Утвержден

РУСБ.30488-04 ЛУ

ПС АРМ АБИ

Руководство системного программиста

РУСБ.30488-04 32 01

Листов 20

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

2019

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является руководством системного программиста Программного средства автоматизированного рабочего места администратора безопасности информации (ПС АРМ АБИ).

Структурно документ состоит из пяти разделов.

В первом разделе указаны назначение и функции ПС АРМ АБИ и сведения о технических и программных средствах, обеспечивающих выполнение данной программы, а также требования к персоналу.

Во втором разделе приведены сведения о структуре ПС АРМ АБИ, его составных частях, о связях между составными частями и о связях с другими программами.

В третьем разделе приведено описание действий по настройке ПС АРМ АБИ на условия конкретного применения.

В четвертом разделе приведено описание способов проверки, позволяющих дать общее заключение о работоспособности.

В пятом разделе указаны тексты сообщений, выдаваемых в ходе выполнения настройки, проверки программы, а также в ходе выполнения программы, описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

Документ предназначен для ознакомления должностным лицам, осуществляющим эксплуатацию ПС АРМ АБИ.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

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» версии 1.6 и выше.

1.2. Функции программы

Программа обеспечивает решение следующих функциональных 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.

1.3. Минимальный состав аппаратных средств

Условием работы программы является наличие технических (аппаратных) средств с параметрами, удовлетворяющими нижеперечисленным 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.

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.

Для инсталляции программы необходимо наличие в ПЭВМ устройства чтения дисков.

1.4. Минимальный состав программных средств

1.4.1. 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;
- защищенная СУБД PostgreSQL.

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

- средства антивирусной защиты (на управляемых устройствах).

1.5. Требования к персоналу (системному программисту)

Системный программист должен иметь минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

- задача поддержания работоспособности технических средств;
- задача установки (инсталляции) и поддержания работоспособности общего программного обеспечения;
- задача установки (инсталляции) и поддержания работоспособности программы.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Сведения о структуре

Структурно программа состоит из двух составных частей:

- клиентская часть;
- серверная часть.

2.2. Сведения о составных частях программы

Клиентская часть, реализованная в виде агента безопасности, устанавливается на все сервера и рабочие станции домена. Агент безопасности функционирует в фоновом режиме как служба и не имеет графического интерфейса.

Серверная часть, реализованная в виде сервера безопасности, устанавливается только на АРМ АБИ. Сервер безопасности предоставляет АБИ эргономичный графический интерфейс для обеспечения автоматизации повседневной деятельности администраторов безопасности информации при выполнении работ на серверах и рабочих станциях домена.

2.3. Сведения о связях между составными частями программы

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

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

2.4. Сведения о связях с другими программами

ПС АРМ АБИ использует компоненты, входящие в состав операционная система специального назначения (ОС СН) «Astra Linux Special Edition» РУСБ.10015-01:

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

Для выполнения сбора и анализа событий информационной безопасности, произошедших на управляемых устройствах, используется система централизованного протоколирования OSSEC.

При выполнении операции генерации паролей пользователей в программе осуществляется вызов компонента «Динамические программные библиотеки» РУСБ.51122-01 из состава изделия КП СГП РУСБ.30563-01.

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Настройка на состав технических средств

Программа не требует каких-либо настроек на состав технических средств.

3.2. Настройка на состав программных средств

Перед началом установки программы необходимо убедиться в том, настроены локальная сеть и требуемые для ее функционирования сетевые службы (DNS, DHCP, NTP и пр.), выполнена установка и первичная настройка средств организации единого пространства пользователей на базе служб организации домена ALD и/или FreeIPA. Дополнительно необходимо убедиться в том, что на серверах БД установлен пакет `postgresql-se-test-9.6` из состава дистрибутива ОС СН «Astra Linux Special Edition». При отсутствии данного пакета необходимо произвести его установку, в соответствии с документом «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 2» РУСБ.10015-01 97 01-2.

Подробная информация о настройке локальной сети, сетевых сервисов, службы организации доменов для управления ЕПП приведена в документе «Операционная система специального назначения “Astra Linux Special Edition”. Руководство администратора» РУСБ.10015-01 95 01.

На устройствах, предназначенных для размещения сервера централизованного протоколирования OSSEC и базы данных сервера безопасности ПС АРМ АБИ, перед началом установки требуется выполнить установку и настройку службы ssh для обеспечения доступа под учётной записью пользователя, имеющего права суперпользователя на данном устройстве.

Внимание! При использования службы организации домена FreeIPA в случае установленного в ОС СН в соответствии с бюллетенем №20190912SE16 кумулятивного обновления необходимо произвести дополнительную настройку службы ssh на устройствах, предназначенных для размещения сервера централизованного протоколирования OSSEC и базы данных сервера безопасности ПС АРМ АБИ. Для этого требуется:

- закомментировать в файле `/etc/ssh/sshd_config` строки:

```
#AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
#GSSAPIAuthentication yes
#ChallengeResponseAuthentication yes
#AuthorizedKeysCommandUser nobody
```

- перезапустить службу ssh, выполнив от имени суперпользователя в окне терминала команду:

```
/etc/init.d/ssh restart
```

После выполнения установки ПС АРМ АБИ требуется вернуть файл `/etc/ssh/sshd_config` в исходное состояние и выполнить перезапуск службы ssh.

Перед началом установки программы также необходимо проверить доступность на управляемом устройстве дистрибутива ОС СН «Astra Linux Special Edition», выполнив от имени суперпользователя в окне терминала команду:

```
apt-get update
```

3.2.1. Установка сервера централизованного протоколирования

Сервер централизованного протоколирования OSSEC устанавливаются в каждом контролируемом домене на одно из управляемых устройств.

Сбор событий информационной безопасности выполняется со всех управляемых устройств контролируемого домена с использованием системного сервиса `rsyslog` с последующей ее обработкой сервером централизованного протоколирования.

Внимание! Установка сервера централизованного протоколирования в домене FreeIPA выполняется пользователем домена admin, создаваемым при инициализации домена.

Для установки сервера централизованного протоколирования необходимо:

- войти в систему под учётной записью пользователя, имеющего права суперпользователя (admin в случае использования службы организации домена FreeIPA);

- выполнить запуск программы «Терминал Fly»;

- получить права суперпользователя путём выполнения команды:

```
sudo –i
```

- установить дистрибутивный носитель в устройство чтения компакт-дисков и монтировать его командой:

```
mount /dev/cdrom /media/cdrom0
```

- перейти в каталог с установочным файлом дистрибутива командой:

```
cd /media/cdrom0/<путь к установочному файлу>
```

- распаковать находящийся на диске архив, выполнив от имени суперпользователя в окне терминала команду:

```
tar –xzvf PsArmAbi.tgz
```

- выполнить от имени суперпользователя в окне терминала команду:

```
Ossec.sh
```

В процессе установки требуется указать значения ряда параметров:

- службу организации домена (ALD или FreeIPA);

- ip-адрес сервера централизованного протоколирования;

- имя и пароль пользователя с правами sudo на сервере централизованного протоколирования (admin при использовании службы организации домена FreeIPA);

- имя и пароль пользователя базы данных сервера централизованного протоколирования.

Значения параметров сохраняются в файлах настройки сервисов системы централизованного протоколирования OSSEC и СУБД PostgreSQL и могут быть отредактированы позднее в текстовом редакторе.

После установки сервера централизованного протоколирования необходимо выполнить перезапуск устройства, выполнив от имени суперпользователя в окне терминала команду:

```
reboot
```

Статус сервиса централизованного протоколирования можно проверить, выполнив от имени суперпользователя в окне терминала команду:

```
systemctl status ossec
```

После установки агентов безопасности на все устройства домена требуется выполнить перезапуск сервиса ossec-hids-server на сервере централизованного протоколирования, выполнив на сервере от имени суперпользователя в окне терминала команду:

```
/etc/init.d/ ossec-hids-server restart
```

3.2.2. Установка сервера безопасности

Сервер безопасности ПС АРМ АБИ устанавливается только на АРМ АБИ.

Внимание! Установка сервера безопасности ПС АРМ АБИ в домене FreeIPA выполняется пользователем домена admin, создаваемым при его инициализации.

Для установки сервера безопасности необходимо выполнить следующее:

- войти в систему под учётной записью пользователя, имеющего права суперпользователя (admin при использовании службы организации домена FreeIPA);

- выполнить запуск программы «Терминал Fly»;

- получить права суперпользователя путём выполнения команды:

```
sudo –i
```

- установить дистрибутивный носитель в устройство чтения компакт-дисков и монтировать его командой:

```
mount /dev/cdrom /media/cdrom0
```

- перейти в каталог с установочным файлом дистрибутива командой:

```
cd /media/cdrom0/<путь к установочному файлу>
```

- распаковать находящийся на диске архив, выполнив от имени суперпользователя в окне терминала команду:

```
tar –xzvf PsArmAbi.tgz
```

- выполнить от имени суперпользователя в окне терминала команду:

```
ArmAbi.sh
```

В процессе установки требуется указать значения ряда параметров:

- службу организации домена (ALD или FreeIPA);

- ip-адрес сервера базы данных ПС АРМ АБИ;

- имя и пароль пользователя с правами sudo на сервере базы данных ПС АРМ АБИ (admin при использовании службы организации домена FreeIPA);

- наименование базы данных ПС АРМ АБИ;

- имя и пароль администратора базы данных ПС АРМ АБИ;

- логин администратора безопасности информации на АРМ АБИ.

Значения параметров сохраняются в файле `/etc/armabi.conf` и в файлах настройки СУБД PostgreSQL и могут быть отредактированы позднее в текстовом редакторе.

В процессе установки сервера безопасности на АРМ АБИ создается локальная группа «abigroup», в которую включается учетная запись администратора безопасности информации. В случае необходимости обеспечения работы с ПС АРМ АБИ под другой учетной записью ее необходимо включить в данную группу, выполнив от имени суперпользователя в окне терминала команду:

```
usermod –a –G abigroup <имя_пользователя>
```

Ярлык для запуска сервера безопасности ПС АРМ АБИ создается в группе «Системные» главного меню системы.

3.2.3. Установка агентов безопасности

Агенты безопасности устанавливаются на все АРМ и сервера (включая АРМ АБИ).

Для установки агента безопасности необходимо:

- войти в систему под учётной записью пользователя, имеющего права суперпользователя (admin при использовании службы организации домена FreeIPA);

- выполнить запуск программы «Терминал Fly»;

- получить права суперпользователя путём выполнения команды:

```
sudo –i
```

- установить дистрибутивный носитель в устройство чтения компакт-дисков и монтировать его командой:

```
mount /dev/cdrom /media/cdrom0
```

- перейти в каталог с установочным файлом дистрибутива командой:

```
cd /media/cdrom0/<путь к установочному файлу>
```

- распаковать находящийся на диске архив, выполнив от имени суперпользователя в окне терминала команду:

```
tar –xzvf PsArmAbi.tgz
```

- выполнить от имени суперпользователя в окне терминала команду:

```
ArmDl.sh
```

В процессе установки требуется указать значения ряда параметров:

- ip адрес АРМ АБИ;

- наличие роли контроллера домена;

- пароль администратора домена;

- ip-адрес сервера централизованного протоколирования.

В случае наличия роли контроллера домена на управляемом устройстве дополнительно требуется указать:

- наименование базы данных сервера централизованного протоколирования;

- имя и пароль пользователя базы данных сервера централизованного протоколирования.

Значения параметров сохраняются в файле `/etc/armdl.conf` и могут быть отредактированы позднее в текстовом редакторе.

При использовании службы организации домена FreeIPA на контроллере домена требуется убедиться, что в файле `/etc/armdl.conf`, значение «IsDomainContr» равно «1»:

```
IsDomainContr=1
```

После завершения установки агента ПС АРМ АБИ рекомендуется включить контроль целостности файлов в директории `/opt/ArmAbi/system/`. Для этого необходимо добавить в файл `/etc/afick.conf` строку

```
/opt/ArmAbi/system/ PARSEC
```

и выполнить от имени суперпользователя в окне терминала команду

```
afick –i
```

Статус сервиса агента безопасности после установки можно проверить, выполнив от имени суперпользователя в окне терминала команду:

```
systemctl status armdl
```

После запуска агента безопасности в файле `/tmp/armdl.log` создается протокол работы, содержащий информацию о подключении к серверу, выполненных командах сервера безопасности и т.д.

После установки агента безопасности происходит попытка его автоматической регистрация на сервере безопасности с выдачей соответствующего сообщения на

сервере безопасности. В случае отсутствия попытки регистрации агента безопасности требуется выполнить от имени суперпользователя в окне терминала команду перезапуска сервиса агента безопасности:

```
systemctl restart armdl
```

При успешной регистрации агента безопасности происходит автоматическое заполнение полей `idDev` и `idDl` в файле `/etc/armdl.conf`.

При необходимости перерегистрации агента безопасности требуется удалить значения параметров `idDev` и `idDl` в файле `/etc/armdl.conf` и выполнить перезапуск сервиса агента безопасности.

3.3. Удаление программы

3.3.1. Удаление агента безопасности

Для удаления агента безопасности необходимо выполнить от имени суперпользователя в окне программы «Терминал Fly» команды:

```
systemctl stop armdl
systemctl disable armdl
rm /etc/armdl.conf
rm –r –f /opt/ArmAbi/system
rm /etc/afick-test.conf
rm /opt/ArmAbi/ArmDl
rm –r –f /opt/ArmAbi/
```

3.3.2. Удаление сервера безопасности ПС АРМ АБИ

Для удаления сервера безопасности необходимо выполнить от имени суперпользователя в окне программы «Терминал Fly» команды:

```
rm /opt/ArmAbi/etc/armabi.conf
rm /opt/ArmAbi/ArmAbi
rm –r –f /opt/ArmAbi/
```

Для удаления базы данных ПС АРМ АБИ необходимо выполнить на сервере базы данных программы от имени суперпользователя в окне программы «Терминал Fly» команды:

```
sudo su postgres
psql -c “drop database <наименование_БД>”
psql -c “drop user <имя_пользователя_БД>”
```

3.3.3. Удаление сервера централизованного протоколирования

Для удаления сервера централизованного протоколирования необходимо выполнить от имени суперпользователя в окне программы «Терминал Fly» команды:

```
systemctl stop ossec
systemctl disable ossec
apt-get remove ossec-hids-server
```

Для удаления базы данных сервера централизованного протоколирования необходимо выполнить на сервере от имени суперпользователя в окне программы «Терминал Fly» команды:

```
sudo su postgres
psql -c “drop database ossec”
psql -c “drop user <имя_пользователя_БД>”
```

4. ПРОВЕРКА ПРОГРАММЫ

4.1. Описание способов проверки

Проверка программы выполняется посредством проверки целостности ПС АРМ АБИ и тестирования его качественных (функциональных) характеристик.

Проверка целостности ПС АРМ АБИ осуществляется посредством проверки целостности носителей информации.

Тестирование качественных (функциональных) характеристик ПС АРМ АБИ осуществляется посредством прогона программы.

4.2. Методы проверки целостности

4.2.1. Проверка целостности носителей информации

Проверка целостности дистрибутивного носителя осуществляется посредством расчета контрольной суммы и ее сравнения со значением, указанным в Формуляре РУСБ.30488-04 30 01.

Для расчета контрольной суммы носителя информации необходимо:

- установить диск в устройство чтения компакт-дисков;

- запустить программу «Терминал Fly»;

- в командной строке ввести команду «`gostsum -d /dev/cdrom`» (для версии ОС СН 1.5 и выше команду «`gostsum -d --gost94 /dev/cdrom`») и нажать клавишу **<Enter>**;

- дождаться завершения работы программы подсчета контрольной суммы;

- сравнить полученное значение со значением контрольной суммы, указанной в Формуляре РУСБ.30488-04 30 01;

- извлечь диск из устройства чтения дисков.

Проверка считается выполненной успешно в случае совпадения контрольной суммы, выданной программой подсчета, со значением контрольной суммы, указанной в Формуляре РУСБ.30488-04 30 01.

4.3. Методы прогона

4.3.1. Запуск программы

Запуск программы осуществляется в соответствии с Руководством оператора РУСБ.30488-04 34 01.

4.3.2. Проверка работы программы

Проверка работы программы состоит в оценке корректности выполнения при работе АБИ нижеперечисленных функций:

- 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 служб организации доменов;
- обнаружение попыток и фактов НСД к защищаемым ресурсам;
- просмотр, печать и экспорт журнала событий информационной безопасности на управляемых устройствах контролируемых доменов за заданный период времени.

4.3.3. Завершение работы программы

Завершение работы программы осуществляется в соответствии с Руководством оператора РУСБ.30488-04 34 01.

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

При установке ПС АРМ АБИ возможно появление сообщения:

«Запустите скрипт с правами суперпользователя»,

при получении данного сообщения требуется получить права суперпользователя, выполнив в окне терминала следующую команду:

```
sudo –i
```

и повторно запустить скрипт установки программы.

В ходе эксплуатации ПС АРМ АБИ возможно появление сообщения:

«О невозможности чтения или переноса лог-файлов из /tmp в /opt/Armabi»,

при получении данного сообщения необходимо выполнить следующее:

- запустить программу «Терминал Fly»;
- от имени суперпользователя выполнить следующую команду:

```
chmod –R (755) abiadmin:Astra-admin /opt/Armabi,
```

где `abiadmin` – наименование учетной записи администратора безопасности информации на АРМ АБИ.

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 № сопроводи- тельного докум. и дата	Подп.	Дата
	изме- ненных	заме- ненных	новых	аннули- рован- ных					
1	1				1	РУСБ.39.04-19			
2		все			20	РУСБ.39.05-19			
3		4, 5, 19			3	РУСБ.39.07-19			