

(код продукции)

Утвержден

РУСБ.30488-02 ЛУ

ПС АРМ АБИ

Руководство оператора

РУСБ.30488-02 34 01

Листов 27

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

Идентификатор документа на электронном носителе: RUSB.30488-02 34 01.pdf

2016

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	4
2. Условие выполнения программы.....	5
3. Выполнение программы и сообщения оператору	6
3.1. Общие сведения о работе с программой.....	6
3.1.1. Вход пользователя в программу.....	6
3.1.2. Раздел [Устройства]	7
3.1.3. Раздел [Пользователи]	12
3.1.4. Раздел [КЦ]	15
3.1.5 Раздел [Антивирус]	17
3.1.6. Раздел [Тестирование]	20
3.1.7. Раздел [Резервное копирование ALD]	21
3.1.8. Раздел [Журналы]	22
3.1.9. Пользовательские настройки программы	23
3.1.10. Журнал действий оператора программы	25
3.1.11. Завершение работы с программой	25
Перечень сокращений	26

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:

- получение реестра устройств и управление доступом к их ресурсам;
- управление доступом пользователей к системе;
- проведение контроля целостности на управляемых устройствах;
- запуск антивирусной проверки на управляемых устройствах ;
- тестирование средств защиты информации на управляемых устройствах;
- резервное копирование данных ALD;
- формирование журналов сообщений системы OSSEC.

2. УСЛОВИЕ ВЫПОЛНЕНИЯ ПРОГРАММЫ

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

- рабочая станция: процессор с тактовой частотой не ниже 2 ГГц, ОЗУ – не менее 1 Гбайт, объем свободного дискового пространства на НЖМД – не менее 20 Гбайт, монитор с разрешением не менее 1024x768;

- 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;

- для представления результатов работы программы в виде выходных документов в печатной форме необходимо наличие печатающего устройства;

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

2.2. Программа функционирует с использованием операционной системы специального назначения «Astra Linux Special Edition» (далее по тексту – ОС СН, сертификат соответствия ФСТЭК России № 2557 от 27 января 2012 г.). Состав ОПО для изделия должен соответствовать перечню, представленному в таблице 1.

Таблица 1

Структурный компонент	ОПО
Серверная часть	ОС СН
	Интерпретатор PHP не ниже 5.4.2
Клиентская часть	ОС СН
	Комплекс программ «Специализированный генератор паролей» (РУСБ.30563-01)
Средства защиты информации	ОС СН
	Программа «Kaspersky Endpoint Security 8 для Linux» Программа «Антивирус Касперского 8.0 для Linux File Server»
Примечание: ОС СН Astra Linux SE включает в себя: - защищенный программный комплекс организации домена; - защищенные WEB-сервер и WEB-браузер (Apache и Firefox).	

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ И СООБЩЕНИЯ ОПЕРАТОРУ

3.1. Общие сведения о работе с программой

3.1.1. Вход пользователя в программу

Вход пользователя в программу происходит после положительного результата процесса аутентификации под учетными данными пользователя АРМ АБИ, указанными в процессе установки программы, на форме, изображенной на Рис. 1.

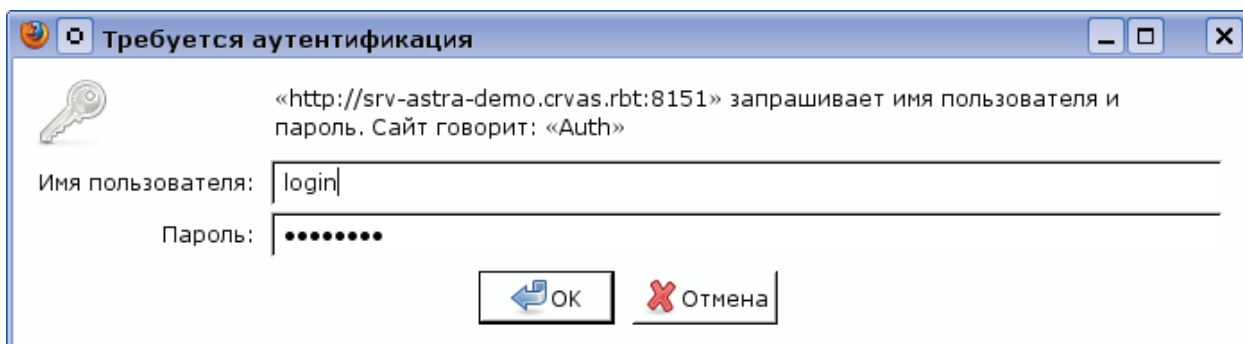
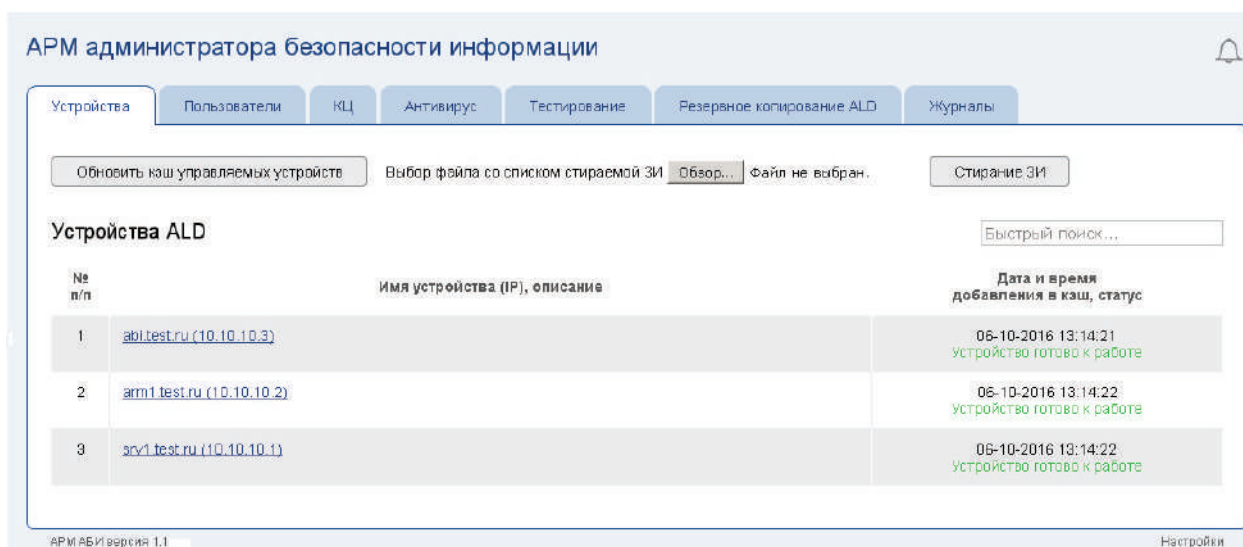


Рис. 1

Форма реализует первоначальную проверку вводимых данных. При некорректном вводе имени пользователя или пароле система повторно отобразит форму аутентификации.

После входа пользователя в программу отображается экранная форма программы с активной вкладкой **[Устройства]** (Рис. 2).



№ п/п	Имя устройства (IP), описание	Дата и время добавления в кэш, статус
1	abl.test.ru (10.10.10.3)	06-10-2016 13:14:21 устройство готово к работе
2	arm1.test.ru (10.10.10.2)	06-10-2016 13:14:22 устройство готово к работе
3	srv1.test.ru (10.10.10.1)	06-10-2016 13:14:22 устройство готово к работе

Рис. 2

Переход между разделами программы осуществляется путем клика «мышью» по соответствующей вкладке меню:

- Устройства;
- Пользователи;
- КЦ;
- Антивирус;
- Тестирование;
- Резервное копирование ALD;
- Журналы.

3.1.2. Раздел [Устройства]

Раздел [Устройства] программы предназначен для управления правами доступа (дискреционными и мандатными) информационных ресурсов на управляемых устройствах, входящих в домен ALD, а также аудитом информационных ресурсов.

Для начала работы с управляемыми устройствами необходимо кликнуть по кнопке [Обновить кэш управляемых устройств]. В этот момент программа начнет опрос всех устройств, входящих в домен ALD. Кнопка [Обновить кэш управляемых устройств] при этом станет неактивной, а рядом с ней появится соответствующее сообщение (Рис. 3).

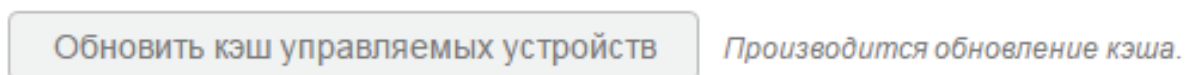


Рис. 3

Обновление кэша может занять от нескольких секунд до нескольких минут. После завершения операции вверху экрана будет выведено всплывающее информационное сообщение, как показано на рис. 4 (информационное сообщение может быть закрыто при клике по нему или при нажатии на кнопку <Esc> на клавиатуре).

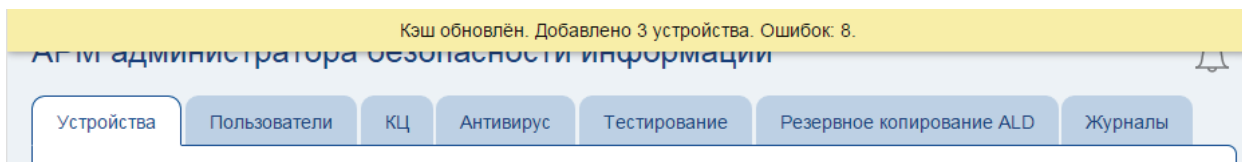


Рис. 4

В сообщении указывается, сколько устройств было добавлено в кэш программы («Добавлено...») и сколько – не добавлено («Ошибок...»). Ошибки могут возникнуть вследствие того, что какие-либо устройства, входящие в домен ALD, во время выполнения операции обновления кэша были выключены. При

возникновении ошибок необходимо убедиться, что все устройства включены и функционируют в штатном режиме, после чего повторить операцию.

После успешного добавления в кэш устройства становятся готовыми к управлению из программы. В списке устройств при этом отображается дата добавления устройства в кэш, а строка с названием устройства и его IP-адресом – становится активной (Рис. 5).

1	armabi.example.com (192.168.1.10) APM Администратора безопасности	04-08-2015 00:56:08 Устройство готово к работе
---	--	---

Рис. 5

Для быстрого поиска устройства по его названию, IP-адресу или описанию, следует использовать поле быстрого поиска, расположенное в верхнем правом углу раздела. Фильтрация списка осуществляется автоматически по мере ввода текста в данное поле.

При клике по строке с названием устройства и его IP-адресом открывается панель с кнопками **[Доступ к ресурсам]** и **[Аудит ресурсов]** (Рис. 6).

1	armabi.example.com (192.168.1.10) APM Администратора безопасности	04-08-2015 00:56:08 Устройство готово к работе
<input type="button" value="Доступ к ресурсам"/> <input type="button" value="Аудит ресурсов"/>		

Рис. 6


3.1.2.1. Управление параметрами доступа к информационным ресурсам

При клике по кнопке **[Доступ к ресурсам]** в списке управляемых устройств открывается всплывающее окно со списком файлов и директорий соответствующего устройства (Рис. 7).



Рис. 7

Имена директорий являются ссылками, при клике по которым на экран выводятся списки файлов и поддиректорий в соответствующих директориях.

Напротив имени файла или директории в списке выводится кнопка [], при клике по которой открывается окно с параметрами редактирования дискреционных и мандатных правил разграничения доступа к соответствующему файлу или директории (информационному ресурсу), как показано на Рис. 8.

Применить рекурсию:

Владелец	Группа	Права пользователя	Права группы	Права остальных
root	root	гwx	г-х	г-х

[Редактировать дискреционные ПРД](#)

Тип субъекта ACL	Имя	Правило	
Пользователь	sync	гwx	⊘
Маска	—	гwx	

[Задать правило ACL](#)

[Удалить все правила](#)

Уровень	Целостность	Категории	Атрибуты
3	low	Все возможные	0x1

[Редактировать мандатные ПРД](#)

Рис. 8

Подробно о дискреционном и мандатном разграничении доступа – см. разделы 3 и 4 документа «Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

При редактировании прав доступа кликните по чек-боксу **[Применить рекурсию]**, если необходимо применить изменения не только для выбранного информационного ресурса, но и для всех информационных ресурсов, содержащихся в нем, рекурсивно.

Для возврата к списку информационных ресурсов кликните по кнопке **[Вернуться к списку файлов и директорий]**.

Для закрытия окна редактирования параметров доступа к информационным ресурсам кликните по крестику в его верхнем правом углу или нажмите кнопку **<Esc>** на клавиатуре.

3.1.2.2. Управление параметрами аудита ресурсов

При клике по кнопке **[Аудит ресурсов]** в списке управляемых устройств открывается всплывающее окно со списком информационных ресурсов, поставленных на аудит на соответствующем устройстве (Рис. 9).

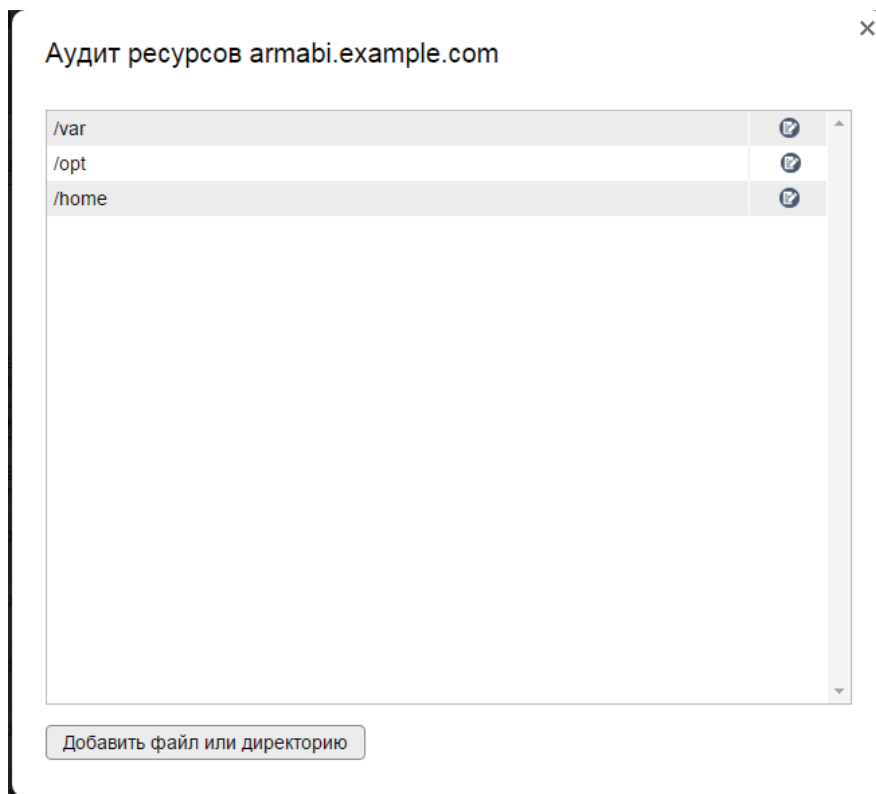



Рис. 9

Напротив имени информационного ресурса в списке выводится кнопка [], при клике по которой открывается окно с параметрами редактирования параметров аудита для соответствующего информационного ресурса (Рис. 10).

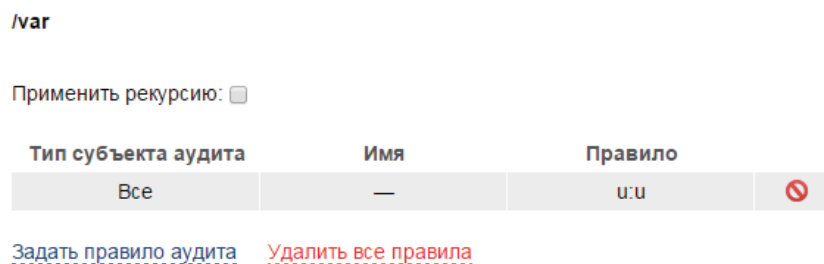


Рис. 10

Подробно об аудите информационных ресурсов – см. раздел 10 документа «Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

При редактировании параметров аудита кликните по чек-боксу **[Применить рекурсию]**, если необходимо применить изменения не только для выбранного информационного ресурса, но и для всех информационных ресурсов, содержащихся в нем, рекурсивно.

Для возврата к списку информационных ресурсов, поставленных на аудит, кликните по кнопке **[Вернуться к списку ресурсов]**.

Для закрытия окна редактирования параметров аудита информационных ресурсов кликните по крестику в его верхнем правом углу или нажмите кнопку **<Esc>** на клавиатуре.

3.1.2.3 Управление стиранием защищаемой информации

При клике на кнопку **[Обзор...]** (Рис. 2) открывается диалоговое окно для выбора текстового файла со сценарием, содержащим адреса машин и пути до файлов с защищаемой информацией. Формат файла выглядит следующим образом:

```
# {адрес}:{путь до файла или директории}
10.10.10.1:/var/user/some_CI
10.10.10.2:/home/user/some_CI
# и т.д.
```

При клике на кнопку **[Стирание ЗИ]** (Рис. 2) происходит удаление всех указанных файлов.

3.1.3. Раздел [Пользователи]

Раздел **[Пользователи]** программы предназначен для блокировки и разблокировки текущих пользовательских сессий в рамках домена ALD. Внешний вид раздела приведен на Рис. 11.

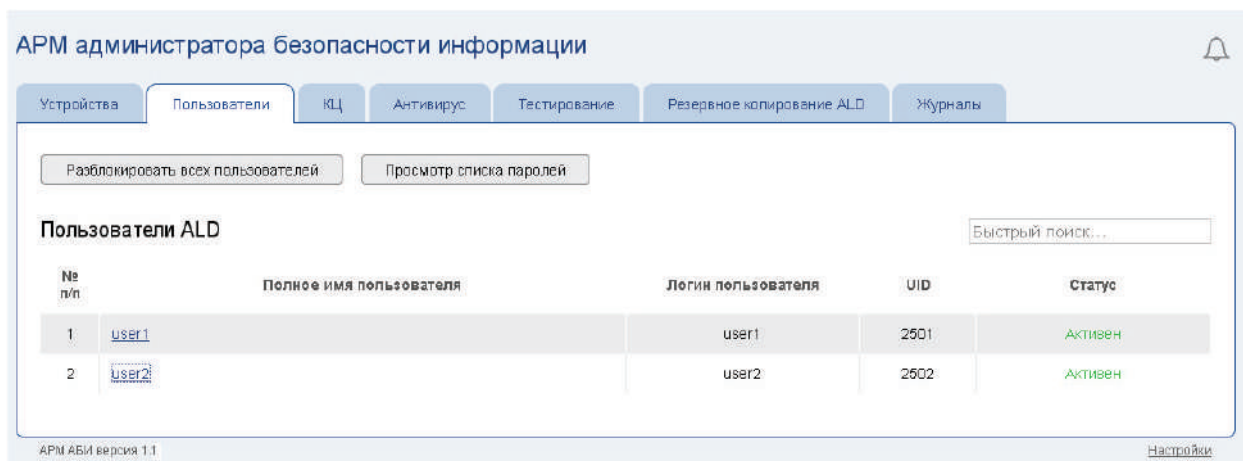


Рис. 11

Для быстрого поиска пользователя по полному имени, логину или UID, следует использовать поле быстрого поиска, расположенное в верхнем правом углу раздела. Фильтрация списка осуществляется автоматически по мере ввода текста в данное поле.

Полное имя пользователя в списке пользователей – активно. При клике по нему открывается панель с кнопками **[Сменить пароль]** и **[Заблокировать]/[Разблокировать]** – в зависимости от текущего статуса соответствующего пользователя (Рис. 12).



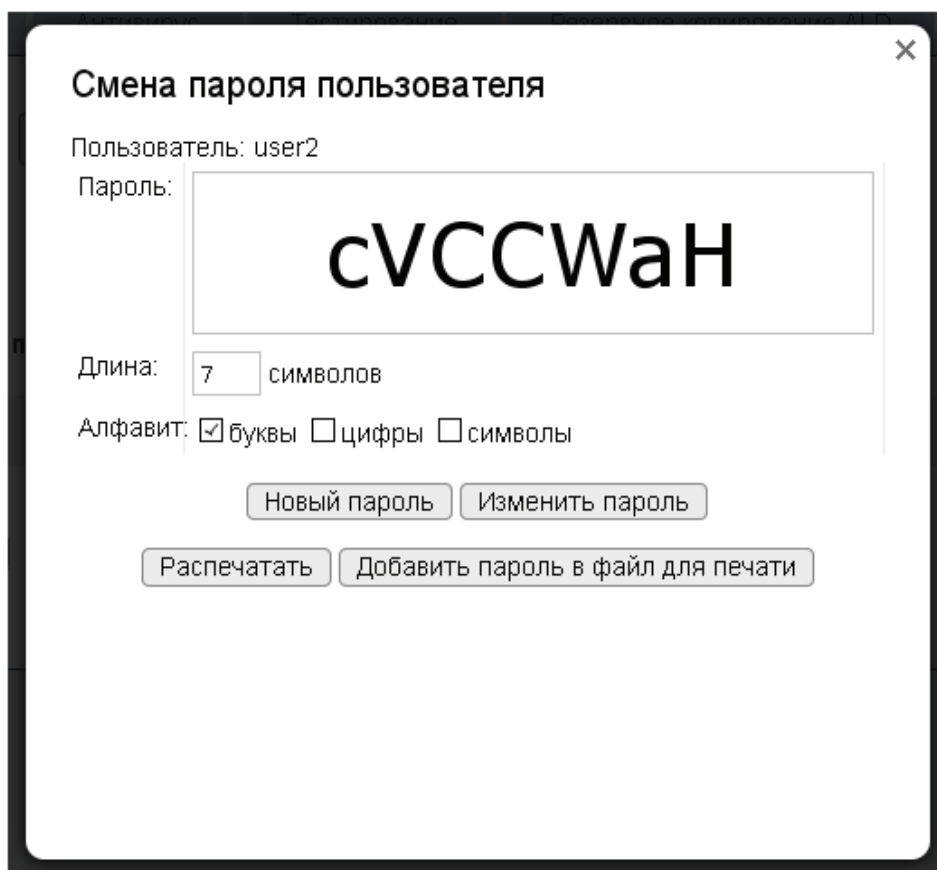
Рис. 12

При клике по кнопке **[Заблокировать]** на экран выводится всплывающее диалоговое окно, в котором требуется подтвердить действие. В случае подтверждения статус соответствующего пользователя в списке меняется на **[Заблокирован]**; при этом текущая сессия пользователя на АРМ прерывается, на экран выводится экран приветствия ОС СН «Astra Linux Special Edition» (все запущенные процессы не будут остановлены). Войти в систему повторно пользователь не сможет до тех пор, пока он не будет разблокирован в программе.

Для разблокирования сразу всех пользователей следует кликнуть по кнопке **[Разблокировать всех пользователей]** (Рис. 11).

3.1.3.1 Управление паролем пользователя

При клике по кнопке **[Сменить пароль]** открывается форма предназначенная для генерации нового пароля, изменения пароля данного пользователя, распечатки пароля данного пользователя и добавления пароля в файл для печати. Данная форма не показывает текущий пароль пользователя (Рис. 13).



Смена пароля пользователя

Пользователь: user2

Пароль:

Длина: символов

Алфавит: буквы цифры символы

Рис. 13

При клике по кнопке **[Новый пароль]** генерируется новый пароль на основании заданных параметров — длина, алфавит. При клике на кнопку **[Изменить пароль]** пароль, отображаемый на форме применяется для выбранного пользователя. При клике по кнопке **[Распечатать]** открывается диалоговое окно для печати данного пароля. При клике по кнопке **[Добавить пароль в файл для печати]** текущий пароль и имя пользователя заносятся во временный файл, который затем можно будет распечатать.

3.1.3.2 Просмотр списка паролей.

При клике по кнопке **[Просмотр списка паролей]** открывается форма с содержанием файла для печати паролей. При клике по кнопке **[Вывести на печать]** открывается диалоговое окно для печати файла. При клике по кнопке **[Очистить список паролей]** файл с паролями очищается (Рис. 14).

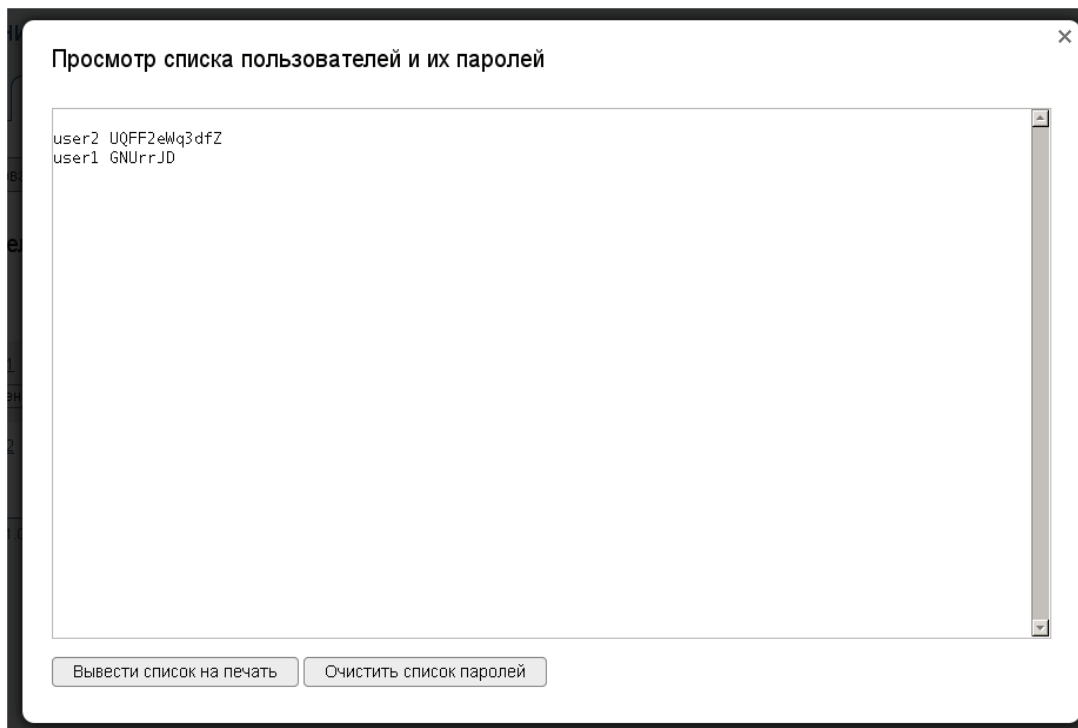


Рис. 14

3.1.4. Раздел [КЦ]

Раздел [КЦ] программы предназначен для редактирования перечня компонентов (информационных ресурсов) контроля целостности (КЦ) устройств, запуска КЦ на управляемых устройствах и просмотра результатов проведенного КЦ. Внешний вид раздела приведен на Рис. 15.

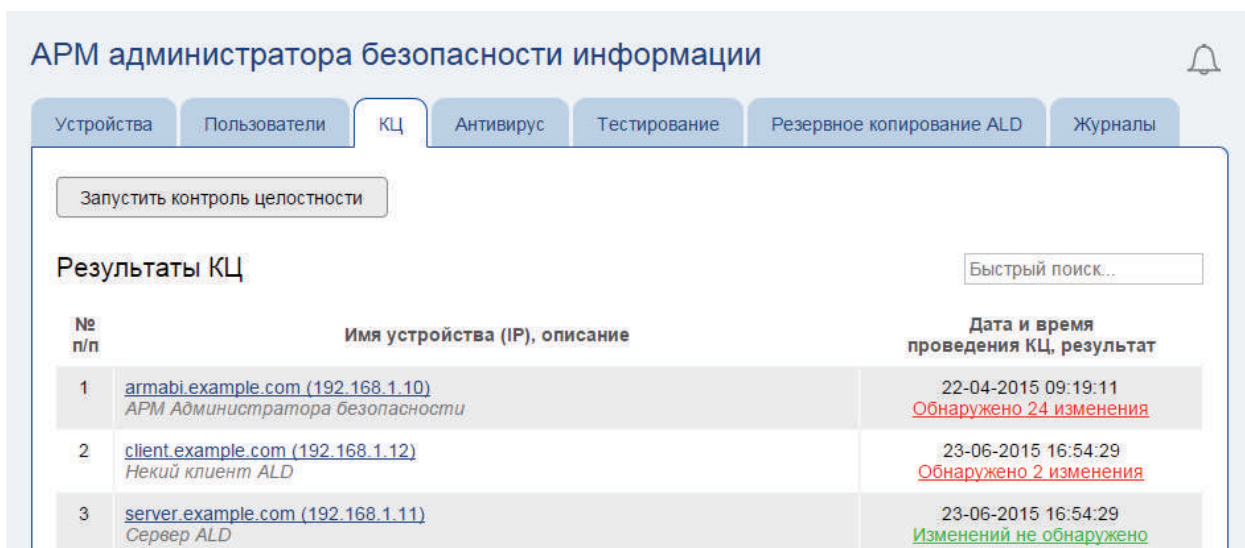


Рис. 15

В основном списке раздела выводятся только устройства из домена ALD, успешно добавленные в кэш программы (см. п. 3.1.2) и результаты последнего контроля целостности для них (если проводился).

Для быстрого поиска устройства по его названию, IP-адресу или описанию, следует использовать поле быстрого поиска, расположенное в верхнем правом углу раздела. Фильтрация списка осуществляется автоматически по мере ввода текста в данное поле.

Имена устройств и их IP-адреса в списке – активны. При клике по ним выводится панель с кнопкой **[Компоненты КЦ]**, как показано на Рис. 16.

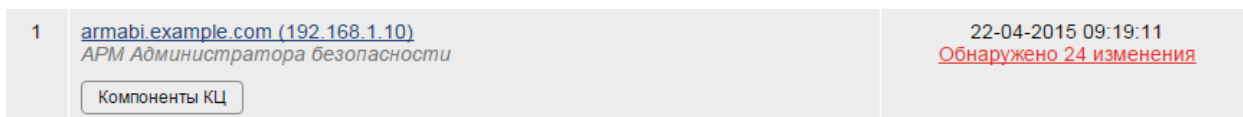


Рис. 16

При клике по кнопке **[Компоненты КЦ]** открывается всплывающее окно со списком компонентов (информационных ресурсов), к которым применяется КЦ на соответствующем устройстве (Рис. 17).

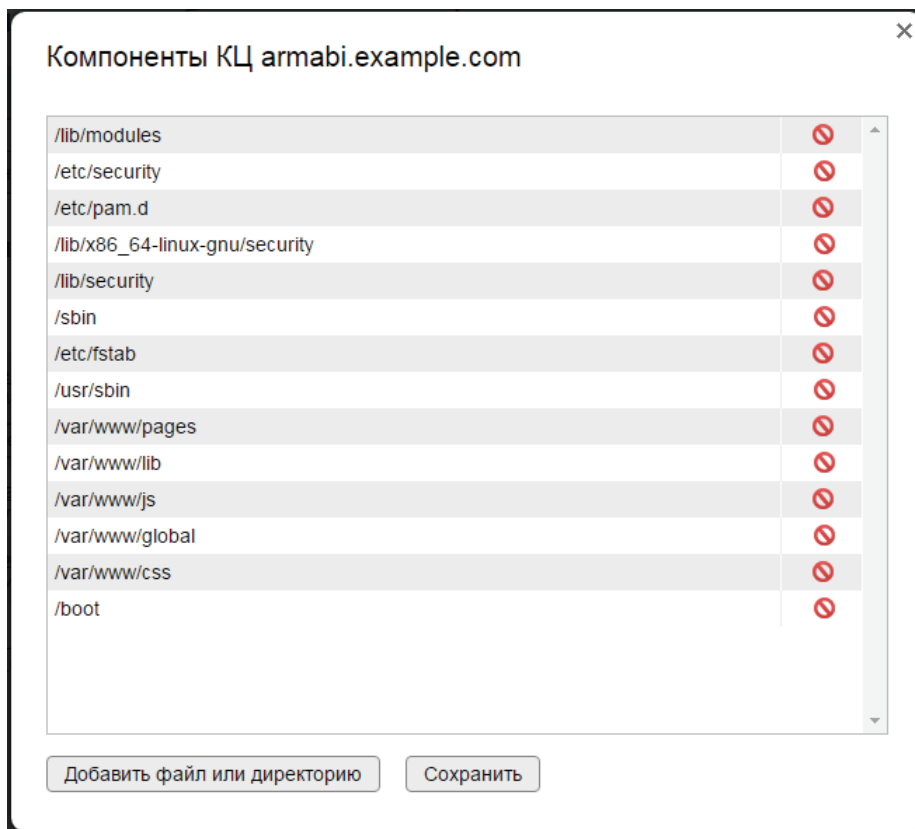


Рис. 17

Для удаления компонента следует кликнуть по кнопке **[X]**, располагающейся справа от него.

Для добавления в список нового компонента, следует кликнуть по кнопке **[Добавить файл или директорию]**, после чего, перейдя к требуемому файлу или директории, кликнуть по соответствующей кнопке **[+]**.

По окончании редактирования списка компонентов КЦ необходимо кликнуть по кнопке **[Сохранить]**.

Запуск КЦ производится путем клика по кнопке **[Запустить контроль целостности]**, расположенной вверху раздела, выбора в открывающемся окне (Рис. 18) необходимых устройств и клику по кнопке **[Продолжить]**.

После запуска КЦ кнопка **[Запустить контроль целостности]** становится неактивной, пока процесс не будет завершен, о чем программа уведомит всплывающим информационным сообщением вверху экрана.

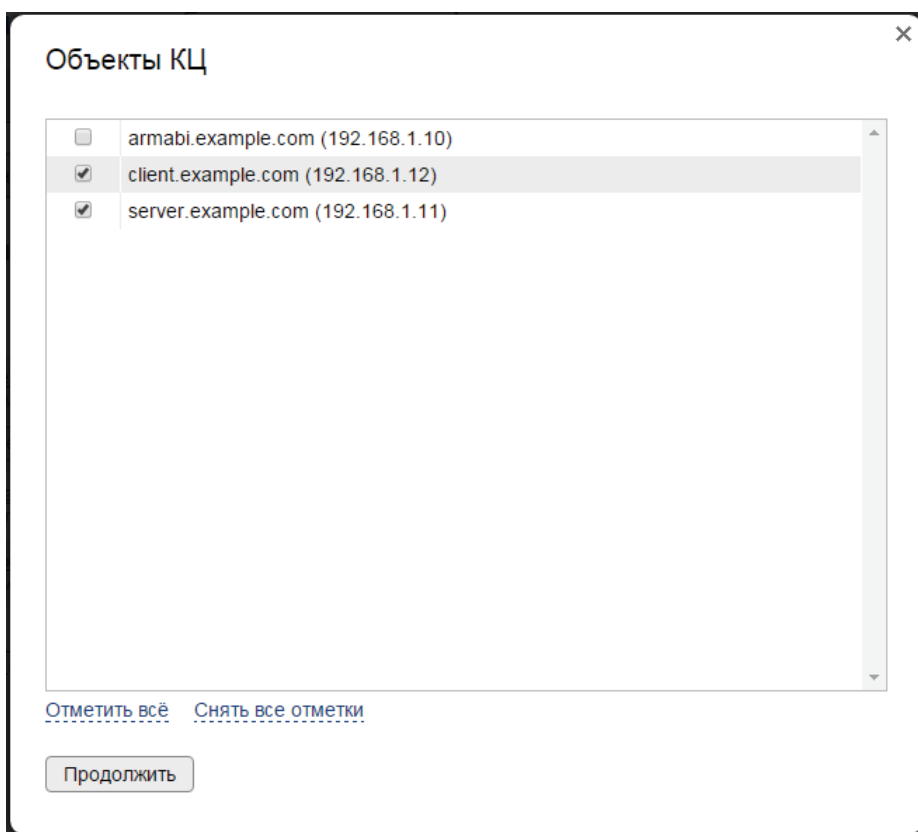


Рис. 18

Для просмотра результатов последнего КЦ (если проводился) для определенного устройства, необходимо кликнуть по соответствующей ссылке в графе «Дата и время проведения КЦ, результат» основного списка раздела.

Подробнее о контроле целостности – см. раздел 13 документа «Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

3.1.5 Раздел [Антивирус]

Раздел **[Антивирус]** программы предназначен для запуска антивирусной проверки на управляемых устройствах и просмотра результатов ее проведения (если проводилась). Внешний вид раздела приведен на Рис. 19.

APM администратора безопасности информации

Устройства Пользователи КЦ Антивирус Тестирование Резервное копирование ALD Журналы

Запустить антивирусную проверку

Результаты антивирусной проверки

№ п/п	Имя устройства (IP), описание	Дата и время проведения проверки, результат
1	armabi.example.com (192.168.1.10) <i>APM Администратора безопасности</i>	22-04-2015 20:36:25 Угроз не обнаружено
2	client.example.com (192.168.1.12) <i>Некий клиент ALD</i>	23-06-2015 17:30:46 Угроз не обнаружено
3	server.example.com (192.168.1.11) <i>Сервер ALD</i>	04-04-2015 19:32:53 Обнаружены 3 угрозы

Рис. 19

В основном списке раздела выводятся только устройства из домена ALD, успешно добавленные в кэш программы (см. п. 3.1.2) и результаты последней антивирусной проверки для них (если проводилась).

Для быстрого поиска устройства по его названию, IP-адресу или описанию, следует использовать поле быстрого поиска, расположенное в верхнем правом углу раздела. Фильтрация списка осуществляется автоматически по мере ввода текста в данное поле.

Запуск антивирусной проверки производится путем клика по кнопке **[Запустить антивирусную проверку]**, расположенной вверху раздела, выбора в открывающемся окне (Рис. 20) необходимых устройств, уточнения (при необходимости) области проверки – полная или выборочная – и клику по кнопке **[Продолжить]**.

После запуска антивирусной проверки кнопка **[Запустить антивирусную проверку]** становится неактивной, пока процесс не будет завершен, о чем программа уведомит всплывающим информационным сообщением вверху экрана.

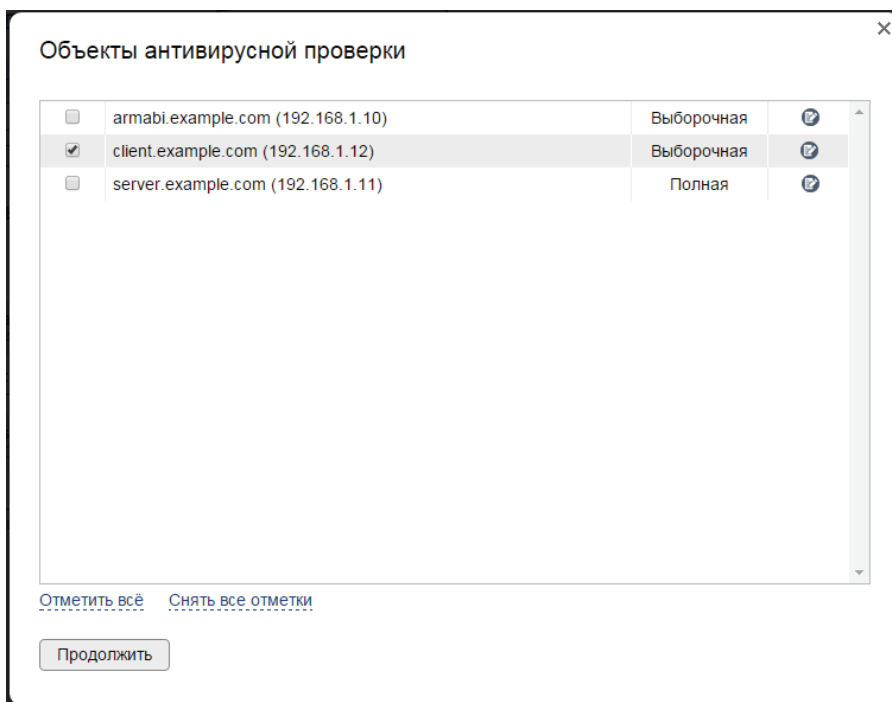



Рис. 20

Для уточнения области проверки (перечня компонентов антивирусной проверки) в окне, изображенном на рис. 20, следует кликнуть по кнопке [] напротив соответствующего устройства. При этом на экран выводится окно со списком (если есть) файлов и директорий, для которых требуется провести антивирусную проверку (Рис. 21).

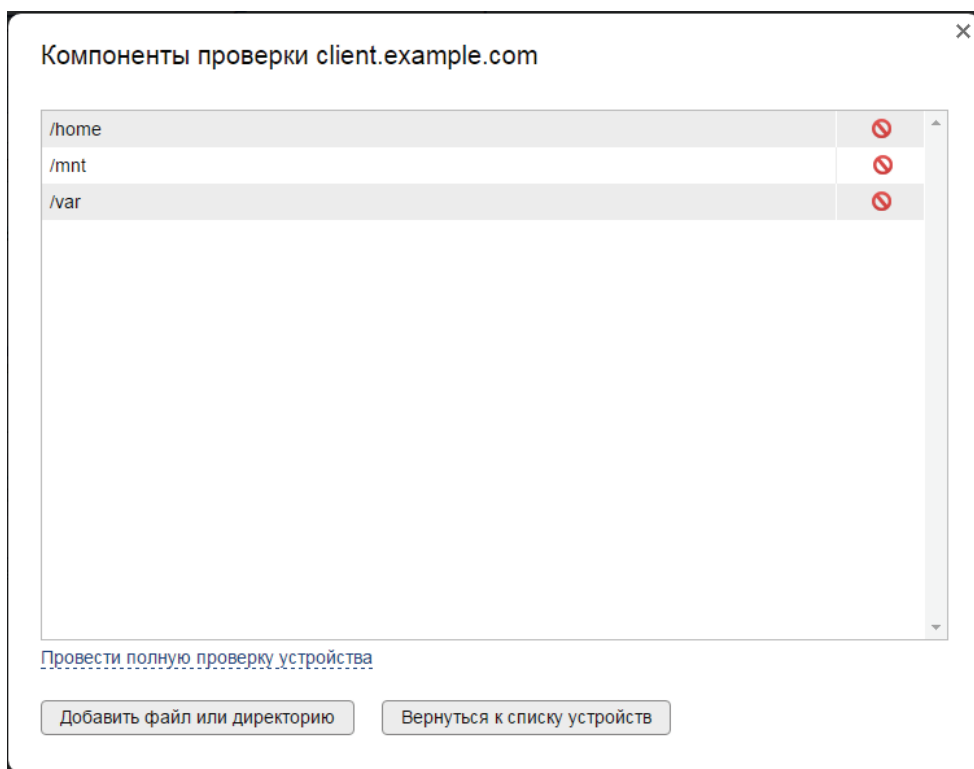



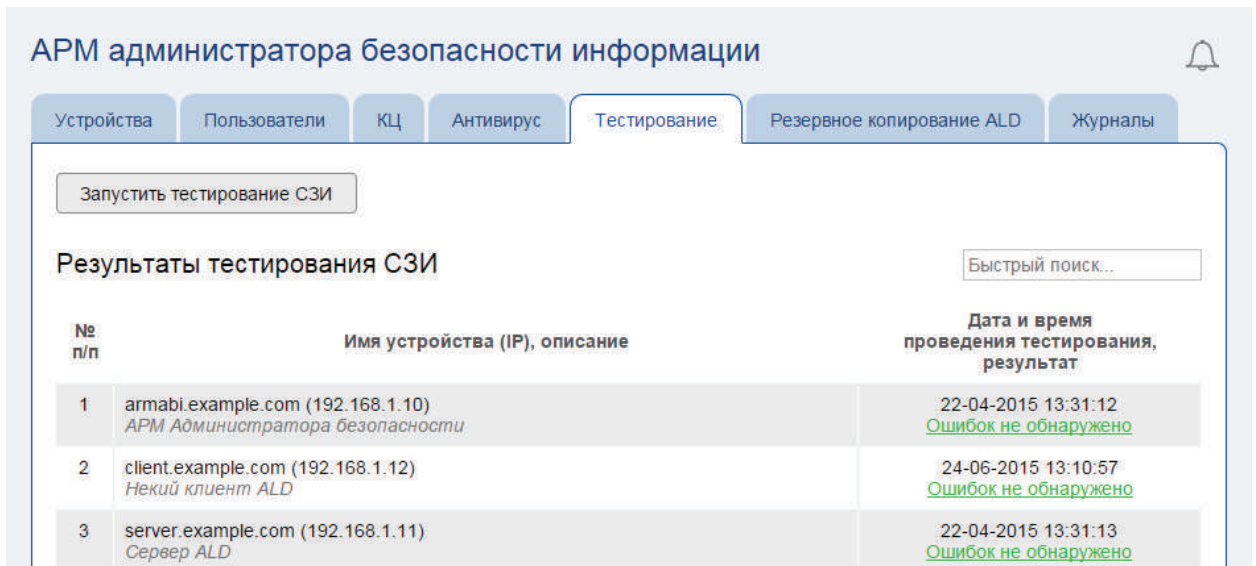
Рис. 21

Для добавления в список нового компонента следует кликнуть по кнопке **[Добавить файл или директорию]**, после чего, перейдя к требуемому файлу или директории, кликнуть по соответствующей кнопке []

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.

3.1.6. Раздел [Тестирование]

Раздел **[Тестирование]** программы предназначено для запуска тестирования КСЗ ОС СН на управляемых устройствах и просмотра результатов его проведения (если проводилось). Внешний вид раздела приведен на Рис. 22.



№ п/п	Имя устройства (IP), описание	Дата и время проведения тестирования, результат
1	armabi.example.com (192.168.1.10) <i>APM Администратора безопасности</i>	22-04-2015 13:31:12 Ошибка не обнаружено
2	client.example.com (192.168.1.12) <i>Некий клиент ALD</i>	24-06-2015 13:10:57 Ошибка не обнаружено
3	server.example.com (192.168.1.11) <i>Сервер ALD</i>	22-04-2015 13:31:13 Ошибка не обнаружено

Рис. 22

В основном списке раздела выводятся только устройства из домена ALD, успешно добавленные в кэш программы (см. п. 3.1.2) и результаты последнего тестирования для них (если проводилось).

Для быстрого поиска устройства по его названию, IP-адресу или описанию, следует использовать поле быстрого поиска, расположенное в верхнем правом углу раздела. Фильтрация списка осуществляется автоматически по мере ввода текста в данное поле.

Запуск тестирования производится путем клика по кнопке **[Запустить тестирование СЗИ]**, расположенной вверху раздела, выбора в открывающемся окне (Рис. 23) необходимых устройств и клику по кнопке **[Продолжить]**.

После запуска тестирования кнопка **[Запустить тестирование СЗИ]** становится неактивной, пока процесс не будет завершен, о чем программа уведомит всплывающим информационным сообщением вверху экрана.

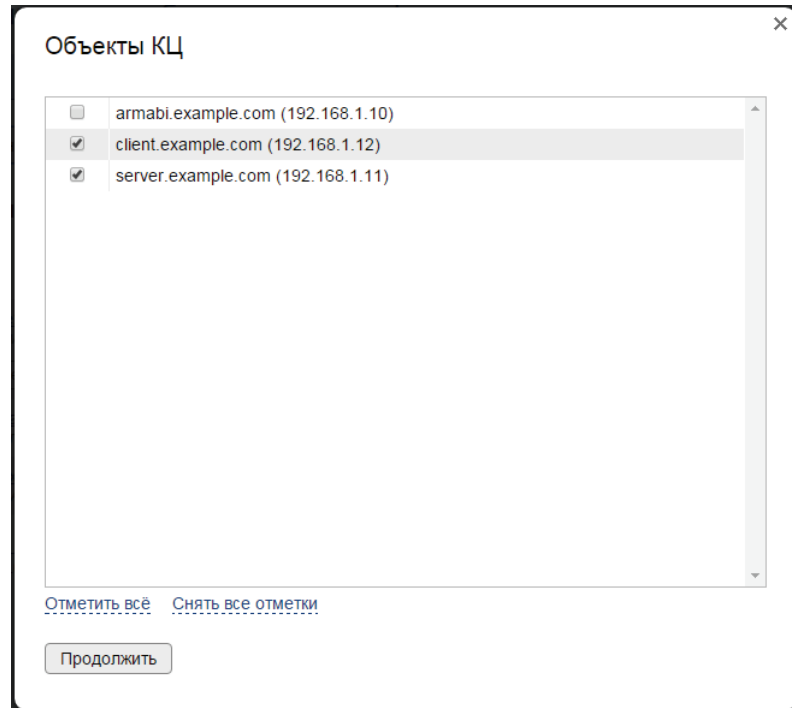


Рис. 23

Для просмотра результатов последнего тестирования (если проводилось) для определенного устройства, необходимо кликнуть по соответствующей ссылке в графе «Дата и время проведения тестирования, результат» основного списка раздела.

Подробнее о тестах КСЗ – см. документ «Руководство по КСЗ. Часть 2» РУСБ.10015-01 97 01-2.

3.1.7. Раздел **[Резервное копирование ALD]**

Раздел **[Резервное копирование ALD]** программы предназначен для создания резервных копий домена ALD, их выгрузки и удаления. Внешний вид раздела представлен на Рис. 24.

APM администратора безопасности информации

Устройства Пользователи КЦ Антивирус Тестирование Резервное копирование ALD Журналы

Создать резервную копию ALD

Резервные копии ALD

№ п/п	Дата и время создания резервной копии	Размер	Путь к файлу	
1	24-06-2015 16:57:28	630 Кб	/var/backups/ald/ald_backup_2015-06-24_1657.tar	
2	24-06-2015 13:27:25	630 Кб	/var/backups/ald/ald_backup_2015-06-24_1327.tar	
3	03-06-2015 15:17:43	620 Кб	/var/backups/ald/ald_backup_2015-06-03_1517.tar	

Рис. 24

В основном списке раздела (если резервные копии создавались ранее) выводится информация о дате/времени создания резервных копий, их размере, а также активные ссылки для скачивания архивов (графа «Путь к файлу»).

Для удаления ранее созданной резервной копии ALD кликните по кнопке напротив соответствующего файла в основном списке раздела.

Для создания резервной копии кликните по кнопке **[Создать резервную копию ALD]** вверху раздела.

3.1.8. Раздел [Журналы]

Раздел **[Журналы]** программы предназначен для архивирования текущего журнала регистрации OSSEC, его очистки, а также управления ранее созданными архивами (их просмотр и удаление). Внешний вид раздела представлен на Рис. 25.

APM администратора безопасности информации

Устройства Пользователи КЦ Антивирус Тестирование Резервное копирование ALD Журналы

Для дат с: 10-08-2016 12:13:25 по: 10-12-2016 10:13:25

Архивировать текущий журнал Очистить весь текущий журнал


Архивы журналов

№ п/п	Дата и время создания архива	Размер	Путь к файлу (на сервере OSSEC — abi.test.ru)	
1	06-10-2016 16:13:24	174 Байт	/var/ossec/logs/alerts/2016/Oct/ossec-alerts-06.log.161323.gz	
2	06-10-2016 12:50:49	174 Байт	/var/ossec/logs/alerts/2016/Oct/ossec-alerts-06.log.125049.gz	

APM АБИ| версия 1.1 Настройки

Рис. 25

В основном списке раздела (если архивы журнала создавались ранее) выводится информация о дате/времени создания архивов, их размере, а также активные ссылки для просмотра архивов (графа «Путь к файлу»).

Для удаления ранее созданного архива журнала кликните по кнопке  напротив соответствующего файла в основном списке раздела.

Для создания архива текущего журнала введите начальные и конечные дату и время для фильтрации событий и кликните по кнопке **[Архивировать текущий журнал]** вверху раздела.

Для очистки текущего журнала кликните по кнопке **[Очистить весь текущий журнал]** вверху раздела.

Примечание: Факт очистки журнала, включая дату и время очистки, фиксируется в текущем журнале OSSEC.

Подробно о средствах централизованного протоколирования ОС СН – см. раздел 15 документа «Руководство администратора. Часть 1» РУСБ.10015-01 95 01-1.

3.1.9. Пользовательские настройки программы

Для перехода в раздел настроек программы необходимо кликнуть по ссылке **[Настройки]** внизу страницы (доступно из любого раздела программы) – Рис. 26.



Рис. 26

Внешний вид раздела представлен на Рис. 27.

APM администратора безопасности информации

Устройства Пользователи КЦ Антивирус Тестирование Резервное копирование ALD Журналы

Настройки

Имя сервера ALD:

Имя сервера OSSEC:

Имя пользователя APM АБИ:

Пароль пользователя APM АБИ:

Начальная директория SSH:
По умолчанию: /

Хранение резервных копий ALD:
По умолчанию: /var/backups/ald/

Хранение логов КЦ:
По умолчанию: /var/www/tmp/logs/lc/

Хранение логов ABC:
По умолчанию: /var/www/tmp/logs/aw/

Хранение логов тестов:
По умолчанию: /var/www/tmp/logs/test/

Интервал проверки процессов:
По умолчанию: 30

Кол-во записей на странице:
По умолчанию: 15

Формат даты/времени:

Временная зона:

Рис. 27

Раздел «Настройки» позволяет изменять следующие параметры программы:

- имя сервера ALD;
- имя сервера OSSEC;
- имя пользователя APM АБИ;
- пароль пользователя APM АБИ;
- начальная директория SSH (директория, список файлов и поддиректорий которой будут выводиться по умолчанию при открытии списков файлов и директорий на управляемых устройствах);
- хранение резервных копий ALD (директория на APM АБИ, в которой будут храниться резервные копии ALD);
- хранение логов КЦ (директория на APM АБИ, в которой будут храниться результаты КЦ);
- хранение логов ABC (директория на APM АБИ, в которой будут храниться результаты антивирусной проверки);
- хранение логов тестов (директория на APM АБИ, в которой будут храниться результаты тестирования КСЗ ОС СН);
- интервал проверки процессов (интервал в секундах, с которым программа проверяет статус процессов КЦ, антивирусной проверки и

тестирования; увеличьте интервал, если потребуется снизить нагрузку на локальную сеть);

- количество записей на странице (количество одновременно выводимых записей в основных списках разделов);

- формат даты/времени (действует глобально);

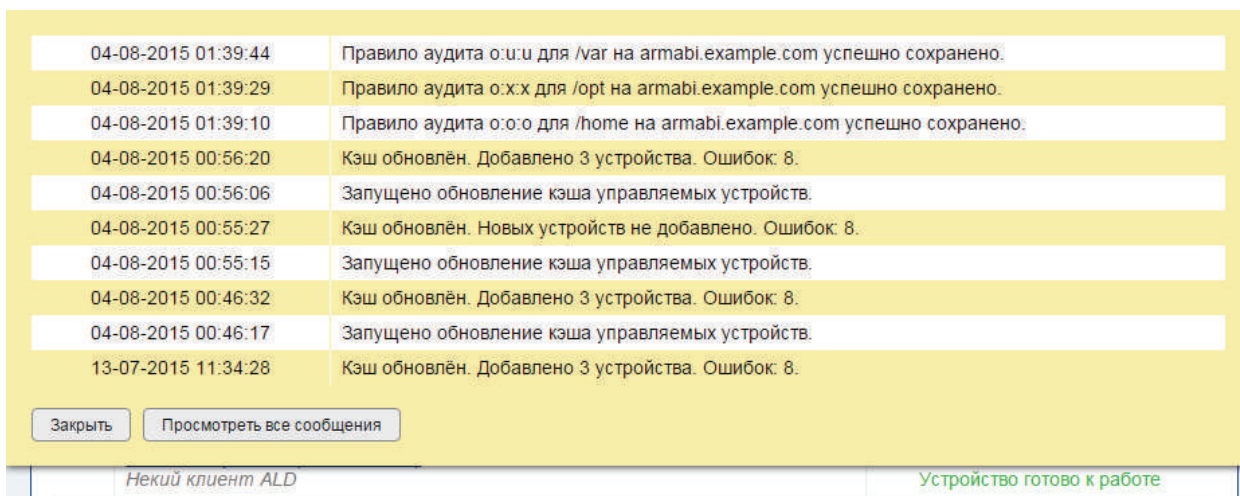
- временная зона (действует глобально).

Для возврата к заводским настройкам, кликните по ссылке **[Прописать настройки по умолчанию]**.

3.1.10. Журнал действий оператора программы

В процессе использования программа ведет журнал всех значимых действий оператора.

Для доступа к журналу действий оператора необходимо кликнуть по кнопке **[🔔]**, расположенной в верхнем правом углу экрана (доступно из любого раздела программы). При этом в верхней части экрана откроется всплывающее окно со списком последних десяти действий (Рис. 28).



04-08-2015 01:39:44	Правило аудита o:u для /var на armabi.example.com успешно сохранено.
04-08-2015 01:39:29	Правило аудита o:x для /opt на armabi.example.com успешно сохранено.
04-08-2015 01:39:10	Правило аудита o:o для /home на armabi.example.com успешно сохранено.
04-08-2015 00:56:20	Кэш обновлён. Добавлено 3 устройства. Ошибок: 8.
04-08-2015 00:56:06	Запущено обновление кэша управляемых устройств.
04-08-2015 00:55:27	Кэш обновлён. Новых устройств не добавлено. Ошибок: 8.
04-08-2015 00:55:15	Запущено обновление кэша управляемых устройств.
04-08-2015 00:46:32	Кэш обновлён. Добавлено 3 устройства. Ошибок: 8.
04-08-2015 00:46:17	Запущено обновление кэша управляемых устройств.
13-07-2015 11:34:28	Кэш обновлён. Добавлено 3 устройства. Ошибок: 8.

Закрыть Посмотреть все сообщения

Некий клиент ALD Устройство готово к работе

Рис. 28

Для того, чтобы посмотреть журнал действий целиком, кликните в открывшемся всплывающем окне по кнопке **[Посмотреть все сообщения]**.

Чтобы закрыть окно, кликните по кнопке **[Закрыть]** или нажмите кнопку **<Esc>** на клавиатуре.

3.1.11. Завершение работы с программой

Для завершения работы с программой необходимо закрыть окна браузера.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ АБИ	– автоматизированное рабочее место администратора безопасности информации
КСЗ	– комплекс средств защиты
КЦ	– контроль целостности
ЛУ	– лист утверждения
НЖМД	– накопитель на жестком магнитном диске
ОЗУ	– оперативное запоминающее устройство
ОПО	– общее программное обеспечение
ОС	– операционная система
ПС АРМ АБИ	– программное средство автоматизированного рабочего места администратора безопасности информации
ПЭВМ	– персональная электронная вычислительная машина
СН	– специальное назначение
ФСТЭК	– Федеральная служба по техническому и экспортному контролю

