

Утвержден
РУСБ.30488-04 ЛУ

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

ПС АРМ АБИ
Руководство оператора
РУСБ.30488-04 34 01
Листов 54

2019

Литера О₁

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	5
2. Условие выполнения программы.....	6
2.1. Минимальный состав аппаратных средств	6
2.2. Минимальный состав программных средств	6
2.3. Требования к персоналу (пользователю).....	6
3. Выполнение программы	8
3.1. Запуск программы.....	8
3.2. Настройка авторизации в управляемых доменах.....	10
3.3. Раздел «Устройства».....	10
3.3.1. Управление дискреционными правами доступа к информационным ресурсам	11
3.3.2. Управление мандатными правами доступа к информационным ресурсам.....	13
3.3.3. Управление параметрами аудита информационных ресурсов	14
3.3.4. Стирание защищаемой информации	15
3.4. Раздел «Пользователи»	17
3.4.1. Создание/редактирование учетной записи пользователя	18
3.4.2. Настройка доступа пользователя к информационным ресурсам на основе ролевой модели	20
3.4.3. Настройка мандатных атрибутов пользователя.....	22
3.4.4. Настройка доменных привилегий пользователя	23
3.4.5. Блокировка/разблокировка учетной записи пользователя	24
3.4.6. Установка/смена пароля учетной записи пользователя.....	25
3.4.7. Настройка должностных и функциональных ролей	27
3.5. Раздел «Контроль целостности»	29
3.5.1. Настройка перечня объектов для КЦ	29
3.5.2. Запуск КЦ.....	30
3.5.3. Отправка конфигурации КЦ на управляемое устройство	32
3.6. Раздел «Антивирусная проверка»	32
3.6.1. Настройка перечня объектов для антивирусной проверки.....	33
3.6.2. Запуск антивирусной проверки	34
3.6.3. Обновление лицензии	35
3.7. Раздел «Тестирование СЗИ»	36
3.8. Раздел «События ИБ»	40
3.8.1. Просмотр событий ИБ	41

3.8.2. Построение отчета о событиях ИБ	42
3.8.3. Архивация событий ИБ	43
3.8.4. Настройка передачи событий ИБ на вышестоящий уровень.....	43
3.8.5. Настройка автоблокировки пользователей по событиям ИБ	44
3.9. Раздел «Внешние события ИБ».....	45
3.9.1. Настройка приема событий ИБ с нижестоящего уровня.....	46
3.10. Резервное копирование конфигурации домена.....	47
3.11. Настройка параметров программы.....	48
3.12. Работа под принуждением	49
3.13. Завершение работы программы	50
3.14. Резервное копирование базы данных	50
4. Сообщения оператору	51
Перечень сокращений	53

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. 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».

1.2. 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) управление доступом пользователей к устройствам домена;

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

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

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

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

8) формирование и просмотр журналов системы централизованного протоколирования;

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

10) резервное копирование данных (конфигурации) управляемых доменов;

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

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

13) передачу событий НСД на АРМ АБИ верхнего уровня.

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

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

2.2.1. Программа предназначена для функционирования в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-01 версии 1.6 и выше (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.

2.2.2. Для реализации функционального предназначения программы необходимо наличие установленного программного обеспечения:

- средства антивирусной защиты (на управляемых устройствах).


2.3. Требования к персоналу (пользователю)

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

Пользователь, допущенный к работе с ПС АРМ АБИ, должен сдать квалификационный экзамен на I группу электробезопасности.

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, наименование БД, имя и пароль пользователя БД), а также единые (по умолчанию) для всех доменов имя и пароль администратора доменов.

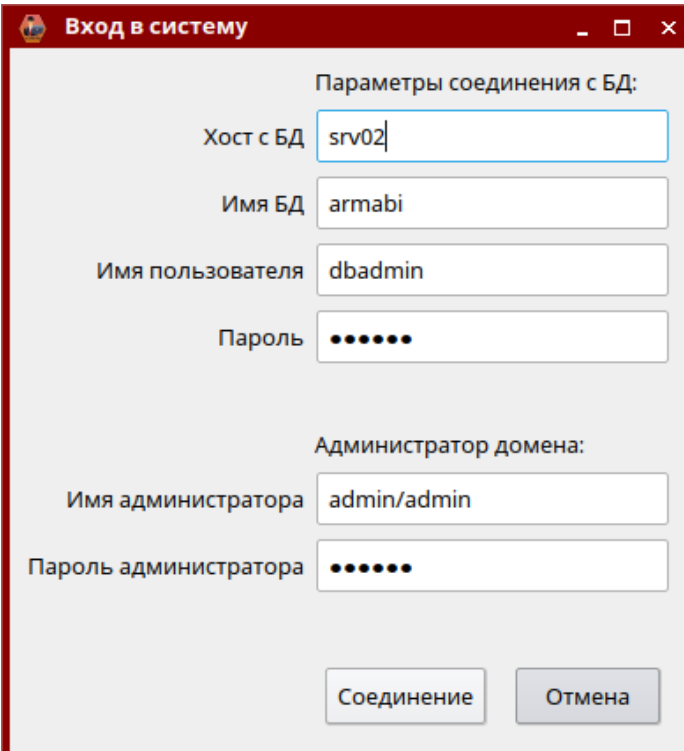


Рис. 1 – Окно аутентификации в БД

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 информацией об управляемых устройствах, образующие соответствующие разделы программы (рис. 2):

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

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

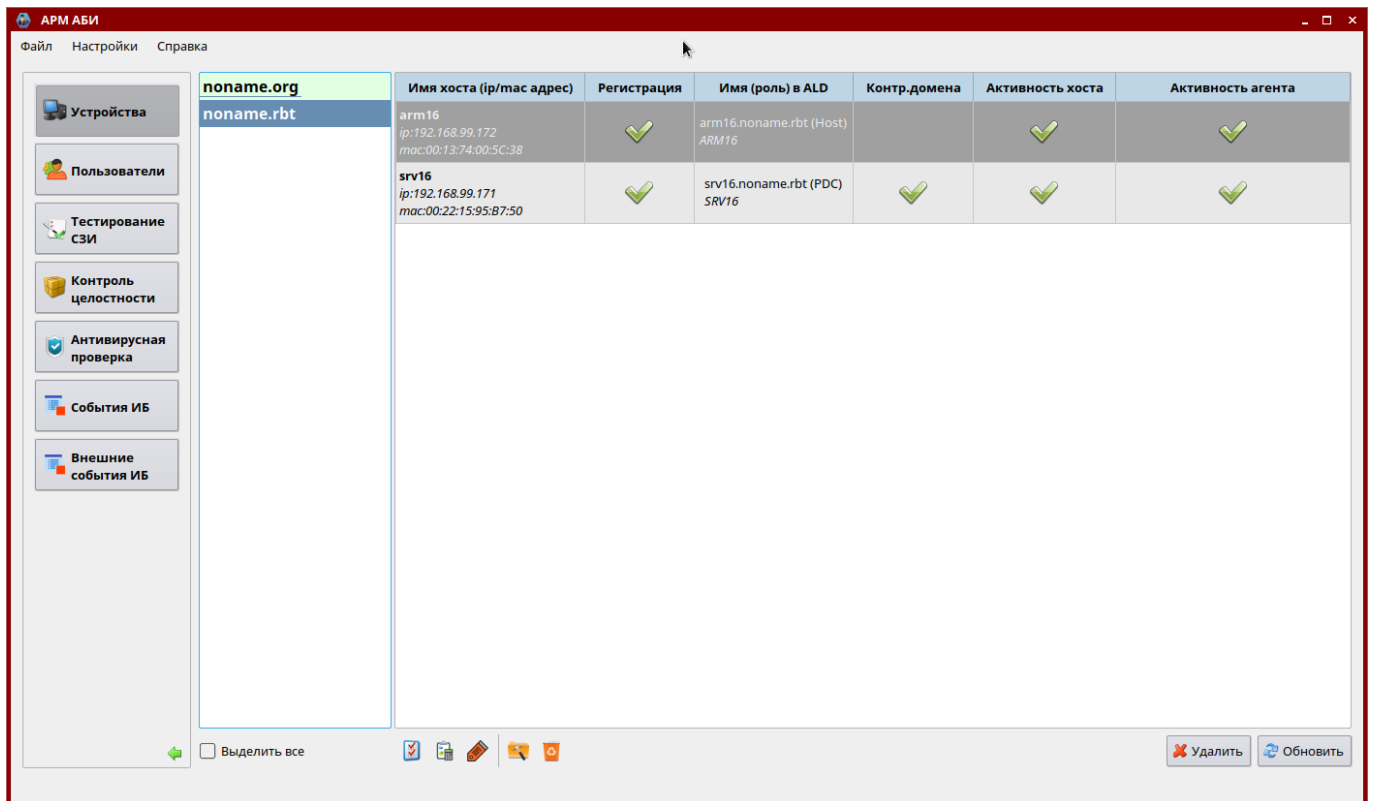


Рис. 2 – Основное окно программы



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, желтым цветом в случае ошибки авторизации администратора домена и красным 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 авторизации в управляемых доменах

По умолчанию при организации единого пространства пользователей службы организации домена для авторизации в домене используются логин и пароль администратора, указанные в диалоге входа в систему (см. рис. 1), но при этом сохраняется возможность установить для каждого контролируемого домена индивидуальные логин и пароль администратора домена.

При клике правой кнопкой мыши на названии домена (доступно во всех разделах программы) открывается меню, в котором при выборе пункта « Установить пароль» обеспечивается возможность установки индивидуальных логина и пароля администратора выбранного домена. Для удаления (индивидуальных) логина и пароля администратора выбранного домена требуется нажать правую кнопку мыши и выбрать пункт « Удалить пароль» (рис. 3).

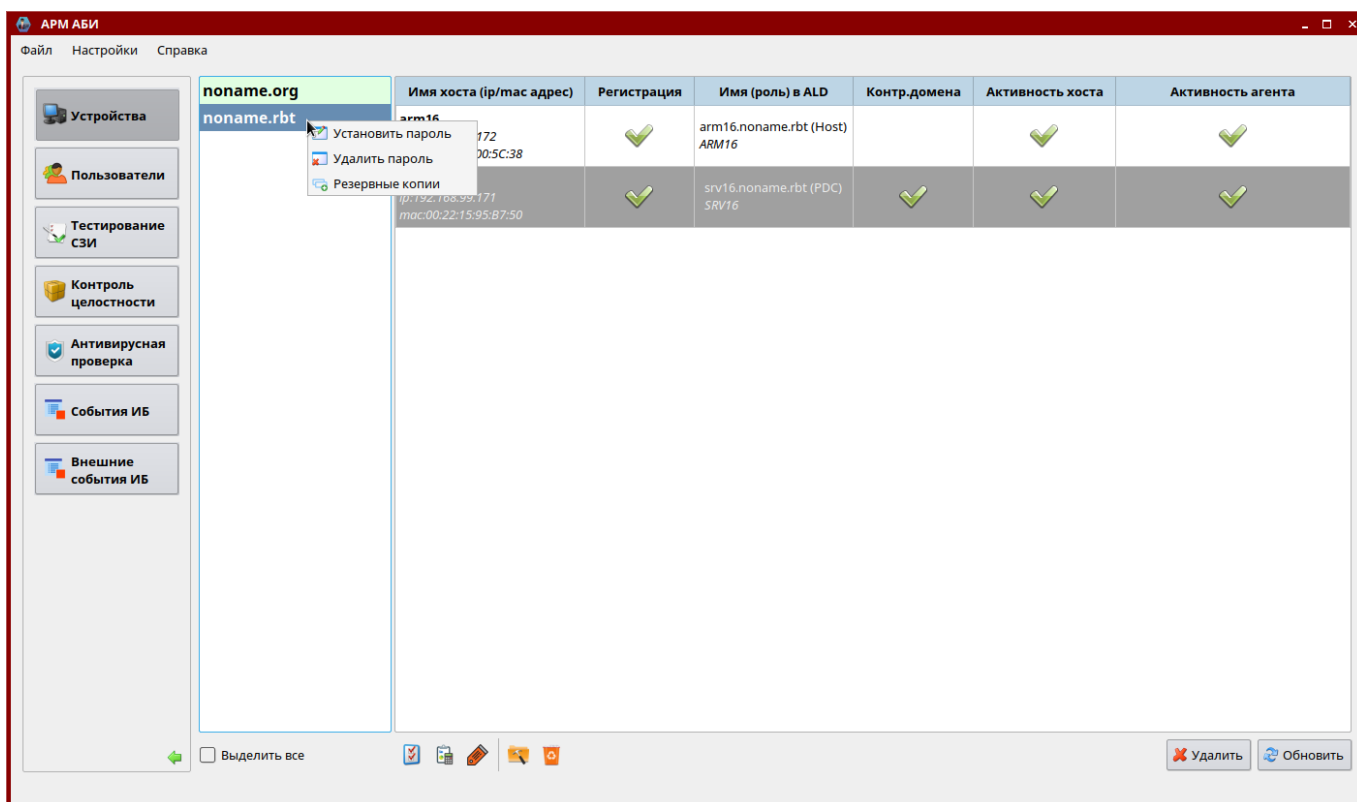


Рис. 3 – Настройка авторизации в контролируемых доменах

3.3. 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. 4):

- 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.

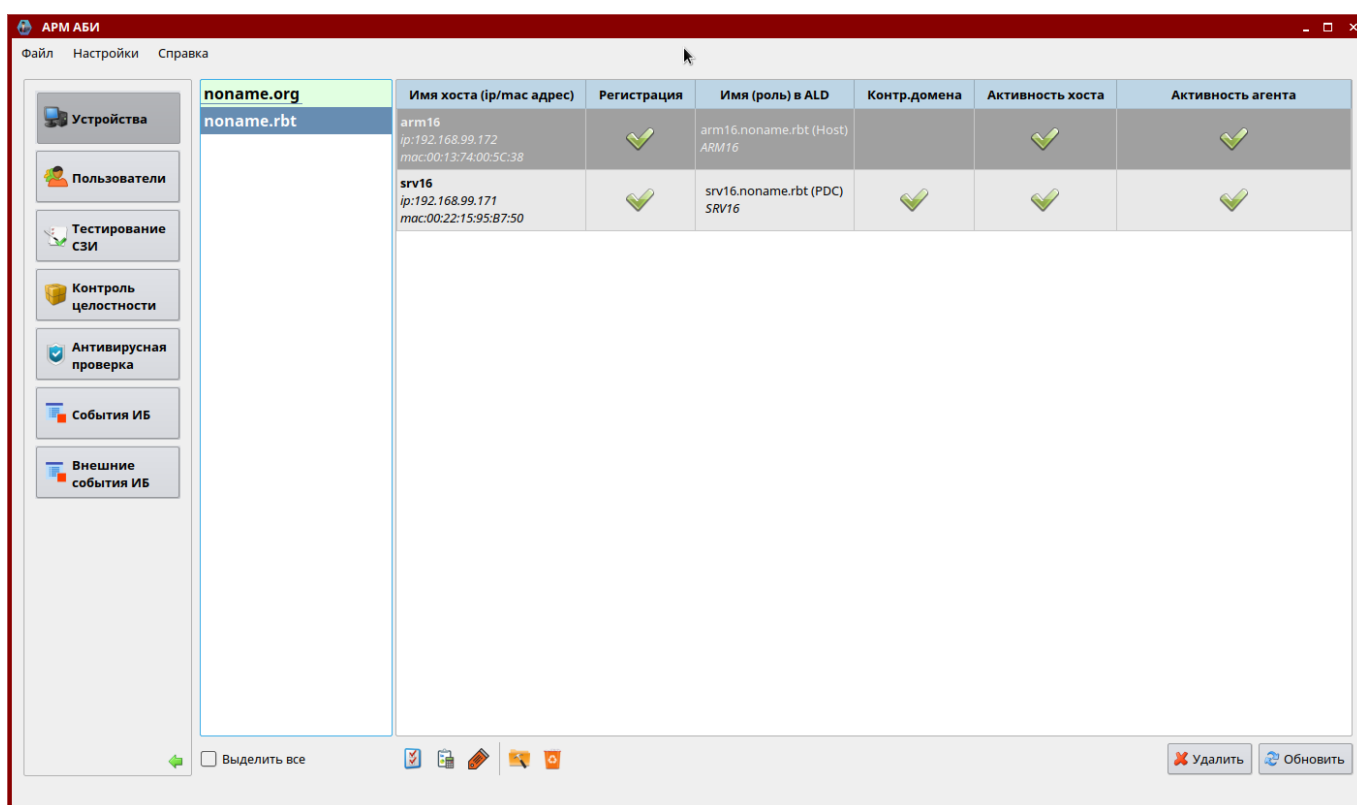



Рис. 4 – Раздел «Устройства»

В нижней части окна программы при этом отображаются кнопки для настройки дискреционных и мандатных прав доступа, аудита доступа к информационным ресурсам на управляемых устройствах, выбора объектов для гарантированного удаления и выполнения операции гарантированного удаления защищаемой информации (объектов) по команде администратора безопасности информации, а также кнопки **[Удалить]** и **[Обновить]**.

3.3.1. 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. 5).

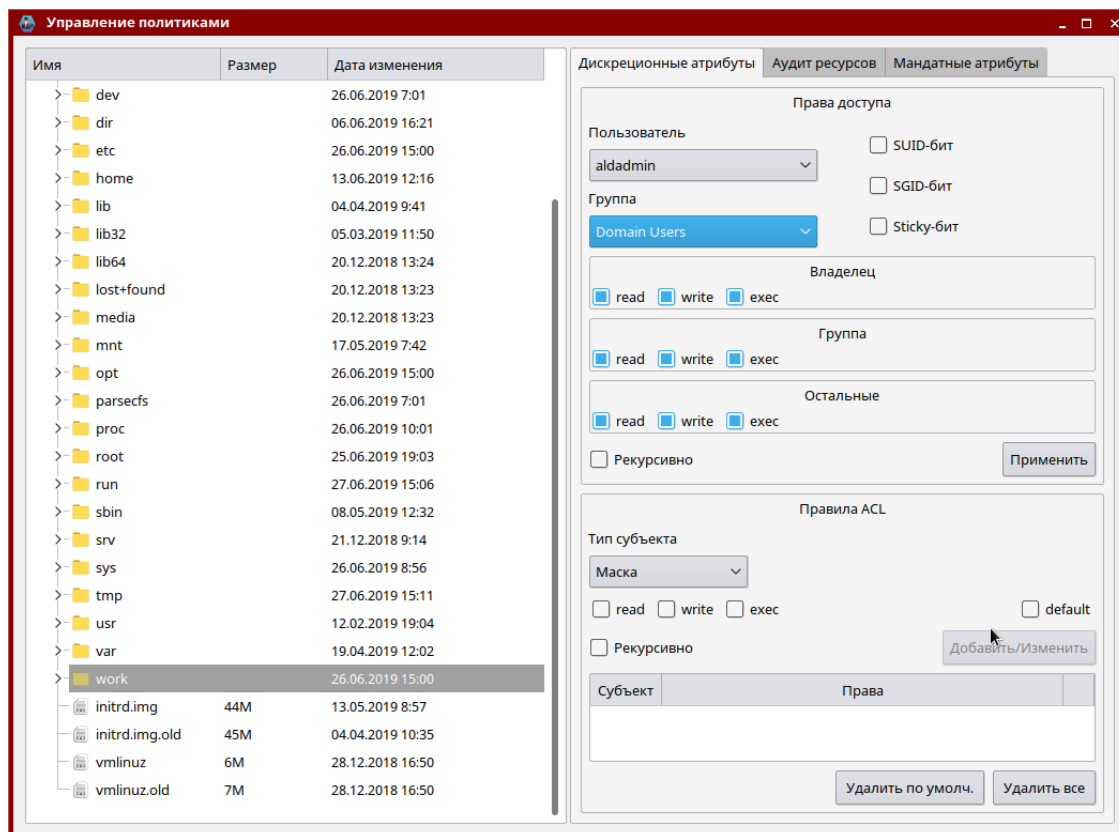


Рис. 5 – Настройка дискреционных прав доступа

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]**.


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

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.

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.

3.3.2. 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. 6).

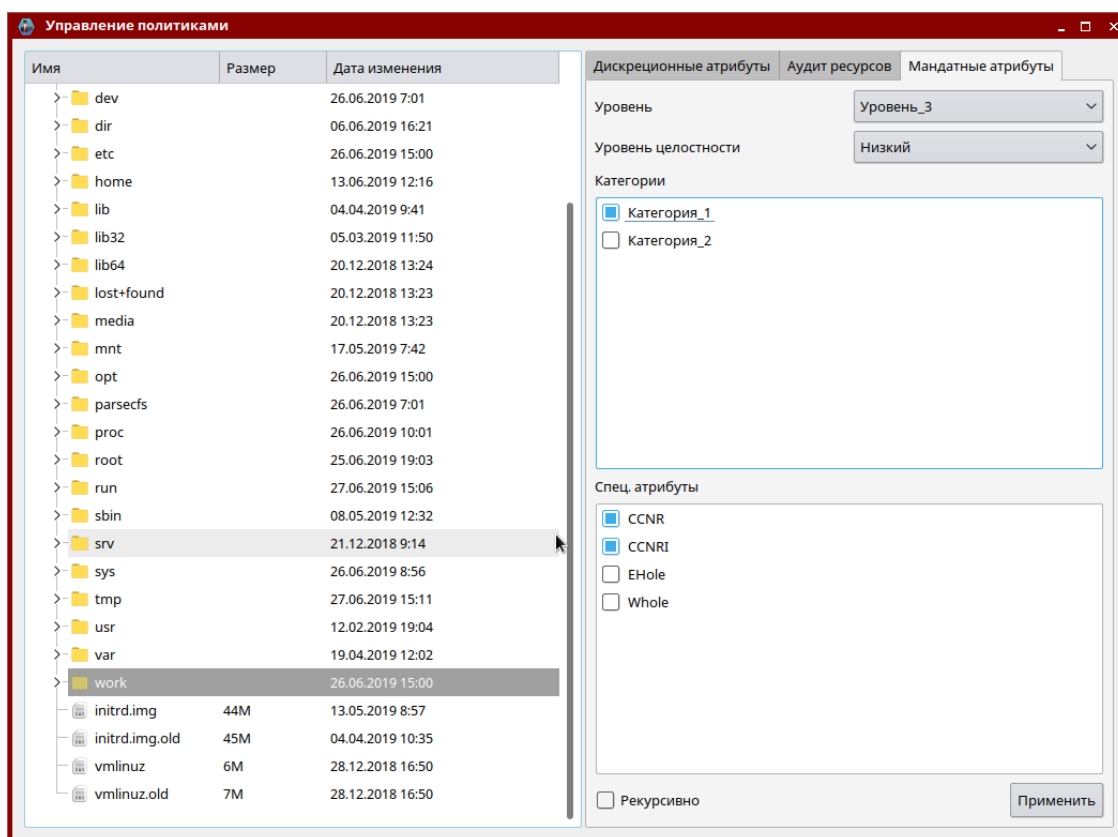


Рис. 6 – Настройка мандатных прав доступа

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 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.

3.3.3. Управление параметрами аудита информационных ресурсов

Для настройки параметров аудита информационных ресурсов 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. 7).

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

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 кнопку закрытия в верхнем правом углу окна.

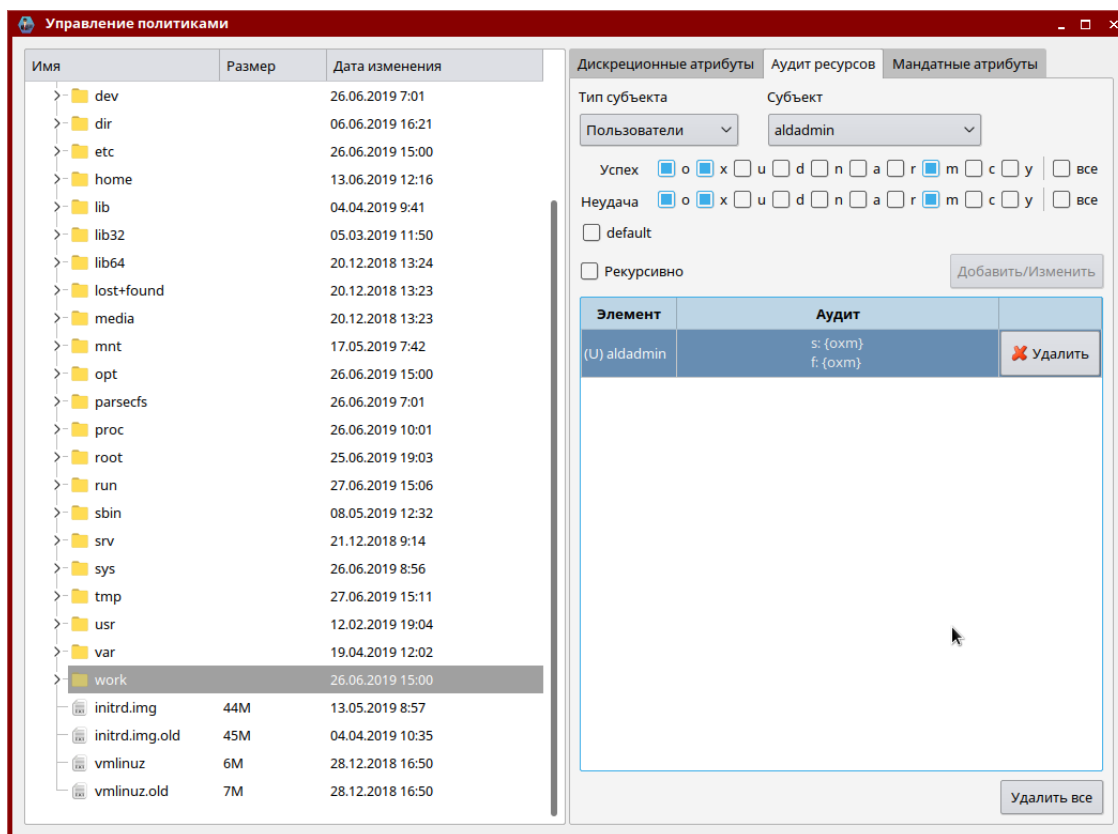




Рис. 7 – Настройка аудита ресурсов


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.

3.3.4. 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. 8).

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 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]**.

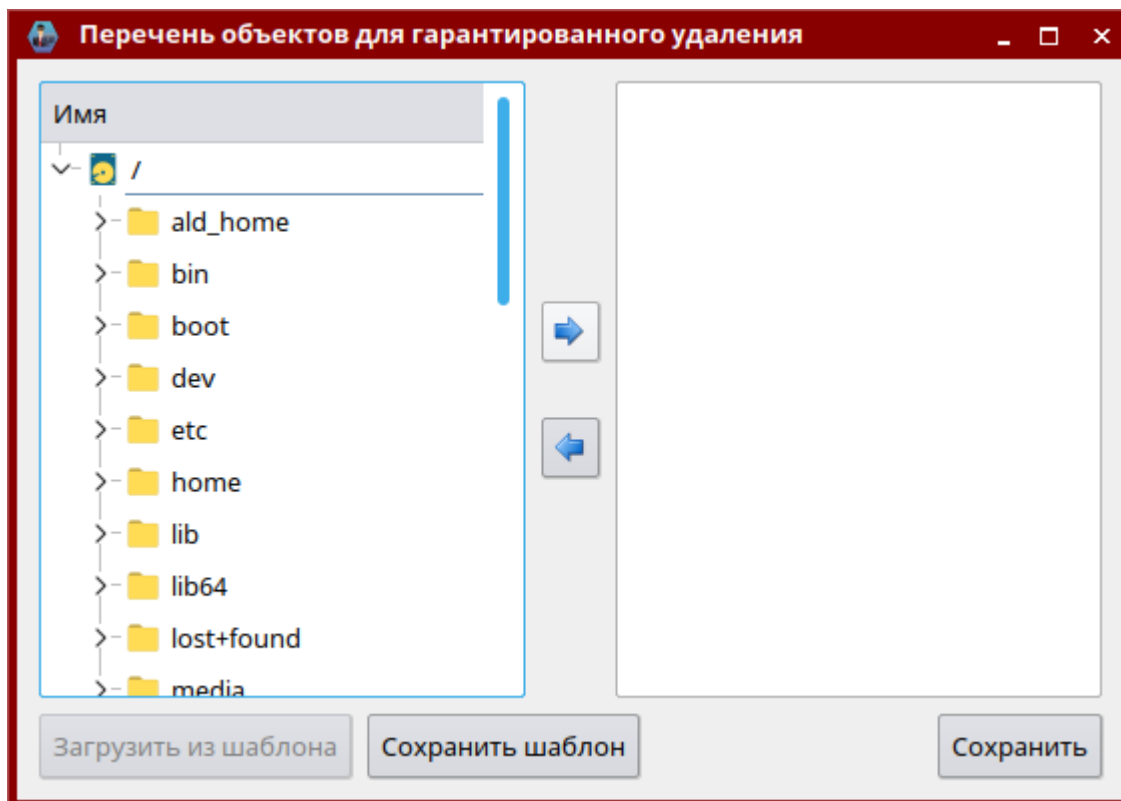



Рис. 8 – Выбор перечня объектов (ресурсов) устройства, подлежащих стиранию по команде администратора безопасности информации

При нажатии на кнопку  после подтверждения операции администратором безопасности информации (рис. 9) происходит удаление всех компонент, заданных в конфигурации устройства.

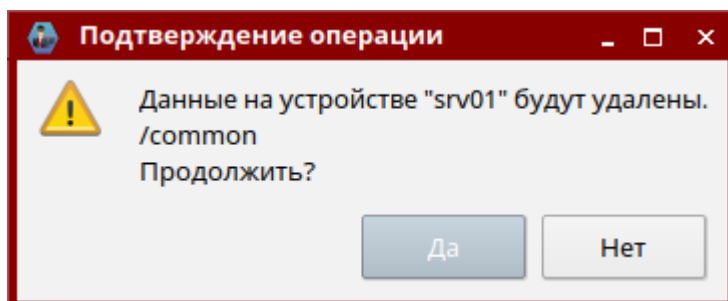


Рис. 9 – Подтверждение операции стирания защищаемой информации

3.4. 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 использовании для организации единого пространства пользователей службы организации домена в данном разделе дополнительно можно выполнить настройку мандатных атрибутов и доменных привилегий пользователей и их доступа к устройствам домена.

Внешний вид раздела приведен на рис. 10 и содержит следующую информацию:

- UID пользователя;
- логин пользователя;
- полное имя пользователя;
- описание;
- статус пользователя (активен/блокирован).


UID	Логин пользователя	Полное имя	Описание	Имя домена	Статус
2501	aldadmin	aldadmin	AldAdmin	noname.rbt	✓
2502	alduser0	alduser0	AldUser0	noname.rbt	✓
2503	alduser1	Alduser1	AldUser1	noname.rbt	✓
2504	alduser2	alduser2	AldUser2	noname.rbt	✓
2505	alduser3	alduser3	AldUser3	noname.rbt	✓

Рис. 10 – Раздел «Пользователи»

В нижней части окна программы отображаются кнопки для редактирования настроек существующей учетной записи, создания новой учетной записи, а также кнопка настройки ресурсов СУБД для обеспечения настройки доступа пользователей к ресурсам на основе ролевой модели.

3.4.1. Создание/редактирование учетной записи пользователя

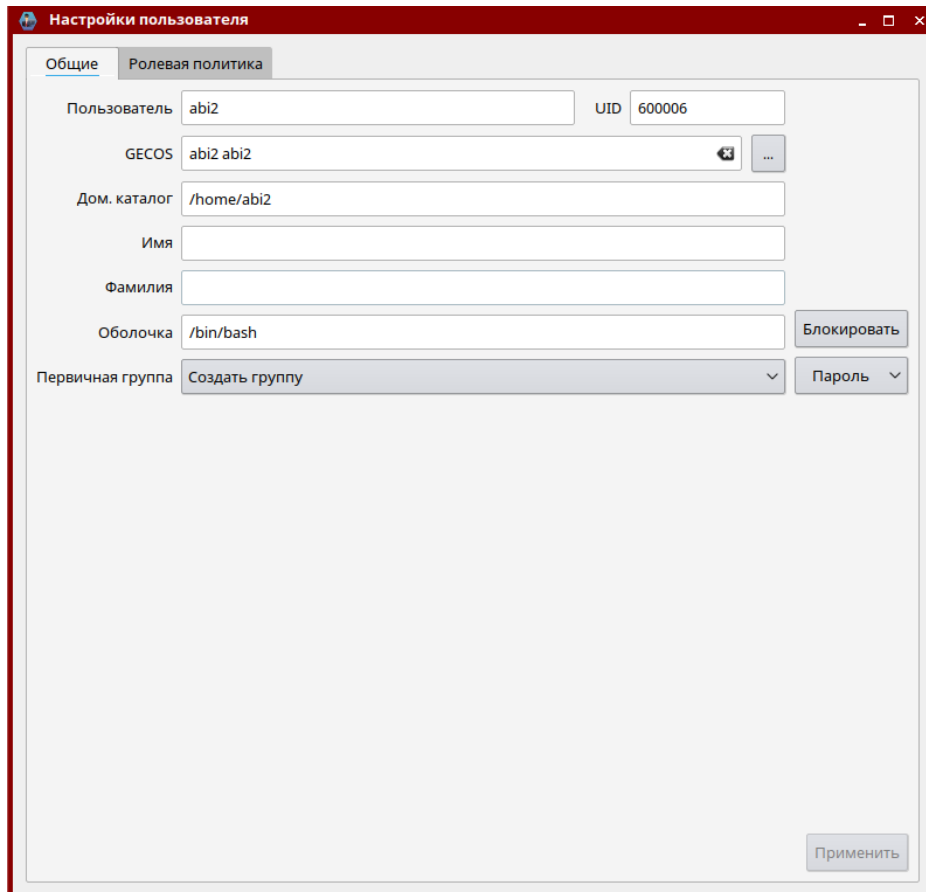
Для создания новой учетной записи пользователя необходимо нажать на кнопку

[Новый пользователь] для изменения настроек существующей – 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. 11). А в случае использования службы ALD окно «Настройки пользователя» содержит вкладки «Общие», «Ролевая политика», «MPД» и «Привилегии домена» (рис. 12).

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

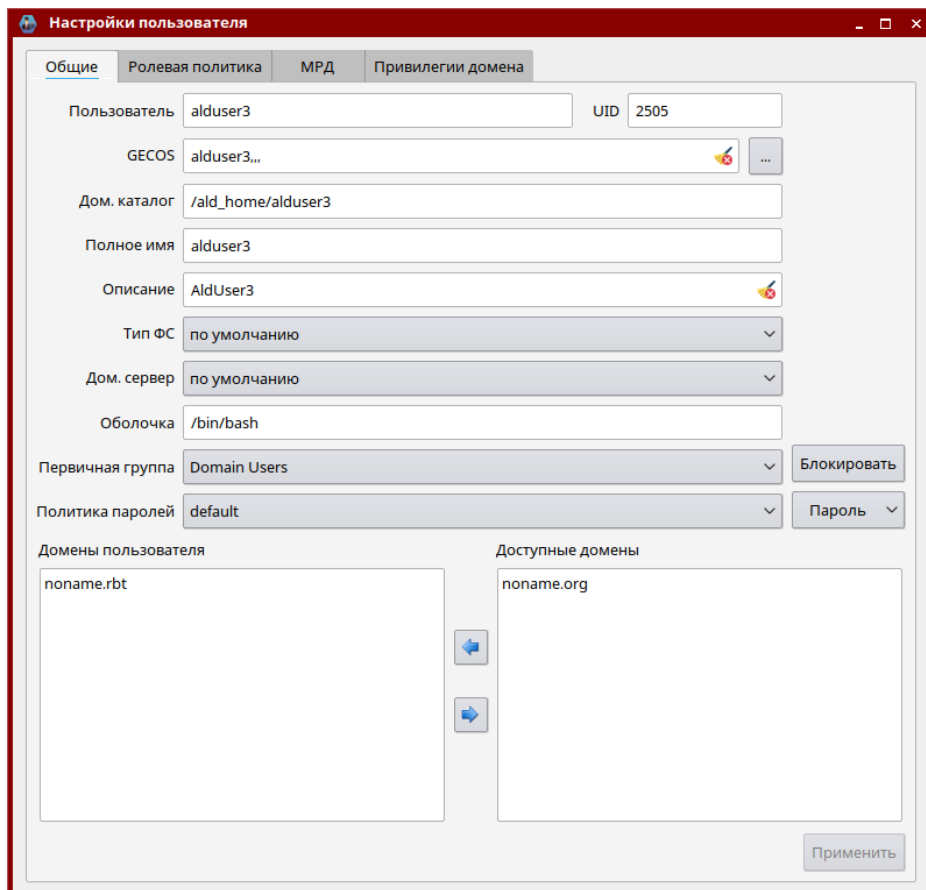
- «Пользователь» (обязательное);
- «UID» (обязательное, формируется автоматически в случае отсутствия);
- «GECOS» (необязательное, заполняется с использованием всплывающего диалогового окна);
- «Домашний каталог» (обязательное, используется значение «по умолчанию»);
- «Полное имя» (в домене ALD, необязательное);
- «Описание» (в домене ALD, необязательное);
- «Тип файловой системы» (в домене ALD, обязательное, используется значение «по умолчанию»);
- «Домашний сервер» (в домене ALD, обязательное, используется значение «по умолчанию»);
- «Оболочка» (обязательное, по умолчанию используется значение «./bin/bash»);
- «Первичная группа» (обязательное, в домене ALD по умолчанию используется значение «Domain Users»);
- «Политика паролей» (в домене ALD, обязательное, по умолчанию используется значение «default»).



The screenshot shows the 'Настройки пользователя' (User Settings) window in FreeIPA. The 'Общие' (General) tab is active. The user name is 'abi2' and the UID is '600006'. The GECOS field contains 'abi2 abi2'. The home directory is '/home/abi2'. The shell is '/bin/bash'. The primary group is set to 'Создать группу' (Create group). There are buttons for 'Блокировать' (Lock) and 'Пароль' (Password). A 'Применить' (Apply) button is at the bottom right.

Пользователь	abi2	UID	600006
GECOS	abi2 abi2		
Дом. каталог	/home/abi2		
Имя			
Фамилия			
Оболочка	/bin/bash		Блокировать
Первичная группа	Создать группу		Пароль

Рис. 11 – Создание/редактирование учетной записи пользователя в домене FreeIPA





The screenshot shows the 'Настройки пользователя' (User Settings) window in FreeIPA. The 'Общие' (General) tab is active. The user name is 'alduser3' and the UID is '2505'. The GECOS field contains 'alduser3...'. The home directory is '/ald_home/alduser3'. The full name is 'alduser3'. The description is 'AldUser3'. The type of OS is 'по умолчанию' (default). The home server is 'по умолчанию' (default). The shell is '/bin/bash'. The primary group is 'Domain Users'. The password policy is 'default'. There are buttons for 'Блокировать' (Lock) and 'Пароль' (Password). At the bottom, there are two lists: 'Домены пользователя' (User domains) containing 'noaname.rbt' and 'Доступные домены' (Available domains) containing 'noaname.org'. There are arrows between the lists to move items. A 'Применить' (Apply) button is at the bottom right.

Пользователь	alduser3	UID	2505
GECOS	alduser3...		
Дом. каталог	/ald_home/alduser3		
Полное имя	alduser3		
Описание	AldUser3		
Тип ОС	по умолчанию		
Дом. сервер	по умолчанию		
Оболочка	/bin/bash		Блокировать
Первичная группа	Domain Users		Пароль
Политика паролей	default		

Домены пользователя: noaname.rbt

Доступные домены: noaname.org

Рис. 12 – Создание/редактирование учетной записи пользователя в домене ALD

В случае использования для организации единого пространства пользователей службы организации домена ALD из списка доступных доменов с использованием кнопок  и  необходимо задать домены, в которых будет создана учетная запись пользователя.

Для установки пароля пользователя необходимо нажать 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]**.

После выполнения редактирование атрибутов учетной записи для сохранения изменений необходимо нажать на кнопку **[Применить]**.

3.4.2. Настройка доступа пользователя к информационным 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 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 доступа пользователя к ресурсам на основе ролевой модели необходимо перейти на вкладку «Ролевая политика» в окне «Настройки пользователя» (рис. 13).

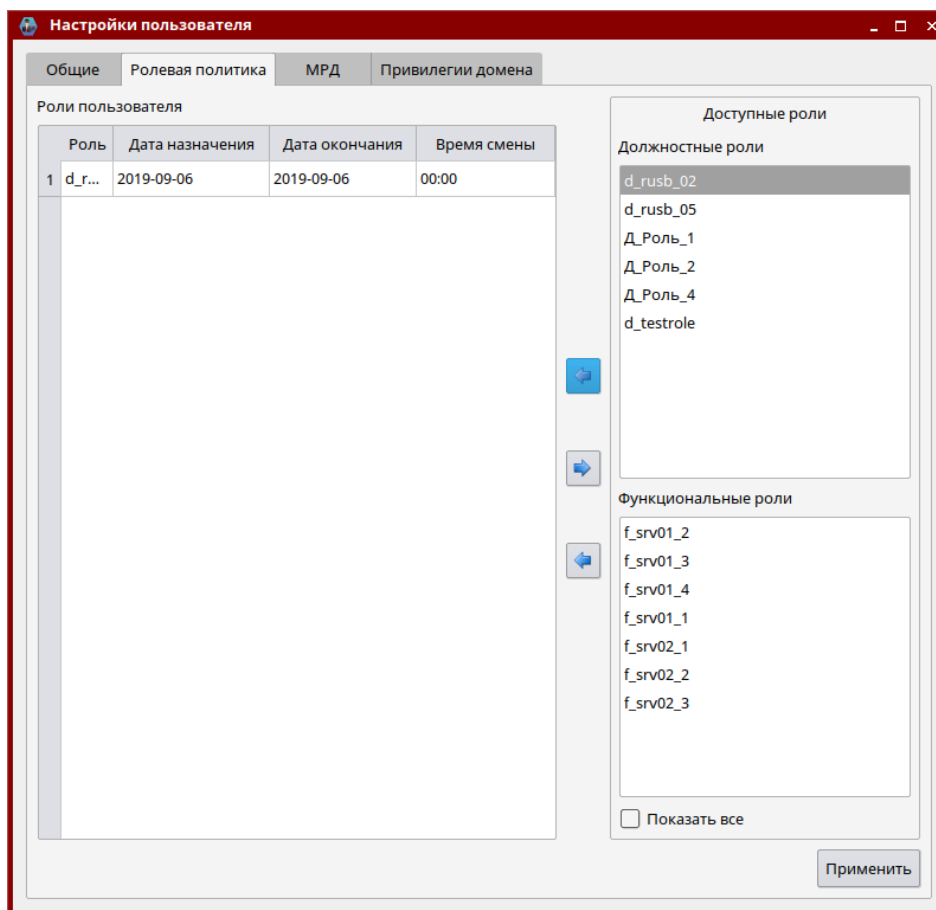




Рис. 13 – Настройка доступа пользователя к ресурсам на основе ролевой модели

Из расположенных в правой части окна списков 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]**.

3.4.3. Настройка мандатных атрибутов пользователя

Для настройки мандатных атрибутов пользователя (при использовании для организации единого пространства пользователей службы организации домена ALD) необходимо перейти в окне «Настройки пользователя» на вкладку «МРД» (рис. 14).

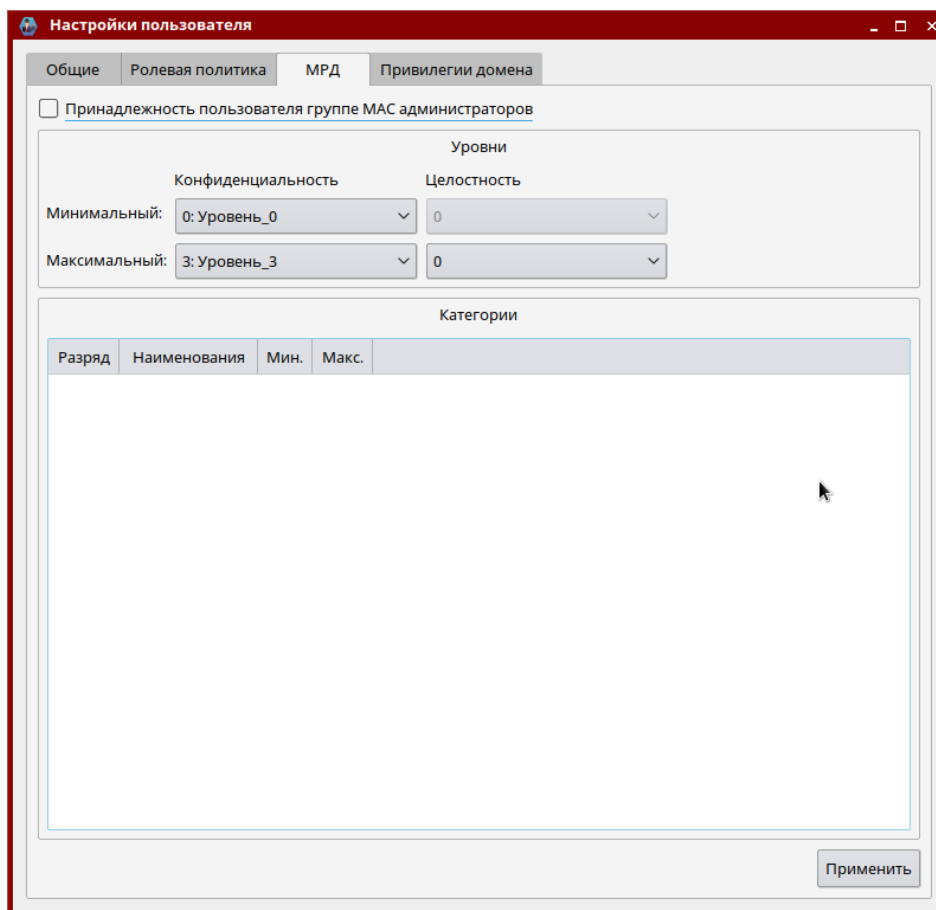


Рис. 14 – Настройка мандатных атрибутов пользователя

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

3.4.4. Настройка доменных привилегий пользователя

Для настройки доменных привилегий пользователя (при использовании для организации единого пространства пользователей службы организации домена ALD) необходимо перейти в окне «Настройки пользователя» на вкладку «Привилегии домена» (рис. 15).

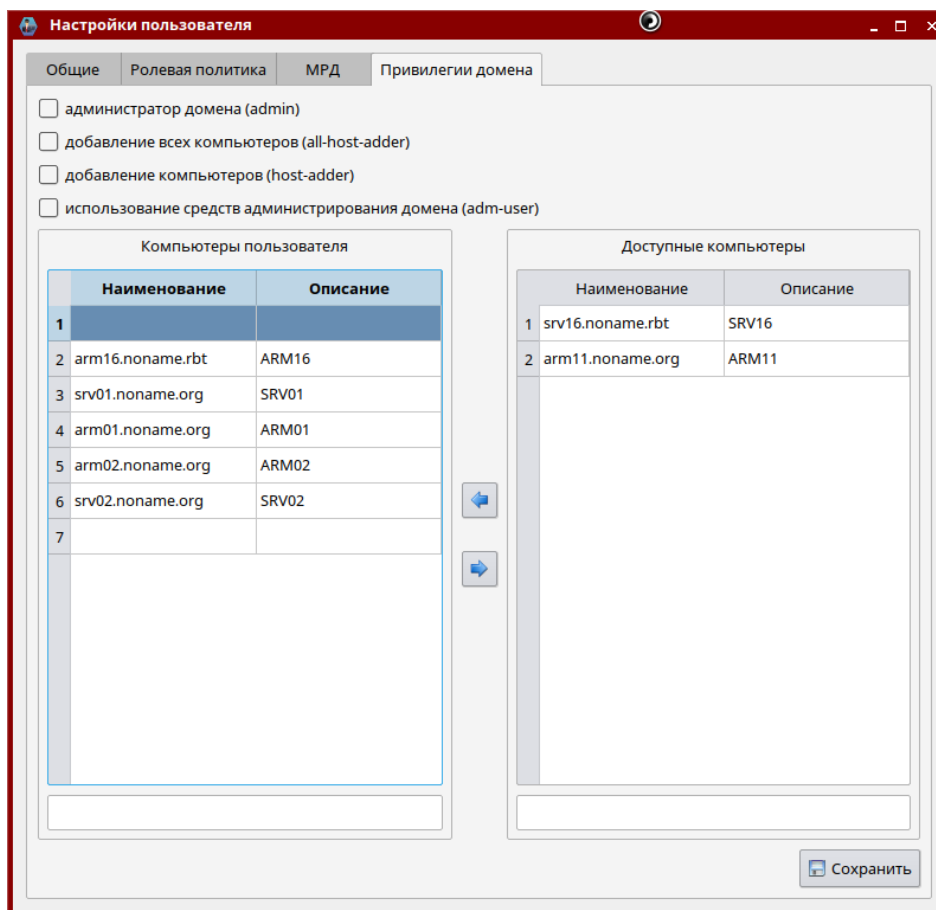




Рис. 15 – Настройка доменных привилегий пользователя

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]**.

3.4.5. Блокировка/разблокировка учетной записи пользователя

Для выполнения блокировки/разблокировки учетной записи пользователя необходимо перейти на вкладку «Общие» в окне «Настройки пользователя» (см рис. 10).

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 **[Заблокировать]** статус учетной записи пользователя меняется на «Заблокирован» (рис. 16), текущие сессии пользователя на APM 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.

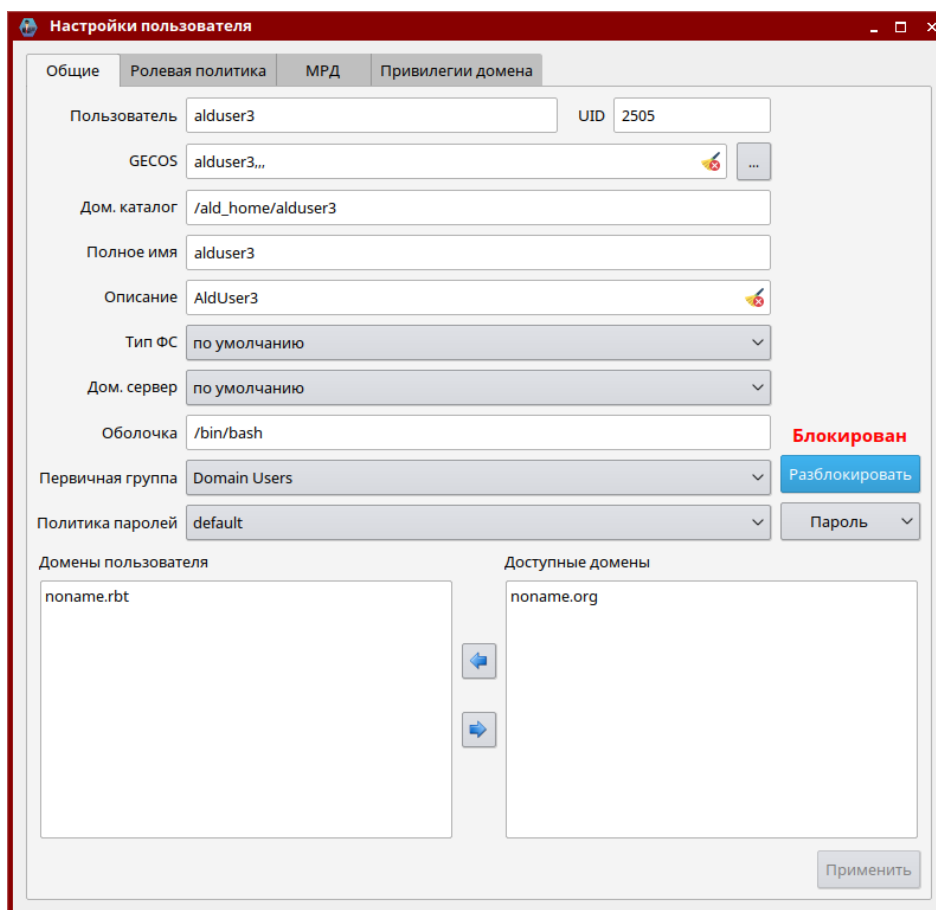


Рис. 16 – Учетная запись пользователя заблокирована

В случае если текущий статус учетной записи пользователя «Заблокирован» при нажатии на кнопку **[Разблокировать]** статус учетной записи пользователя меняется на «Активен».

3.4.6. Установка/смена пароля учетной записи пользователя

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

Установки/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 кнопку **[Пароль]** и выбрать один из способов: «Генерировать пароль» или «Задать пароль» (рис. 17).

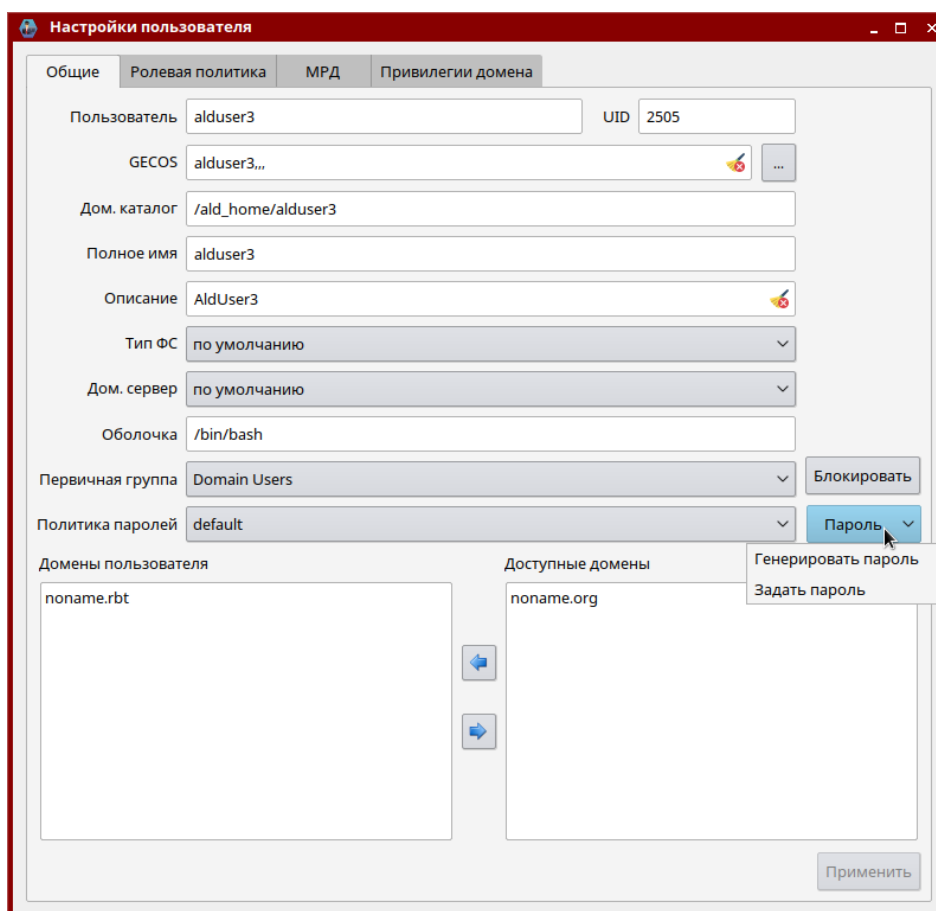


Рис. 17 – Выбор способа генерации пароля

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. 18).

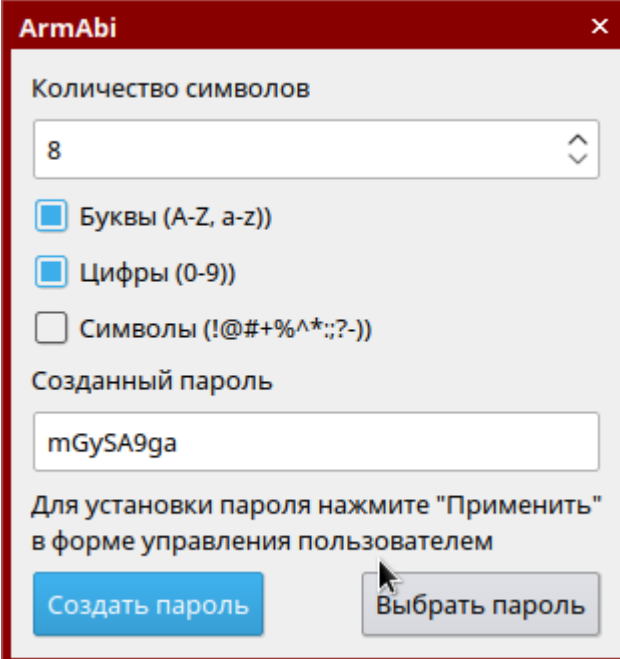
The image shows a dialog box titled "ArmAbi" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Количество символов" (Number of symbols) with a dropdown menu showing the value "8". Below this are three checkboxes: "Буквы (A-Z, a-z)" (checked), "Цифры (0-9)" (checked), and "Символы (!@#+%^*.;?-)" (unchecked). Underneath is a text field labeled "Созданный пароль" (Generated password) containing the text "mGySA9ga". At the bottom, there is a blue button labeled "Создать пароль" (Create password) and a grey button labeled "Выбрать пароль" (Select password). A mouse cursor is pointing at the "Выбрать пароль" button. A note at the bottom of the dialog reads: "Для установки пароля нажмите 'Применить' в форме управления пользователем" (To set the password, click 'Apply' in the user management form).

Рис. 18 – Генерация пароля учетной записи пользователя

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

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

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. 19).

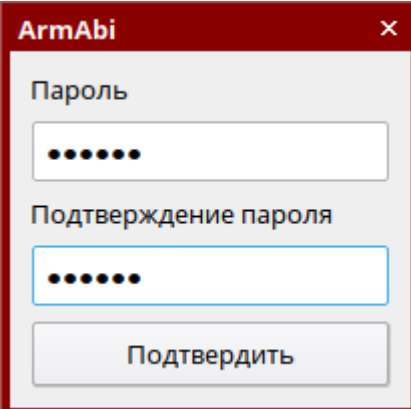
The image shows a dialog box titled "ArmAbi" with a close button (X) in the top right corner. It contains two text input fields. The first field is labeled "Пароль" (Password) and contains seven dots. The second field is labeled "Подтверждение пароля" (Confirm password) and also contains seven dots. Below the fields is a button labeled "Подтвердить" (Confirm).



Рис. 19 – Ручной ввод пароля учетной записи пользователя

3.4.7. Настройка должностных и функциональных ролей

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

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

В открывшемся окне «Ресурсы/Роли» требуется:

- задать местонахождение и параметры соединения с ресурсными СУБД, в которых хранятся системные наименования должностных и функциональных ролей;
- задать местонахождение и параметры соединения со справочниками ролей, 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. 20);
- в открывшемся окне «Подтверждение изменений» для сохранения изменений нажать кнопку **[Подтвердить]** или **[Отменить]** для их отмены.

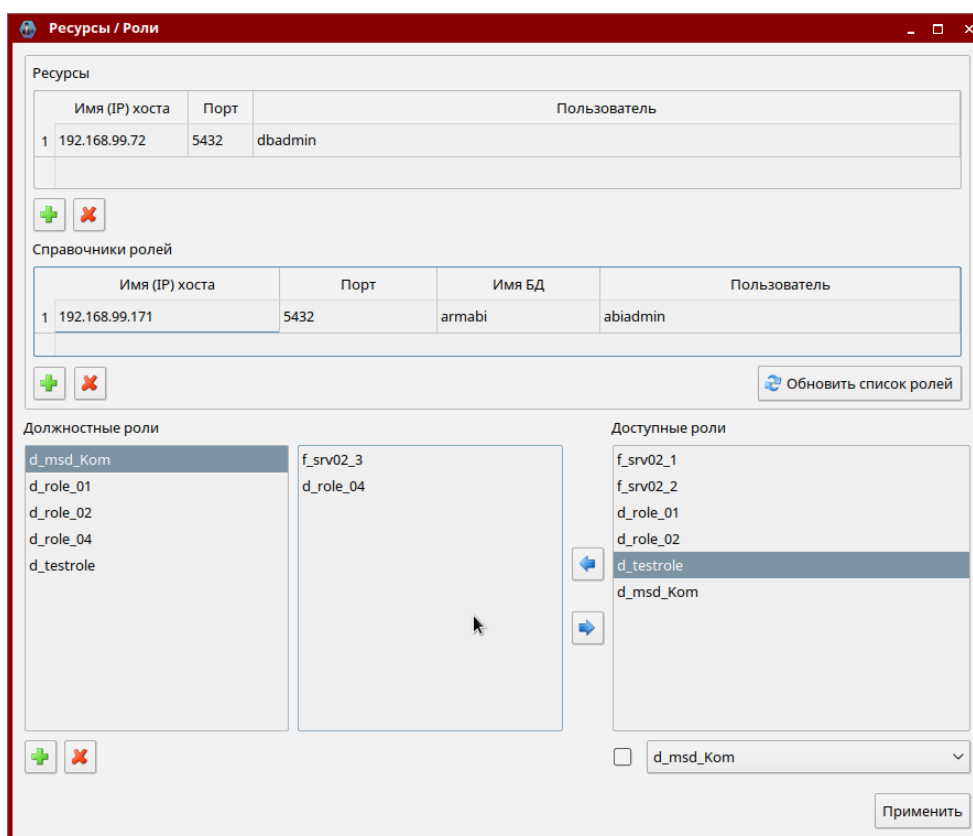


Рис. 20 – Настройка должностных и функциональных ролей

Для организации доступа к справочнику ролей устанавливаются следующие наименования:

- наименование таблицы – roleDict;
- поле для системного наименования ролей – roleCode;

- поле для полного наименования ролей – roleName.

3.5. 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. 21 и содержит следующую информацию:

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

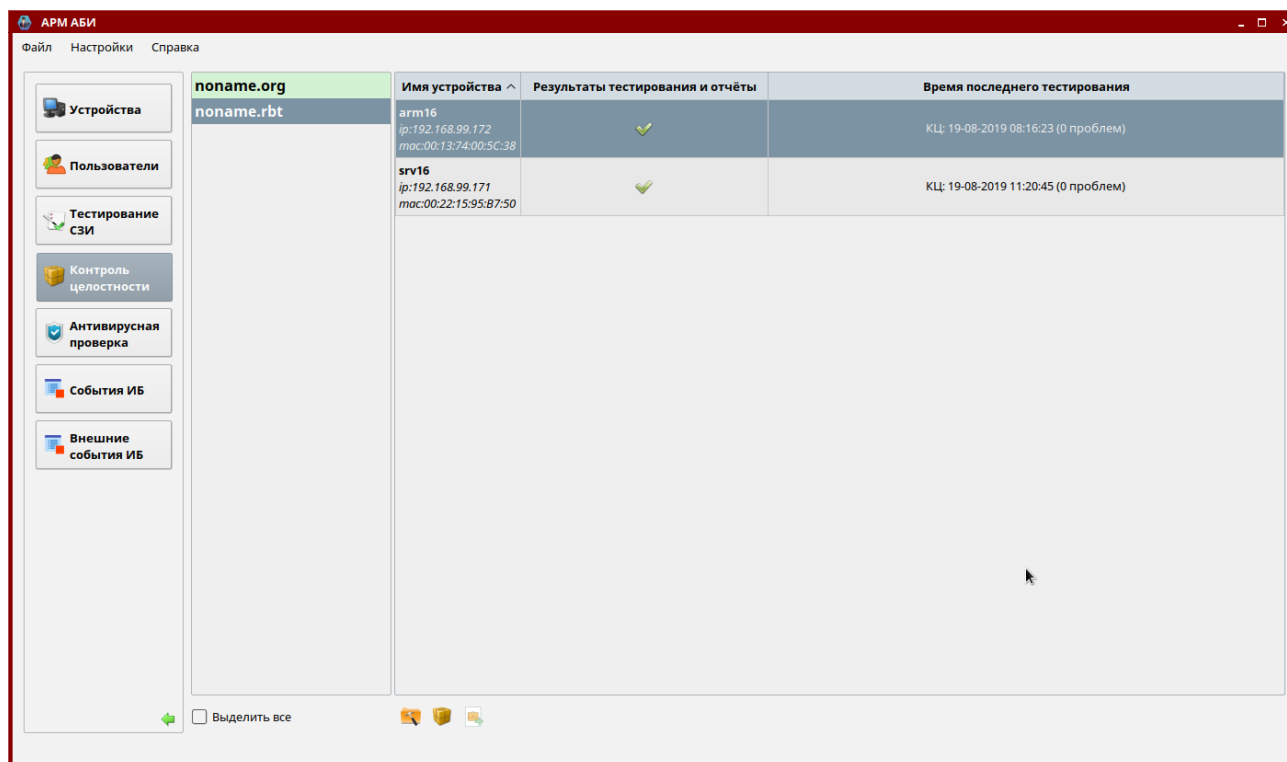



Рис. 21 – Раздел «Контроль целостности»

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

3.5.1. 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. 22).

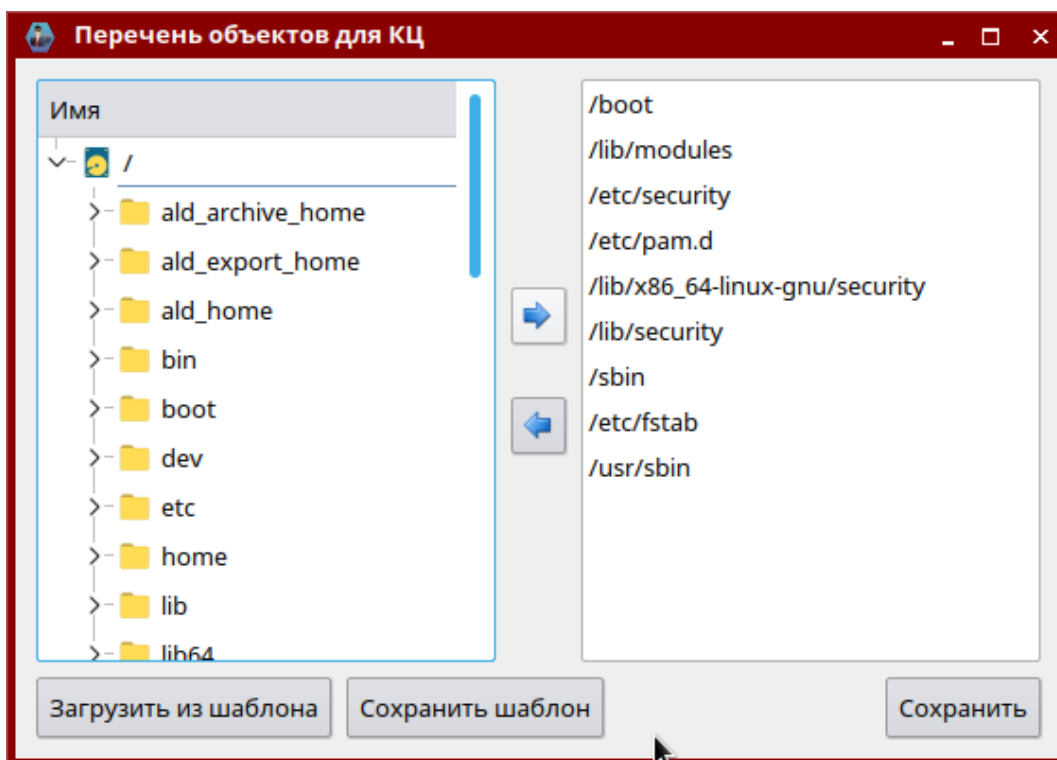




Рис. 22 – Назначение компонент КЦ

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 кнопку .

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]**.



Настроенный перечень объектов, к которым применяется КЦ на данном устройстве, можно сохранить в качестве шаблона конфигурации КЦ, нажав на кнопку **[Сохранить шаблон]**.

3.5.2. Запуск КЦ

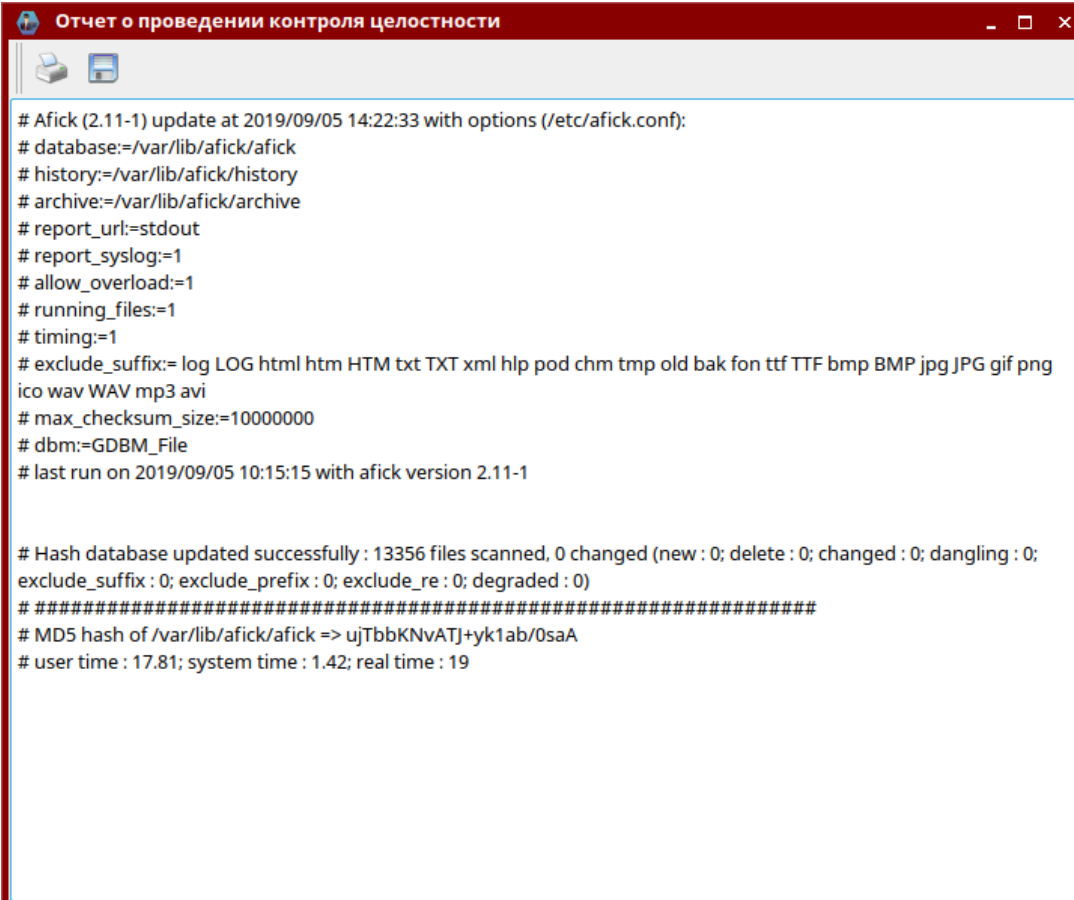
Для запуска регламентного КЦ необходимо выбрать из списка управляемое устройство и нажать на кнопку .

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

В случае, если регламентный контроль целостности на устройстве не проводился, в столбце «Результаты тестирования и отчеты» в соответствующей строке отображается значок .

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. 23.




```
# Afick (2.11-1) update at 2019/09/05 14:22:33 with options (/etc/afick.conf):
# database:=/var/lib/afick/afick
# history:=/var/lib/afick/history
# archive:=/var/lib/afick/archive
# report_url:=stdout
# report_syslog:=1
# allow_overload:=1
# running_files:=1
# timing:=1
# exclude_suffix:= log LOG html htm HTM txt TXT xml hlp pod chm tmp old bak fon ttf TTF bmp BMP jpg JPG gif png
ico wav WAV mp3 avi
# max_checksum_size:=10000000
# dbm:=GDBM_File
# last run on 2019/09/05 10:15:15 with afick version 2.11-1

# Hash database updated successfully : 13356 files scanned, 0 changed (new : 0; delete : 0; changed : 0; dangling : 0;
exclude_suffix : 0; exclude_prefix : 0; exclude_re : 0; degraded : 0)
# #####
# MD5 hash of /var/lib/afick/afick => ujTbbKNvATJ+yk1ab/0saA
# user time : 17.81; system time : 1.42; real time : 19
```

Рис. 23 – 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.

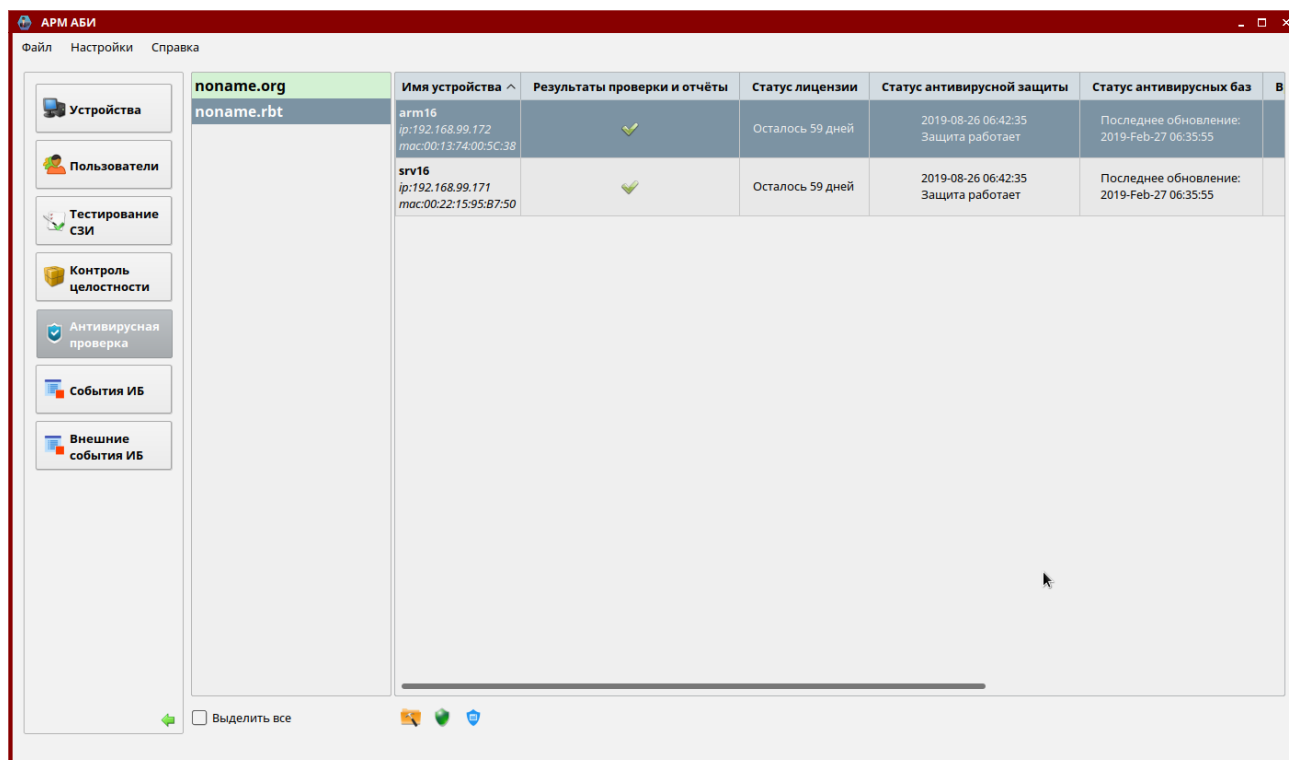
3.5.3. Отправка конфигурации КЦ на управляемое устройство

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

3.6. Раздел «Антивирусная проверка»

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. 24 и содержит следующую информацию:

- имя, ip-адрес и mac-адрес устройства;
- статус лицензии;
- статус антивирусной защиты;
- статус антивирусных баз;
- дату и время последнего проведения антивирусной проверки.




Имя устройства	Результаты проверки и отчёты	Статус лицензии	Статус антивирусной защиты	Статус антивирусных баз
arm16 ip:192.168.99.172 mac:00:13:74:00:5C:38	✓	Осталось 59 дней	2019-08-26 06:42:35 Защита работает	Последнее обновление: 2019-Feb-27 06:35:55
srv16 ip:192.168.99.171 mac:00:22:15:95:87:50	✓	Осталось 59 дней	2019-08-26 06:42:35 Защита работает	Последнее обновление: 2019-Feb-27 06:35:55


Рис. 24 – Раздел «Антивирусная проверка»


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

3.6.1. 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. 25).

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 кнопку .

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]**.

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

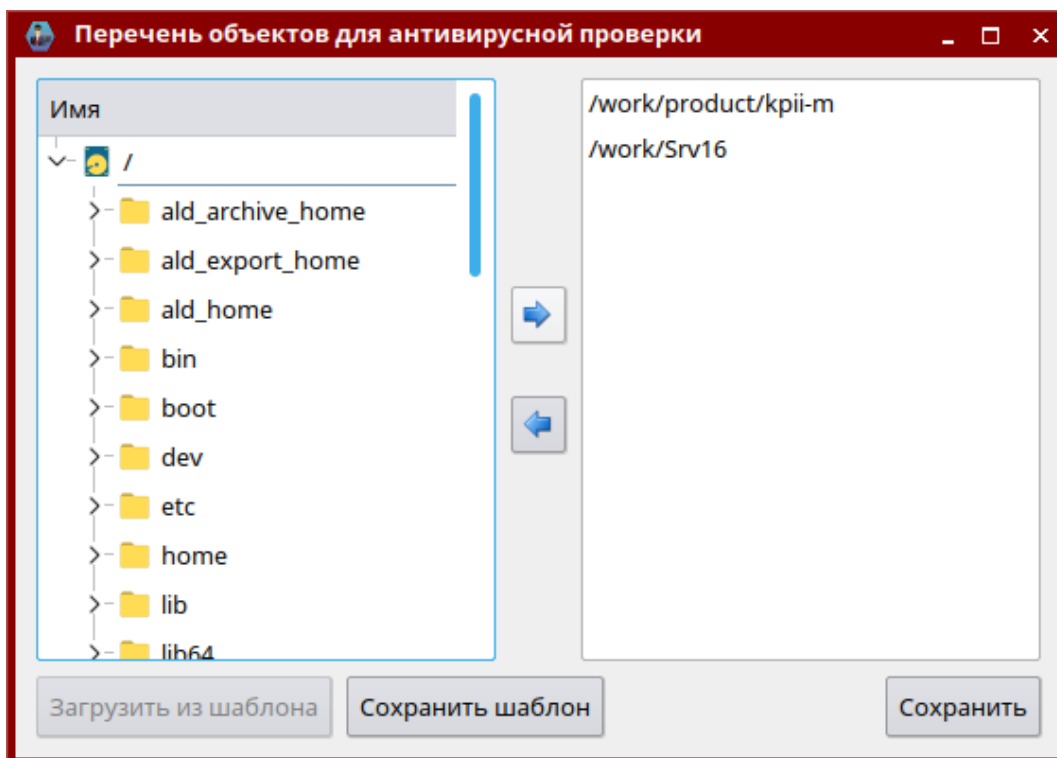



Рис. 25 – Настройка перечня объектов для антивирусной проверки

3.6.2. Запуск антивирусной проверки

Для запуска антивирусной проверки устройства необходимо выбрать его из списка управляемое устройство 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 соответствующей ссылке в графе «Дата и время проведения проверки, результат» основного списка раздела. Внешний вид отчета о результатах антивирусной проверки представлен на рис. 26.

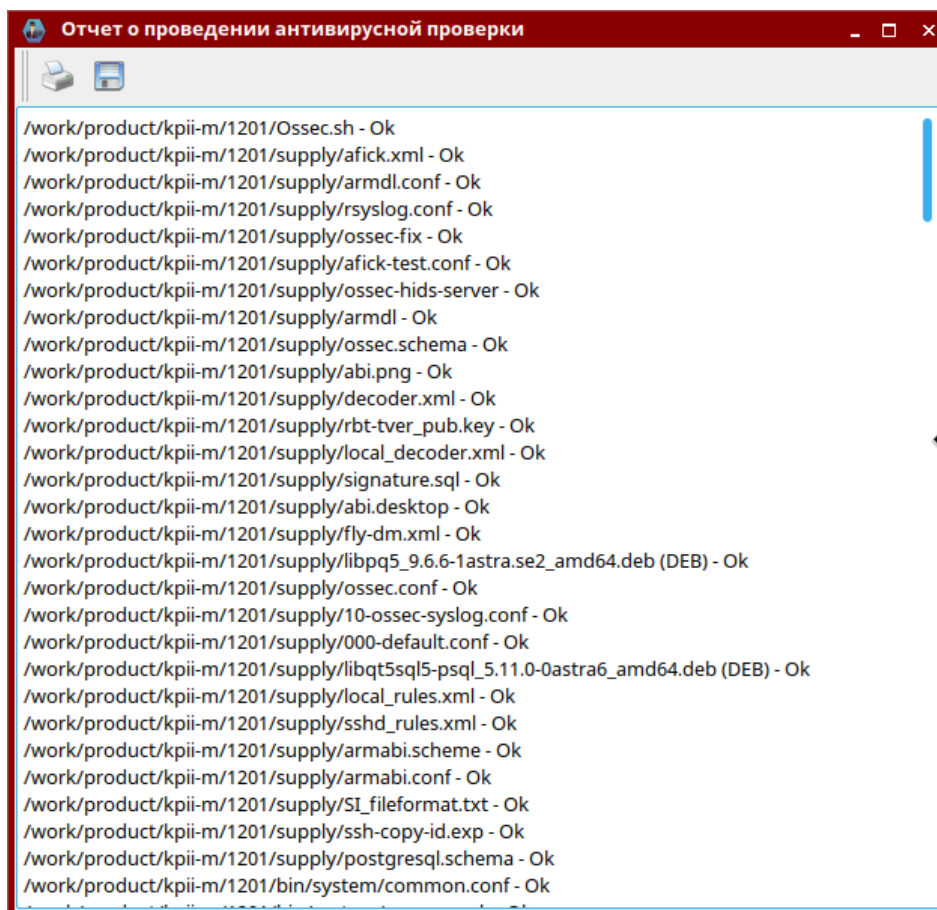



Рис. 26 – Отчет о результатах проведения антивирусной проверки устройства

3.6.3. Обновление лицензии

Для обновления лицензии необходимо выбрать из списка управляемое устройство и нажать на кнопку . В открывшемся диалоге необходимо выбрать ключевой файл *.key, содержащий информацию о лицензии, и нажать кнопку **[Открыть]**. В данном примере приведен ключевой файл для САВЗ «Dr.Web» (рис. 27).

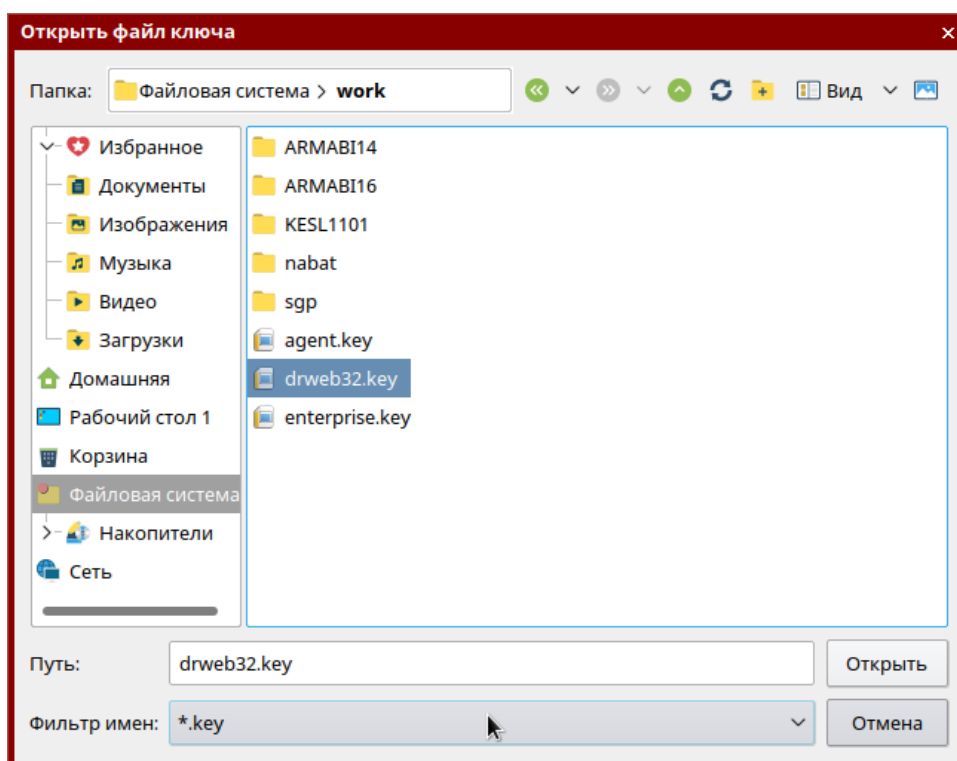


Рис. 27 – Выбор ключевого файла

3.7. 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. 28 и содержит следующую информацию:

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

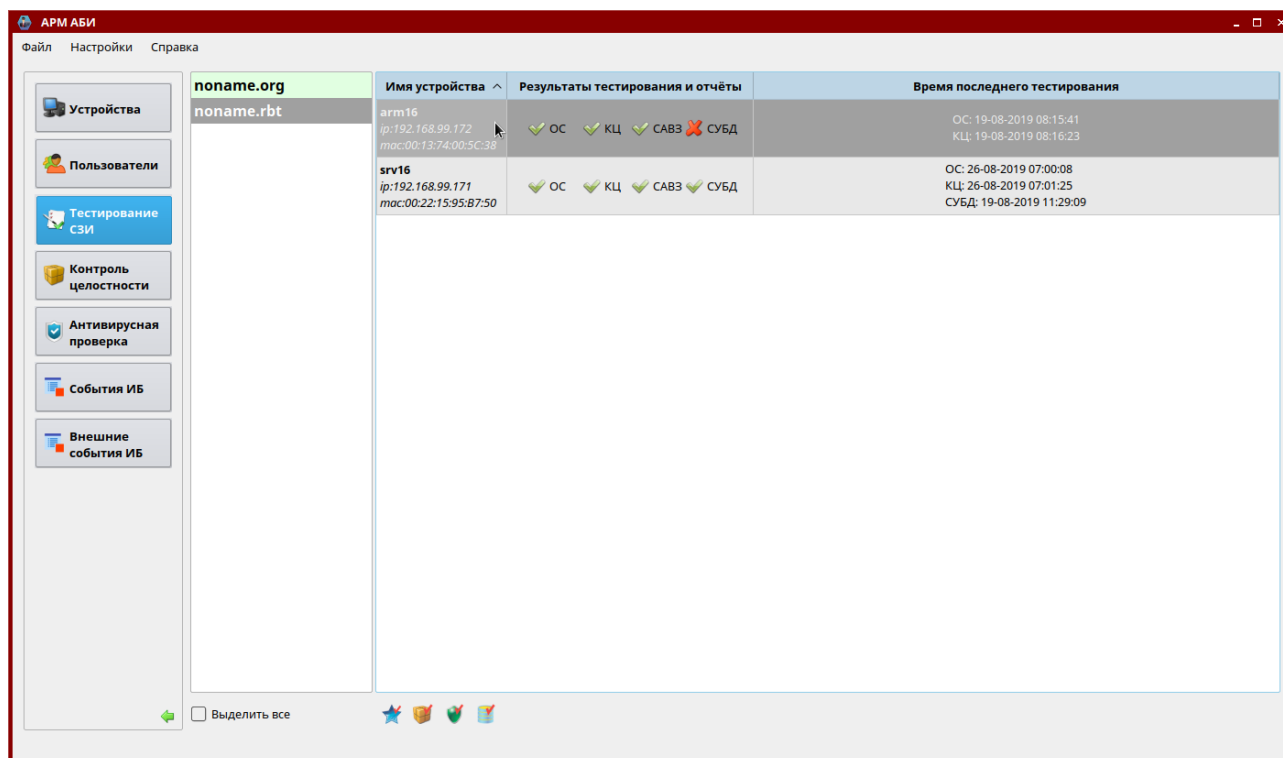







Рис. 28 – Раздел «Тестирование СЗИ»



В нижней части окна программы отображаются кнопки запуска тестирования КСЗ ОС СН и СУБД, работоспособности КЦ и САВЗ.

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  .

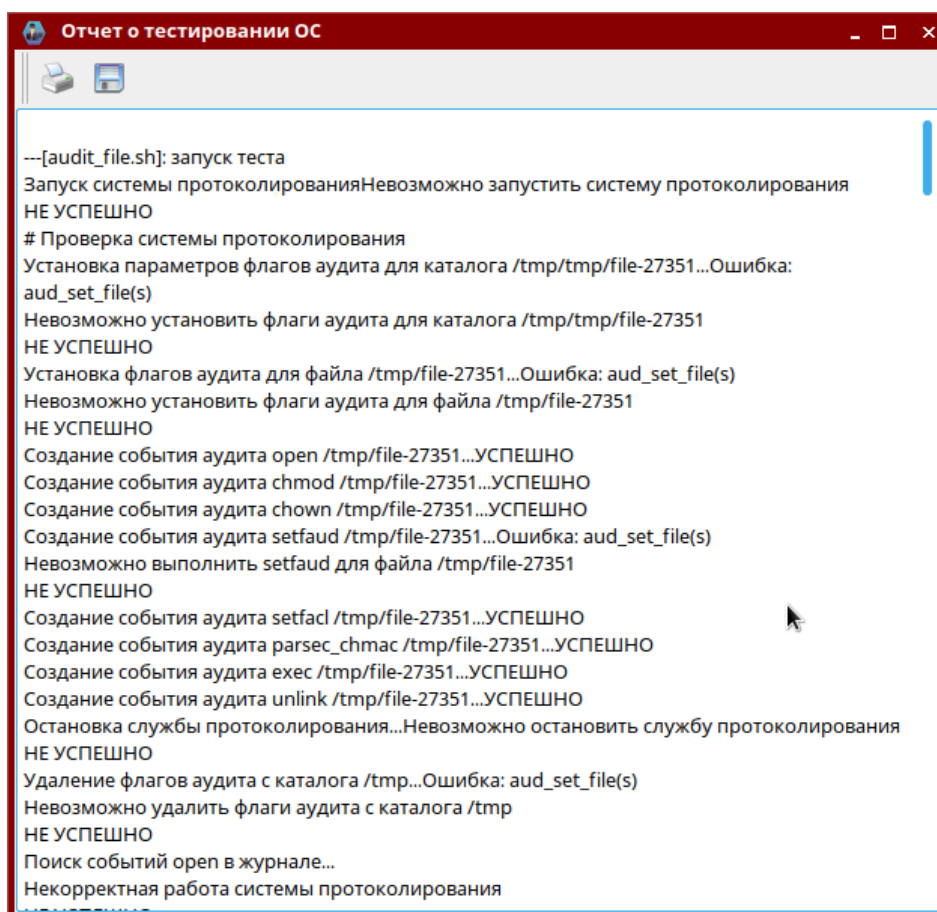
После запуска тестирования СЗИ кнопки запуска тестов становятся неактивными до тех пор, пока процесс не будет завершен.

В случае если тестирование работоспособности средства защиты не проводилось, в столбце «Результаты тестирования и отчеты» у наименования соответствующего теста отображается значок .

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

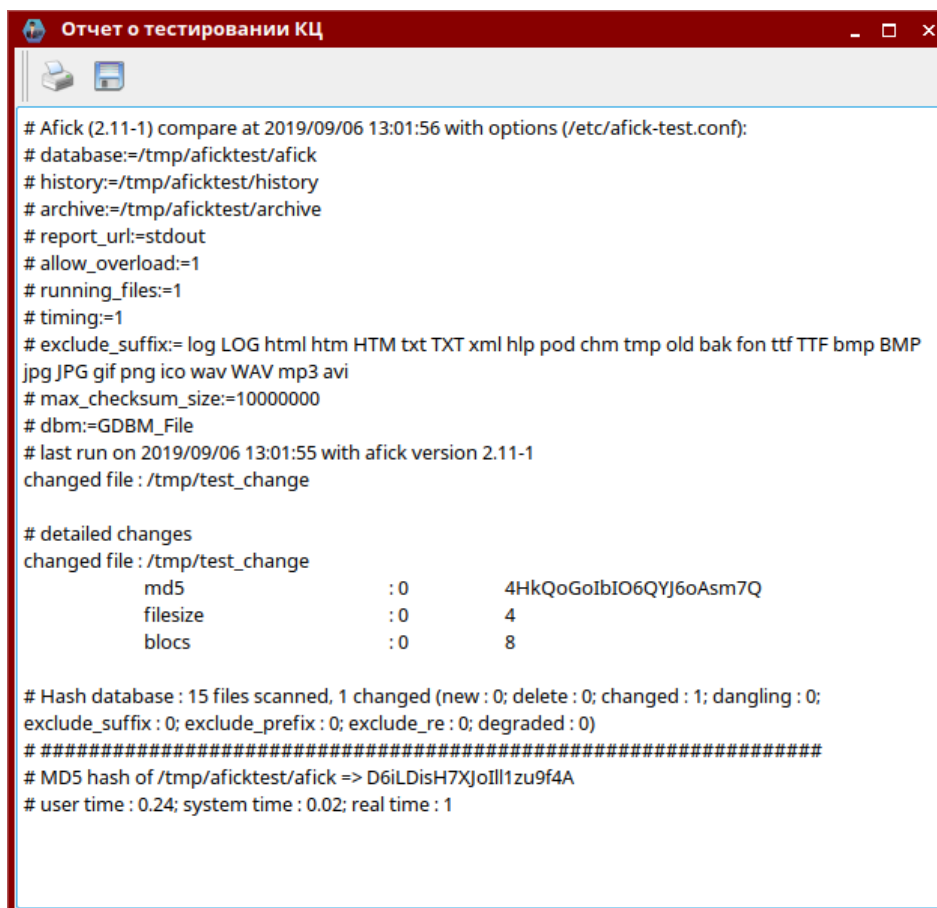
последнего тестирования» при этом выводится информация о дате и времени проведения тестирования работоспособности средства защиты.

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. 29 - 32.



```
---[audit_file.sh]: запуск теста
Запуск системы протоколированияНевозможно запустить систему протоколирования
НЕ УСПЕШНО
# Проверка системы протоколирования
Установка параметров флагов аудита для каталога /tmp/tmp/file-27351...Ошибка:
aud_set_file(s)
Невозможно установить флаги аудита для каталога /tmp/tmp/file-27351
НЕ УСПЕШНО
Установка флагов аудита для файла /tmp/file-27351...Ошибка: aud_set_file(s)
Невозможно установить флаги аудита для файла /tmp/file-27351
НЕ УСПЕШНО
Создание события аудита open /tmp/file-27351...УСПЕШНО
Создание события аудита chmod /tmp/file-27351...УСПЕШНО
Создание события аудита chown /tmp/file-27351...УСПЕШНО
Создание события аудита setfaud /tmp/file-27351...Ошибка: aud_set_file(s)
Невозможно выполнить setfaud для файла /tmp/file-27351
НЕ УСПЕШНО
Создание события аудита setfacl /tmp/file-27351...УСПЕШНО
Создание события аудита parsec_chmac /tmp/file-27351...УСПЕШНО
Создание события аудита exec /tmp/file-27351...УСПЕШНО
Создание события аудита unlink /tmp/file-27351...УСПЕШНО
Остановка службы протоколирования...Невозможно остановить службу протоколирования
НЕ УСПЕШНО
Удаление флагов аудита с каталога /tmp...Ошибка: aud_set_file(s)
Невозможно удалить флаги аудита с каталога /tmp
НЕ УСПЕШНО
Поиск событий open в журнале...
Некорректная работа системы протоколирования
```

Рис. 29 – Отчет о результатах тестирования КСЗ ОС СН

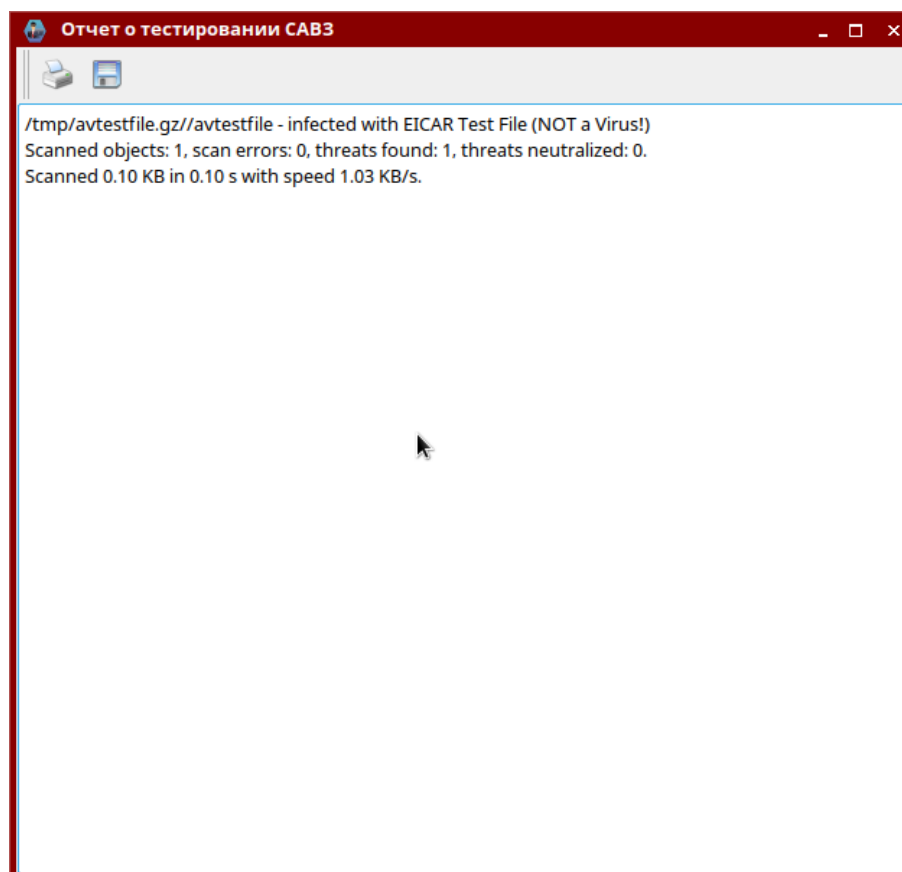


```
# Afick (2.11-1) compare at 2019/09/06 13:01:56 with options (/etc/afick-test.conf):
# database:=/tmp/aficktest/afick
# history:=/tmp/aficktest/history
# archive:=/tmp/aficktest/archive
# report_url:=stdout
# allow_overload:=1
# running_files:=1
# timing:=1
# exclude_suffix:= log LOG html htm HTM txt TXT xml hlp pod chm tmp old bak fon ttf TTF bmp BMP
jpg JPG gif png ico wav WAV mp3 avi
# max_checksum_size:=10000000
# dbm:=GDBM_File
# last run on 2019/09/06 13:01:55 with afick version 2.11-1
changed file : /tmp/test_change

# detailed changes
changed file : /tmp/test_change
      md5                : 0          4HkQoGoIbIO6QYJ6oAsm7Q
      filesize            : 0          4
      blocs               : 0          8

# Hash database : 15 files scanned, 1 changed (new : 0; delete : 0; changed : 1; dangling : 0;
exclude_suffix : 0; exclude_prefix : 0; exclude_re : 0; degraded : 0)
#####
# MD5 hash of /tmp/aficktest/afick => D6iLDisH7XJoIl1zu9f4A
# user time : 0.24; system time : 0.02; real time : 1
```

Рис. 30 – Отчет о результатах тестирования работоспособности КЦ



```
/tmp/avtestfile.gz//avtestfile - infected with EICAR Test File (NOT a Virus!)
Scanned objects: 1, scan errors: 0, threats found: 1, threats neutralized: 0.
Scanned 0.10 KB in 0.10 s with speed 1.03 KB/s.
```

Рис. 31 – Отчет о результатах тестирования работоспособности САВЗ

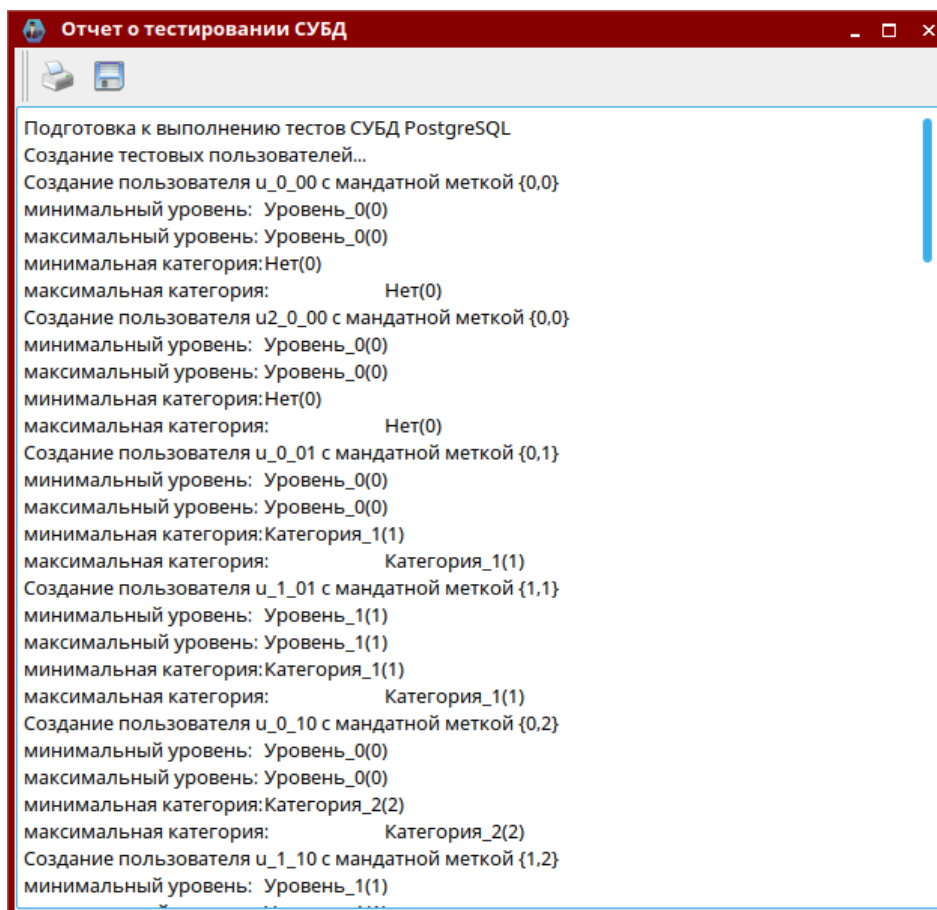


Рис. 32 – Отчет о результатах тестирования КСЗ СУБД

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.

3.8. 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. Внешний вид раздела приведен на рис. 33 и содержит следующую информацию:

- наименование устройства;
- дата и время события;
- уровень опасности;
- описание события.

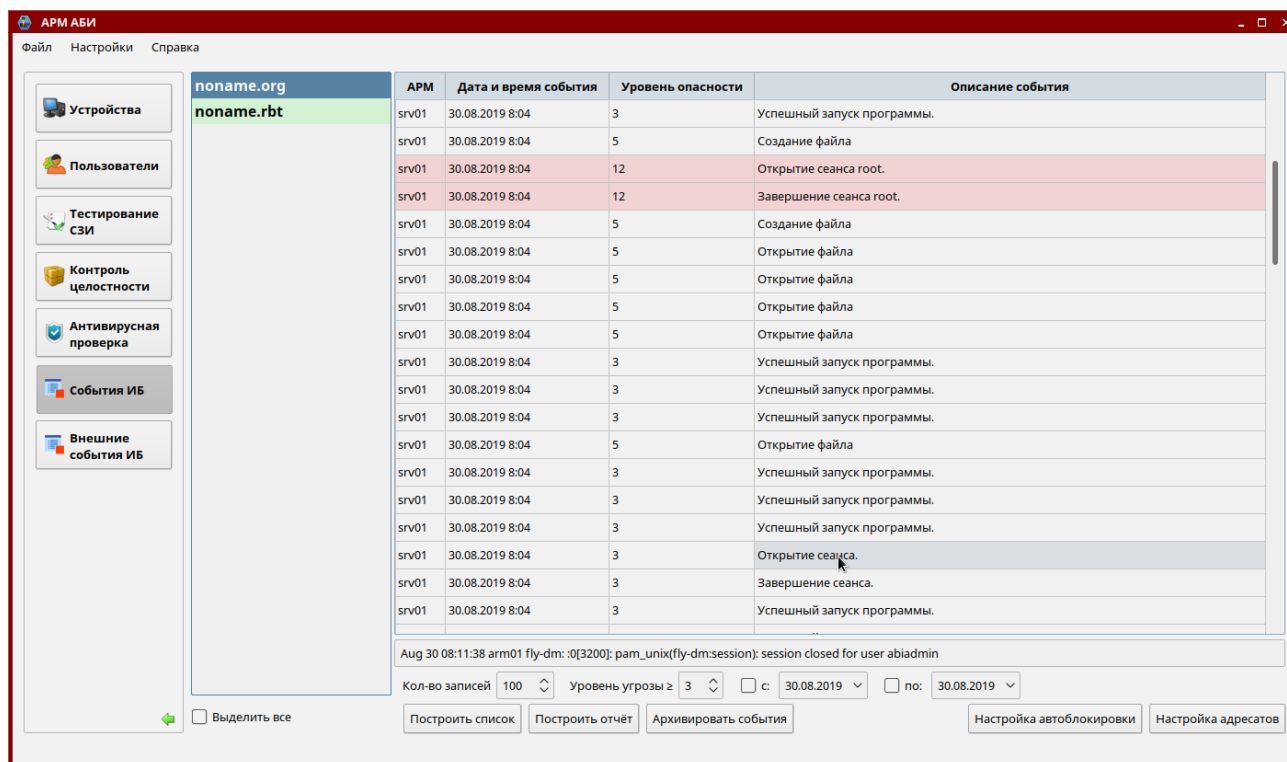


Рис. 33 – Раздел «События ИБ»

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

3.8.1. Просмотр 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 расположенных в нижней части окна полей «Количество записей», «Уровень угрозы», 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.

События в таблице обновляются автоматически.

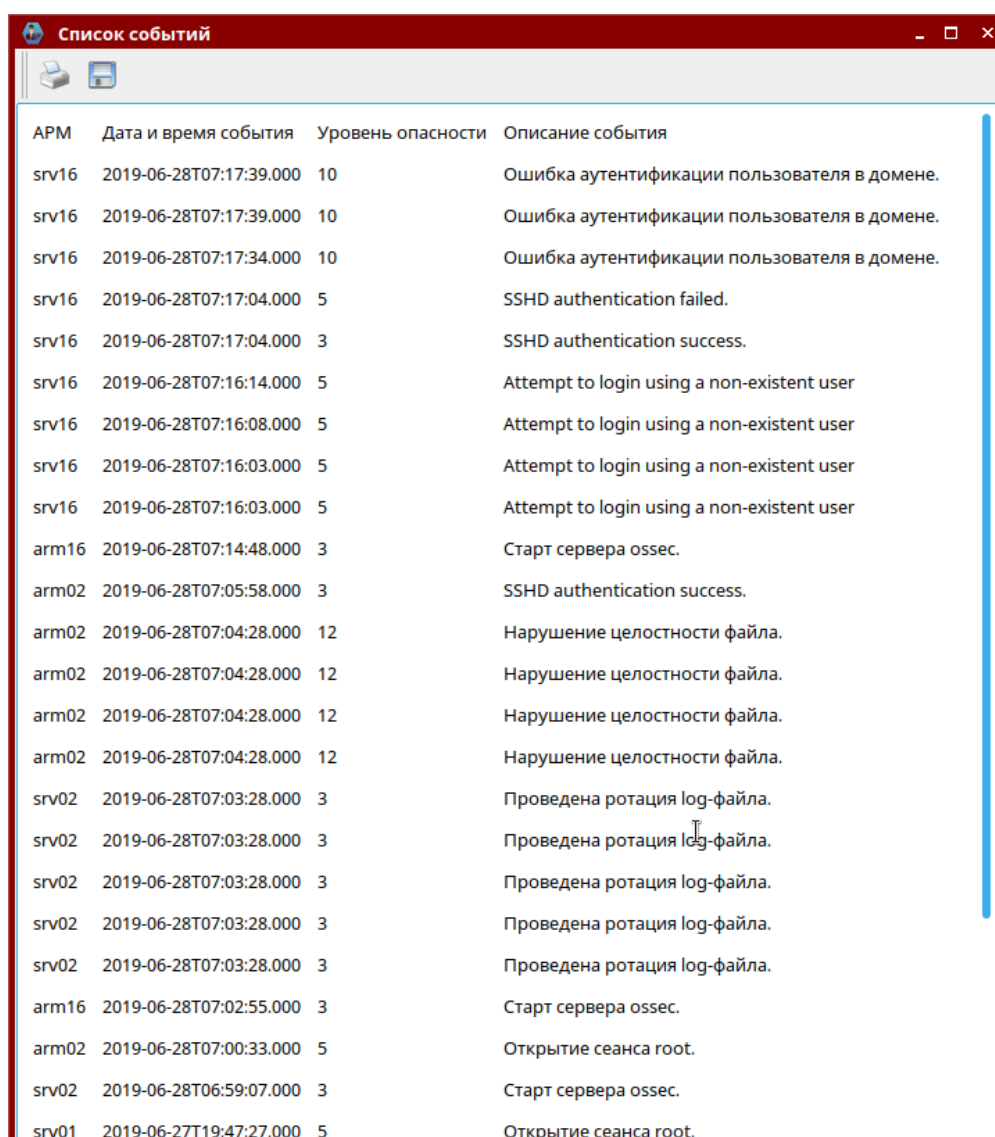
В поле «Количество записей» задается количество отображаемых в таблице записей. При установке значений полей «с» и/или «по» с соответствующими датами периода обнаружения событий поле «Количество записей» становится неактивным, и наоборот.

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.

Для обновления списка отображаемых в таблице событий информационной безопасности необходимо нажать кнопку **[Построить список]**.


3.8.2. Построение отчета о событиях ИБ

Для построения отчета отображаемых в таблице событий информационной безопасности требуется нажать кнопку **[Построить отчет]**. Внешний вид отчета о событиях информационной безопасности представлен на рис. 34.



APM	Дата и время события	Уровень опасности	Описание события
srv16	2019-06-28T07:17:39.000	10	Ошибка аутентификации пользователя в домене.
srv16	2019-06-28T07:17:39.000	10	Ошибка аутентификации пользователя в домене.
srv16	2019-06-28T07:17:34.000	10	Ошибка аутентификации пользователя в домене.
srv16	2019-06-28T07:17:04.000	5	SSHD authentication failed.
srv16	2019-06-28T07:17:04.000	3	SSHD authentication success.
srv16	2019-06-28T07:16:14.000	5	Attempt to login using a non-existent user
srv16	2019-06-28T07:16:08.000	5	Attempt to login using a non-existent user
srv16	2019-06-28T07:16:03.000	5	Attempt to login using a non-existent user
srv16	2019-06-28T07:16:03.000	5	Attempt to login using a non-existent user
arm16	2019-06-28T07:14:48.000	3	Старт сервера ossec.
arm02	2019-06-28T07:05:58.000	3	SSHD authentication success.
arm02	2019-06-28T07:04:28.000	12	Нарушение целостности файла.
arm02	2019-06-28T07:04:28.000	12	Нарушение целостности файла.
arm02	2019-06-28T07:04:28.000	12	Нарушение целостности файла.
arm02	2019-06-28T07:04:28.000	12	Нарушение целостности файла.
srv02	2019-06-28T07:03:28.000	3	Проведена ротация log-файла.
srv02	2019-06-28T07:03:28.000	3	Проведена ротация log-файла.
srv02	2019-06-28T07:03:28.000	3	Проведена ротация log-файла.
srv02	2019-06-28T07:03:28.000	3	Проведена ротация log-файла.
srv02	2019-06-28T07:03:28.000	3	Проведена ротация log-файла.
arm16	2019-06-28T07:02:55.000	3	Старт сервера ossec.
arm02	2019-06-28T07:00:33.000	5	Открытие сеанса root.
srv02	2019-06-28T06:59:07.000	3	Старт сервера ossec.
srv01	2019-06-27T19:47:27.000	5	Открытие сеанса root.

Рис. 34 – Отчет о событиях информационной безопасности

Для выполнения печати отчета о событиях информационной безопасности требуется нажать кнопку  .

3.8.3. Архивация событий ИБ

Для выполнения операции архивации событий информационной безопасности требуется перейти в раздел «События ИБ» и нажать кнопку **[Архивировать события]**.

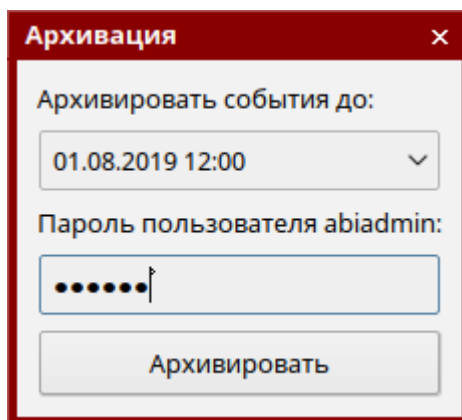




Рис. 35 – Архивация событий информационной безопасности

В открывшемся окне (рис. 35) требуется задать значения даты/времени возникновения событий и указать пароль пользователя БД. При нажатии на кнопку **[Архивировать]** в каталоге `/opt/ArmAbi/archives/` создается архивированный файл, содержащий информацию о событиях информационной безопасности старше указанных даты/времени, и они удаляются из базы данных.

3.8.4. Настройка передачи событий ИБ на вышестоящий уровень

Для выполнения настройки передачи событий информационной безопасности на вышестоящий уровень требуется перейти в раздел «События ИБ» и нажать кнопку **[Настройка адресатов]**.

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 (рис. 36).

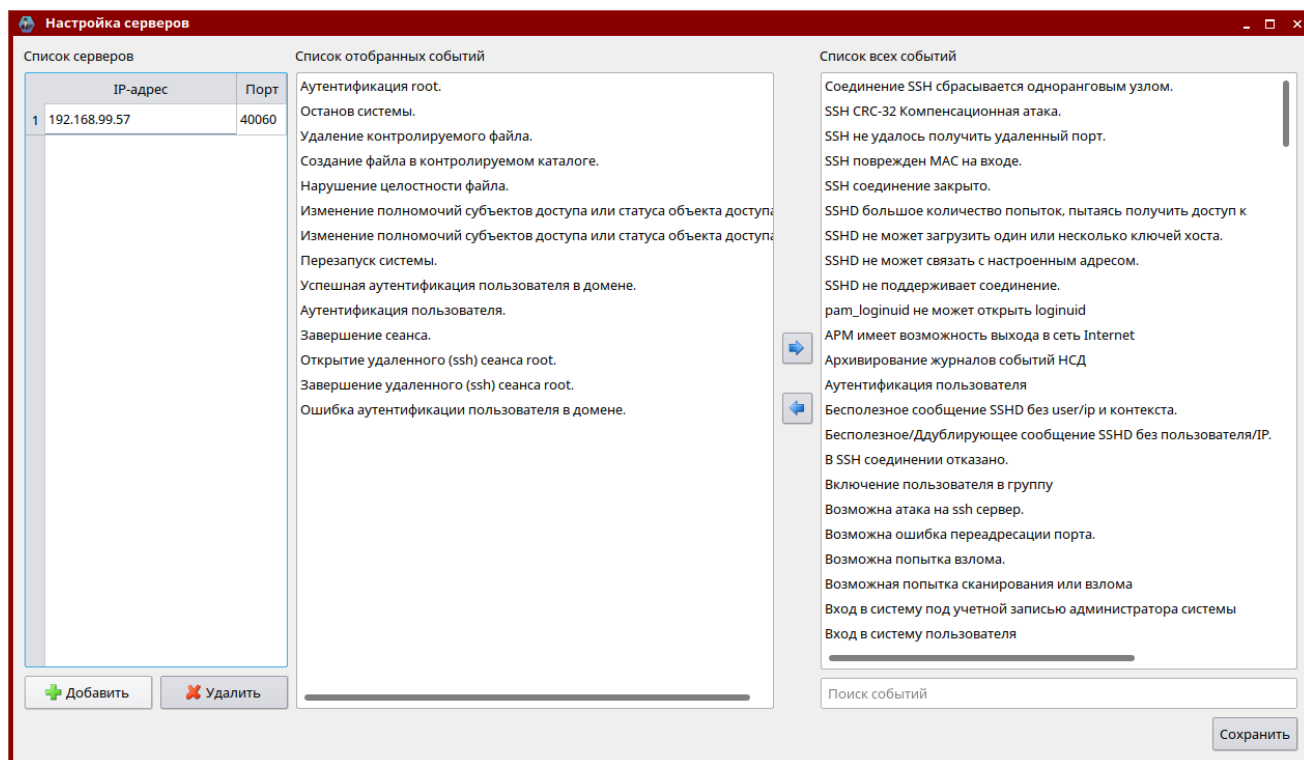




Рис. 36 – Настройка передачи событий на вышестоящий уровень

3.8.5. Настройка автоблокировки пользователей по событиям ИБ

Для выполнения настройки автоблокировки пользователей по событиям информационной безопасности требуется перейти в раздел «События ИБ» и нажать кнопку **[Настройка автоблокировки]** (см. рис. 33).

В открывшемся окне «Настройка автоблокировки пользователей» (рис. 37) 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 кнопку **[Сохранить]**.

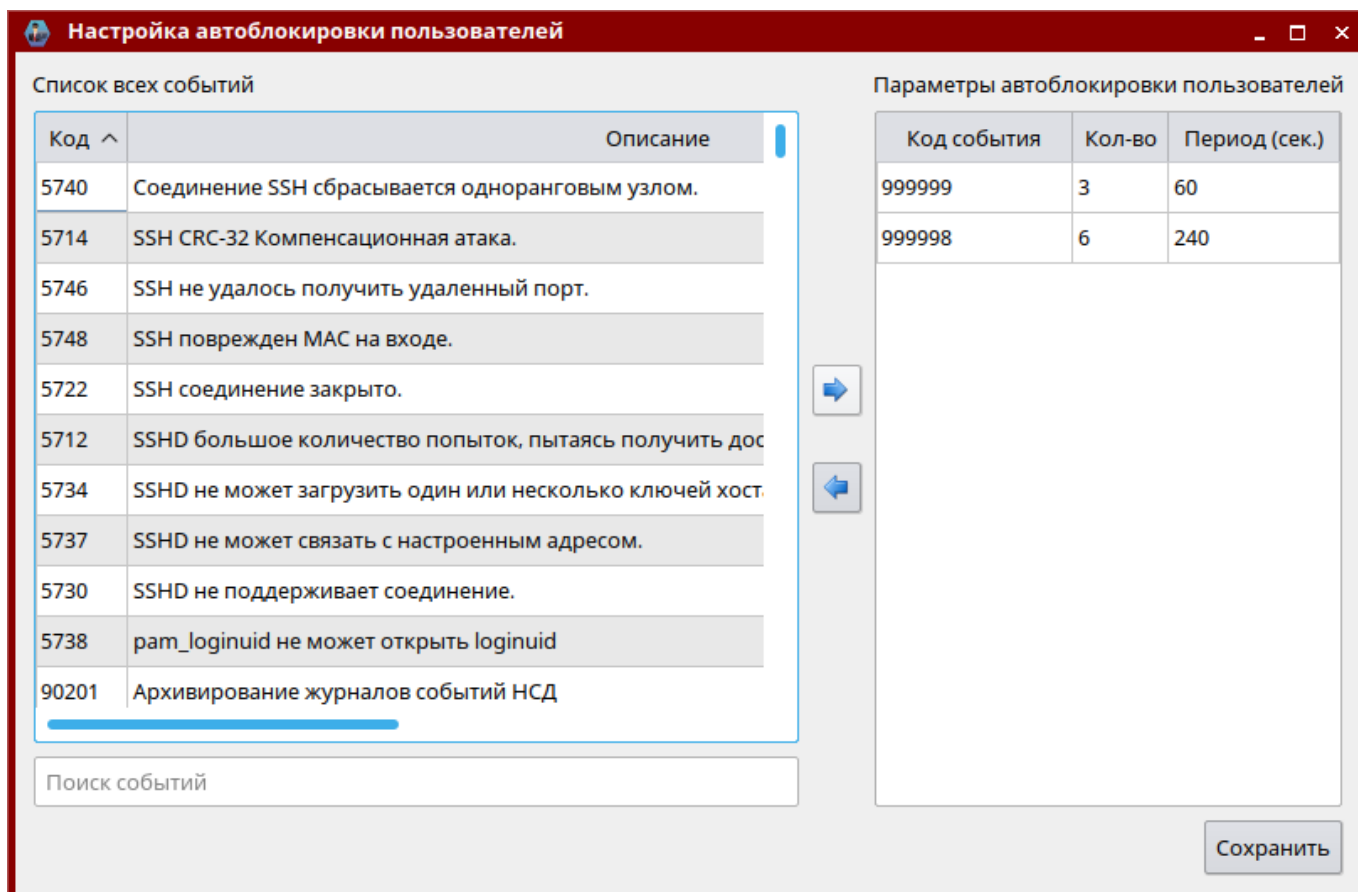


Рис. 37 – Настройка автоблокировки пользователей

3.9. 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. 38 и содержит следующую информацию:

- наименование системы автоматизации нижестоящего уровня;
- наименование устройства;
- дата и время события;
- уровень опасности;
- описание события.

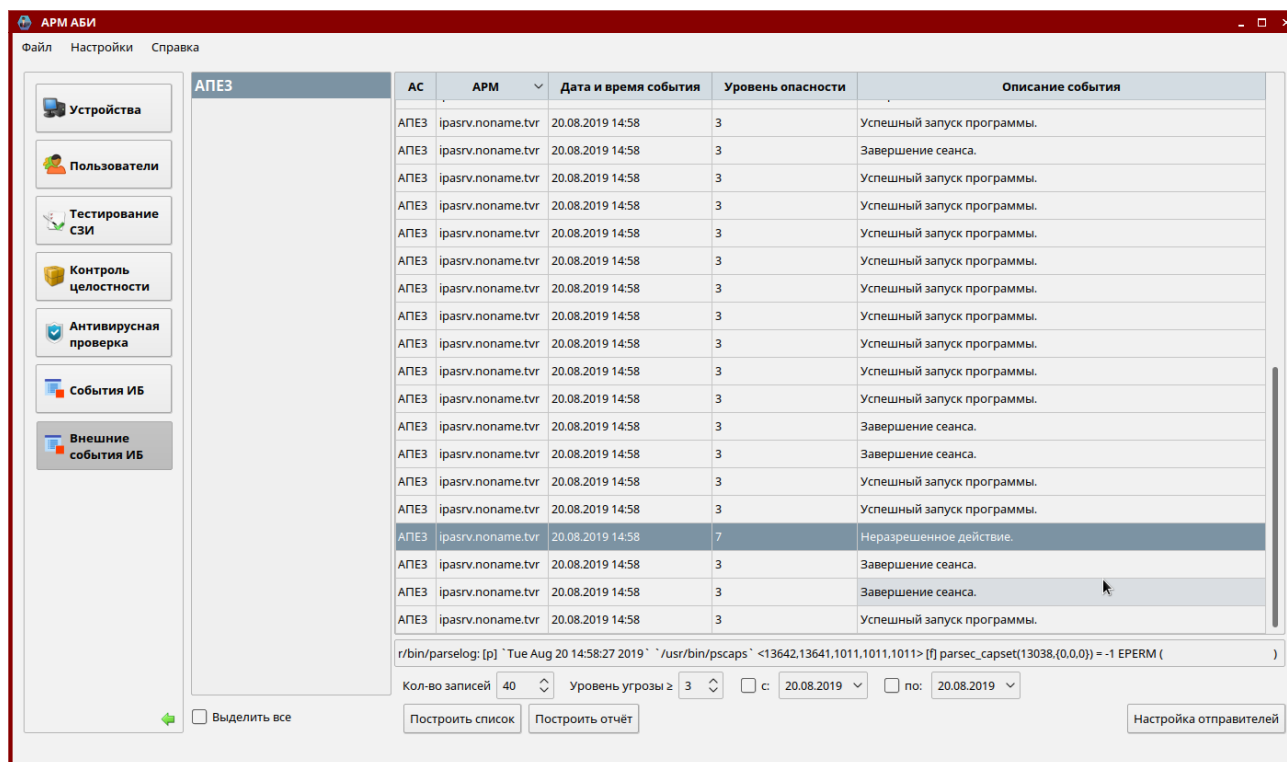


Рис. 38 – Раздел «Внешние события ИБ»

3.9.1. Настройка приема событий ИБ с нижестоящего уровня

Для обеспечения приема событий информационной безопасности с нижестоящего уровня необходимо нажать кнопку **[Настройка отправителей]**. В открывшемся окне с использованием кнопок **[Добавить]** / **[Удалить]** требуется построить список, указав значения параметров (рис. 39):

- «id» – идентификатор системы автоматизации нижестоящего уровня, указанный в настройках ПК АРМ АБИ;

- «name» – наименование системы автоматизации нижестоящего уровня.

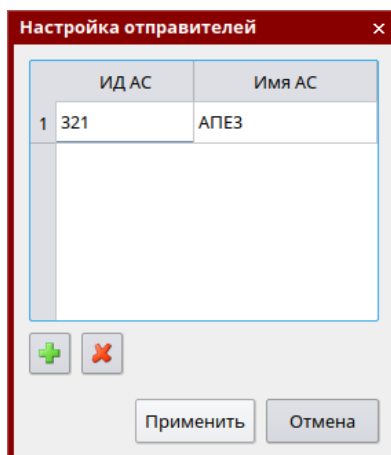



Рис. 39 – Настройка приема событий с нижестоящего уровня

3.10. Резервное копирование конфигурации домена

При использовании для организации единого пространства пользователей службы организации домена для создания/удаления резервной копии конфигурации домена требуется кликнуть правой кнопкой мыши на названии домена и выбрать пункт меню « Резервные копии» (рис. 40).

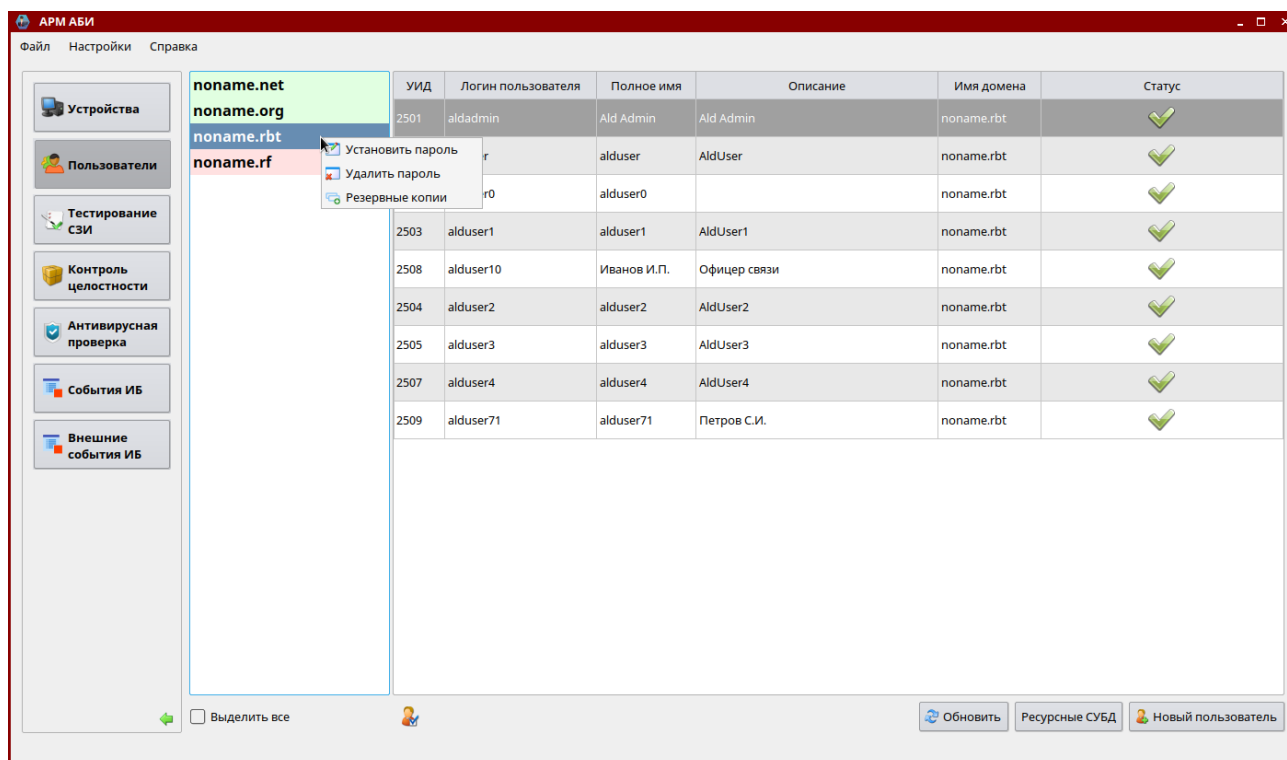


Рис. 40 – Резервное копирование конфигурации домена

Открывшееся окно «Резервные копии домена» содержит список, содержащий информацию о созданных ранее резервных копиях, включающий в себя дату создания и путь к файлу резервной копии (рис. 41).

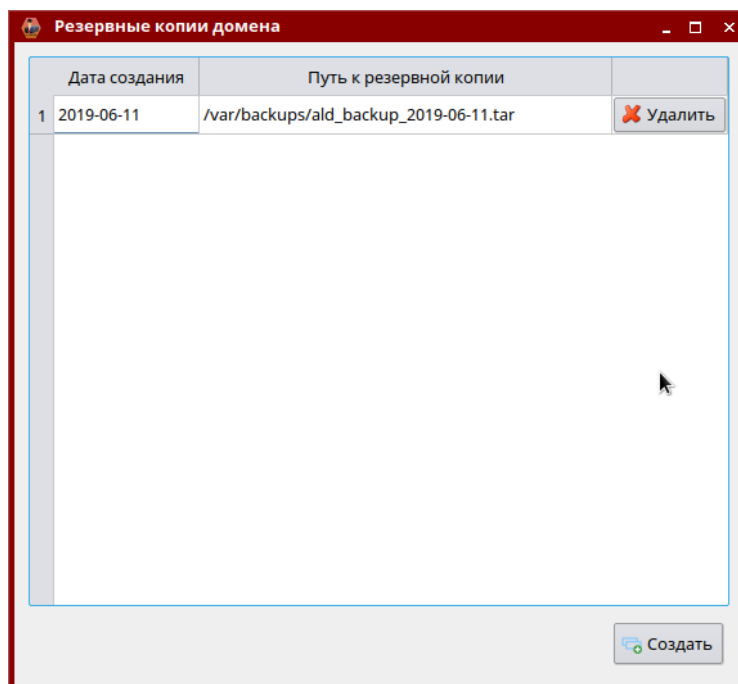


Рис. 41 – Резервные копии домена

Для создания резервной копии необходимо нажать на кнопку **[Создать]**.

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

3.11. Настройка параметров программы

Для настройки параметров программы требуется выбрать пункт меню «Настройки». В окне «Настройка параметров» можно просмотреть и в случае необходимости изменить значения параметров (рис. 42):

- «Работа в среде» – используемая для организации единого пространства пользователей служба организации домена (ALD или FreeIPA);
- «ИД АС» – идентификатор системы автоматизации, используемый при передаче информации о событиях информационной безопасности на вышестоящий уровень;
- «Порт АРМ АБИ» – порт сервера безопасности, используемый для обмена информацией с агентами безопасности;
- «Имя БД АРМ АБИ» – наименование базы данных ПС АРМ АБИ;
- «Каталог для log-файлов тестирования» – каталог для хранения протоколов проведения КЦ, антивирусной проверки и тестирования СЗИ устройств;
- «Каталог для шаблонов файлов конфигураций» – каталог для хранения шаблонов файлов конфигураций САВЗ и КЦ;

- «Каталог для хранения архивов событий» – каталог для хранения архивированных файлов, содержащих информацию о событиях информационной безопасности;

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

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

Настройка параметров

Работа в среде:
ALD

ИД АС:
0

Порт АРМ АБИ*:
40060

Имя БД АРМ АБИ*:
armabi

Каталог для log-файлов тестирования:
/opt/ArmAbi/log/

Каталог для шаблонов файлов конфигураций:
/opt/ArmAbi/resources/

Каталог для хранения архивов событий:
/opt/ArmAbi/archives

Минимальный уровень события для сигнализирования
10

*Требуется перезапуск ArmAbi

Сохранить

Рис. 42 – Настройка параметров программы

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. 43).

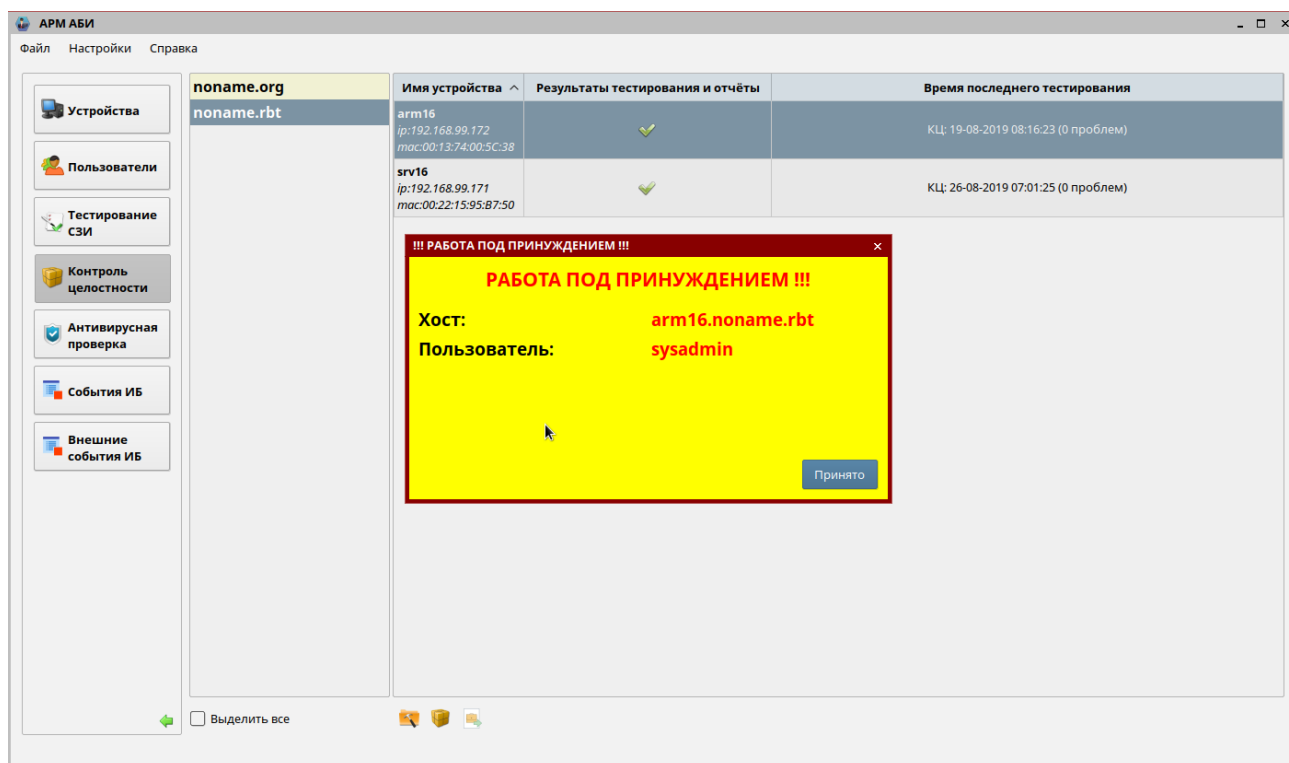


Рис. 43 – Сообщение АБИ о работе «под принуждением»

3.13. Завершение работы программы

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

3.14. Резервное копирование базы данных

Для создания резервной копии БД в виде файла используется утилита `pg_dump`, которая создает ее согласованную копию в виде файла скрипта. Скрипт содержит последовательность SQL-команд, необходимых для воссоздания БД до состояния, в котором она была сохранена.

Для выполнения резервного копирования базы данных требуется выполнить от имени суперпользователя в окне программы «Терминал Fly» команду:

```
pg_dump -U <логин администратора БД> -d <наименование БД>
-h <ip-адрес сервера БД> -f <Наименование файла>
```

4. СООБЩЕНИЯ ОПЕРАТОРУ

При эксплуатации ПС АРМ АБИ возможно появление нижеперечисленных сообщений:

- «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 возникновении данных сообщений 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;

- «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 возникновении данных сообщений 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;

- «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 возникновении данных сообщений необходимо проверить доступность сервера контролируемого домена;

- «Библиотека ПДСЧ выдала ошибку!»;

- «Функция генерации пароля недоступна!»;

при возникновении данных сообщений необходимо проверить работоспособность КП СГП РУСБ.30563-01 и в случае обнаружения ошибок выполнить его переустановку;

- «Попытка повторной регистрации клиента»,

при возникновении данного сообщения 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
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)

