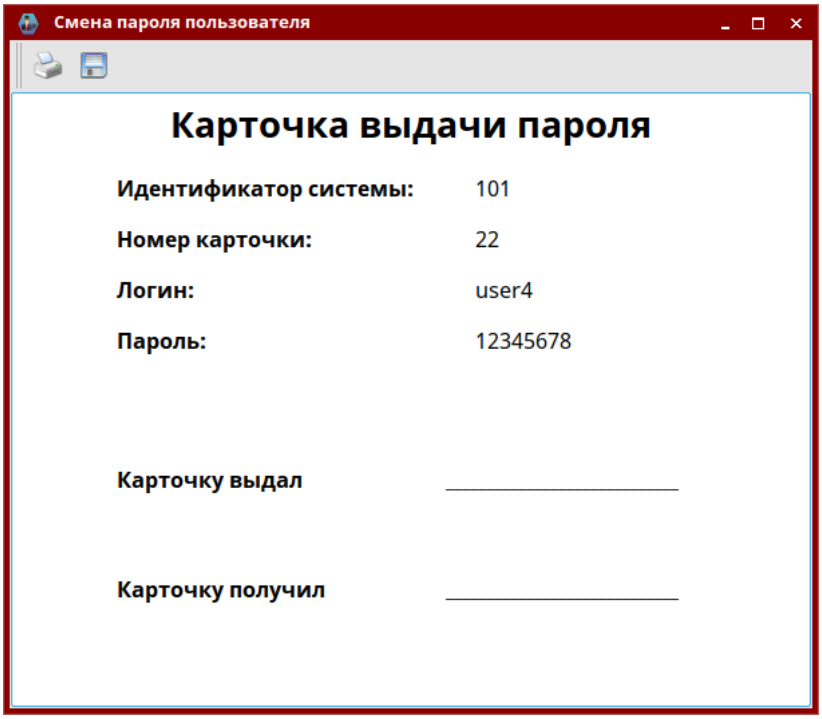


Рис. 29 – Карточка выдачи пароля

Если срок действия учётной записи пользователя (учётной записи Kerberos) истёк, то будет выведено сообщение об ошибке (рис. 30).

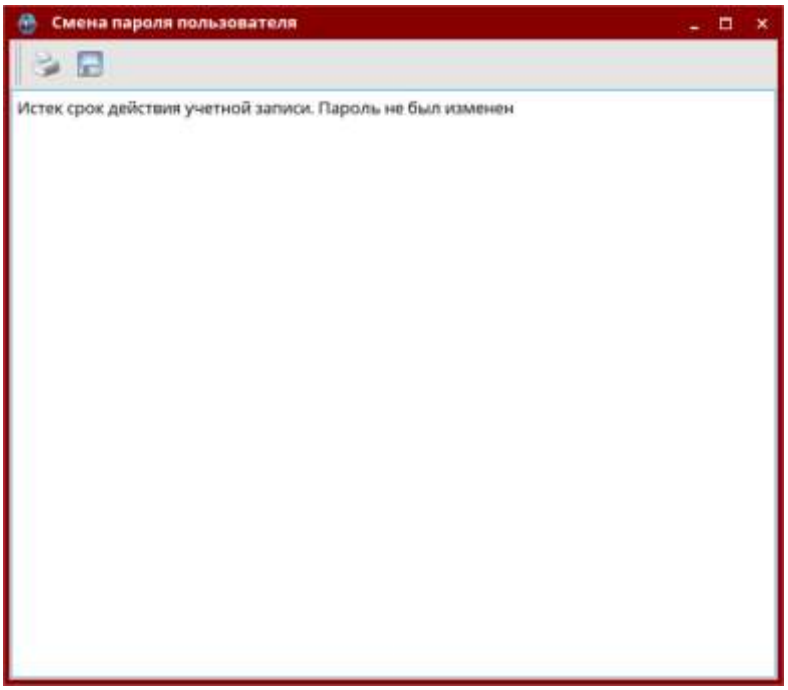


Рис. 30 – Ошибка для истекшей учётной записи

3.6. Раздел «Тестирование СЗИ»

Раздел программы «Тестирование» предназначен для запуска тестирования работоспособности СЗИ (КСЗ ОС СН и СУБД, КЦ, САВЗ) на управляемых устройствах и просмотра результатов его проведения (если проводилось). Внешний вид раздела приведен на рис. 31 и содержит следующую информацию:

- имя, ip-адрес и mac-адрес устройства;
- результаты проведения тестирования СЗИ устройства;
- дату и время проведения тестирования СЗИ устройства.

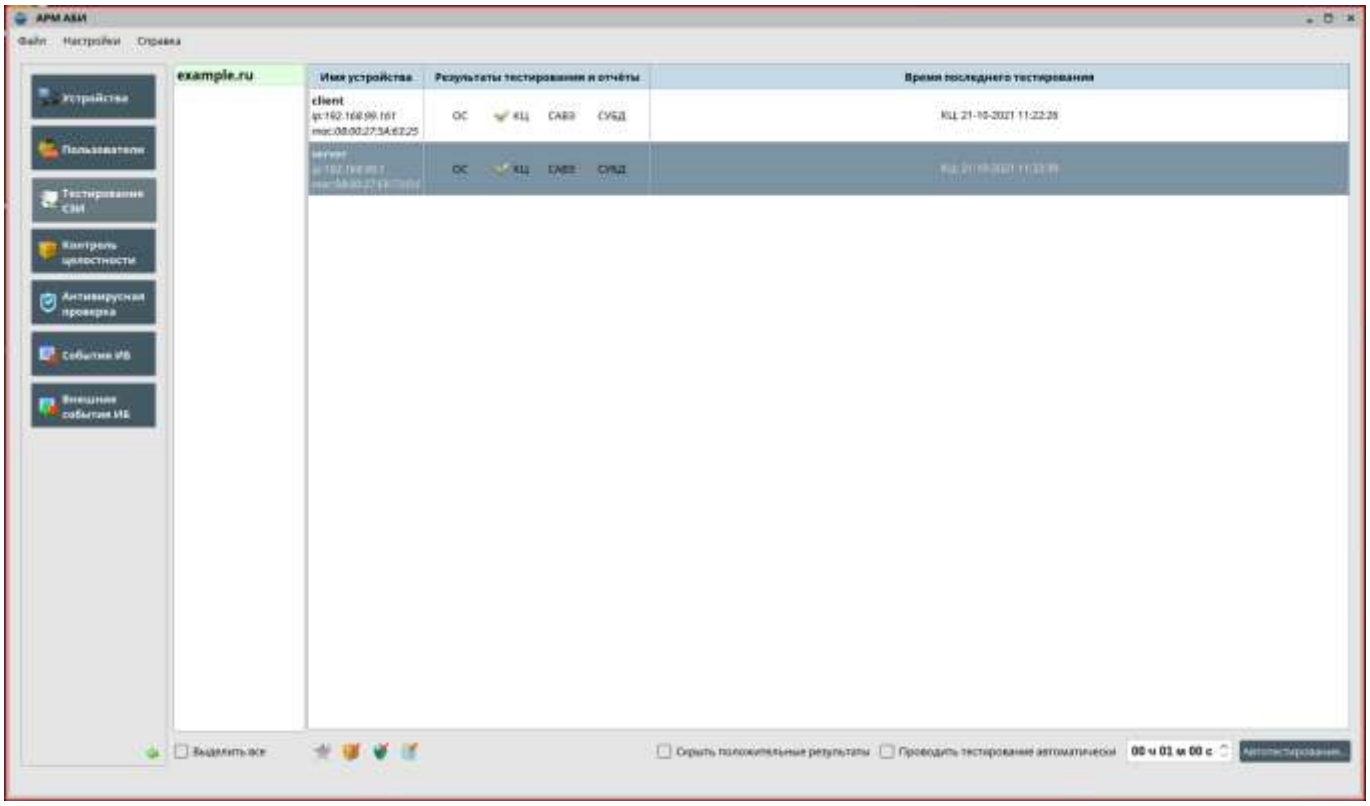


Рис. 31 – Раздел «Тестирование СЗИ»

В нижней части окна программы отображаются кнопки запуска тестирования КСЗ ОС СН и СУБД, работоспособности КЦ и САВЗ, параметры для настройки автотестирования, а также флажок для скрытия положительных результатов тестирования.

Для выполнения тестирования СЗИ необходимо выбрать из списка управляемое устройство и нажать:

- для проведения тестирования КСЗ ОС СН кнопку ;
- для проведения тестирования работоспособности КЦ кнопку ;
- для проведения тестирования работоспособности САВЗ кнопку ;

- для проведения тестирования КСЗ СУБД кнопку .

После запуска тестирования СЗИ кнопки запуска тестов становятся неактивными до тех пор, пока процесс не будет завершен.

После выполнения тестирования работоспособности средства защиты результат проведения отображается в столбце «Результаты тестирования и отчеты» в виде значка в случае отсутствия ошибок или в случае их наличия. В столбце «Время последнего тестирования» при этом выводится информация о дате и времени проведения тестирования работоспособности средства защиты.

Если необходимо скрыть положительные результаты тестирования (например, в том случае, когда в программе находится большое количество контролируемых устройств и необходим анализ устройств с ошибками в работоспособности СЗИ) то необходимо установить флажок «Скрыть положительные результаты».

Для просмотра отчета о результатах тестирования СЗИ для определенного устройства необходимо выбрать его в списке и кликнуть на соответствующем тесте левой клавишей «мыши» в графе «Результаты тестирования и отчеты» значок результата проведения тестирования работоспособности соответствующего средства защиты. Внешний вид отчетов о результатах тестирования средств защиты устройства представлен на рис. 32 - 35.

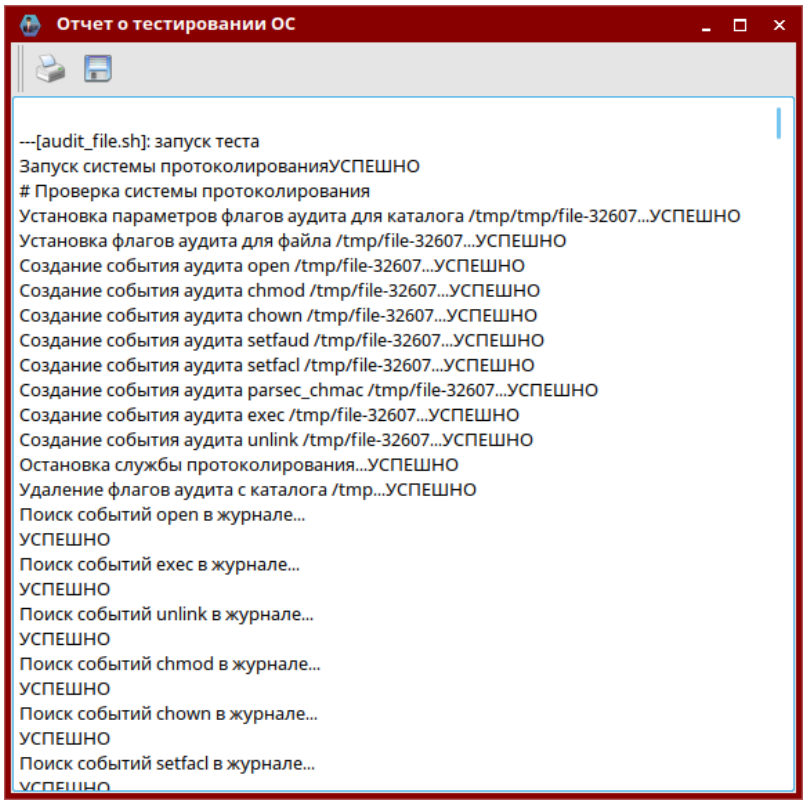


Рис. 32 – Отчет о результатах тестирования КСЗ ОС СН

Рис. 33 – Отчет о результатах тестирования работоспособности КЦ

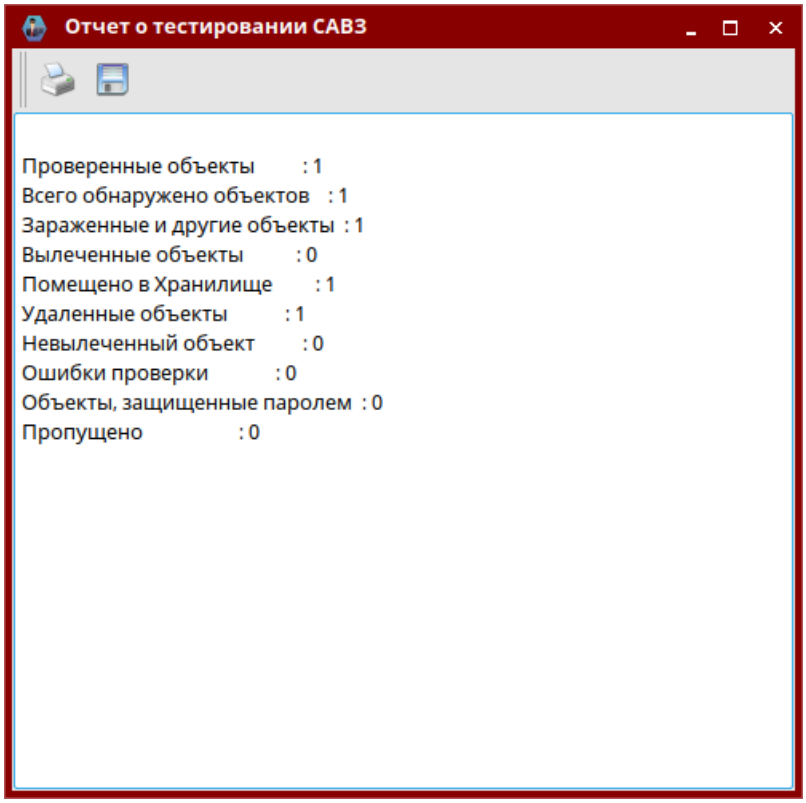


Рис. 34 – Отчет о результатах тестирования работоспособности САВЗ

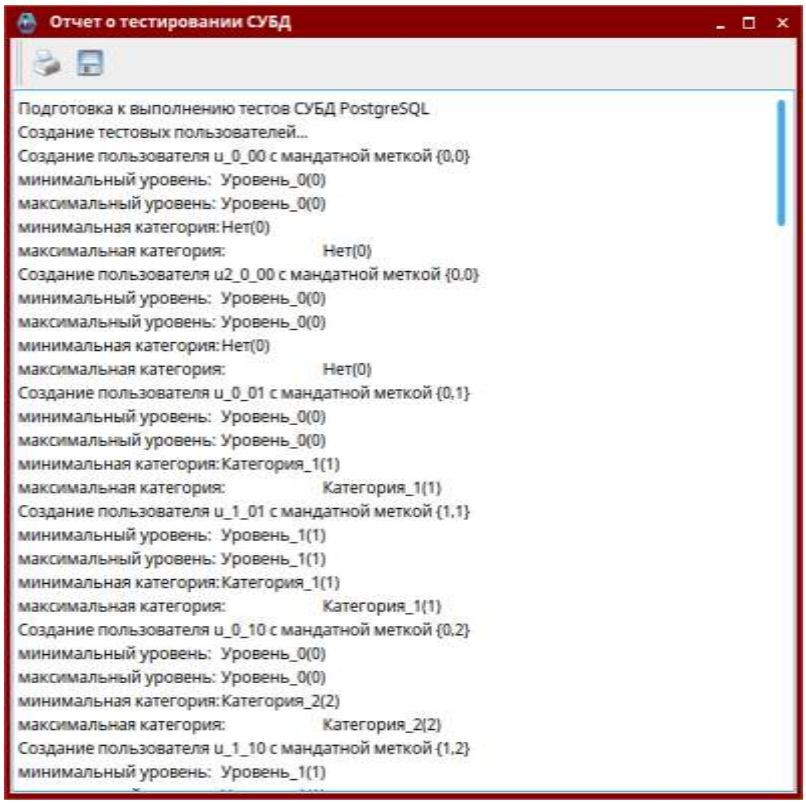


Рис. 35 – Отчет о результатах тестирования КСЗ СУБД

Подробные сведения о тестировании КСЗ ОС СН и СУБД приведены в «Операционная система специального назначения «Astra Linux Special Edition» Руководство по КСЗ. Часть 2» РУСБ.10015-01 97 01-2.

3.6.1. Настройка автотестирования СЗИ

В программе реализована возможность проведения автотестирования средств защиты информации.

Для настройки автотестирования СЗИ необходимо:

- в нижней части окна программы установить флажок «Проводить тестирование автоматически»;

- выбрать временной интервал (таймер, по истечении которого будет запускаться автотестирование выбранных компонент);

- выбрать устройство из списка и нажать на кнопку **[Автотестирование]**. В открывшемся окне (рис. 36) выбрать компоненты для проверки и нажать на кнопку [**Применить]**.

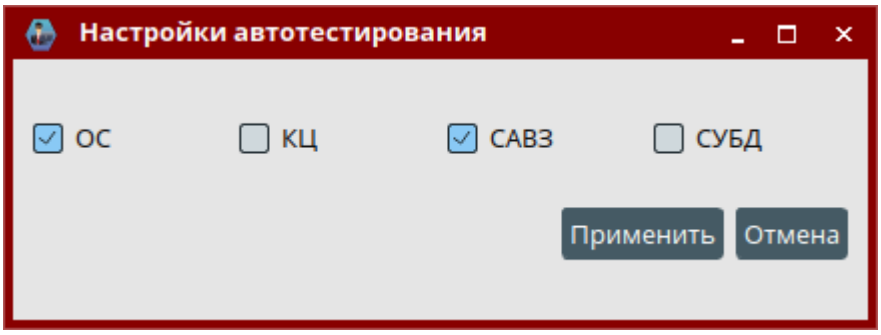


Рис. 36 – Настройки автотестирования

Компоненты, для которых настроено автотестирование, будут подсвечиваться синим цветом (рис. 37).

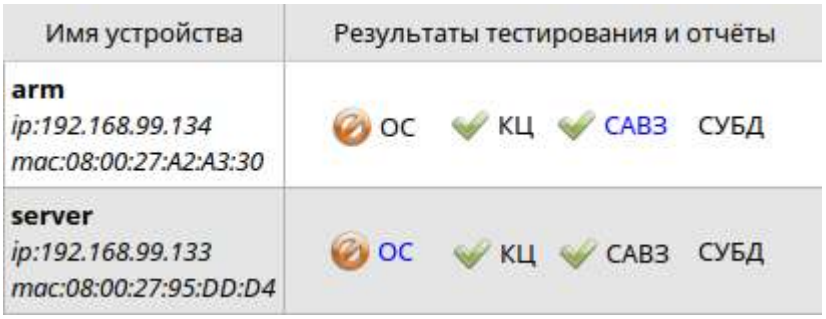


Рис. 37 – Компоненты автотестирования (САВЗ и ОС)

3.7. Раздел «Контроль целостности»

Раздел «Контроль целостности» программы предназначен для редактирования перечня объектов (информационных ресурсов) регламентного контроля целостности (КЦ) устройств, запуска регламентного КЦ на управляемых устройствах и просмотра результатов его проведения. Внешний вид раздела приведен на рис. 38 и содержит следующую информацию:

- имя, ip-адрес и mac-адрес устройства;
- результаты тестирования КЦ;
- дату и время проведения КЦ.

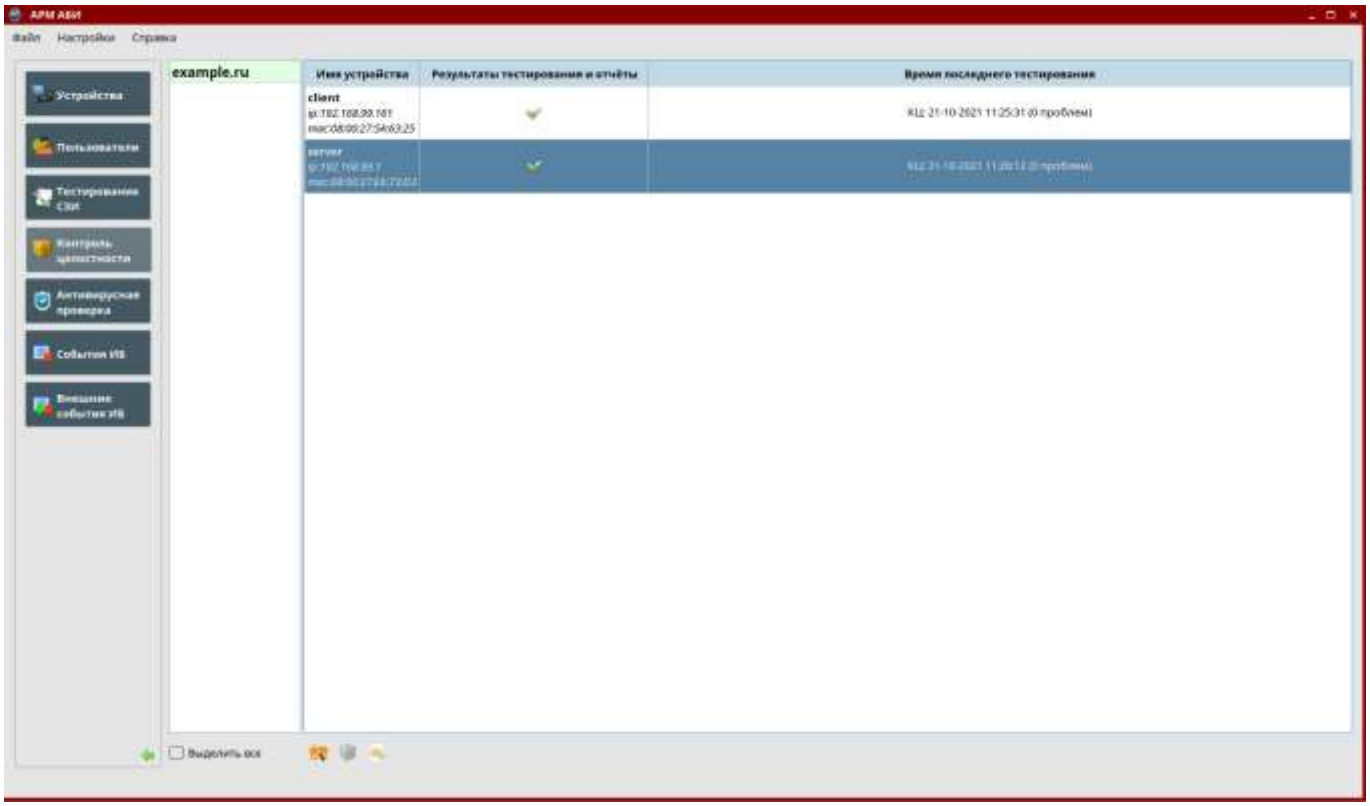


Рис. 38 – Раздел «Контроль целостности»

В нижней части окна программы отображаются кнопка запуска КЦ, кнопка настройки перечня объектов для КЦ и кнопка отправки конфигурации КЦ на управляемое устройство.

3.7.1. Настройка перечня объектов для КЦ

Для настройки перечня объектов регламентного КЦ устройства необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Перечень объектов для КЦ» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части – перечень объектов, к которым применяется КЦ на данном устройстве (рис. 39).

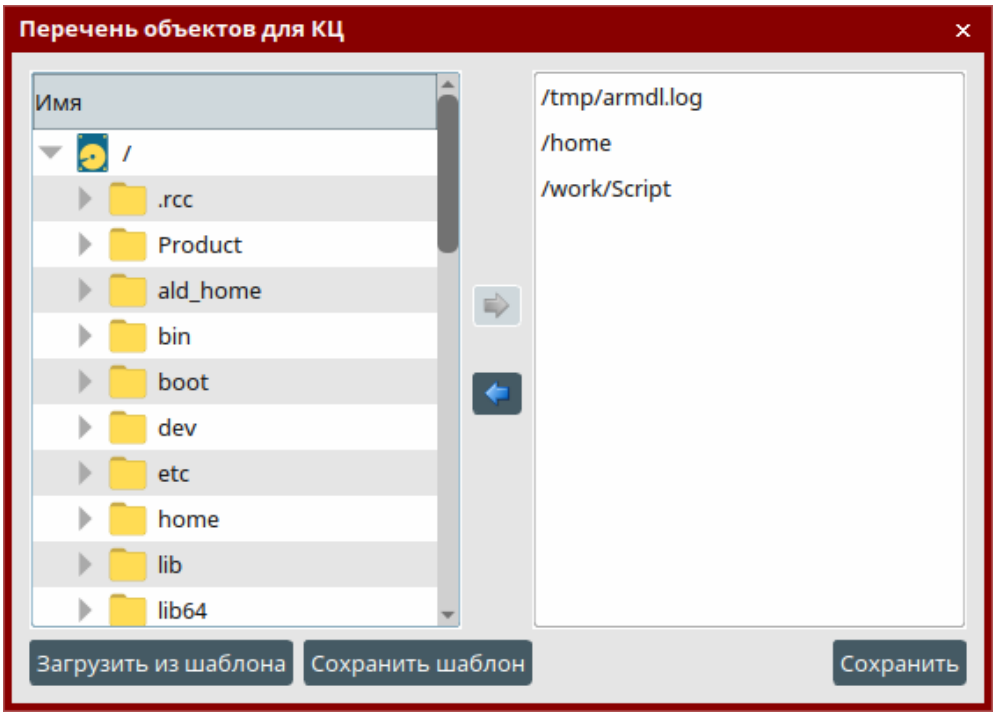


Рис. 39 – Назначение компонент КЦ

Для добавления в перечень нового объекта необходимо выбрать соответствующий файл или директорию в левой части окна и нажать на кнопку  .

Для удаления объекта из перечня необходимо выбрать соответствующий файл или директорию в правой части окна и нажать на кнопку  .

Настроенный перечень объектов, к которым применяется КЦ на данном устройстве, можно сохранить в качестве шаблона конфигурации КЦ, нажав на кнопку **[Сохранить шаблон]**. Шаблон будет сохранен в каталог для шаблонов файлов конфигурации (`/opt/ArmAbi/resources` по умолчанию).

Примечание. Сохраненный шаблон не привязывается к конкретному устройству и одинаков для всей системы. Таким образом, при изменении перечня объектов на устройстве и сохранения шаблона предыдущий шаблон будет перезаписан.

Перечень объектов, к которым применяется КЦ на данном устройстве, можно загрузить из ранее созданного шаблона конфигурации КЦ, нажав на кнопку **[Загрузить из шаблона]**.

По окончании редактирования перечня объектов для КЦ необходимо нажать на кнопку **[Сохранить]**.

3.7.2. Запуск КЦ

Для запуска регламентного КЦ необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

После запуска КЦ кнопка становится неактивной до тех пор, пока процесс не будет завершен.

После проведения регламентного контроля целостности на устройстве результат проведения регламентного КЦ отображается в столбце «Результаты тестирования и отчеты» в виде значка  в случае отсутствия ошибок или  в случае их наличия. В столбце «Время последнего тестирования» при этом выводится информация о дате и времени проведения КЦ, а также количестве ошибок.

Для просмотра отчета о результатах проведения КЦ для определенного устройства необходимо выбрать его в списке и кликнуть левой клавишей «мыши» в графе «Результаты тестирования и отчеты» значок результата проведения КЦ. Внешний вид отчета о результатах проведения КЦ устройства представлен на рис. 40.

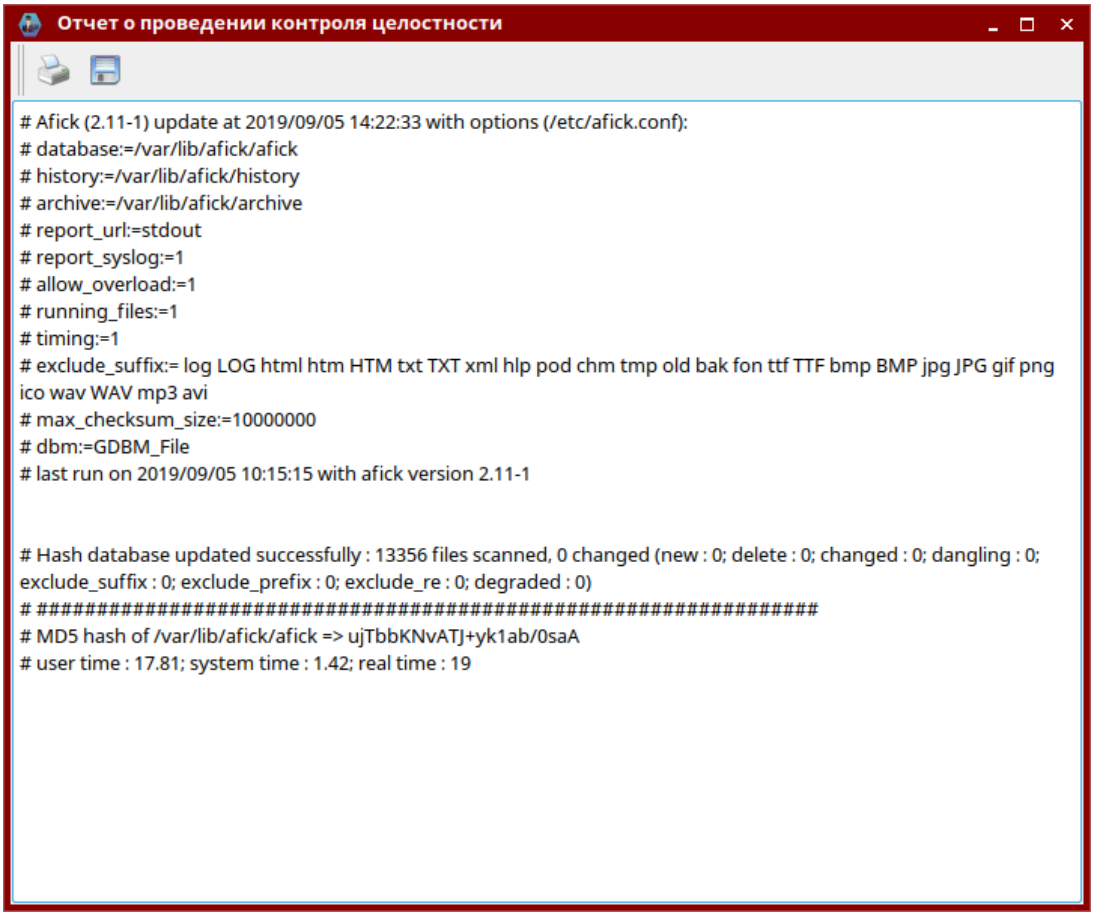


Рис. 40 – Отчет о результатах проведения КЦ устройства

Подробные сведения о контроле целостности приведены в разделе 9 документа «Операционная система специального назначения «Astra Linux Special Edition» Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

3.7.3. Отправка конфигурации КЦ на управляемое устройство

Для отправки ранее сформированного шаблона конфигурации КЦ, содержащего перечень объектов, к которым применяется КЦ, необходимо выбрать устройство из списка и нажать на кнопку  .

Обычно шаблон используется при наличии большого количества устройств с одинаковым перечнем объектов для КЦ. В таком случае необходимо отправить ранее сформированный шаблон, выделив все необходимые устройства из списка (**<Ctrl>**+левая кнопка «мыши») и нажав на кнопку  .

3.8. Раздел «Антивирусная проверка»

Программой поддерживаются следующие антивирусы:

- «Dr.Web Enterprise Security Suite»;
- «Kaspersky Endpoint Security для Linux».

Раздел программы «Антивирусная проверка» предназначен для получения информации о статусе антивирусной защиты, статусе обновления антивирусных баз, статусе и сроке действия лицензионного ключа, запуска антивирусной проверки на управляемых устройствах и просмотра результатов ее проведения (если проводилась). Внешний вид раздела приведен на рис. 41 и содержит следующую информацию:

- имя, ip-адрес и mac-адрес устройства;
- используемый на этом устройстве антивирус (Kaspersky, DrWeb);
- результаты проверки и отчёты;
- статус лицензии;
- статус антивирусной защиты;
- статус антивирусных баз;
- дату и время последнего проведения антивирусной проверки.

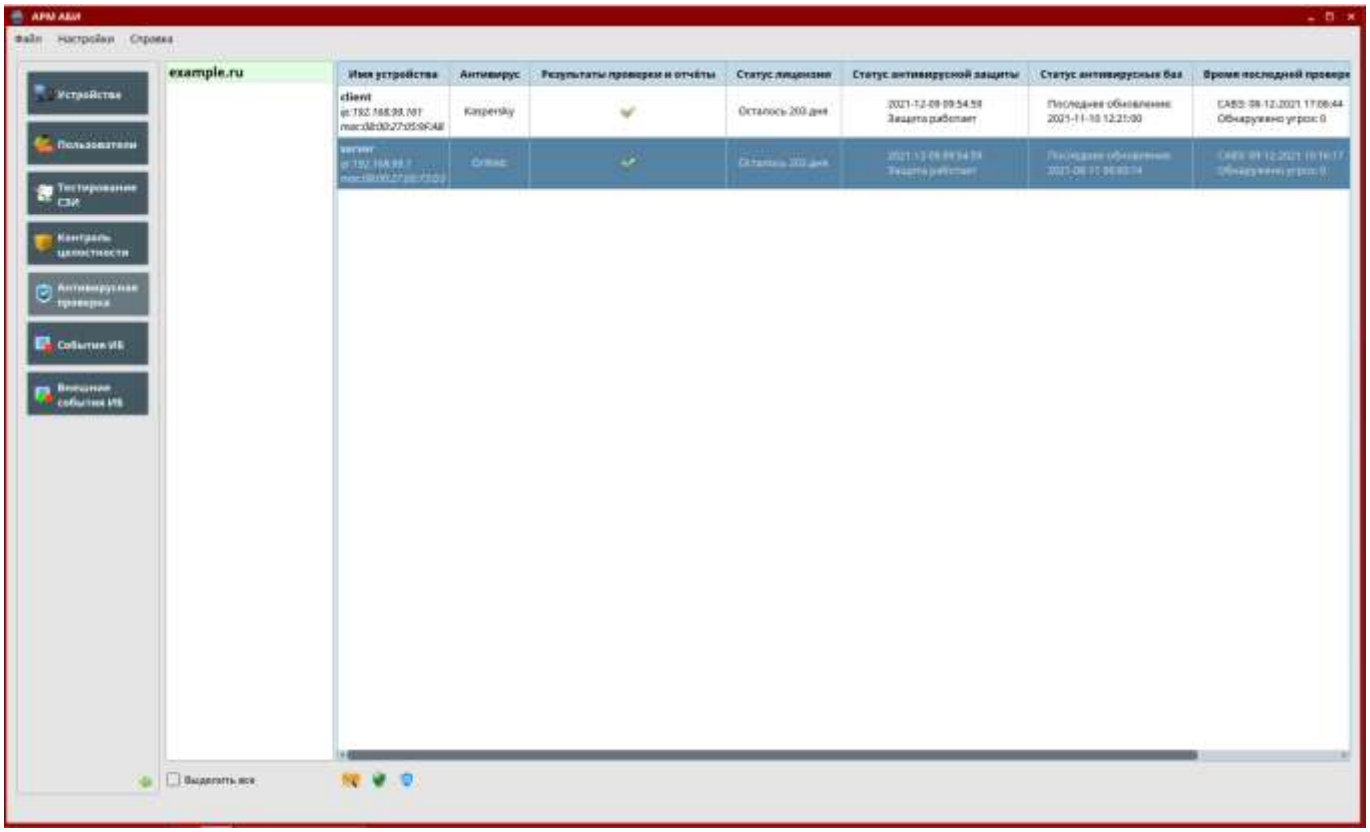


Рис. 41 – Раздел «Антивирусная проверка»

В нижней части окна программы отображаются кнопки запуска антивирусной проверки, перечня объектов для антивирусной проверки и обновления лицензионного ключа.

3.8.1. Настройка перечня объектов для антивирусной проверки

Для выполнения настройки перечня объектов для проведения антивирусной проверки необходимо выбрать из списка управляемое устройство и нажать на кнопку  .

Открывшееся окно «Перечень объектов для антивирусной проверки» состоит из двух частей. В левой части окна располагаются информационные ресурсы устройства (файлы или директории), в правой части – перечень объектов для проведения антивирусной проверки (рис. 42).

Для добавления в перечень нового объекта необходимо выбрать соответствующий файл или директорию в левой части окна и нажать на кнопку  .

Для удаления объекта из перечня необходимо выбрать соответствующий файл или директорию в правой части окна и нажать на кнопку  .

Настроенный перечень объектов для проведения антивирусной проверки можно сохранить в качестве шаблона, нажав на кнопку **[Сохранить шаблон]**. Шаблон будет

сохранен в каталог для шаблонов файлов конфигурации (`/opt/ArmAbi/resources` по умолчанию).

Примечание. Сохраненный шаблон не привязывается к конкретному устройству и одинаков для всей системы. Таким образом, при изменении перечня объектов на устройстве и сохранения шаблона предыдущий шаблон будет перезаписан.

Перечень объектов для проведения антивирусной проверки устройства можно загрузить из ранее созданного шаблона, нажав на кнопку **[Загрузить из шаблона]**.

По окончании редактирования перечня объектов для проведения антивирусной проверки необходимо нажать на кнопку **[Сохранить]**.

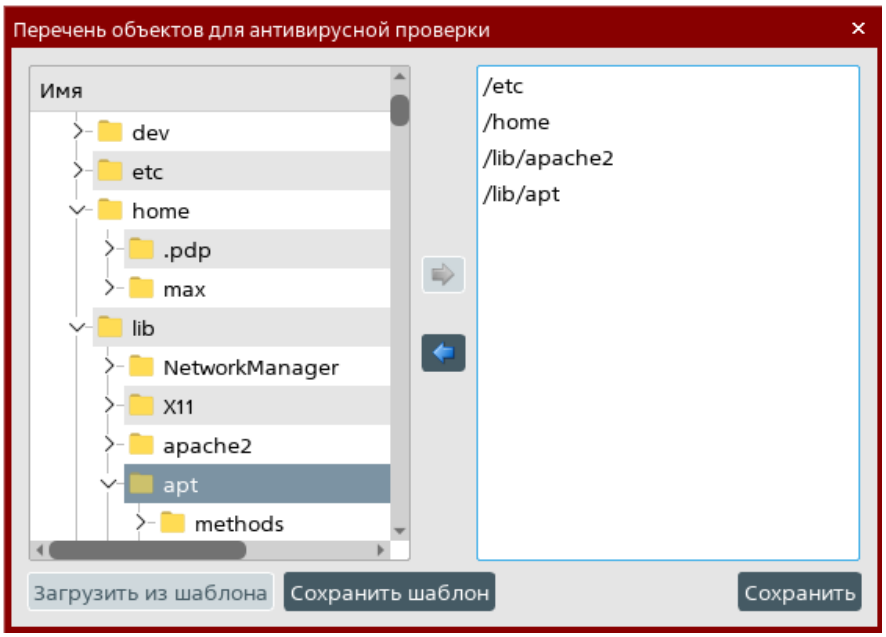


Рис. 42 – Настройка перечня объектов для антивирусной проверки

3.8.2. Запуск антивирусной проверки

Для запуска антивирусной проверки устройства необходимо выбрать его из списка управляемых устройств и нажать на кнопку  .

После запуска антивирусной проверки кнопка становится неактивной до тех пор, пока процесс не будет завершен.

Для просмотра результатов последней антивирусной проверки (если проводилась) для определенного устройства необходимо кликнуть по соответствующему статусу графе «Результаты проверки и отчеты» основного списка раздела. Внешний вид отчета о результатах антивирусной проверки представлен на рис. 43.

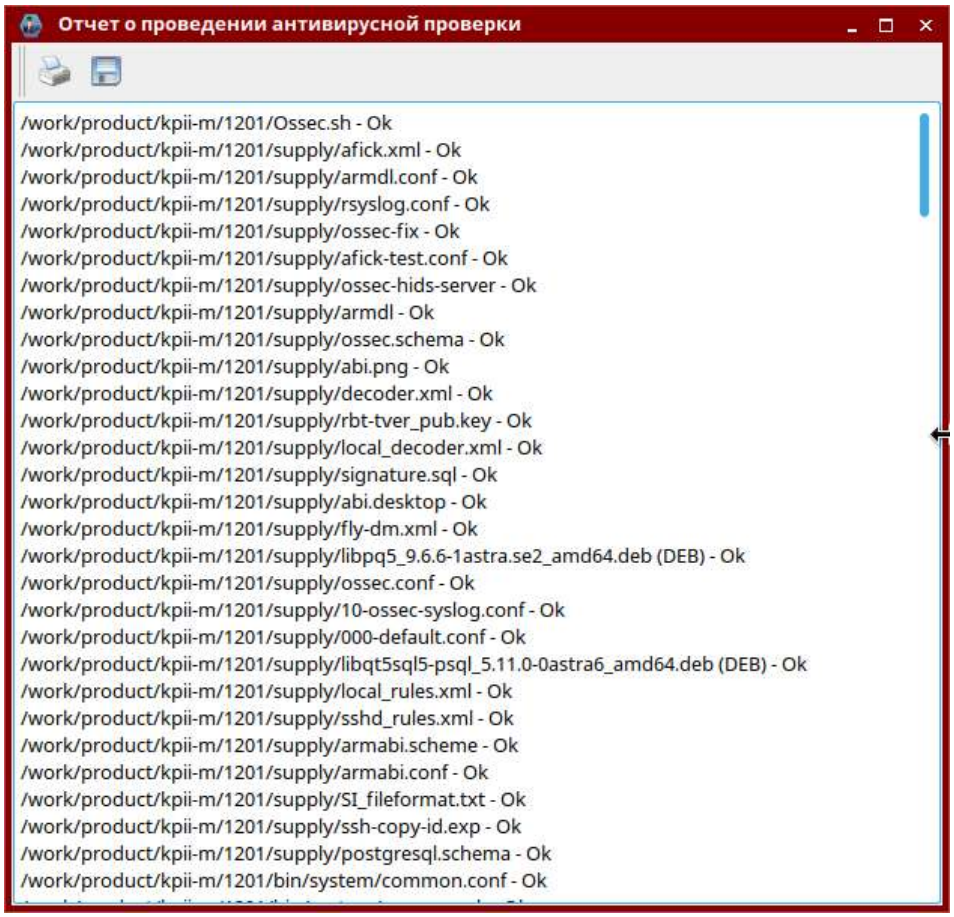


Рис. 43 – Отчет о результатах проведения антивирусной проверки устройства

3.8.3. Обновление лицензии

Для обновления лицензии необходимо выбрать из списка управляемое устройство и нажать на кнопку . В открывшемся диалоге необходимо выбрать ключевой файл `drweb32.key`, содержащий информацию о лицензии, и нажать на кнопку **[Открыть]**. В данном примере приведен ключевой файл для САВЗ «Dr.Web» (рис. 44).

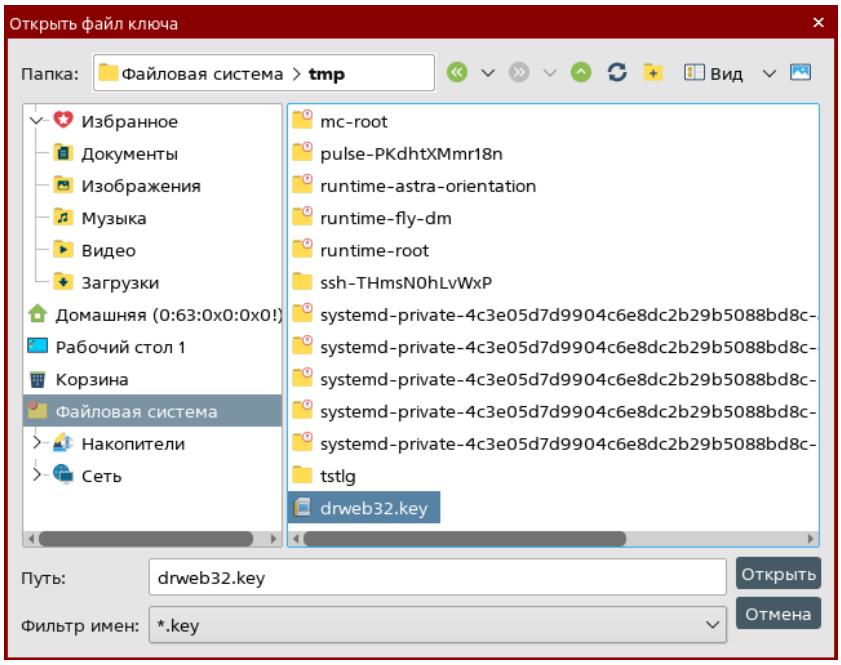


Рис. 44 – Выбор ключевого файла

Примечание. При работе Dr.Web Desktop Security Suite под управлением Центра управления Dr.Web установка ключевого файла лицензии не требуется, поэтому для таких устройств кнопка неактивна и подсвечивается серым цветом.

3.9. Раздел «События ИБ»

Раздел программы «События ИБ» предназначен для отображения в виде таблицы зафиксированных системой централизованного протоколирования на управляемых устройствах контролируемых доменов событий информационной безопасности и обнаружения попыток и фактов НСД к защищаемым ресурсам.

Программой регистрируются не только события операционной системы, но и события от следующих программных и программно-аппаратных средств:

- «Dr.Web Enterprise Security Suite»;
- «Kaspersky Endpoint Security для Linux»;
- ПАК «Набат»;
- ПК ОВ «Ребус-СОВ».

Примечание. Для обеспечения возможности регистрации событий от ПАК «Набат» необходимо при установке агента указать на каком именно устройстве находится база данных ПАК «Набат». Подробные сведения о установке агентов приведены в «ПС АРМ АБИ. Руководство системного программиста» РУСБ.30488-04 32 01.

Внешний вид раздела приведен на рис. 45 и содержит следующую информацию:

- наименование устройства;
- дата и время события;

- уровень опасности;
- пользователь, совершивший событие;
- описание события.

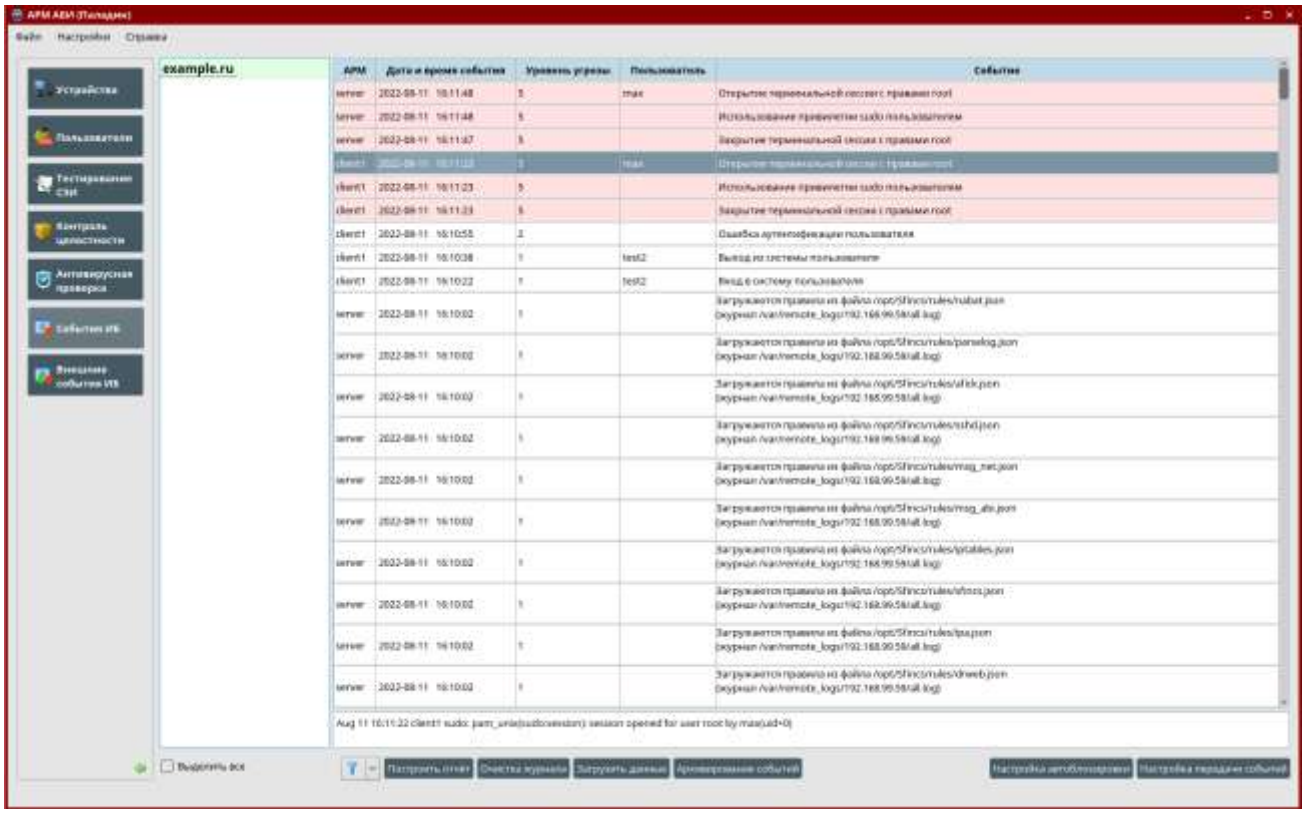


Рис. 45 – Раздел «События ИБ»

В нижней части окна программы отображаются кнопки для отображения отчета, архивирования событий информационной безопасности, очистки журнала и загрузки данных, а также кнопка настройки автоблокировки пользователей при возникновении определенных событий и кнопка настройки передачи событий информационной безопасности на вышестоящий уровень.

Также в нижней части окна программы размещена кнопка **[Фильтры]** для фильтрации событий.

Следует отметить, что подсистема регистрации событий не работает в течении некоторого времени (до тех пор, пока не стартует сервер sfincs). В этом случае следует провести анализ системного журнала ОС штатными средствами.

3.9.1. Настройка фильтра событий ИБ

События в таблице сортируются по дате обнаружения в порядке убывания даты/времени (самое последнее событие отображается в верхней строке таблицы) с учетом установленных значений в менеджере фильтров. Для настройки фильтрации событий информационной безопасности требуется нажать кнопку **[Настроить**

фильтры…] в нижней части окна. В открывшемся окне (рис. 46) настроить следующие поля: «Количество записей», «Уровень угрозы», «Тип события», «Устройство отображения», а также задающих период обнаружения событий полей «с» и «по» с соответствующими датами. Содержимое строк таблицы при этом подкрашивается в зависимости от уровня опасности события, заданного в системе централизованного протоколирования.

В поле «Количество записей» задается количество отображаемых в таблице записей. При установке значений полей «с» и/или «по» с соответствующими датами периода обнаружения событий поле «Количество записей» становится неактивным.

В поле «Уровень угрозы» задается минимальный уровень опасности событий, отображаемых в таблице и действует как при установке значения поля «Количество записей», так и при установке значений полей периода обнаружения событий.

При установке флажка «Тип события» будут отображаться только те типы событий, которые указаны справа от флажка в раскрывающемся списке.

При установке флажка «АРМ» будут отображаться события, которые возникают на выбранном устройстве.

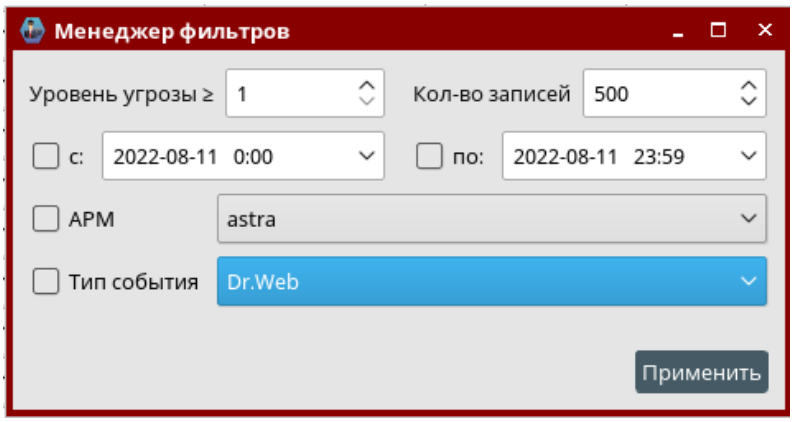
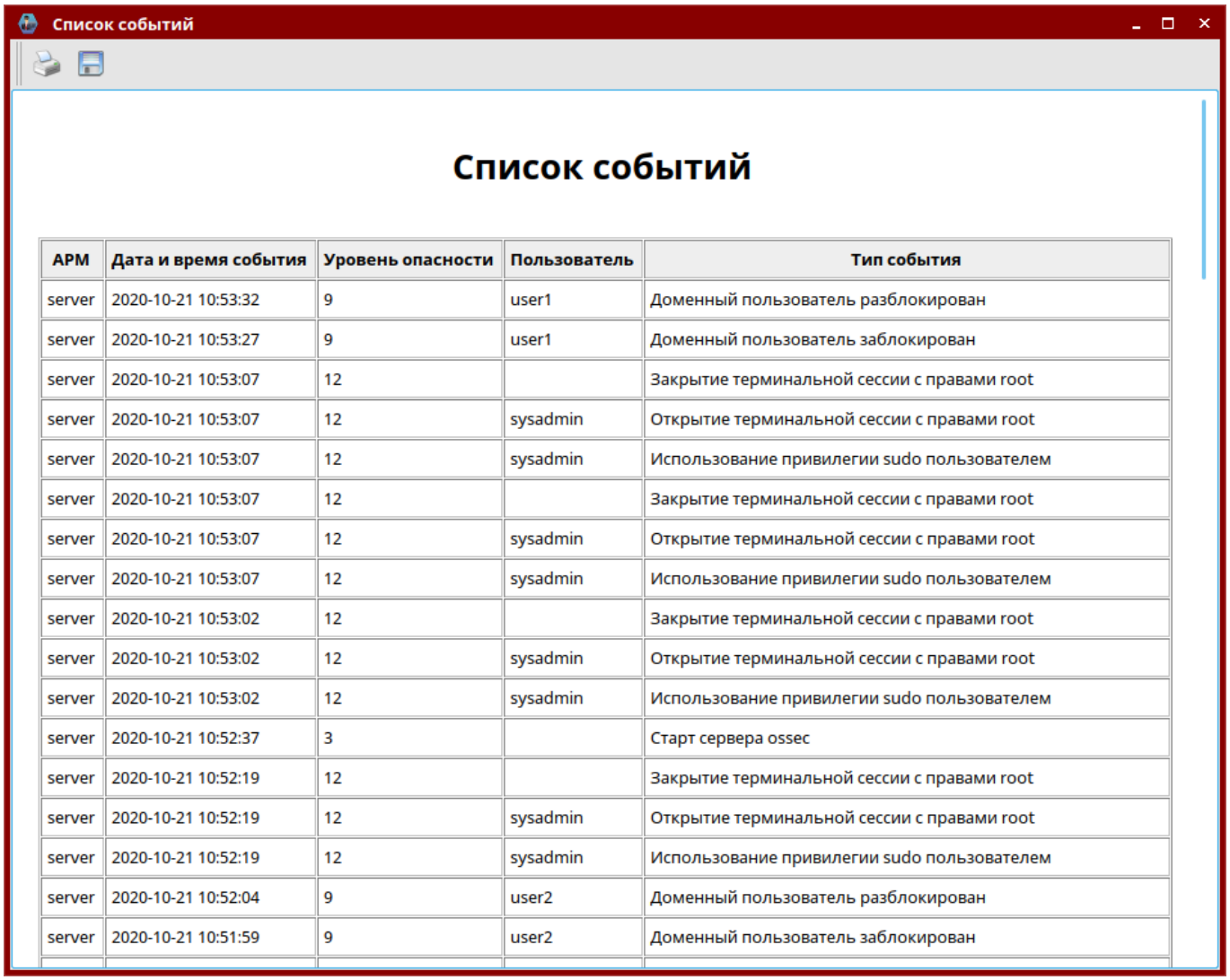


Рис. 46 – Менеджер фильтров

3.9.2. Построение отчета о событиях ИБ

Для построения отчета отображаемых в таблице событий информационной безопасности требуется нажать на кнопку **[Построить отчет]**. Внешний вид отчета о событиях информационной безопасности представлен на (рис. 47).



Список событий

АРМ	Дата и время события	Уровень опасности	Пользователь	Тип события
server	2020-10-21 10:53:32	9	user1	Доменный пользователь разблокирован
server	2020-10-21 10:53:27	9	user1	Доменный пользователь заблокирован
server	2020-10-21 10:53:07	12		Закрытие терминальной сессии с правами root
server	2020-10-21 10:53:07	12	sysadmin	Открытие терминальной сессии с правами root
server	2020-10-21 10:53:07	12	sysadmin	Использование привилегии sudo пользователем
server	2020-10-21 10:53:07	12		Закрытие терминальной сессии с правами root
server	2020-10-21 10:53:07	12	sysadmin	Открытие терминальной сессии с правами root
server	2020-10-21 10:53:07	12	sysadmin	Использование привилегии sudo пользователем
server	2020-10-21 10:53:02	12		Закрытие терминальной сессии с правами root
server	2020-10-21 10:53:02	12	sysadmin	Открытие терминальной сессии с правами root
server	2020-10-21 10:53:02	12	sysadmin	Использование привилегии sudo пользователем
server	2020-10-21 10:52:37	3		Старт сервера ossec
server	2020-10-21 10:52:19	12		Закрытие терминальной сессии с правами root
server	2020-10-21 10:52:19	12	sysadmin	Открытие терминальной сессии с правами root
server	2020-10-21 10:52:19	12	sysadmin	Использование привилегии sudo пользователем
server	2020-10-21 10:52:04	9	user2	Доменный пользователь разблокирован
server	2020-10-21 10:51:59	9	user2	Доменный пользователь заблокирован

Рис. 47 – Отчет о событиях информационной безопасности

3.9.3. Архивирование событий ИБ

Для выполнения операции архивации событий информационной безопасности требуется нажать на кнопку **[Архивирование событий]** (рис.48).

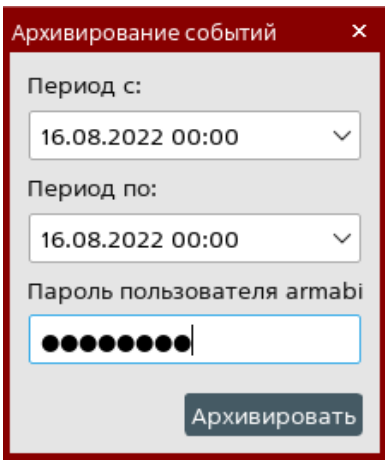


Рис. 48 – Архивация событий информационной безопасности

В открывшемся окне необходимо задать границы значения даты/времени возникновения событий и указать пароль пользователя БД. При нажатии на кнопку **[Архивировать]** появится окно, в котором необходимо указать путь, по которому сохранится архивированный файл и нажать на кнопку **[Открыть]** (рис. 49).

ВНИМАНИЕ! При сохранении архива нужно убедиться, что пользователь из-под которого запущена программа обладает необходимыми правами доступа для записи файлов в выбранный каталог.

Примечание. Архивированные события не будут удалены из БД АРМ АБИ и будут отображаться в программе, так как архивирование событий представляет собой экспорт событий в файл (например, для их последующего анализа или отправки).

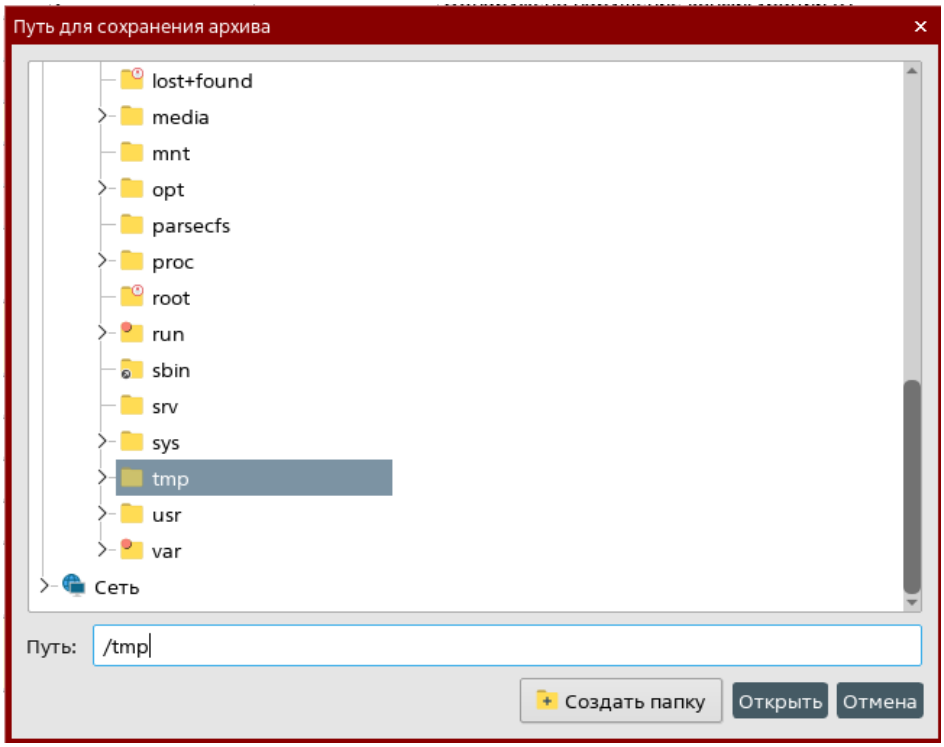


Рис. 49 – Путь для создания архива

3.9.4. Очистка журнала событий

Для выполнения операции архивации событий информационной безопасности необходимо нажать на кнопку **[Очистка журнала]**.

В открывшемся окне (рис. 50) необходимо задать верхнюю границу значения даты/времени возникновения событий, указать пароль пользователя БД и нажать на кнопку **[Очистить]**.

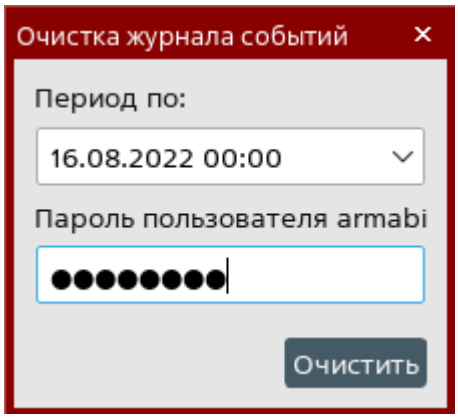


Рис. 50 – Очистка журнала событий

В результате в каталоге для архивов событий (по умолчанию `/opt/ArmAbi/archives/`) будет создан архив с указанными событиями. Данные события будут удалены из БД АРМ АБИ и не будут отображаться в разделе «События ИБ».

Примечание. При создании архива событий ему присваивается имя, содержащее дату и время, указанные в окне «Очистка журнала событий», а не дату и время фактического создания файла. В случае наличия ранее созданного архива с такой же датой и временем он будет перезаписан.

3.9.5. Загрузка событий

Загрузка событий осуществляется из архивов, созданных при очистке журнала событий. При этом следует учитывать, что события загружаются во временную таблицу базы данных АРМ АБИ и перестанут отображаться после следующего перезапуска АРМ АБИ.

Для загрузки событий необходимо нажать на кнопку **[Загрузить данные]**. В открывшемся окне (рис. 51) отобразится список созданных архивов. В данном списке необходимо выбрать нужный архив, ввести пароль пользователя БД АРМ АБИ и нажать на кнопку **[Восстановить]**.

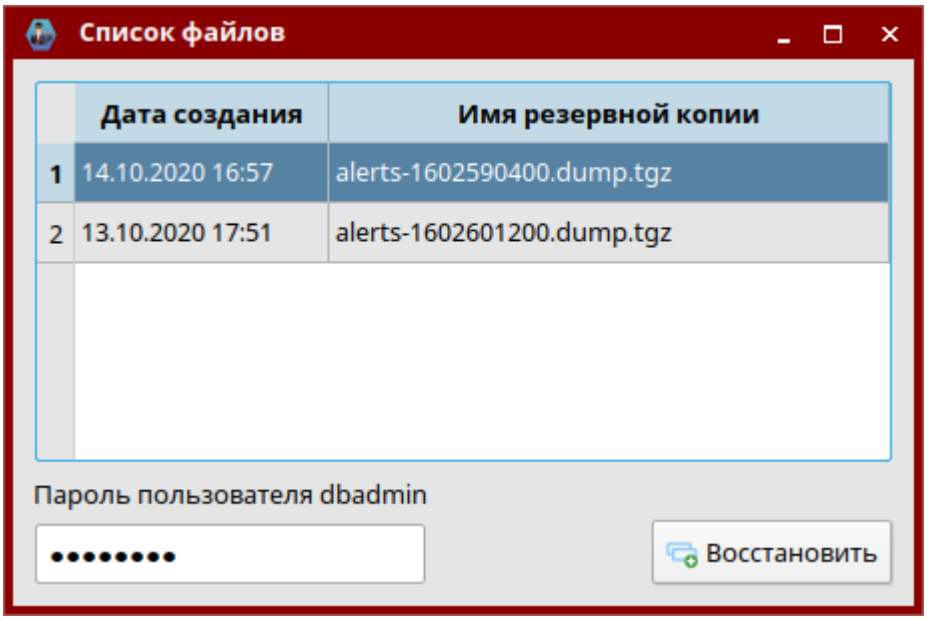


Рис. 51 – Загрузка данных из архивов

3.9.6. Настройка передачи событий ИБ на вышестоящий уровень

Для настройки передачи событий информационной безопасности на вышестоящий уровень требуется нажать на кнопку **[Настройка передачи событий]**.

В открывшемся окне «Настройка серверов» с использованием кнопок  и  из расположенного в правой части окна списка событий информационной безопасности требуется построить список передаваемых на вышестоящий уровень событий, а также с использованием кнопок **[Добавить]** / **[Удалить]** настроить список получателей, указав значения их ip-адресов и портов (по умолчанию используется порт 40060) (рис. 52).

Для корректной работы передачи событий необходимо в настройках программы задать ИД АС, отличный от значения по умолчанию и настроить прием событий на вышестоящем АРМ АБИ.

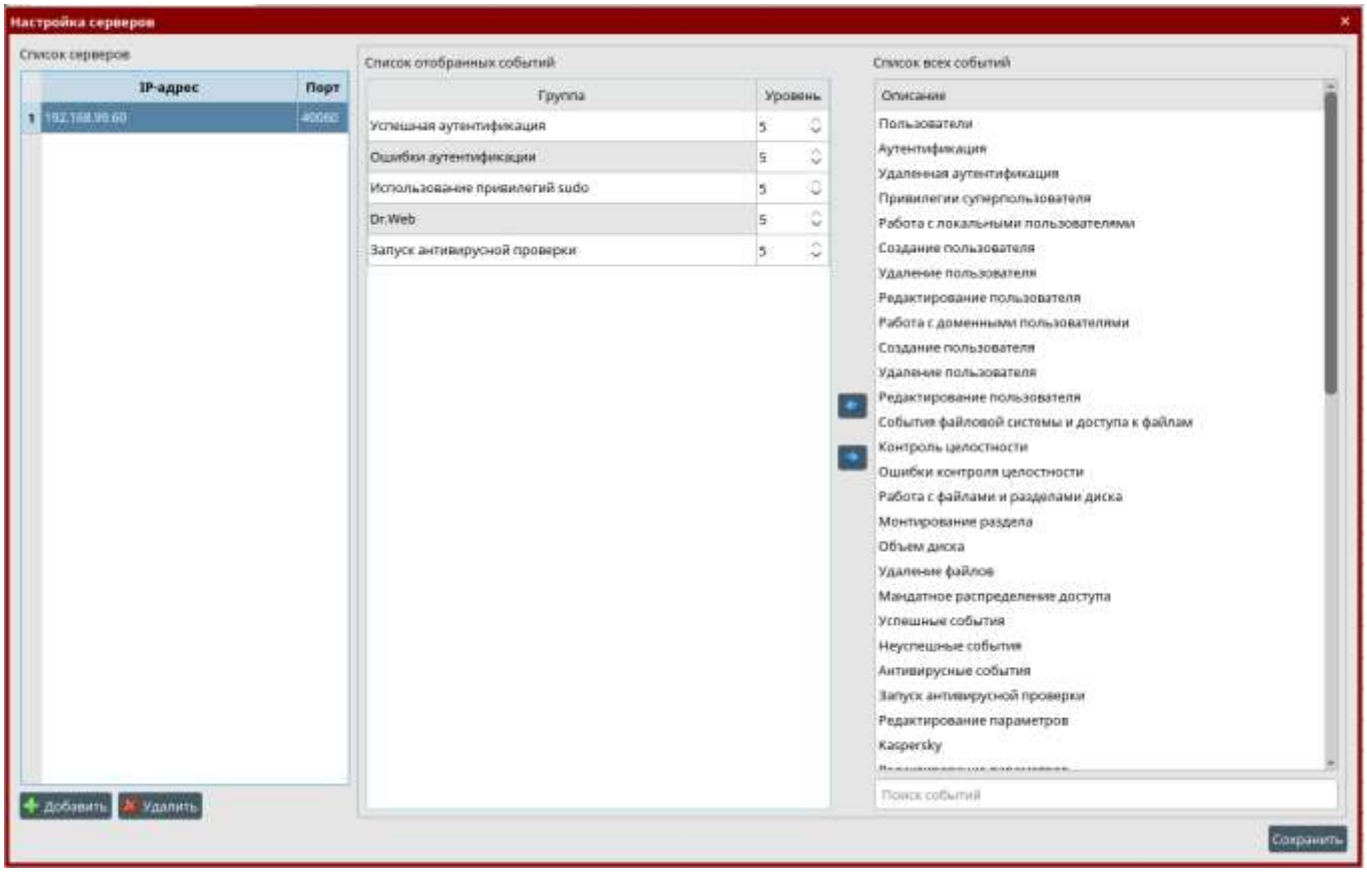


Рис. 52 – Настройка передачи событий на вышестоящий уровень

3.9.7. Настройка автоблокировки пользователей по событиям ИБ

Для выполнения настройки автоблокировки пользователей по событиям информационной безопасности требуется нажать на кнопку **[Настройка автоблокировки]**.

В открывшемся окне «Настройка автоблокировки пользователей» (рис. 53) с использованием кнопок  и  из расположенного в левой части окна списка событий информационной безопасности требуется отобрать события, возникновение которых при заданной периодичности должно приводить к автоматической блокировке учетной записи пользователя. Периодичность для отобранных событий информационной безопасности задается значениями полей «Количество» и «Период времени». После завершения настройки нажать на кнопку **[Сохранить]**.

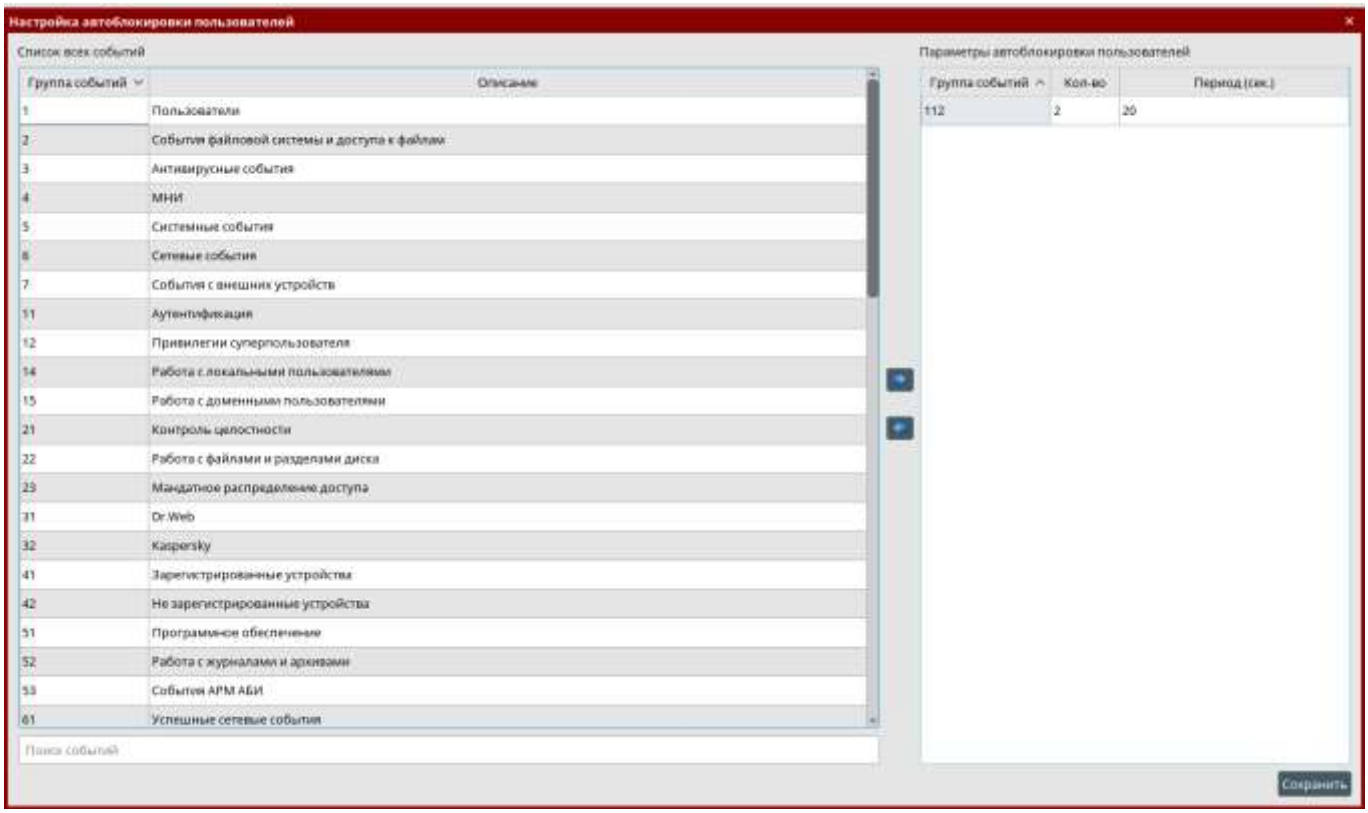


Рис. 53 – Настройка автоблокировки пользователей

В списке отобранных событий отображаются только коды событий, однако при наведении курсора «мыши» на код события появится всплывающая подсказка с описанием данного события (рис. 54).

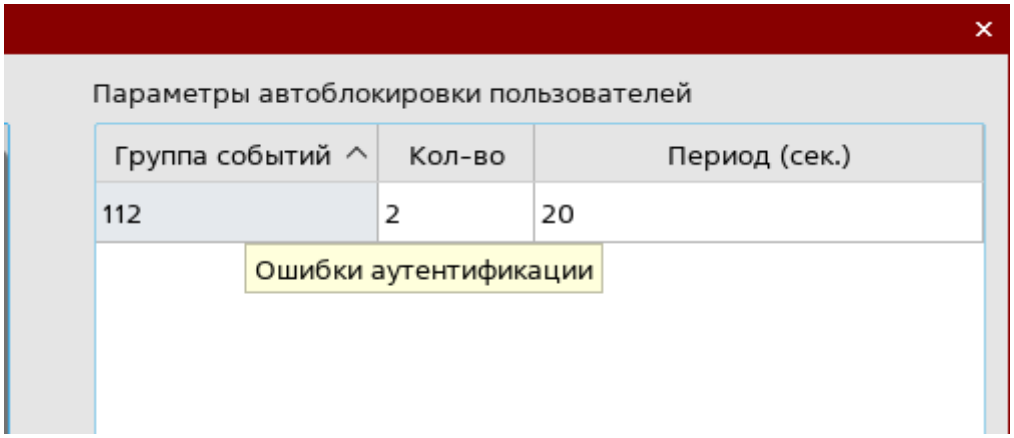


Рис. 54 – Подсказка для событий

3.10. Раздел «Внешние события ИБ»

Раздел программы «Внешние события ИБ» предназначен для отображения в виде таблицы полученных с нижестоящих уровней событий информационной безопасности. Внешний вид раздела приведен на рис. 55 и содержит следующую информацию:

- наименование системы автоматизации нижестоящего уровня;
- наименование устройства;

- дата и время события;
- уровень опасности;
- пользователь, совершающий событие;
- тип события;
- время отправки;
- время приема.

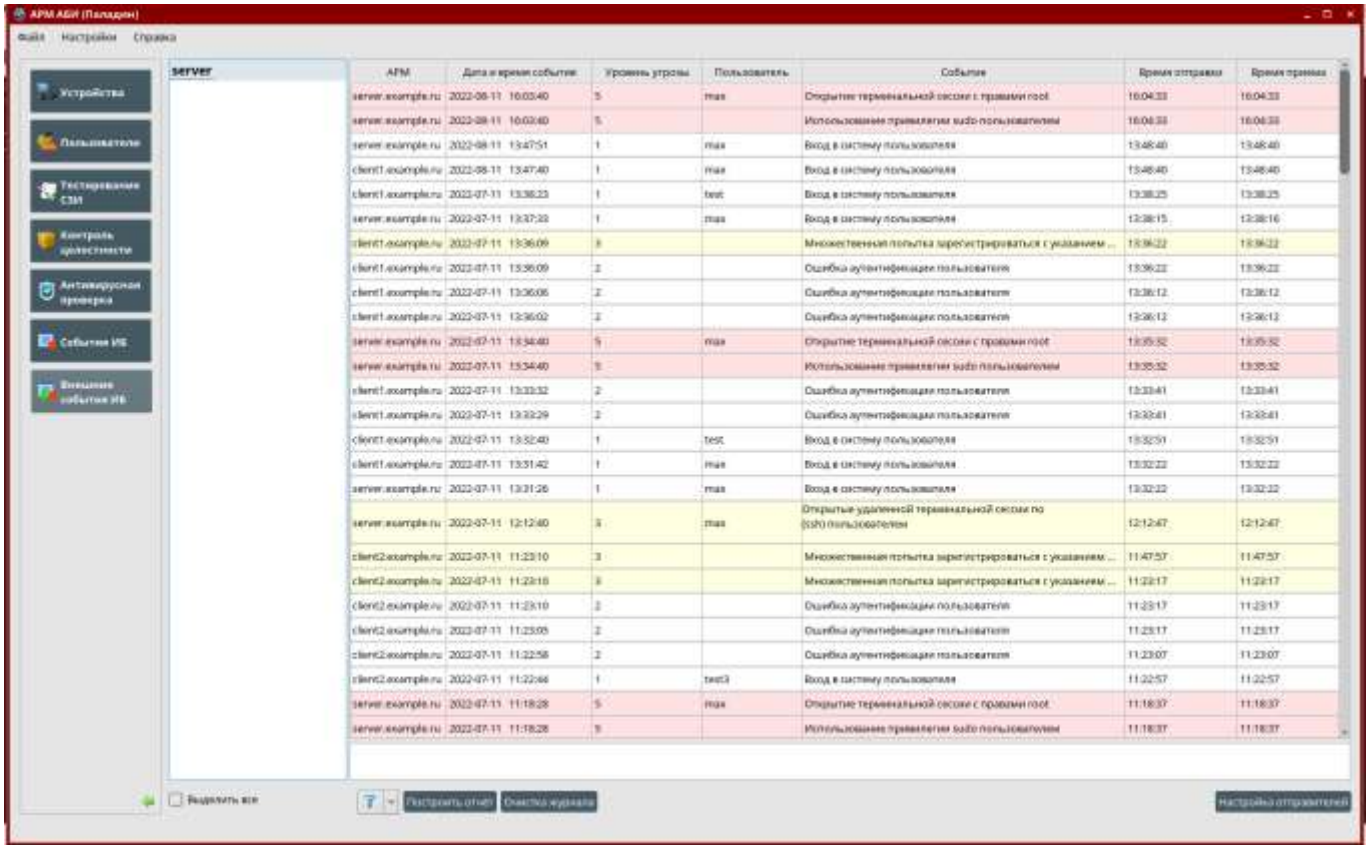


Рис. 55 – Раздел «Внешние события ИБ»

В нижней части окна программы отображаются кнопки для настройки фильтра отображения событий ИБ, отображения отчета, архивирования событий информационной безопасности и кнопка настройки отправителей для приема событий информационной безопасности с нижестоящего уровня.

3.10.1. Настройка приема событий ИБ с нижестоящего уровня

Для обеспечения приема событий информационной безопасности с нижестоящего уровня необходимо нажать на кнопку **[Настройка отправителей]**. В открывшемся окне с использованием кнопок **[Добавить]** / **[Удалить]** требуется построить список, указав значения параметров (рис. 56):

- «id» – идентификатор системы автоматизации нижестоящего уровня, указанный в настройках ПС АРМ АБИ;
- «name» – наименование системы автоматизации нижестоящего уровня.

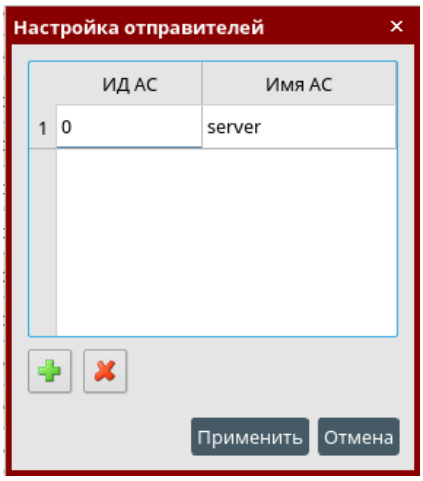


Рис. 56 – Настройка приема событий с нижестоящего уровня

Нажать на кнопку **[Применить]** для сохранения изменений.

3.11. Резервное копирование конфигурации домена

3.11.1. Резервное копирование конфигурации домена ALD

Для создания резервной копии данных домена ALD необходимо нажать правой кнопкой «мыши» на название домена и выбрать пункт меню « Резервные копии данных» (рис. 57).

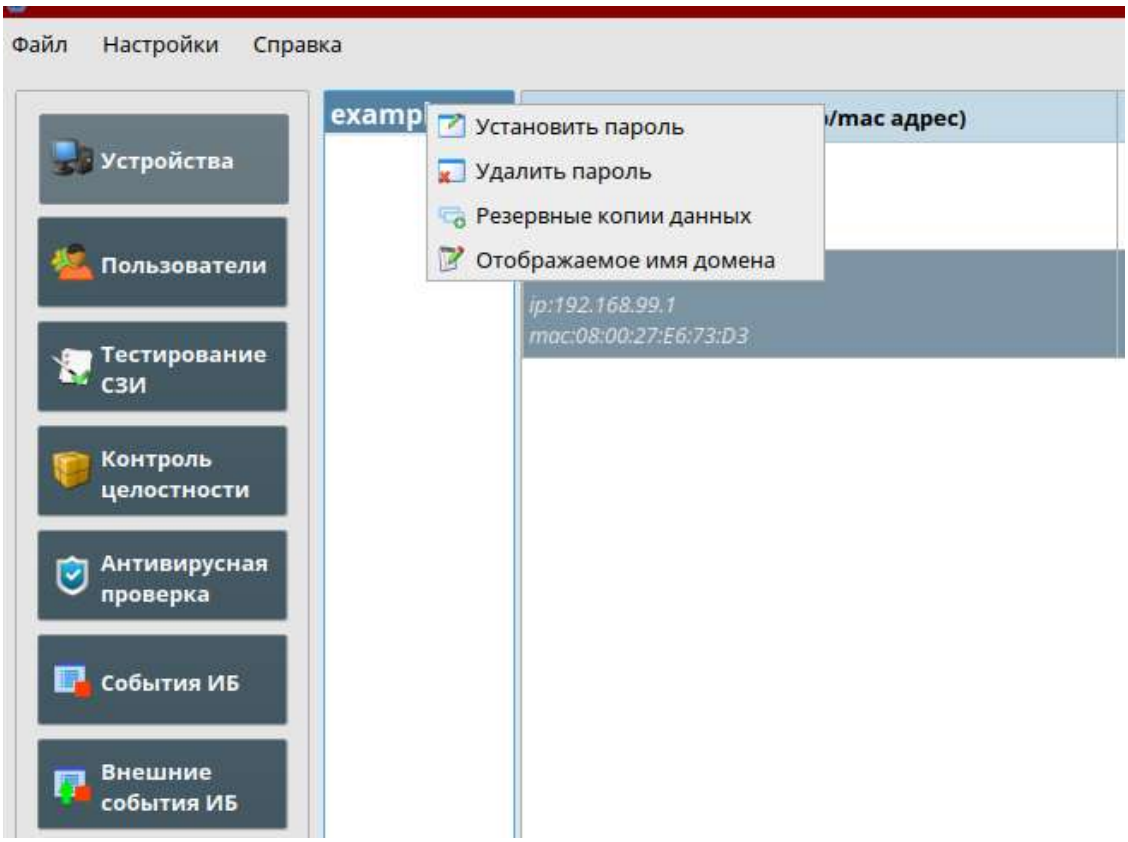


Рис. 57 – Резервное копирование конфигурации домена

Открывшееся окно «Резервные копии данных домена» содержит список созданных ранее резервных копий, включающий в себя дату создания и путь к файлу резервной копии (рис. 58).

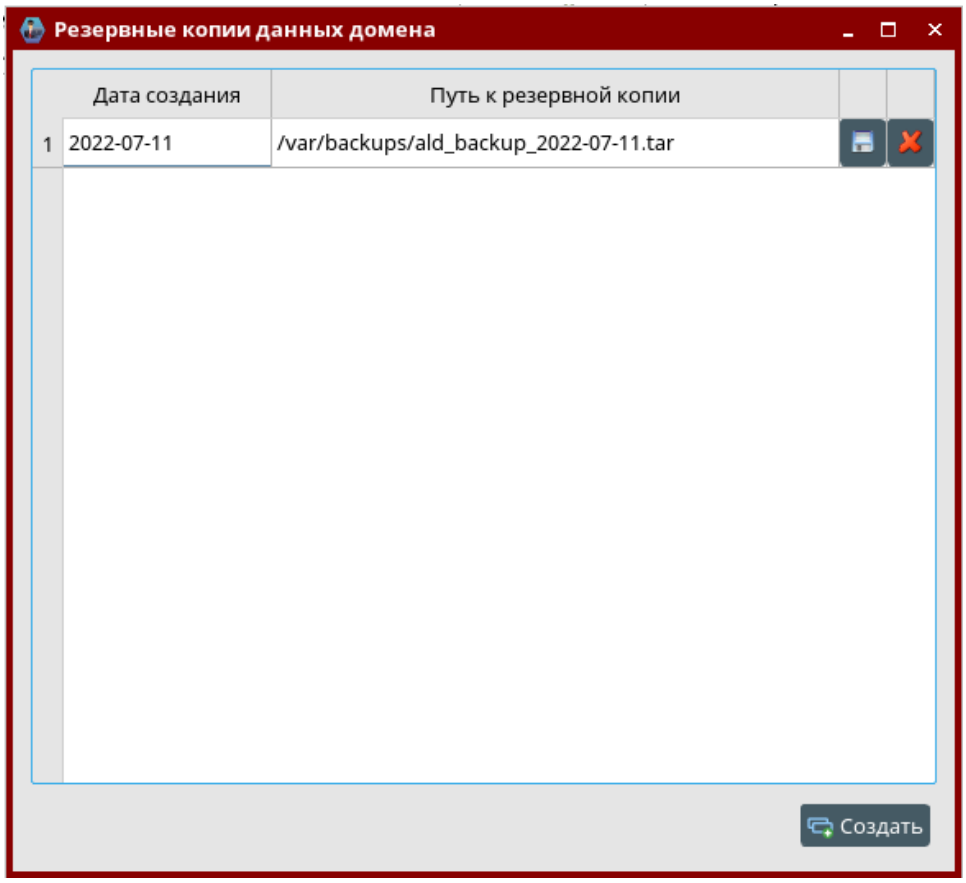


Рис. 58 – Резервные копии домена

Для создания резервной копии необходимо нажать на кнопку **[Создать]**. Полученный архив будет сохранен на контроллере выбранного домена в каталоге `/var/backups`.

Для локального сохранения резервной копии необходимо нажать на кнопку .В открывшемся окне «Выбор каталога» (рис. 59) необходимо выбрать путь для сохранения полученной копии на локальной машине (по умолчанию рекомендуется использовать каталог для backup-файлов).

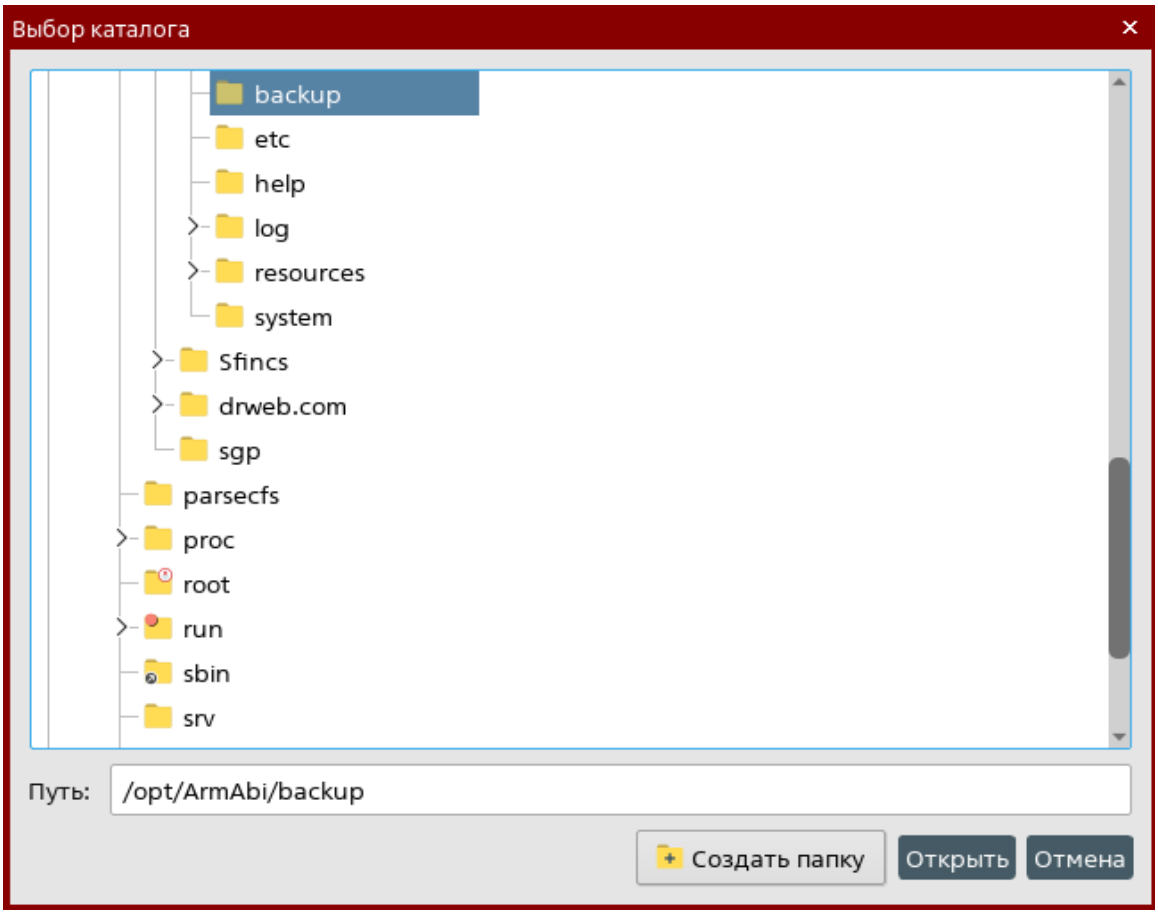


Рис. 59 – Выбор каталога

Для удаления ранее созданной резервной копии необходимо нажать на кнопку  напротив соответствующего файла в списке.

Восстановление резервных копий выполняется средствами ОС СН. Для восстановления необходимо использовать команды `ald-init restore-backup` и `ald-init restore-backup-portable`.

Подробные сведения о создании и восстановлении резервных копий в среде ALD приведены в «Операционная система специального назначения «Astra Linux Special Edition» Руководство администратора. Часть 1» РУСБ.10015-01 95 01-1.

3.11.2. Резервное копирование данных домена FreeIPA

При использовании для организации единого пространства пользователей домена FreeIPA поддерживается создание резервных копий двух типов:

- резервная копия данных домена;
- полная резервная копия домена.

При создании полной резервной копии сохраняются не только данные домена, а также системные файлы, которые задействованы при работе домена FreeIPA (/etc/passwd, /etc/group, /etc/resolv.conf и др.).

Резервные копии сохраняются в каталоге /var/lib/ipa/backup. Для полного резервного копирования и резервного копирования данных используются, соответственно, обозначения ipa-full-YEAR-MM-DD-HH-MM-SS и ipa-data-YEAR-MM-DD-HH-MM-SS, где YEAR-MM-DD-HH-MM-SS — год, месяц, день, час, минуты и секунды в часовом поясе GMT создания резервной копии.

В каталоге /var/lib/ipa/backup размещается файл, в котором приведена информация о резервных копиях: тип, система, даты резервного копирования, версия FreeIPA, версия резервного копирования и др.

3.11.2.1. Резервное копирование данных домена FreeIPA

Для создания резервной копии данных домена FreeIPA необходимо нажать правой кнопкой мыши на название домена и выбрать пункт меню « Резервные копии данных» (рис. 60).

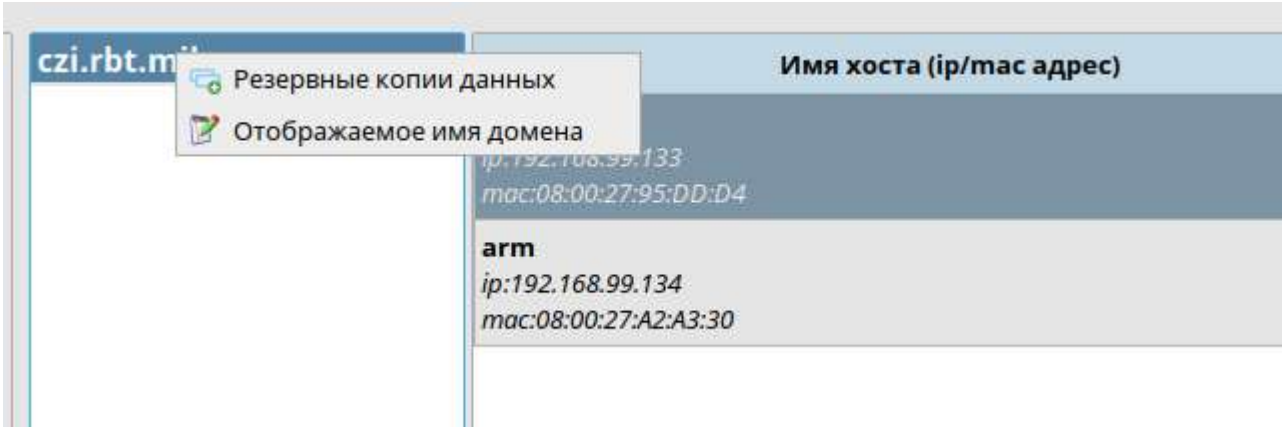


Рис. 60 – Резервные копии данных

Открывшееся окно «Резервные копии домена» содержит список созданных ранее резервных копий, включающий в себя дату создания и путь к файлу резервной копии (рис. 61).

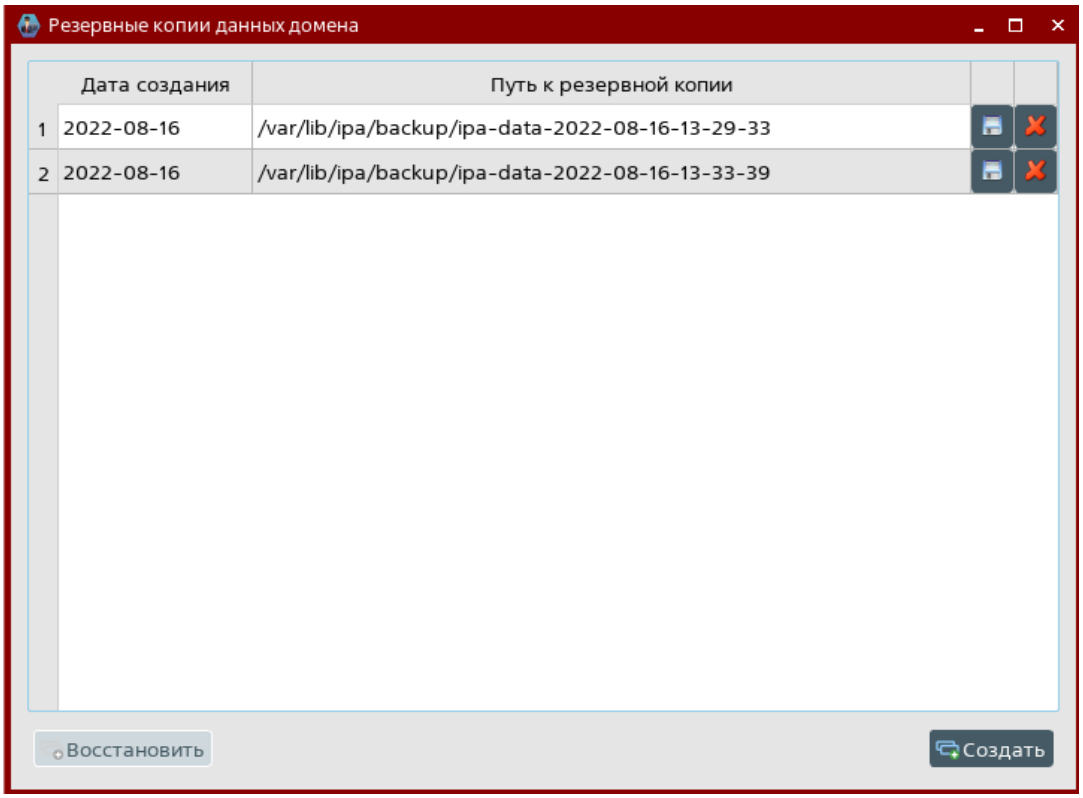


Рис. 61 – Резервные копии данных домена

Для создания резервной копии необходимо нажать на кнопку **[Создать]**. Полученный архив будет сохранен на контроллере домена в каталоге `/var/lib/ipa/backup`.

Для локального сохранения резервной копии необходимо нажать на кнопку  .В открывшемся окне «Выбор каталога» (рис. 62) необходимо выбрать путь для сохранения полученной копии на локальной машине (по умолчанию рекомендуется использовать каталог для backup-файлов).

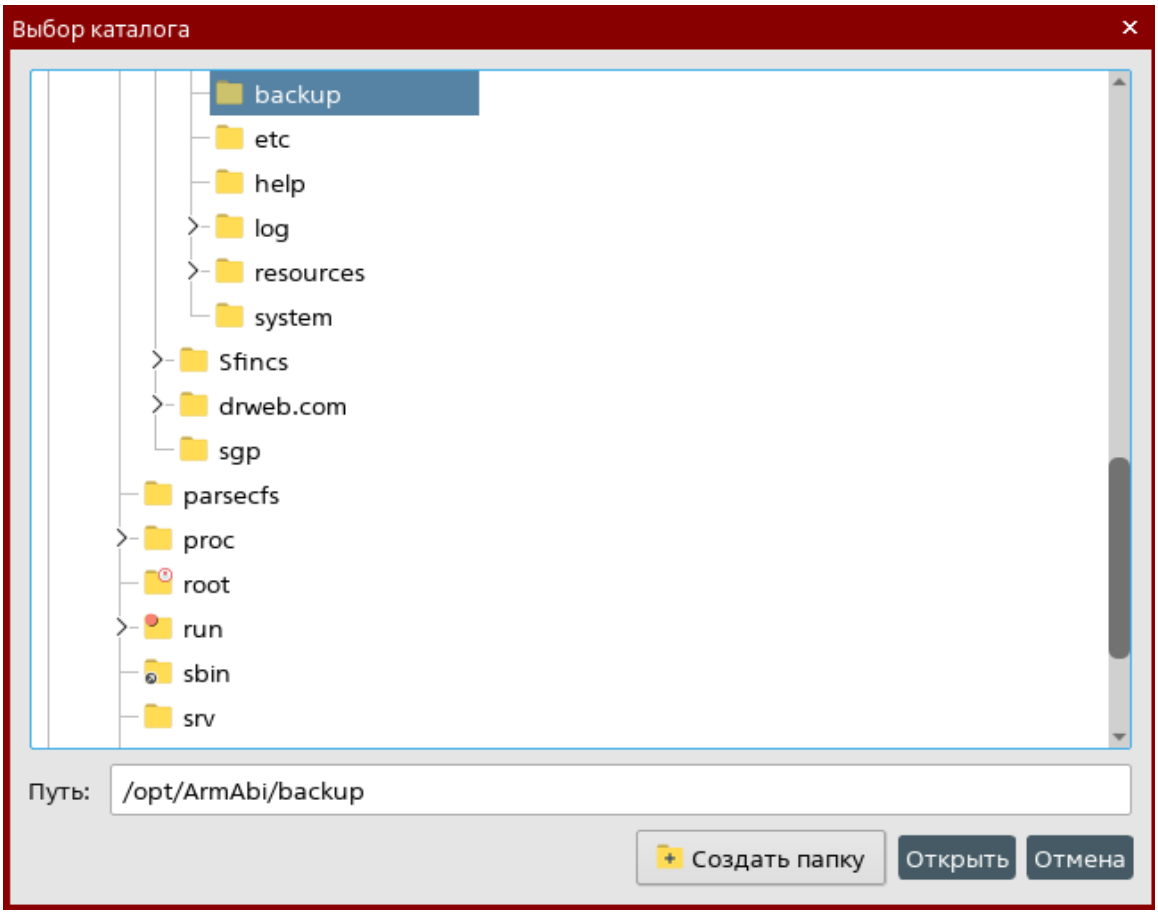


Рис. 62 – Выбор каталога

Для удаления ранее созданной резервной копии необходимо нажать на кнопку  напротив соответствующего файла в списке.

Чтобы восстановить данные домена из резервной копии следует выбрать необходимую копию и нажать на кнопку **[Восстановить]**.

При корректном восстановлении появится окно об успешном завершении операции (рис. 63).

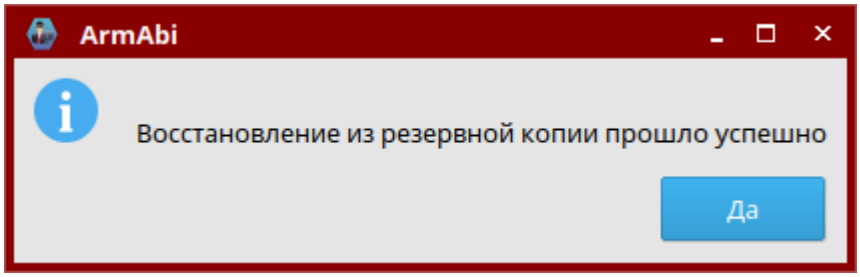


Рис. 63 – Успешное восстановлении резервной копии

Если резервная копия повреждена будет выведено сообщение с информацией об ошибке. Например, если в каталоге резервной копии отсутствует заголовок будет выведено сообщение, представленное на рис. 64.

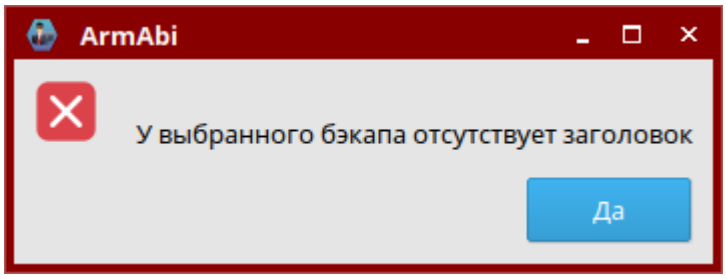


Рис. 64 – Ошибка при восстановлении резервной копии

Ниже перечислены все возможные ошибки и причины их возникновения при восстановлении из резервной копии:

- «У выбранного бэкапа отсутствует заголовок» – в каталоге резервной копии отсутствует файл `header`;

- «По указанному пути бэкапа не обнаружено» – резервная копия была удалена или переименована. Такая ошибка возможна только если указанные выше действия были произведены до обновления окна «Резервные копии данных домена», в противном случае удаленная/переименованная копия не будет отображена в списке.

- «Выбранный бэкап не относится к домену» – был изменен файл header;

- «У выбранного бэкапа отсутствует архив» – в каталоге резервной копии отсутствует или был переименован архив с данными;

- «У выбранного бэкапа поврежден архив» – в архиве с данными были повреждены (удалены, изменены) или добавлены новые данные.

ВНИМАНИЕ! Для восстановления резервной копии в домене FreeIPA используется пароль Directory Manager (LDAP). При установке сервера FreeIPA пароль администратора домена (admin) автоматически устанавливается в качестве пароля Directory Manager (LDAP), однако при смене пароля пользователя admin, пароль LDAP автоматически не изменяется. В связи с этим при восстановлении данных из резервной копии программа сначала пытается использовать пароль админа, указанный в форме при входе в программу (этот пароль подойдёт в ситуации, когда пароль для пользователя admin не менялся), а если этот пароль не подходит появится окно с сообщением "Введите пароль, указанный при создании домена" (рис. 65). Данный пароль подойдёт в той ситуации, если по каким-то причинам пароль пользователя admin был изменен, или в системе создано несколько администраторов домена FreeIPA, данные одного из которых указываются при входе в программу.

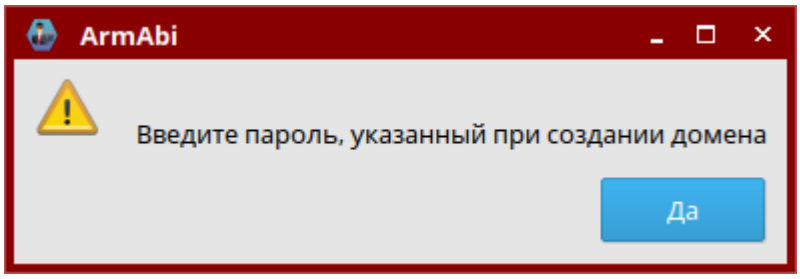


Рис. 65 – Запрос ввода пароля

В открывшемся окне необходимо нажать на кнопку **[Да]**. В окне «Резервные копии данных домена» появится поле (рис. 66), в котором необходимо указать пароль и нажать на кнопку **[Восстановить]**.

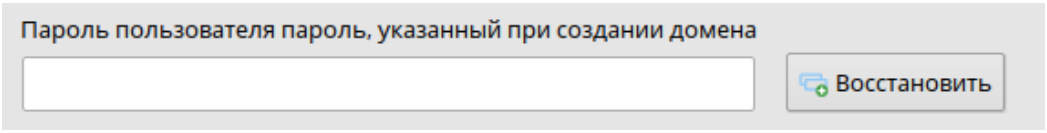


Рис. 66 – Ввод пароля пользователя

3.11.2.2. Полное резервное копирование домена FreeIPA

Для создания полной резервной копии необходимо выбрать из списка устройств контроллер домена, нажать на кнопку и подтвердить создание резервной копии в появившемся диалоговом окне, нажав на кнопку **[Да]**. Полученный архив будет сохранен на выбранном контроллере домена в подкаталоге каталоге `/var/lib/ipa/backup`, содержащем дату и время создания резервной копии. После завершения создания резервной копии откроется окно «Выбор каталога» (рис. 67), в котором можно выбрать путь для сохранения полученной копии на АРМ АБИ (по умолчанию используется каталог для backup-файлов, указанный в настройках программы).

Восстановление полных настроек домена в случае необходимости осуществляется средствами операционной системы с использованием команды ipa restore.

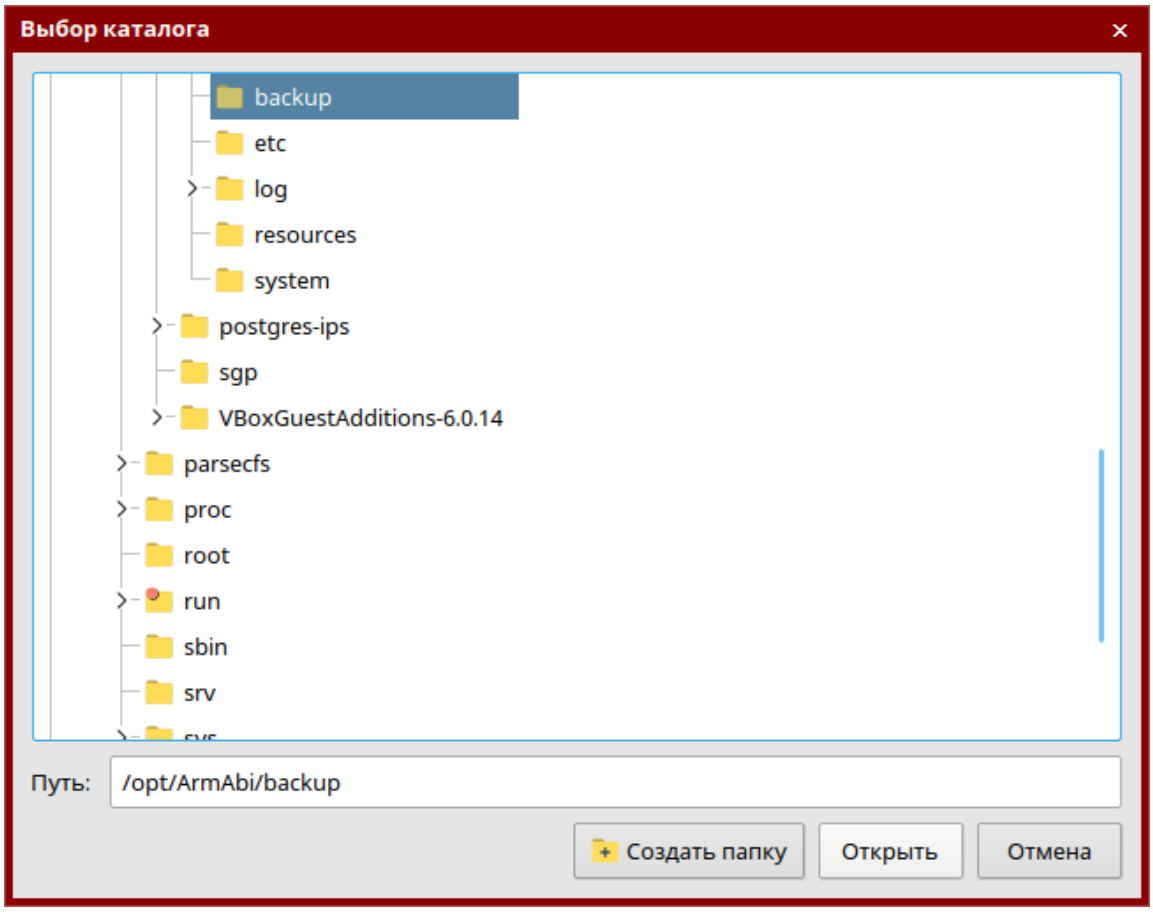


Рис. 67 – Выбор каталога для сохранения полной резервной копии домена на АРМ АБИ

3.12. Работа под принуждением

В ПС АРМ АБИ реализован механизм, обеспечивающий скрытую передачу на АРМ АБИ экстренного сообщения о возникновении внештатной ситуации («Работа под принуждением») с любого управляемого устройства.

Для передачи сообщения о внештатной ситуации пользователю требуется нажать комбинацию клавиш **<Ctrl+Alt+P>**.

На АРМ АБИ появится модальное окно, содержащее информацию об имени устройства и имени пользователя, отправившего сообщение (рис. 68).

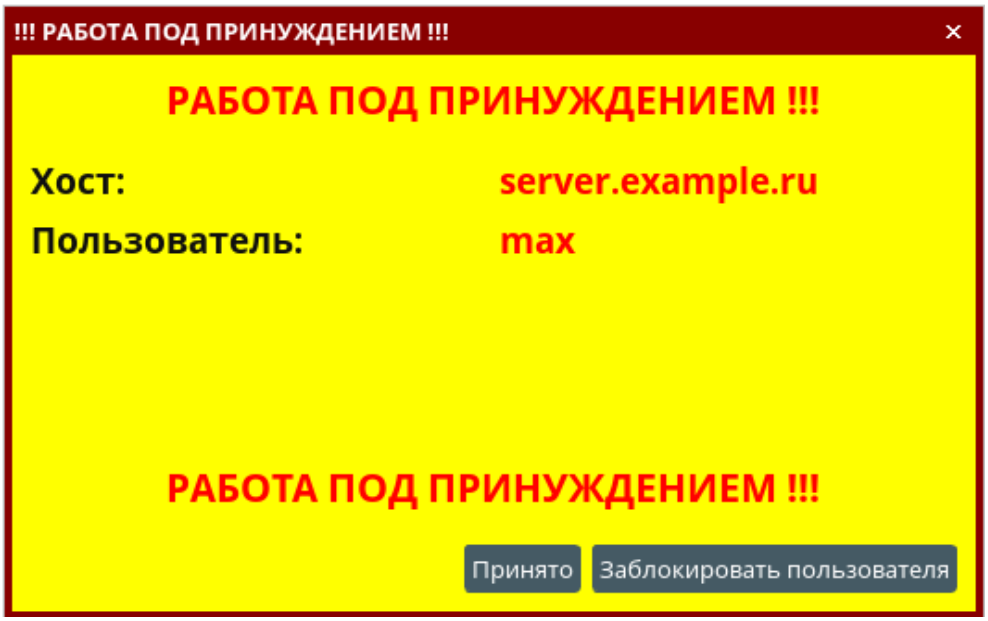


Рис. 68 – Сообщение АБИ о работе «под принуждением»

Для того, чтобы заблокировать пользователя, отправившего сообщение, необходимо нажать на кнопку **[Заблокировать пользователя]**.

Для закрытия модального окна необходимо нажать на кнопку **[Принято].**

3.13. Резервное копирование базы данных ПС АРМ АБИ

Для создания резервной копии базы данных программы требуется выбрать в пункте меню «Файл» подпункт «Резервная копия БД». В открывшемся окне (рис. 69) необходимо выбрать каталог для сохранения резервной копии (`/opt/ArmAbi/backup` по умолчанию) и ввести пароль администратора базы данных.

Если требуется удалить все ранее созданные копии из выбранного каталога необходимо установить флажок «Удалить предыдущие копии из этого каталога» (установлен по умолчанию).

После установки требуемых значений необходимо нажать на кнопку **[Создать копию]**.

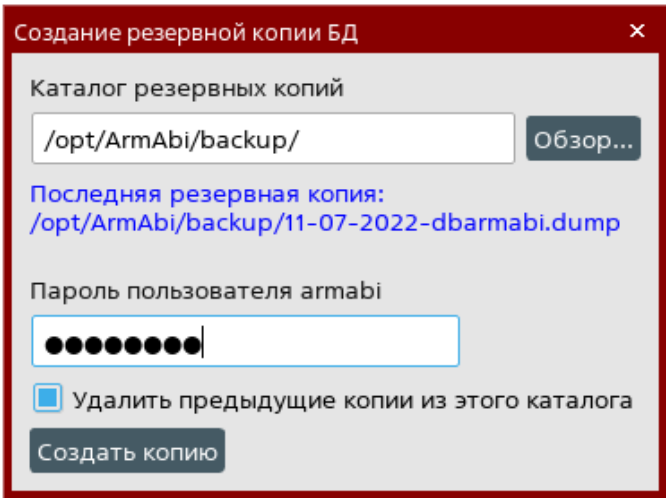


Рис. 69 – Создание резервной копии БД

Для восстановления резервной копии базы данных программы требуется выбрать в пункте меню «Файл» подпункт «Восстановление БД». В открывшемся окне (рис. 70) необходимо выбрать резервную копию, ввести пароль администратора базы данных и нажать на кнопку **[Восстановить копию]**.

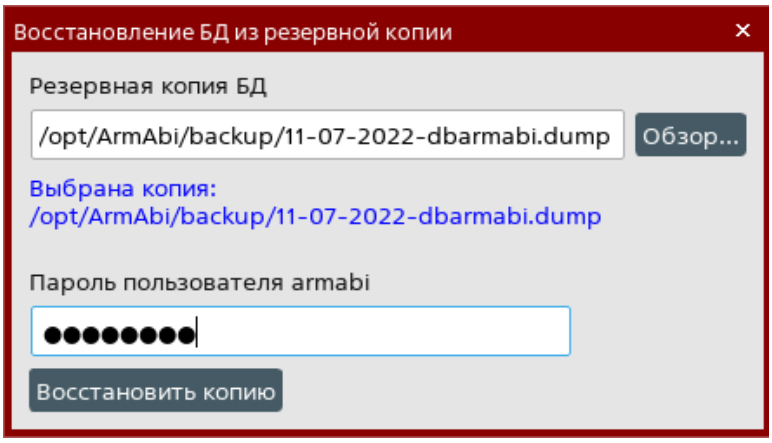


Рис. 70 – Восстановление БД из резервной копии

ВНИМАНИЕ! Если после создания резервной копии БД были перерегистрированы агенты устройств, то после восстановления в базе данных будут восстановлены данные агентов до перерегистрации, однако на самих агентах (в файлах `/etc/armdl.conf`) останутся старые данные. В связи с этим необходима перерегистрация данных агентов после восстановления БД из резервной копии.

Подробные сведения о перерегистрации агентов приведены в «ПС АРМ АБИ. Руководство системного программиста» РУСБ.30488-04 32 01.

3.14. Сохранение и печать отчётов

В программе выводятся отчёты о тестировании СЗИ, проведении контроля целостности, проведении антивирусной проверки, списке событий ИБ.

Для сохранения отчёта необходимо нажать на кнопку  . В открывшемся окне «Сохранение отчёта» (рис. 71) необходимо выбрать путь для сохранения отчёта и нажать на кнопку **[Сохранить]**.

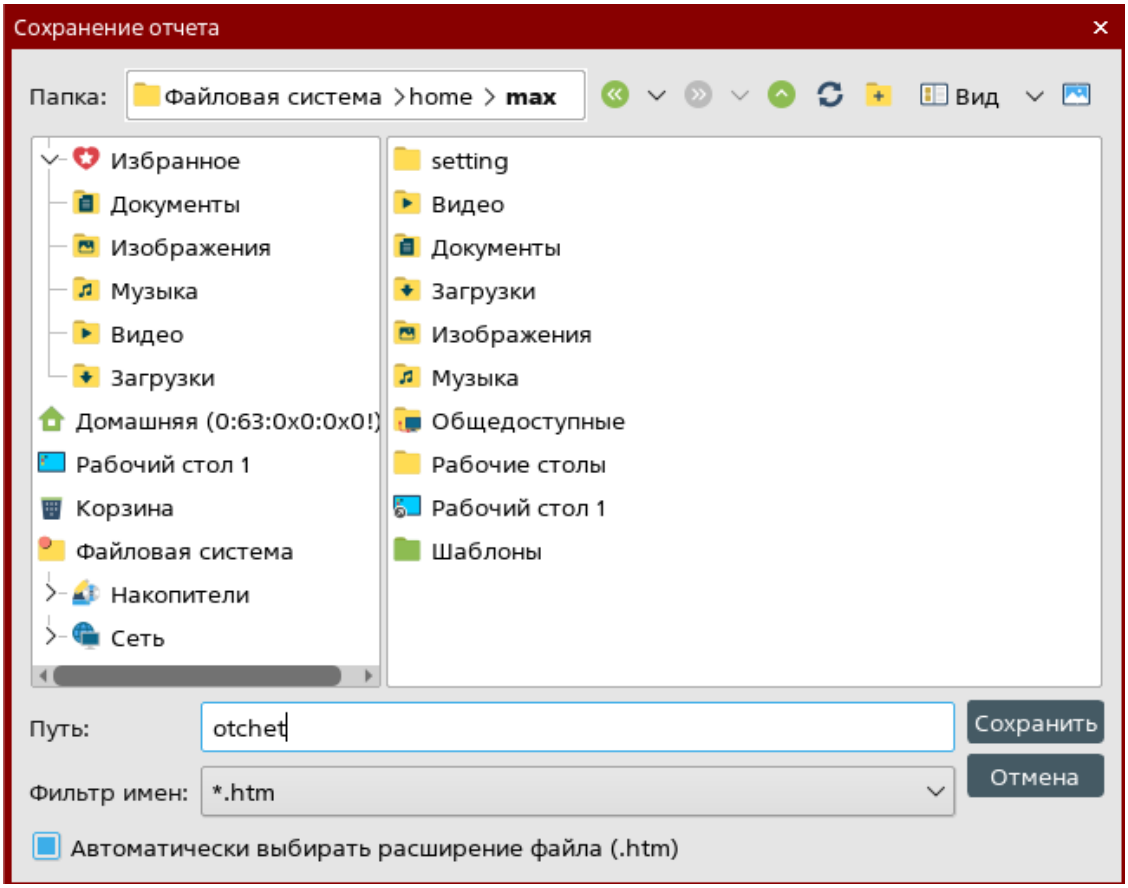


Рис. 71 – Сохранение отчета

Для выполнения печати отчета требуется нажать на кнопку  . В открывшемся окне «Печать» (рис. 72) необходимо выбрать принтер и нажать на кнопку **[Печать]**.

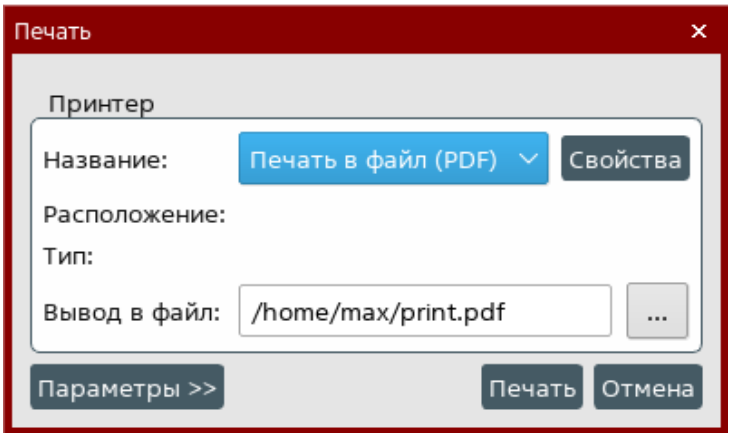


Рис. 72 – Печать отчета

Для изменения свойств принтера необходимо нажать на кнопку **[Свойства]**.

Для изменения параметров печати необходимо нажать на кнопку **[Параметры]** и в открывшейся вкладке «Копии» (рис. 73) настроить параметры печати.

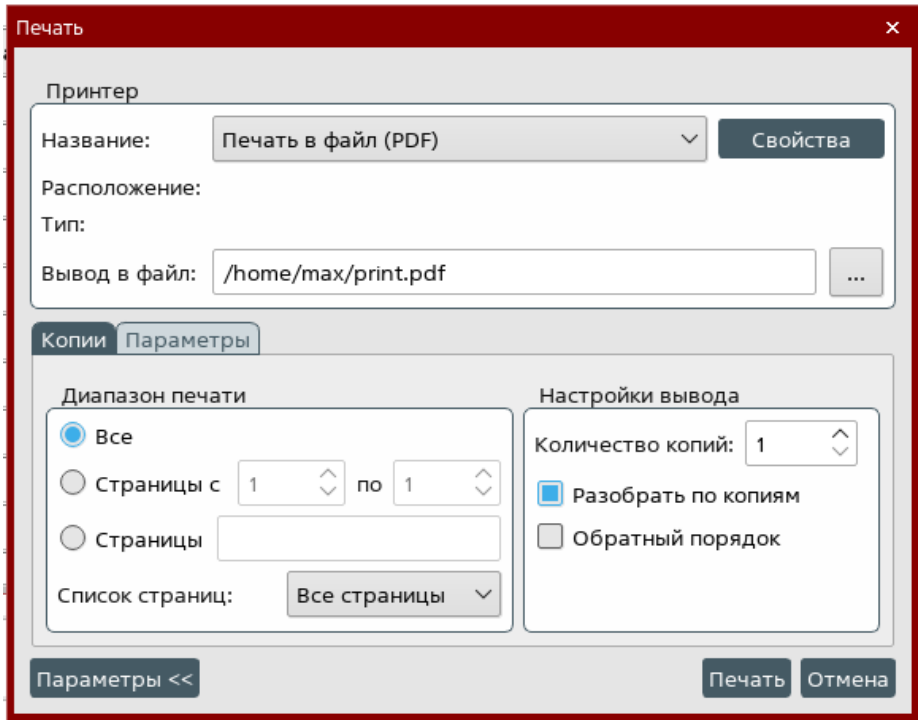


Рис. 73 – Параметры печати

3.15. Тиражирование правил разграничения доступа к отчуждаемым машинным носителям информации

Для создания и передачи на контролируемые устройства правил разграничения доступа к отчуждаемым машинным носителям информации необходимо выбрать пункт «Отчуждаемые МНИ» меню «Файл» (доступно только при использовании для организации единого пространства пользователей домена FreeIPA). В открывшемся окне «Настройка правил доступа к МНИ» отображаются устройства МНИ и правила которые заданы для устройства (рис. 74).

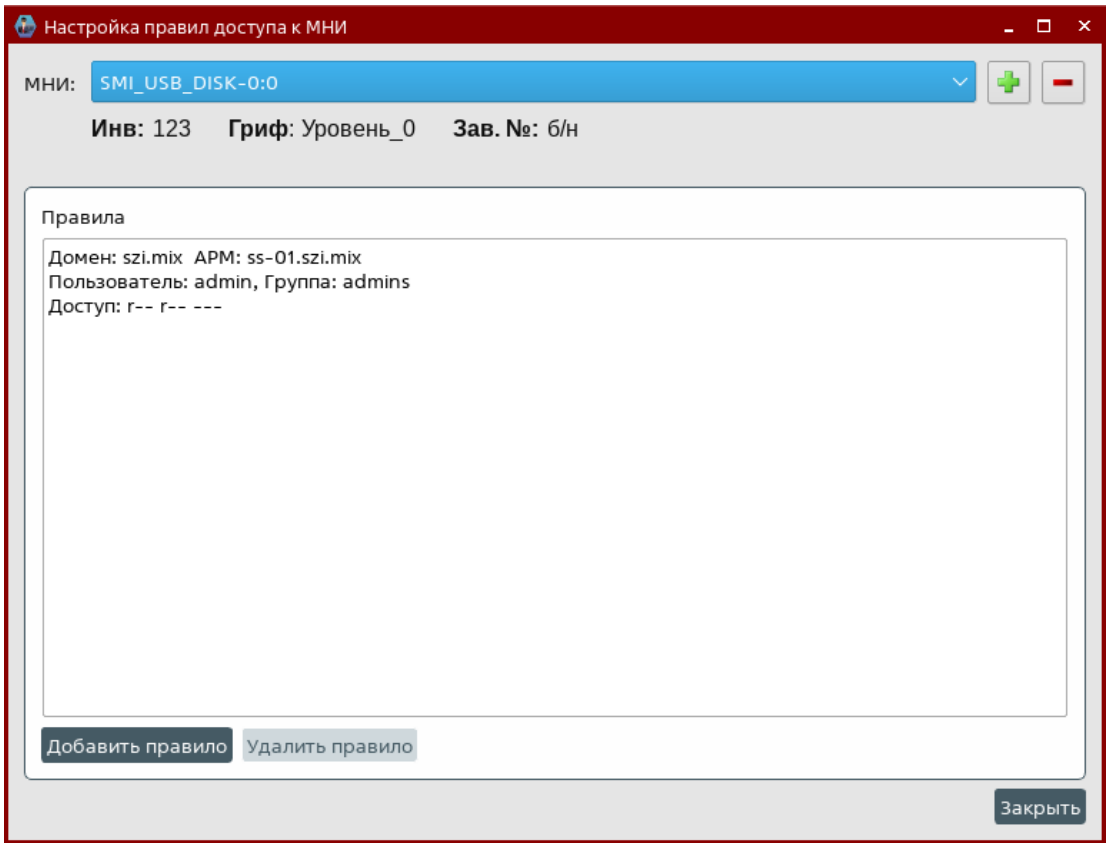


Рис. 74 – Тиражирование правил отчуждаемых носителей

Для создания правила необходимо нажать на кнопку  . Откроется окно «Добавить устройство» (рис. 75).

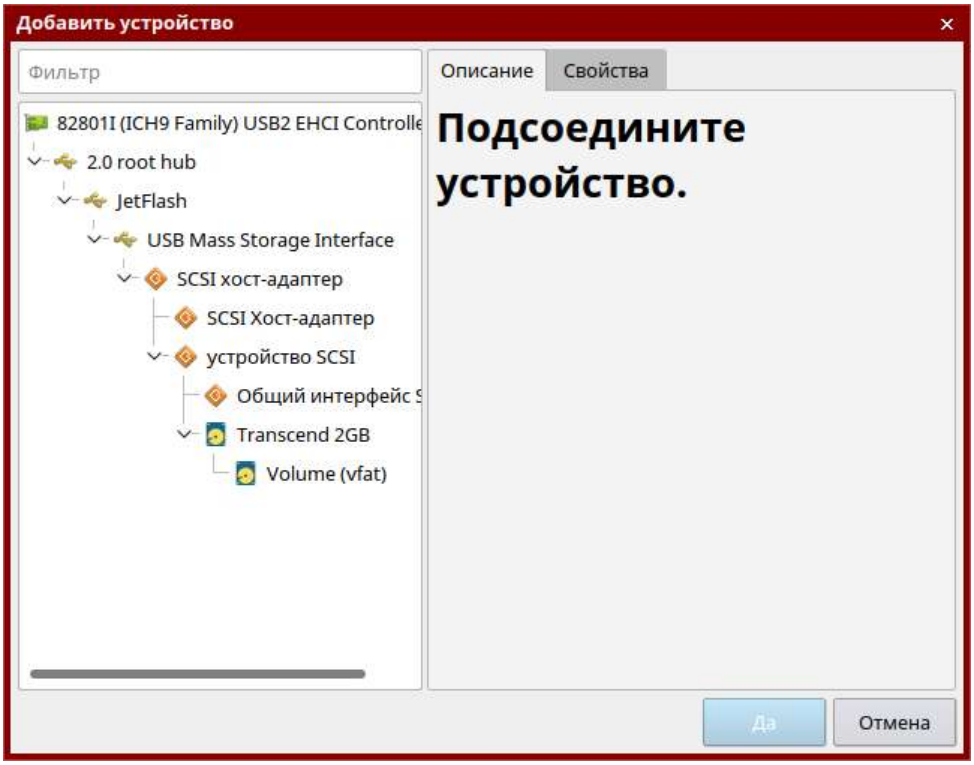


Рис. 75 – Окно для добавления устройства

Далее необходимо подключить носитель. В окне «Добавить устройство» необходимо выбрать подключенный носитель и нажать на кнопку **[Да]** (рис. 76).

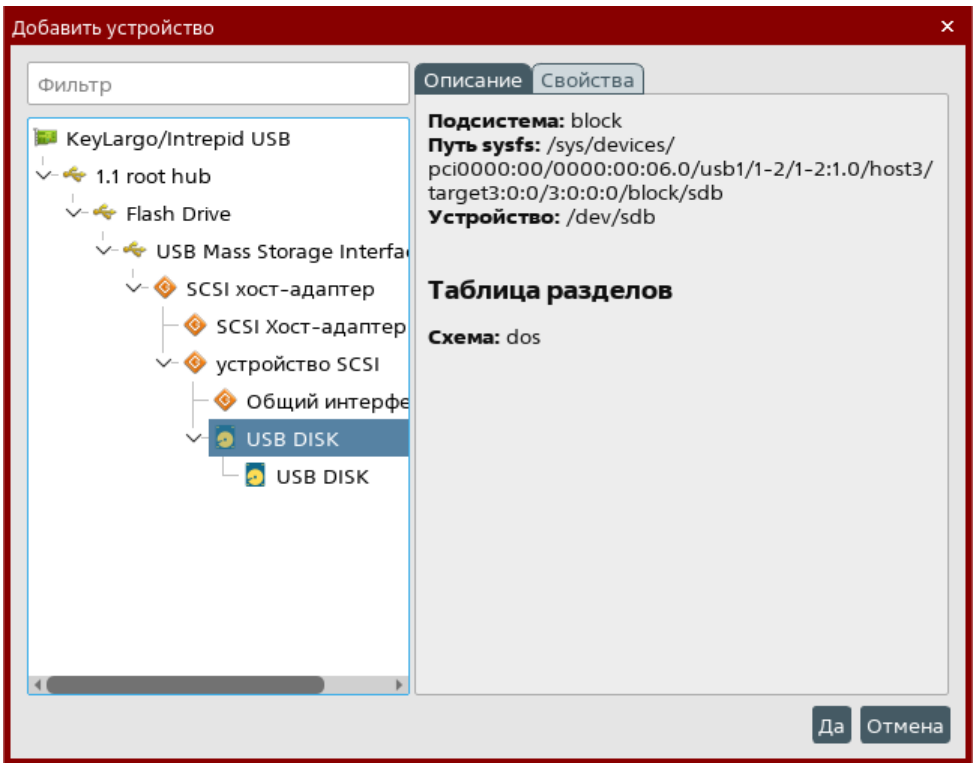


Рис. 76 – Добавление устройства

В открывшемся окне «Тиражирование правил отчуждаемых носителей» требуется задать значения полей «Зав.№» (устанавливается автоматически), «Инв.№» (учитывается и выдается в соответствующем делопроизводстве (режимно-секретном подразделении объекта эксплуатации)), установить владельца и группу, задать дискреционные и мандатные атрибуты доступа к отчуждаемому МНИ (рис. 77).

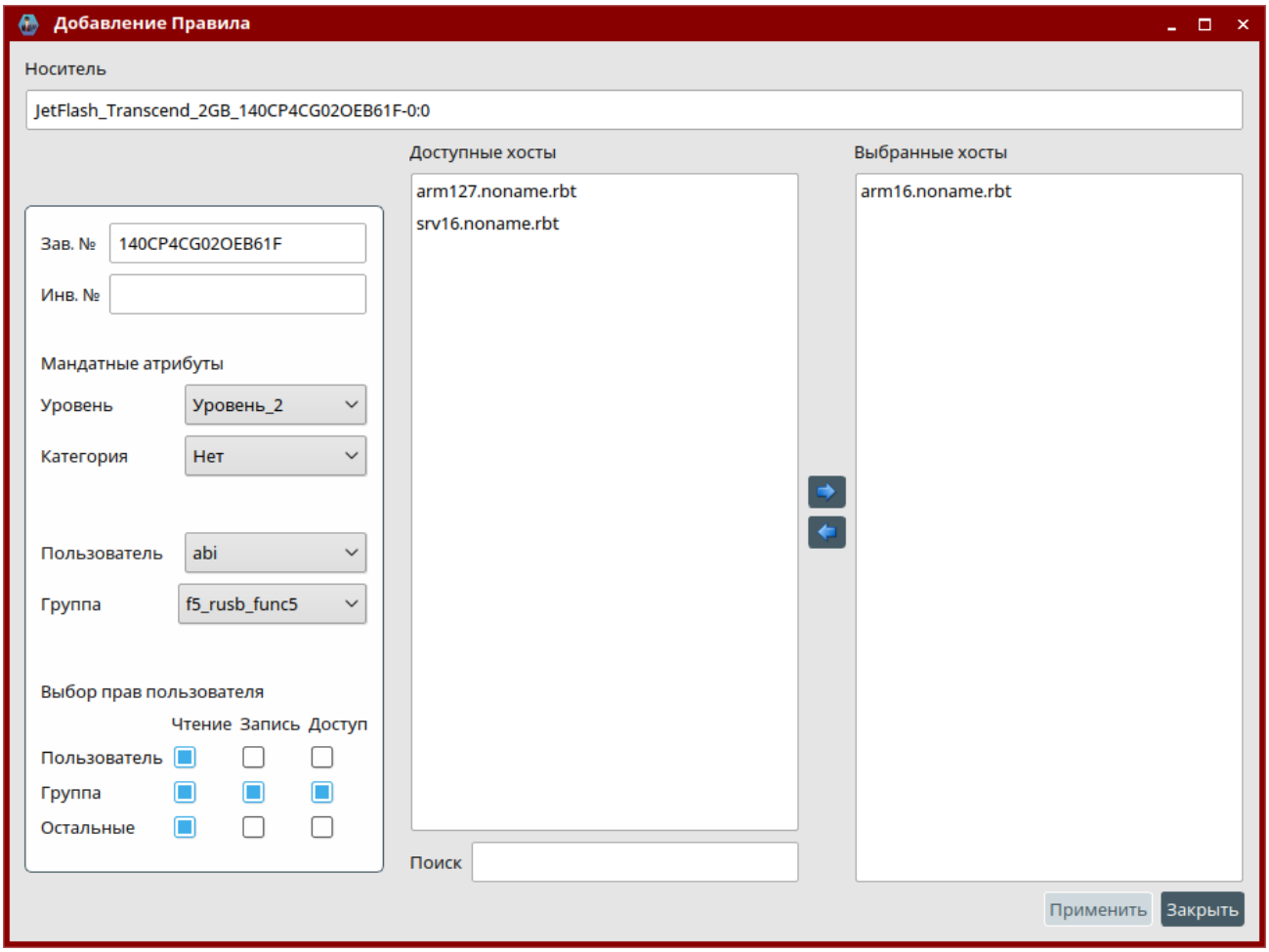


Рис. 77 – Тиражирование правил отчуждаемых носителей

Для того, чтобы отправить созданное правило на хосты, необходимо с использованием кнопок  и  из расположенного в левой части окна списка хостов выбрать устройства для отправления и нажать на кнопку **[Применить]**. При успешном выполнении появляется сообщение (рис. 78).

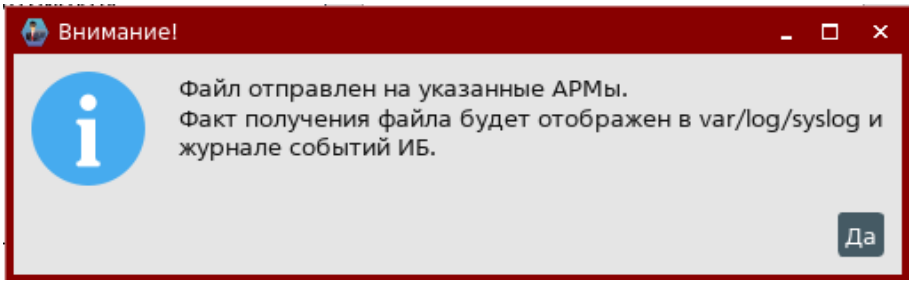


Рис. 78 – Сообщение о регистрации МНИ

После добавления вновь созданное правило разграничения доступа к отчуждаемым машинным носителям отразится в списке «Правила» в окне «Настройка правил доступа к МНИ».

Для добавления нового правила разграничения доступа к отчуждаемому машинному носителю информации необходимо нажать кнопку **[Добавить правило]**.

Для удаления существующего правила разграничения доступа к отчуждаемому машинному носителю информации необходимо нажать кнопку **[Удалить правило]** и подтвердить действие, нажав на кнопку **[Да]**. При этом правило будет удалено со всех доступных в данный момент АРМ, на которые оно было растиражировано. В случае недоступности АРМ будет создано задание, которое периодически будет осуществлять попытки удаления правила.

3.16. Формирование и ведение таблицы разграничения доступа к защищаемым ресурсам

Для формирования и ведения таблицы разграничения доступа к защищаемым ресурсам необходимо выбрать пункт «Правила РД» в меню «Файл». Открывшееся окно содержит пункты меню (рис. 79):

- «Формирование ПРД»;
- «Редактирование»;
- «Доступ к устройству»;
- «Контроль»;
- «Вид»;
- «Выгрузка/загрузка»;
- «Отчеты».

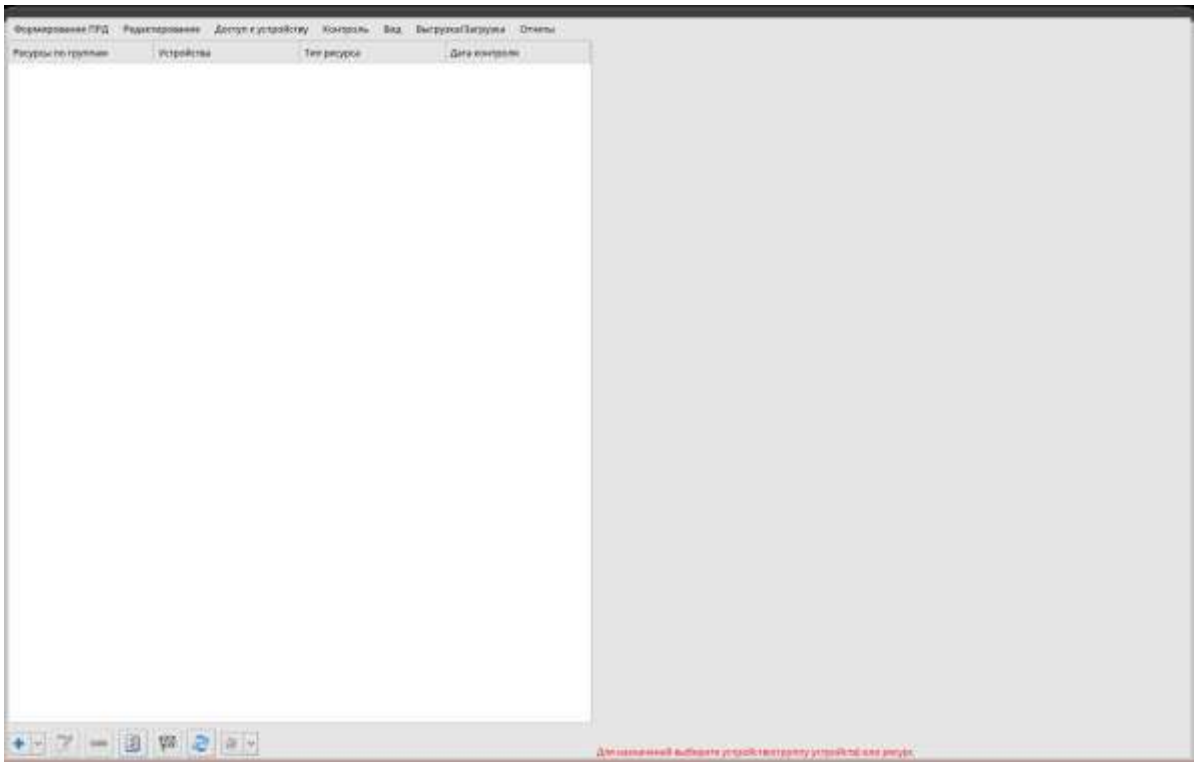


Рис. 79 – Окно «Правила разграничения доступа»

3.16.1. Формирование перечня и таблицы разграничения доступа к защищаемым ресурсам

Для формирования и ведения перечня защищаемых ресурсов и таблицы разграничения доступа к защищаемым ресурсам предназначен пункт меню «Формирование ПРД».

Пункт меню «Формирование ПРД» содержит подпункты (рис. 80):

- «Добавить группу устройств»;
- «Редактировать наименование группы»;
- «Удалить группу устройств»;
- «Добавить устройство»;
- «Добавить устройство к группе»;
- «Исключить устройство из группы»;
- «Добавить ресурс»;
- «Отключить ресурс».

Функционал пункта меню «Формирование групп» дублируется расположенной в нижней части окна кнопкой  .

Защищаемые ресурсы находятся на управляемых устройствах. В случае, если защищаемые ресурсы на различных устройствах однотипны (находятся по одним и тем же путям, а правила разграничения доступа идентичны), устройства могут быть объединены в группы.

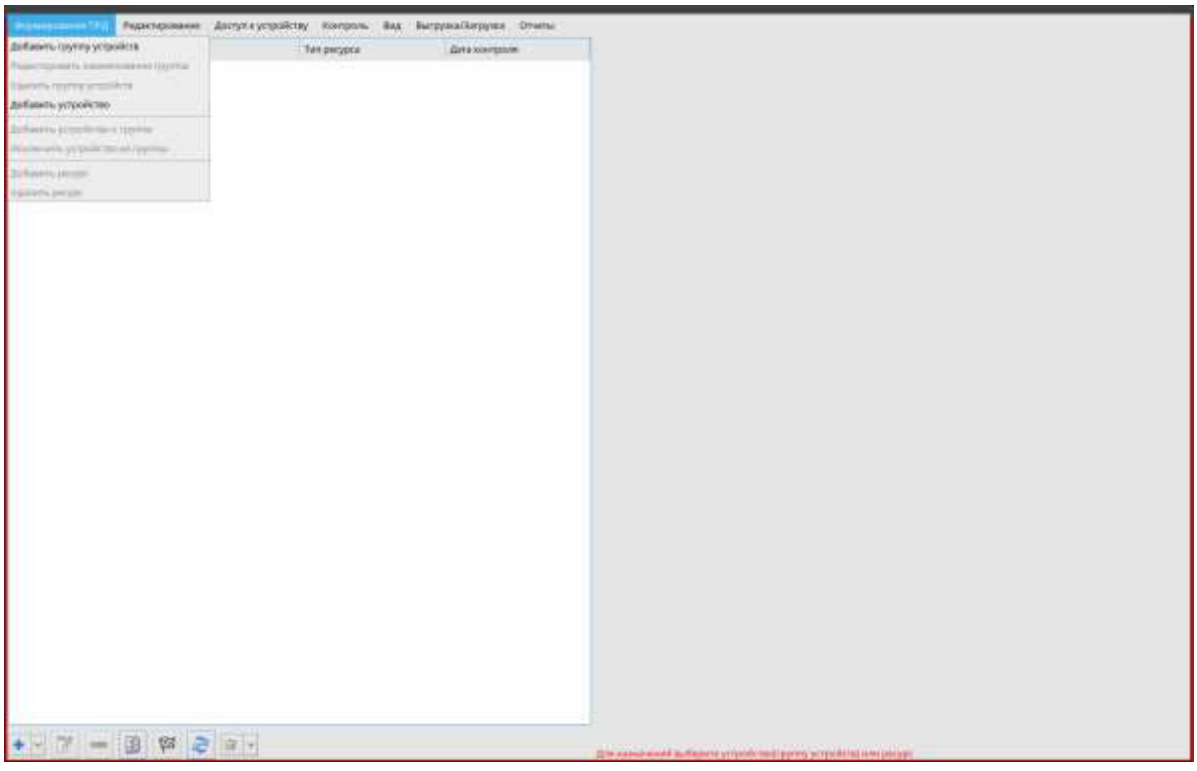


Рис. 80 – Пункт меню «Формирование ПРД»

Для добавления группы устройств требуется выбрать подпункт «Добавить группу устройств», указать в появившемся окне «Группы устройств» наименование группы и нажать кнопку **[Принять]** (рис. 81).

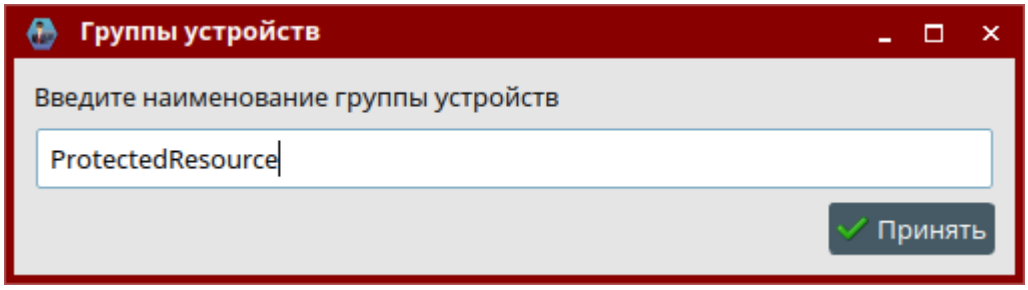


Рис. 81 – Диалоговое окно ввода наименования группы устройств

Для переименования группы устройств необходимо выбрать подпункт «Редактировать наименование группы», указать в появившемся окне новое наименование группы и нажать кнопку **[Принять]**.

Для удаления группы устройств требуется выбрать подпункт «Удалить группу устройств» и подтвердить действие, нажав на кнопку **[Да]**.

Для добавления/удаления устройства в группу устройств требуется выбрать ее в списке в левой части окна и выбрать подпункт «Добавить устройство в группу» или «Отключить устройство из группы» (рис. 82).

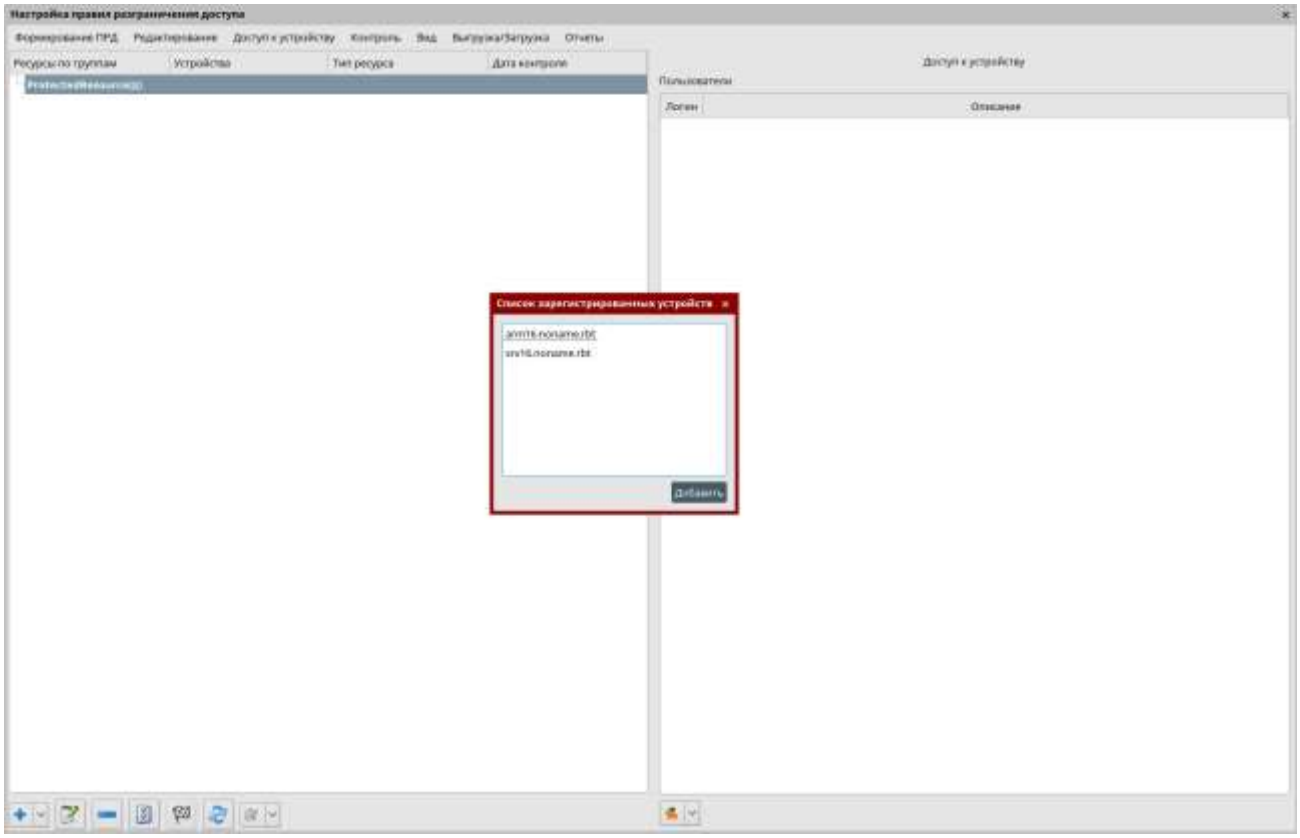


Рис. 82 – Диалоговое окно добавления устройства в группу

Для добавления содержащего защищаемые ресурсы отдельного устройства (без включения в группу) необходимо выбрать пункт меню «Добавить устройство», выделить в появившемся диалоговом окне необходимое устройство и нажать кнопку **[Добавить]**.

Для добавления защищаемого ресурса устройства (группы устройств) требуется выбрать подпункт «Добавить ресурс», указать путь к нему в появившемся диалоговом окне, задать наименование ресурса в поле «Псевдоним», указать тип рекурсии и нажать кнопку **[Ok]** (рис. 83).

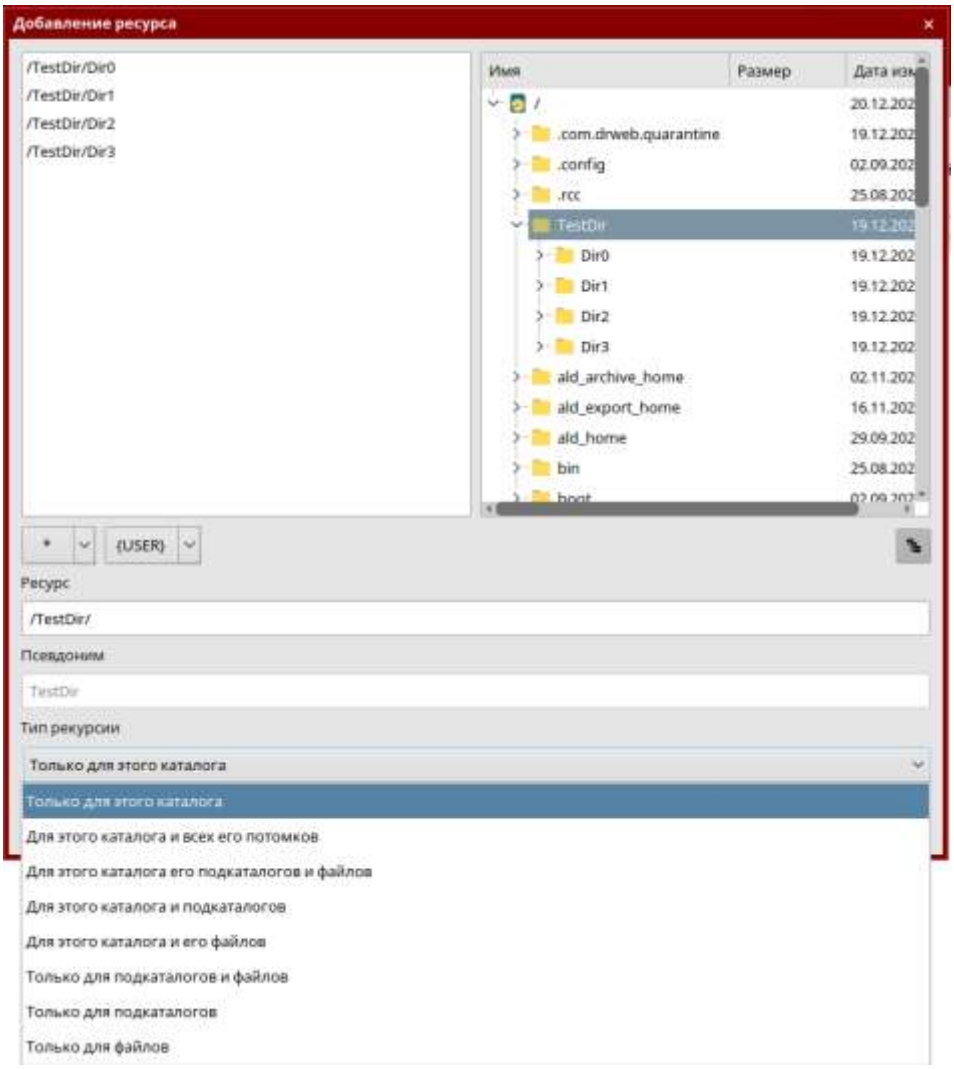


Рис. 83 – Диалоговое окно добавления защищаемого ресурса

При добавлении ресурса устройства (группы устройств) можно использовать специальные символы, определенные в шаблоне подстановки shell:

- * – любое количество любых символов (в том числе и их отсутствие);

- ? – один любой символ;

- [1-9] – любой символ из перечня или диапазона (здесь цифры можно заменить любыми символами);

- {,} – соответствует одному либо другому набору символов.

Также определены специальные переменные:

- {USER} – в этом месте будет подставлено имя пользователя (для всех пользователей, определенных в системе, доменных и локальных);

- {UID} – в этом месте должен быть UID пользователя;

- {GROUP} – в этом месте будет подставлено имя группы пользователя.

В случае задействования этих переменных при определении ресурса их можно указывать в качестве значений полей "Владелец" "Группа" для установки атрибутов дискреционной политики.

Для отключения защищаемого ресурса требуется выбрать его из списка и подпункт «Отключить ресурс».

Для установки требуемых прав дискреционных и мандатных прав доступа и политики аудита защищаемого ресурса требуется выбрать его из списка в левой части окна. Правила разграничения доступа для дискреционных (рис. 84) и мандатных (рис. 85) прав доступа к защищаемого ресурса, политики аудита (рис. 86) защищаемого ресурса задаются на одноименных вкладках в правой части окна программы.

После установки требуемых прав доступа и политики аудита на соответствующей вкладке требуется нажать кнопку **[Применить]**.

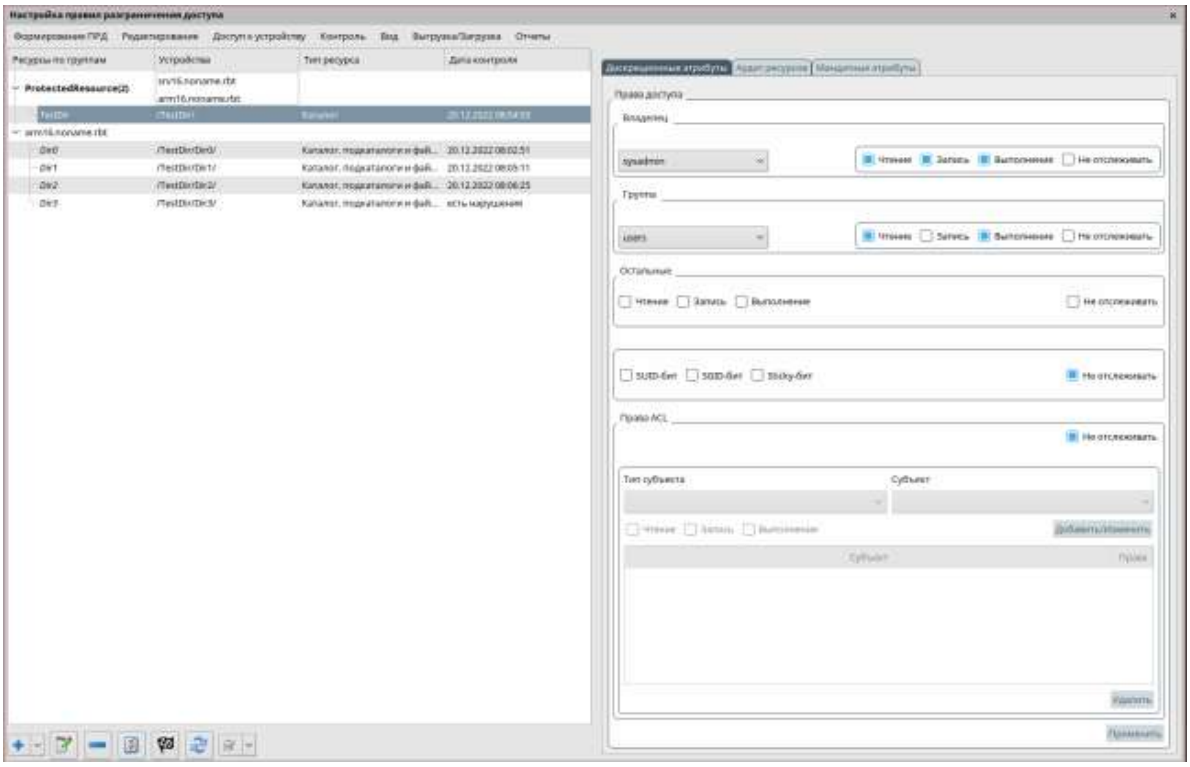


Рис. 84 – Установка требуемых дискреционных прав доступа к защищаемому ресурсу

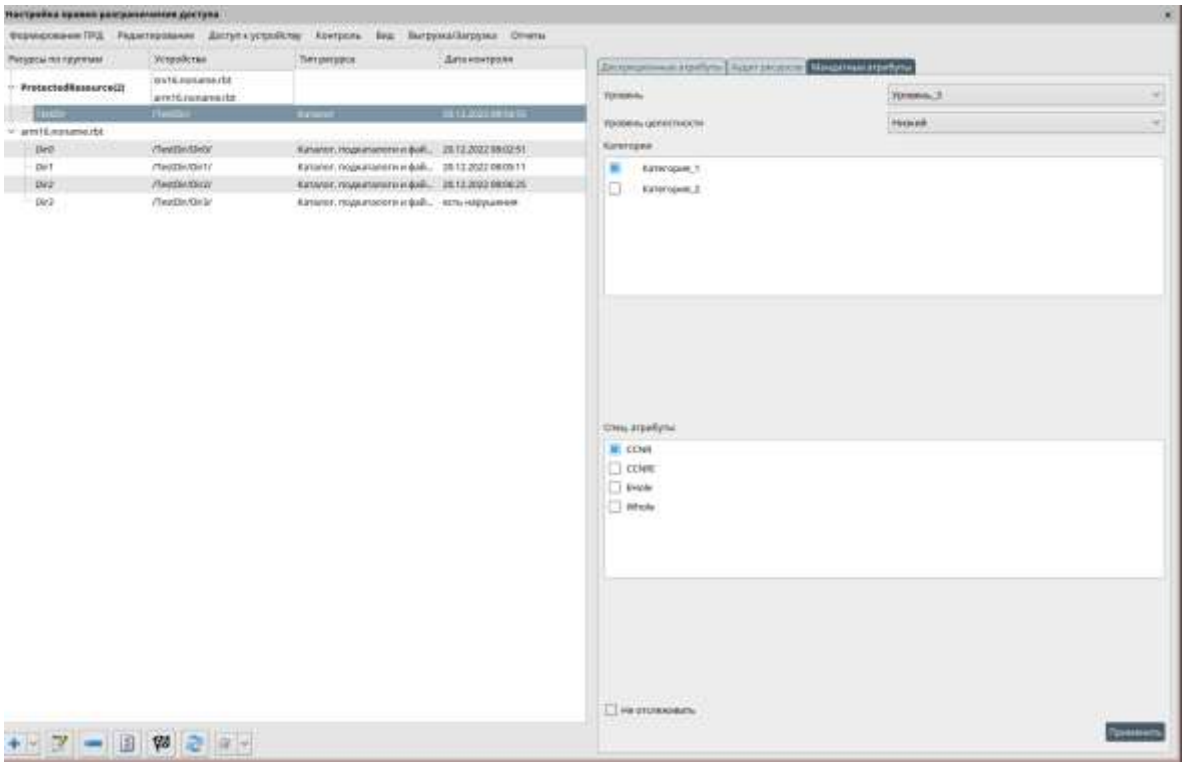


Рис. 85 – Установка требуемых мандатных прав доступа к защищаемому ресурсу

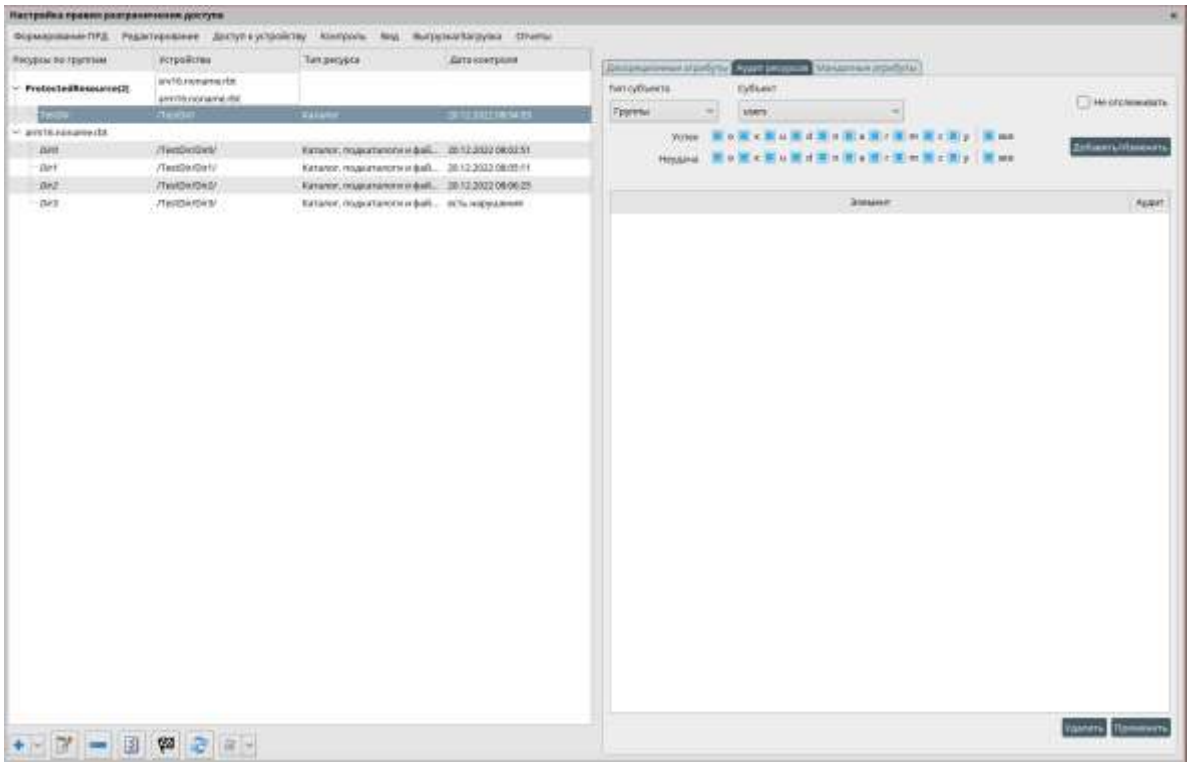


Рис. 86 – Установка требуемой политики аудита к защищаемому ресурсу

3.16.2. Формирование списка локальных пользователей и групп, используемых для формирования таблицы разграничения доступа к защищаемым ресурсам

Для добавления/удаления локальных пользователей и групп, используемых для формирования таблицы разграничения доступа к защищаемым ресурсам, предназначен пункт меню «Редактирование».

Для добавления/удаления локальных пользователей и локальных групп требуется выбрать подпункт «Локальные пользователи и группы».

Для добавления локальной группы в открывшемся диалоговом окне (рис. 84) требуется нажать на кнопку  и указать наименование группы. Для удаления локальной группы необходимо нажать кнопку  . Для сохранения изменений требуется нажать кнопку  .

Для добавления локального пользователя в открывшемся диалоговом окне (рис. 87) требуется нажать на кнопку  и указать логин пользователя, его имя, фамилию, полное имя и основную группу. Для удаления локального пользователя или группы необходимо нажать кнопку  . Для сохранения изменений требуется нажать кнопку  .

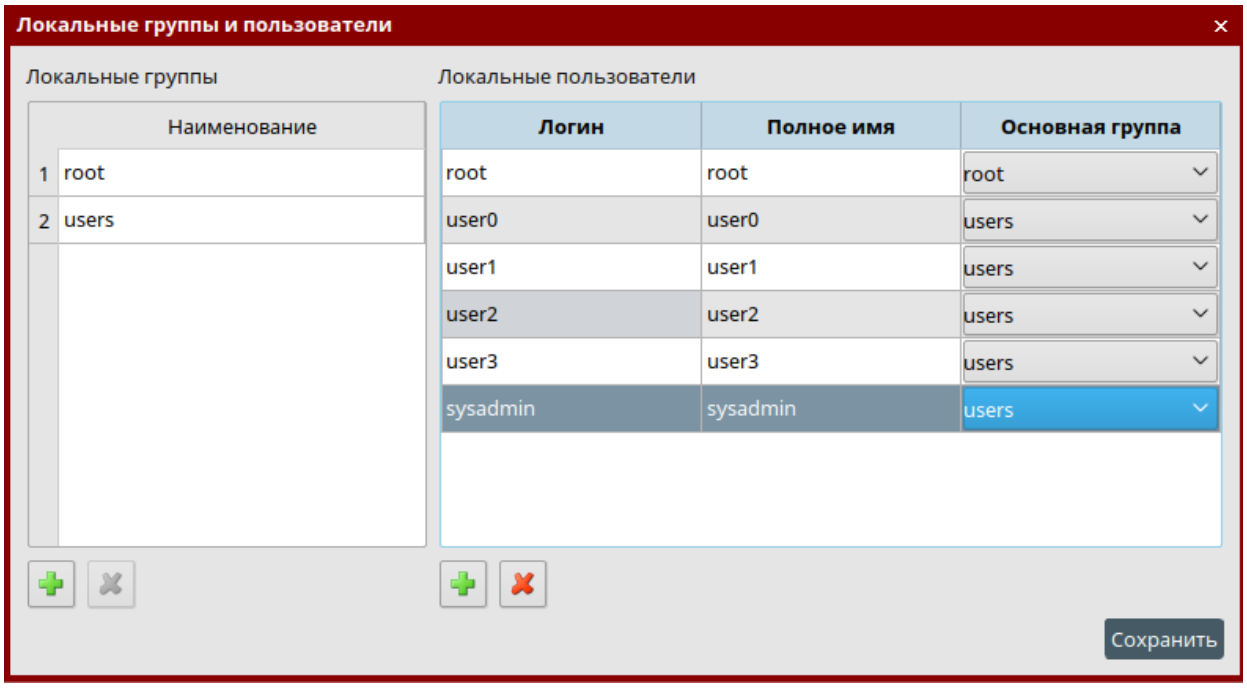


Рис. 87 – Диалоговое окно «Локальные группы и пользователи»

После ввода информации о локальных группах и пользователей необходимо нажать кнопку **[Закрыть]**.

3.16.3. Формирование списка пользователей, имеющих право входа на защищаемое устройство

Для определения пользователей, имеющих право входа на устройство, содержащее защищаемые ресурсы, предназначен пункт меню «Доступ к устройству».

Пункт меню «Доступ у устройству» содержит подпункты:

- «Добавить пользователю доступ к устройству (группе устройств)»;
- «Отменить пользователю доступ к устройству (группе устройств)».

Для добавления пользователю доступа к устройству (группе устройств) необходимо выбрать устройство из списка в левой части окна и выбрать подпункт «Добавить пользователю доступ к устройству (группе устройств)». В появившемся окне «Добавление пользователя» требуется выбрать учетную запись пользователя из списка и нажать кнопку **[Добавить]** (рис. 88), после чего наименование соответствующей учетной записи пользователя появится в правой части окна (рис. 89).

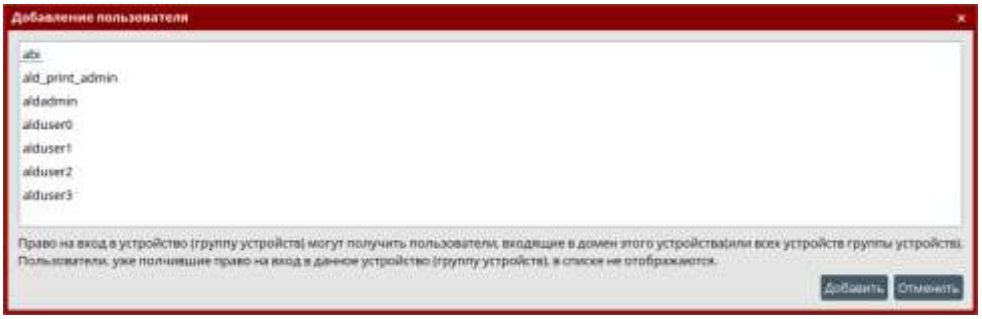


Рис. 88 – Диалоговое окно «Добавление пользователя»

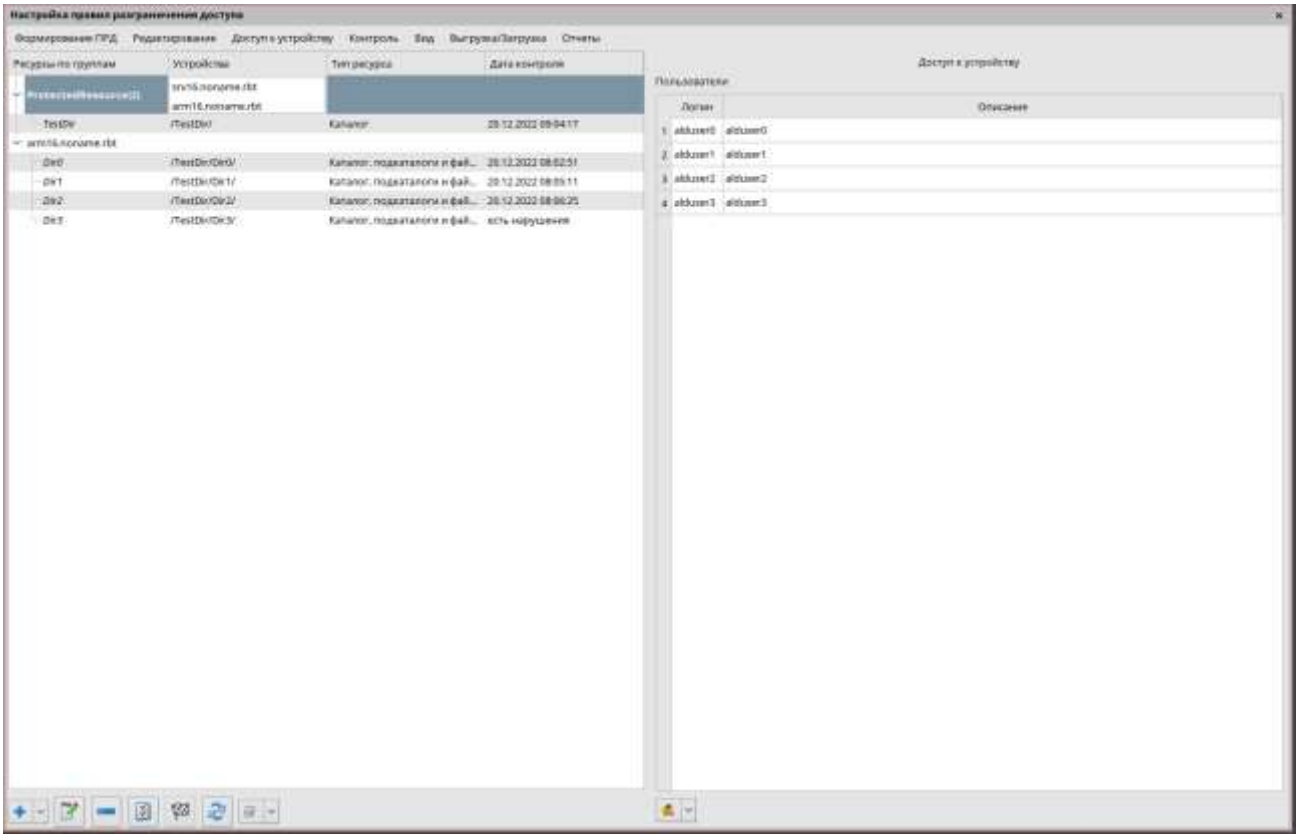


Рис. 89 – Доступ пользователей к устройству

Для отмены пользователю доступа к устройству требуется выбрать устройство из списка в левой части окна и наименование учетной записи пользователя в правой части окна, выбрать подпункт «Отменить пользователю доступ к устройству (группе

устройств)», после чего наименование соответствующей учетной записи пользователя будет удалено.

3.16.4. Проведение контроля соответствия действующих прав доступа значениям, указанным в таблице разграничения доступа к защищаемым ресурсам

Для проведения контроля соответствия действующих дискреционных, мандатных прав доступа и политики аудита требуемым значениям, указанным в таблице разграничения доступа к защищаемым ресурсам, предназначен пункт меню «Контроль».

Для проведения контроля необходимо выбрать защищаемый ресурс и открыть подпункт «Запустить контроль доступа». В случае положительных итогов проведения операции контроля в столбце «Дата контроля» устанавливается соответствующие дата и время. В противном случае в столбце «Дата контроля» устанавливается значение «Есть нарушения» (рис. 90).

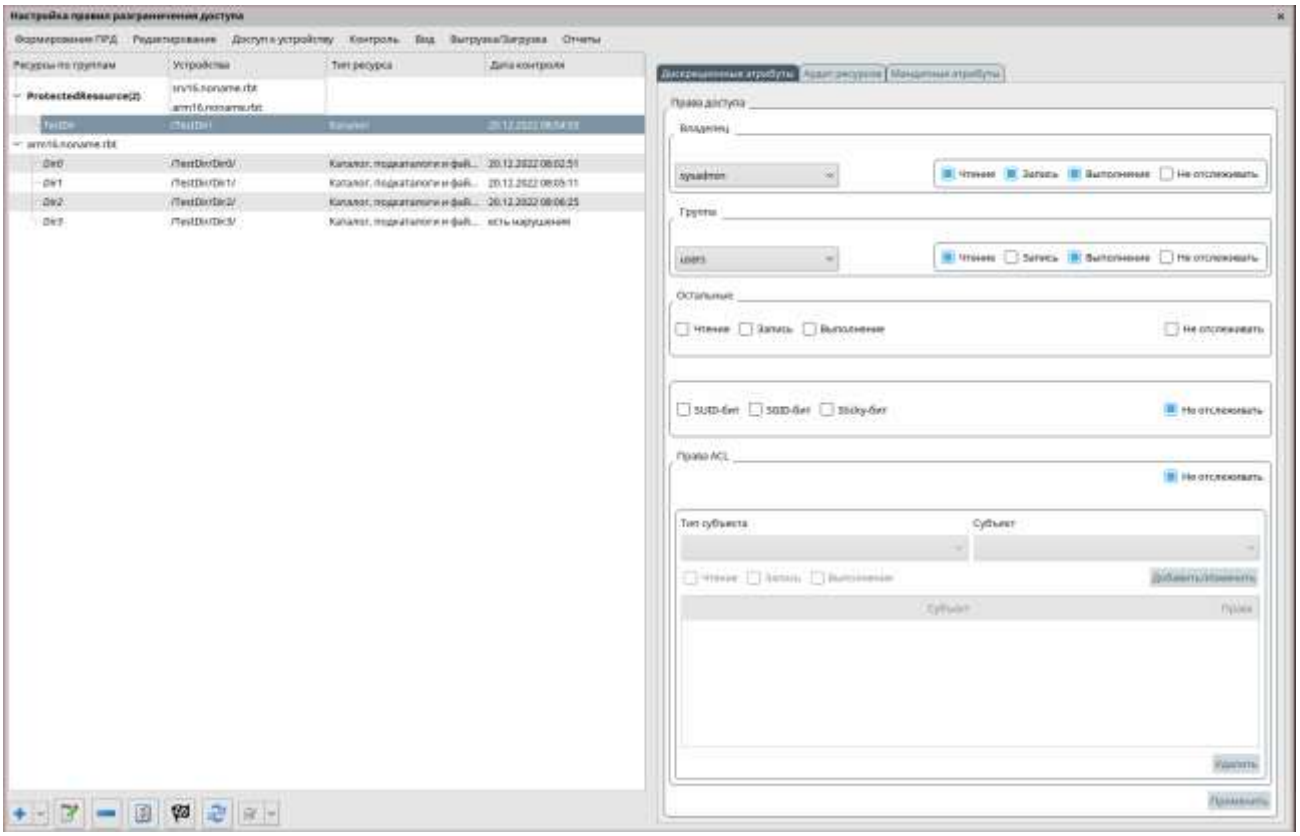


Рис. 90 – Контроль защищаемых ресурсов

3.16.5. Настройка отображения окна настройки правил разграничения доступа

Для включения или отключения отображения назначенных АРМ и назначенных ресурсов предназначен пункт меню «Вид». Для того, чтобы включить или отключить отображение назначенных АРМ и назначенных ресурсов необходимо установить или

убрать соответствующие флажки в подпунктах «Назначенные АРМ» и «Назначенные ресурсы».

3.16.6. Выгрузка и загрузка перечня и таблицы разграничения доступа к защищаемым ресурсам

Для выполнения выгрузки/загрузки и таблицы разграничения доступа к защищаемым ресурсам предназначен пункт меню «Выгрузка/Загрузка».

Пункт меню «Выгрузка/Загрузка» содержит подпункты (рис. 91):

- «Выгрузить дерево назначений групп устройств и ресурсов»;
- «Загрузить дерево назначений групп устройств и ресурсов»;
- «Загрузить ПРД для ресурса с устройства».

Подпункт «Загрузить ПРД для ресурса с устройства» содержит элементы:

- «Загрузить Дискреционные права для ресурса с устройства»;
- «Загрузить Аудит для ресурса с устройства»;
- «Загрузить Мандатные права для ресурса с устройства».

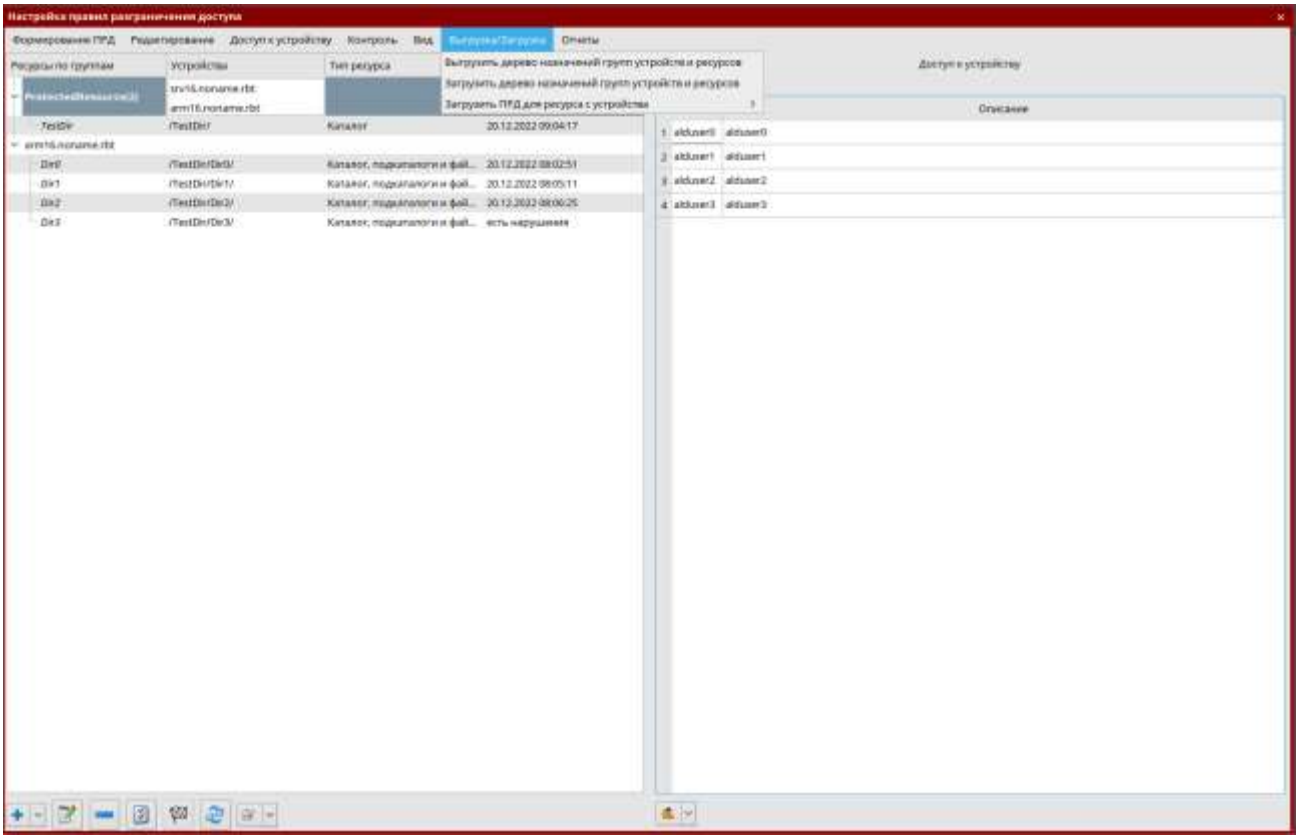


Рис. 91 – Пункт меню «Выгрузка/Загрузка»

Для выполнения выгрузки перечня защищаемых ресурсов необходимо выбрать подпункт «Выгрузить дерево назначений групп устройств и ресурсов», указать каталог для выгрузки в появившемся окне «Открыть файл» и нажать кнопку **[Открыть]**, после

чего в выбранном каталоге будет сформирован файл `exportfile.txt` с результатами выгрузки.

Для выполнения загрузки перечня защищаемых ресурсов необходимо выбрать подпункт «Загрузить дерево назначений групп устройств и ресурсов», выбрать в появившемся окне «Открыть файл» файл `exportfile.txt`, содержащий результаты ранее выполненной выгрузки, нажать кнопку **[Открыть]**, после чего в программу будут загружены перечни защищаемых ресурсов.

Для загрузки с устройства действующих дискреционных, мандатных прав доступа и политики аудита созданного защищаемого ресурса требуется выбрать соответствующий элемент подменю «Загрузить ПРД для ресурса с устройства», после чего будут установлены соответствующие значения дискреционных, мандатных прав доступа и политики аудита защищаемым ресурсам.

3.16.7. Построение отчетов о правилах разграничения доступа к защищаемым ресурсам.

Для построения отчетов о правилах разграничения доступа к защищаемым ресурсам и проведения контроля соответствия действующих дискреционных, мандатных прав доступа и политики аудита требуемым значениям, указанным в таблице разграничения доступа к защищаемым ресурсам, предназначен пункт меню «Отчеты».

Пункт меню «Отчеты» содержит подпункты:

- «Перечень защищаемых ресурсов»;
- «Отчет контроль доступа»;
- «Анализ проблемных ресурсов».

Подпункт «Перечень защищаемых ресурсов» предназначен для построения отчета, содержащего перечень защищаемых ресурсов. Внешний вид отчета приведен на рис. 92.

Рис. 92 – Отчет «Перечень защищаемых ресурсов»

Для выявления ресурсов, содержащих расхождения дискреционных, мандатных прав доступа и политики аудита к защищаемым ресурсам, служит отчет «Отчет контроль доступа». Для его запуска предназначен подпункт «Отчет контроль доступа» пункта меню «Отчеты». Внешний вид отчета приведен на рис. 93.

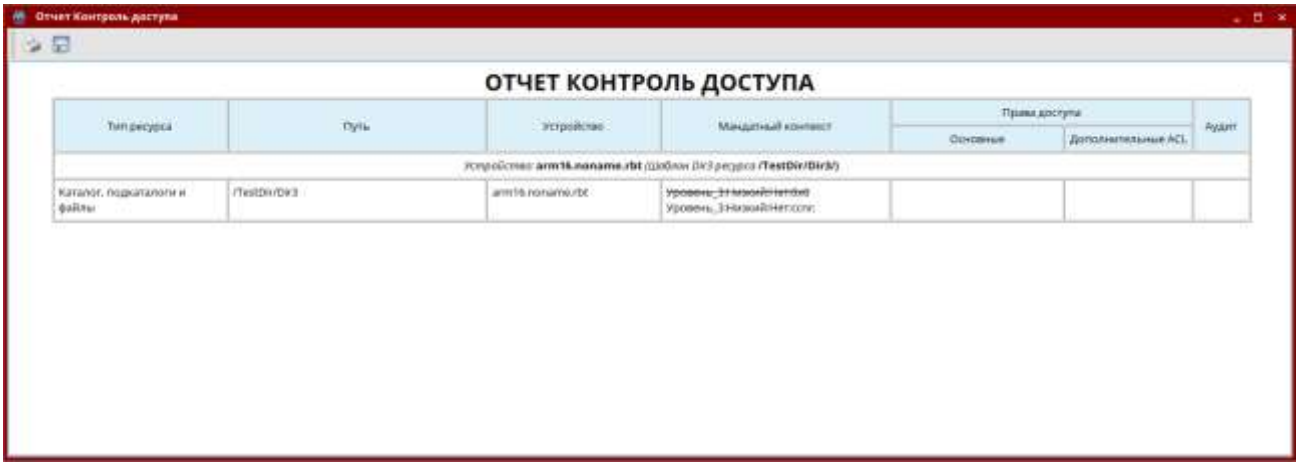


Рис. 93 – Отчет «Отчет контроль доступа»

Отчет «Анализ проблемных ресурсов» предназначен для выявления защищаемых ресурсов устройств, у которых некорректно заданы правила разграничения доступа (например, удалены пользователь или группа, заданные при установке дискреционных правил разграничения доступа к ресурсу). Внешний вид отчета приведен на рис. 94.

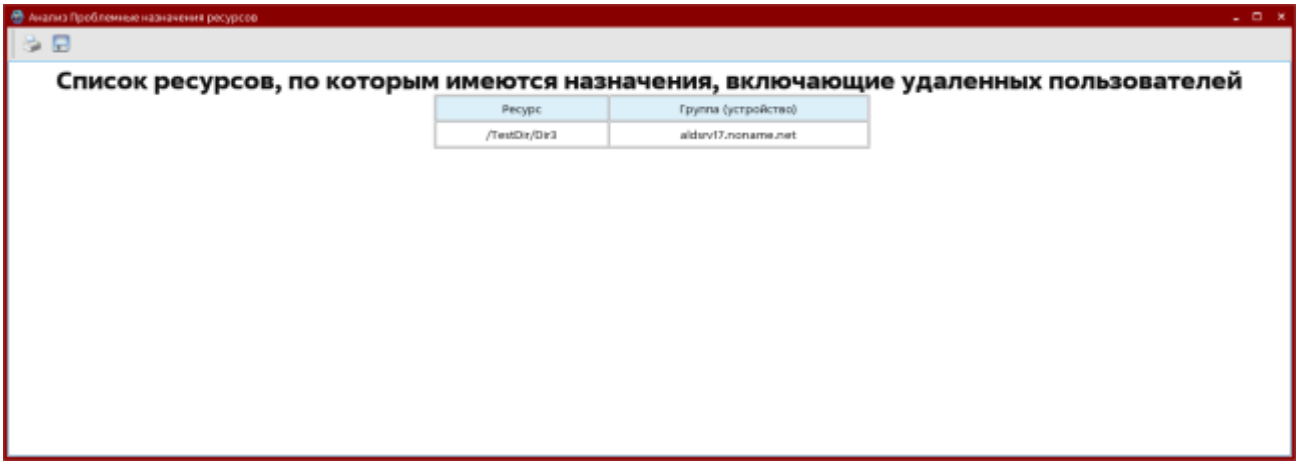


Рис. 94 – Отчет «Анализ проблемных ресурсов»

3.17. Работа со справочной системой

Для вызова справки необходимо переместить указатель «мыши» на элемент, для которого необходимо получить справочную информацию, и нажать клавишу **<F1>**. В браузере по умолчанию откроется страница, содержащая справочную информацию по выбранному элементу. На рис. 95 приведен пример справочной информации для окна «Тиражирование правил отчуждаемых носителей».

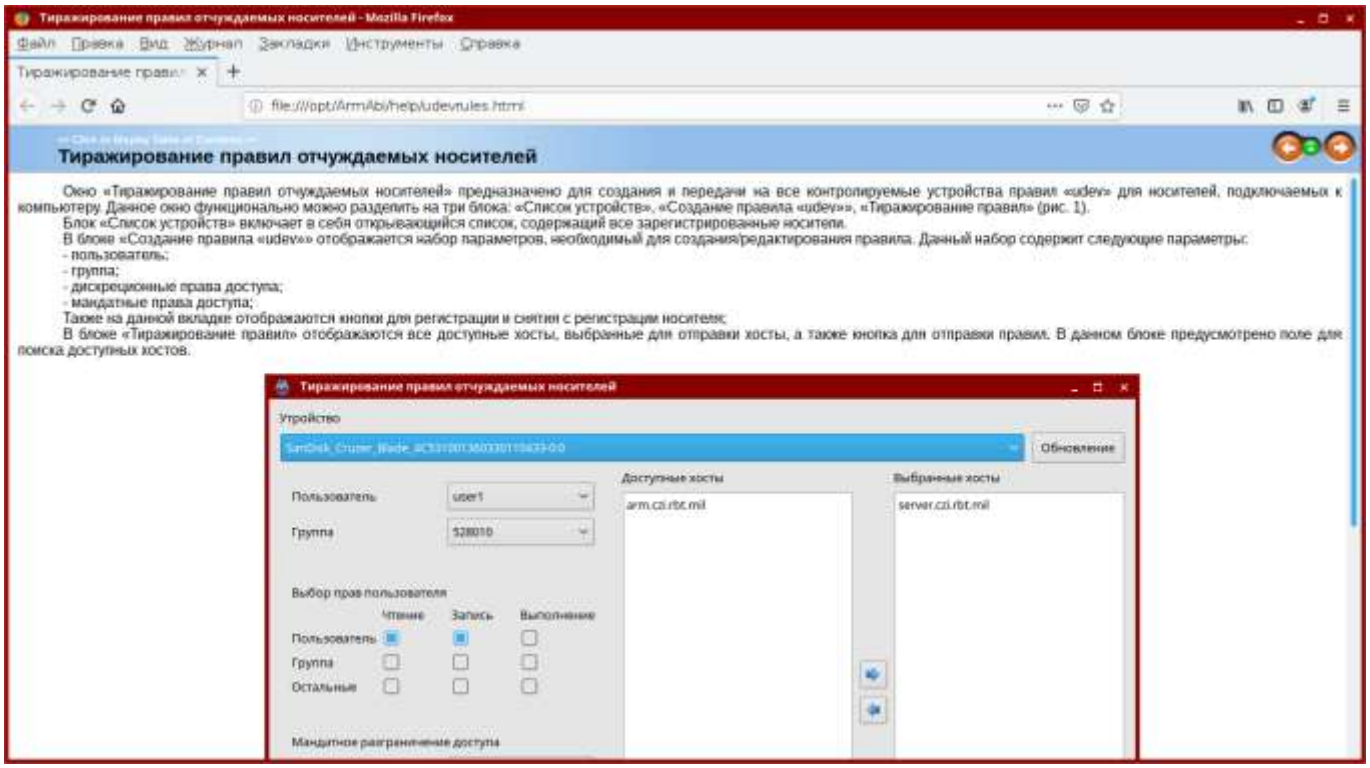


Рис. 95 – Web-страница со справочной информацией

Если для выбранного элемента не существует справки, будет открыта справочная страница для основного окна программы.

3.18. Завершение работы программы

Для завершения работы с программой необходимо закрыть главное окно программы или выбрать подпункт «Выход» пункта меню «Файл».

4. СООБЩЕНИЯ ОПЕРАТОРУ

При эксплуатации ПС АРМ АБИ возможно появление сообщений оператору об ошибках работы программы и информационных сообщений.

4.1. Сообщения об ошибках соединения с базой данных программы

К сообщениям об ошибках соединения с базой данных программы относятся сообщения вида:

- «Не удалось установить соединение с БД. СБОЙ: в pg_hba.conf нет записи, разрешающей подключение…»;
- «Не удалось установить соединение с БД. СБОЙ: пользователь … не прошел проверку подлинности …»;
- «Не удалось установить соединение с БД. FATAL: база данных … не существует…».

При их возникновении необходимо проверить значения параметров соединения с базой данных (значения полей «Хост с БД», «Имя БД», «Имя пользователя», «Пароль»), заданных при установке сервера безопасности ПС АРМ АБИ.

4.2. Сообщения об ошибках работы с файлами протоколов проведения проверок КЦ, САВЗ и тестирования СЗИ

К сообщениям об ошибках работы с файлами протоколов проведения проверок КЦ, САВЗ и тестирования СЗИ относятся сообщения вида:

- «Журнал не найден»;
- «Ошибка создания файла»;
- «Ошибка записи файла»;
- «Ошибка открытия файла»;
- «Ошибка чтения файла»;
- «Не удалось переместить файл»;
- «Нет прав доступа. Не записаны данные в .log»;
- «Нет прав доступа. .log не создан».

При их возникновении необходимо повторно выполнить соответствующую операцию (проведения КЦ, антивирусную проверку, тестирование СЗИ устройства) и проверить права доступа учетной записи администратора безопасности информации к каталогу `/opt/ArmAbi/log`.

4.3. Сообщения об ошибках работы с доменом

К сообщениям об ошибках работы с доменом относятся сообщения:

- «Не удалось получить список хостов»;
- «Не удалось получить список пользователей»;
- «Не удалось получить список групп»;
- «Не удалось получить список атрибутов хостов»;
- «Не удалось получить список атрибутов пользователей».

При их возникновении необходимо проверить доступность сервера контролируемого домена.

4.4. Сообщения об ошибках обращения к генератору пароля

К сообщениям об ошибках обращения к генератору пароля относятся сообщения:

- «Библиотека ПДСЧ выдала ошибку!»;
- «Функция генерации пароля недоступна!».

При их возникновении необходимо проверить работоспособность КП СГП РУСБ.30563-01 и в случае обнаружения ошибок выполнить его переустановку.

4.5. Сообщение о попытке перерегистрации устройства

При возникновении сообщения «Попытка повторной регистрации клиента» администратору информационной безопасности требуется принять решение о необходимости повторной регистрации устройства и нажать кнопку **[Да]** при согласии или **[Нет]** в противном случае.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБИ	– администратор безопасности информации
АРМ	– автоматизированное рабочее место
БД	– база данных
ЕПП	– единое пространство пользователей
ИБ	– информационная безопасность
КП	– комплекс программ
КСЗ	– комплекс средств защиты
КЦ	– контроль целостности
ЛУ	– лист утверждения
НЖМД	– накопитель на жестком магнитном диске
НСД	– несанкционированный доступ
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПС	– программное средство
САВЗ	– средства антивирусной защиты
СЗИ	– средства защиты информации
СГП	– специализированный генератор паролей
СН	– специальное назначение
СПО	– специальное программное обеспечение
СУБД	– система управления базами данных
ПРД	– правила разграничения доступа
ACL	– Access Control List (список управления доступом)
ALD	– Astra Linux Directory (служба доменов Astra Linux)
FreeIPA	– Free Identity, Policy and Audit (свободная идентификация, политика и аудит)
UID	– User Identifier (Идентификатор пользователя)

Лист регистрации изменений										
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изменённых	заменённых	новых	аннулированных					