Утвержден

РУСБ.30488-04 ЛУ

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

ПС АРМ АБИ

Описание применения

РУСБ.30488-04 31 01

Листов 12

2022

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения Программного средства автоматизированного рабочего места администратора безопасности информации (ПС АРМ АБИ, далее по тексту – программа).

В документе описывается назначение, основные возможности и условия применения программы.

Документ предназначен для ознакомления должностным лицам, осуществляющим и обеспечивающим эксплуатацию программы.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ

Программное средство автоматизированного рабочего места администратора безопасности информации (ПС АРМ АБИ) РУСБ.30488-04 (далее по тексту – программа) предназначено для автоматизации повседневной деятельности администраторов безопасности информации при выполнении работ на серверах и рабочих станциях, функционирующих под управлением операционной системы специального назначения «Astra Linux Special Edition» очередное обновление 1.6 (без обновлений или установленными оперативными обновлениями 6, 10, 12) и очередное обновление 1.7 (без обновлений или установленными оперативными обновлениями 1.7.1, 1.7.3) с версиями ядра 4.15, 5.4, 5.10, 5.15.

2. УСЛОВИЯ ПРИМЕНЕНИЯ ПРОГРАММЫ

2.1. Минимальный состав аппаратных средств

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

1) серверная часть:

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

2) клиентская часть:

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

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

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

2.2. Минимальный состав программных средств

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

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

Для реализации функционального назначения программы необходимо наличие установленного программного обеспечения:

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

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Определение задачи

Программа обеспечивает решение следующих основных задач:

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

2) управление разграничением доступа к ресурсам управляемых устройств;

3) получение списка процессов, запущенных на управляемом устройстве;

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

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

6) управление доступом пользователей к устройствам домена;

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

8) создание/редактирование учётных записей пользователей;

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

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

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

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

13) формирование и просмотр журналов событий информационной безопасности;

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

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

16) автоблокировка пользователя при возникновении заданных событий НСД;

17) резервное копирование данных (конфигурации) управляемых доменов;

18) резервное копирование и восстановление базы данных программы;

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

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

21) тиражирование правил доступа к отчуждаемым носителям информации;

22) ведение таблицы разграничения доступа пользователей к защищаемым ресурсам;

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

3.2. Методы решения задачи

ПС АРМ АБИ включает в себя следующие компоненты:

- программное средство анализа событий информационной безопасности, устанавливаемое на сервер централизованного протоколирования;
- агентов безопасности, устанавливаемых на все управляемые устройства контролируемых доменов;
- сервер безопасности, устанавливаемый на АРМ АБИ.

Программное средство анализа событий информационной безопасности обеспечивает определение значимости с точки зрения обеспечения информационной безопасности собранных с управляемых устройств контролируемого домена с использованием системного сервиса `rsyslog` событий.

Агенты безопасности обеспечивают выполнение команд, поступивших от сервера безопасности, получение результатов их выполнения и отправку на сервер безопасности. Взаимодействие между агентами и сервером безопасности при этом осуществляется по специальному протоколу, обеспечивающему установление между ними логического соединения и кодирования данных с вычислением контрольной суммы.

Агенты безопасности, устанавливаемые на контроллер домена, кроме того, обеспечивают сбор информации о конфигурации домена и отправку ее на сервер безопасности, выполнение команд по управлению доменом, полученных от сервера безопасности, а также передачу на сервер безопасности событий информационной безопасности из программного средства анализа событий информационной безопасности.

Решение функциональных задач программы достигается предоставлением администратору безопасности информации эргономичного графического интерфейса. После запуска на АРМ АБИ сервера безопасности и успешного прохождения процедуры аутентификации отображается основное окно программы, содержащее меню с логически сгруппированной по функционалу информаций об управляемых устройствах контролируемых доменов (рис. 1).

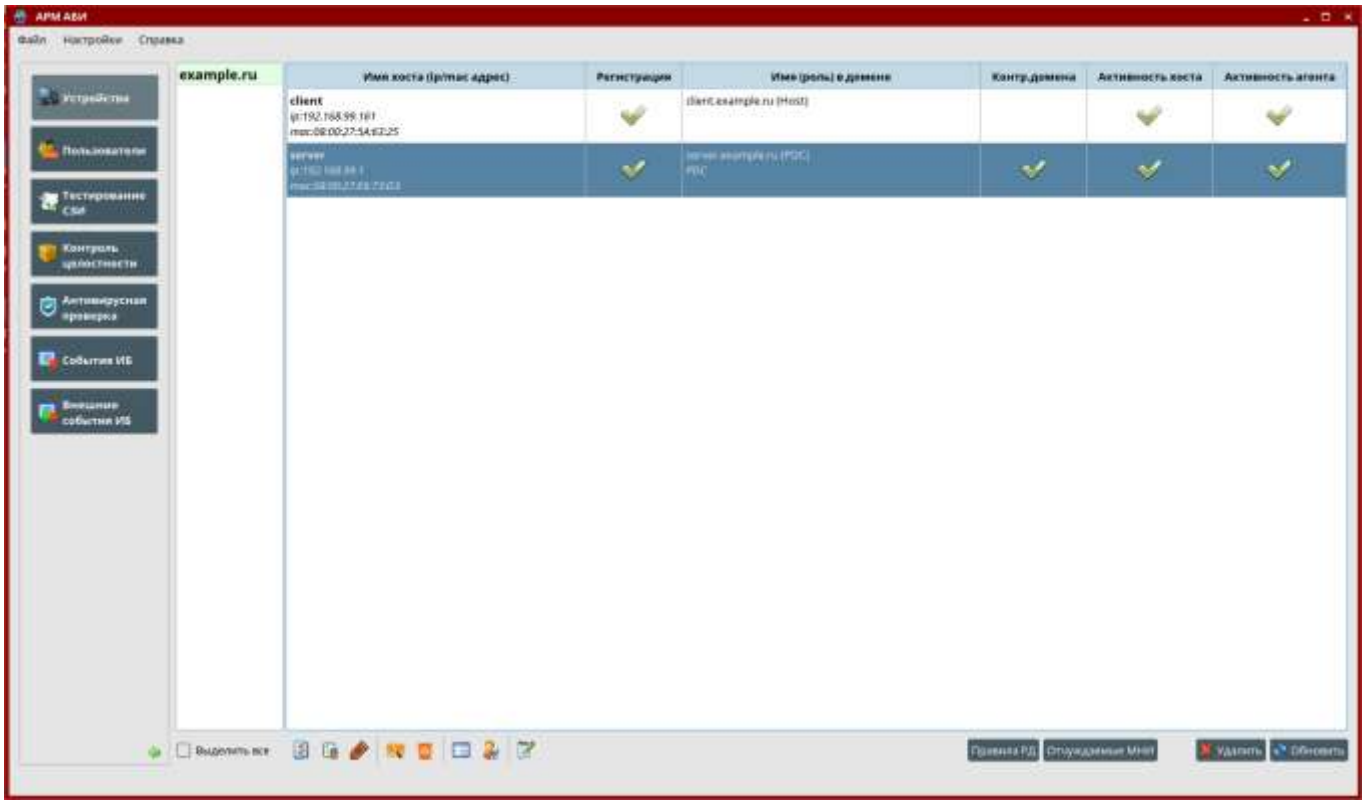

Рис. 1 – Основное окно программы

Порядок работы с программой, описание типовых элементов и окон, типовых форм отчетных документов изложены в «ПС АРМ АБИ. Руководство оператора» РУСБ.30488-04 34 01.

Схема взаимодействия сервера безопасности с агентами безопасности, установленными на управляемых устройствах контролируемых доменов, приведена на рис. 2.

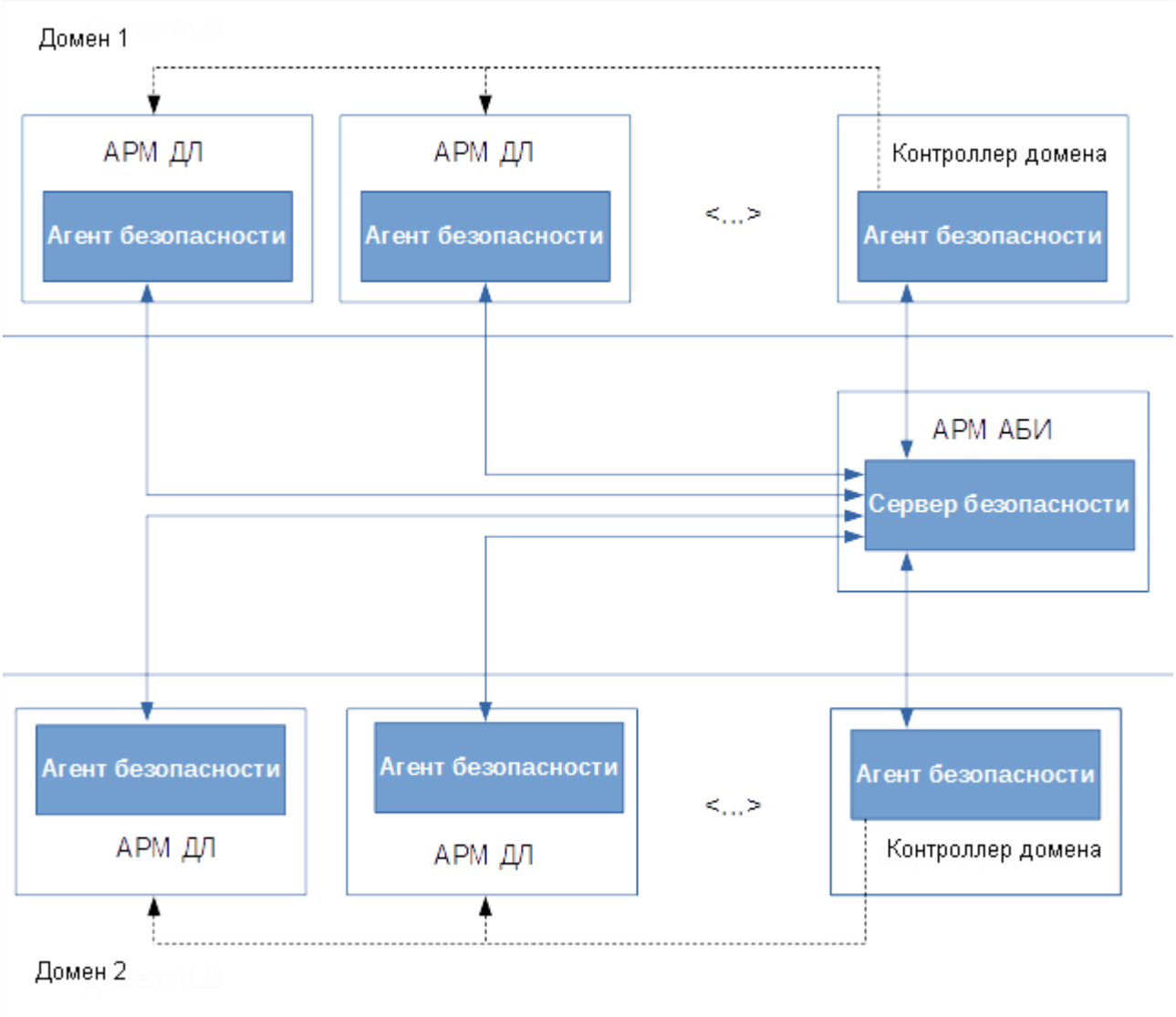

Рис. 2 – Схема взаимодействия сервера безопасности с агентами безопасности

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными является информация, полученная от агентов безопасности, установленных на контролируемых устройствах автоматизированной системы, программного средства анализа событий информационной безопасности, а также информация, полученная от ПС АРМ АБИ автоматизированных систем нижестоящего уровня.

Выходными данными программы является вся отображенная на дисплее (экране) или выведенная на печать текстовая (гипертекстовая) и графическая информация:

- об управляемых устройствах, входящих в состав автоматизированной системы, в том числе от информации о текущем состоянии устройства (устройство выключено/включено, агент ПС АРМ АБИ зарегистрирован/не зарегистрирован, агент отвечает/не отвечает);
- о пользователях автоматизированной системы;
- о состоянии контроля целостности на управляемых устройствах;
- о состоянии антивирусной защиты на управляемых устройствах;
- о результатах тестирования средств защиты информации на управляемых устройствах;
- о состоянии резервного копирования данных контроллера домена;
- о событиях информационной безопасности на управляемых устройствах, полученная от программного средства анализа событий информационной безопасности, в том числе о попытках и фактах НСД к защищаемым ресурсам;
- о событиях информационной безопасности, полученная из автоматизированных систем нижестоящего уровня;
- о перечне защищаемых ресурсов и таблице разграничения доступа к защищаемым ресурсам.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБИ	– администратор безопасности информации
АРМ	– автоматизированное рабочее место
БД	– база данных
ЕПП	– единое пространство пользователей
КП	– комплекс программ
ЛУ	– лист утверждения
НЖМД	– накопитель на жестком магнитном диске
НСД	– несанкционированный доступ
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПС	– программное средство
СГП	– специализированный генератор паролей
СН	– специальное назначение
СУБД	– система управления базами данных
ALD	– Astra Linux Directory (служба доменов Astra Linux)
FreeIPA	– Free Identity, Policy and Audit (свободная идентификация, политика и аудит)

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рован-ных					