Утвержден

РУСБ.30488-04 ЛУ

ПС АРМ АБИ

Руководство системного программиста

РУСБ.30488-04 32 01

Листов 22

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

2022

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» 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.

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) получение списка процессов, запущенных на управляемом устройстве;

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

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

6) управление доступом пользователей к устройствам домена;

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

8) создание/редактирование учётных записей пользователей;

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

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

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

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

13) формирование и просмотр журналов событий информационной безопасности;

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

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

16) автоблокировка пользователя при возникновении заданных событий НСД;

17) резервное копирование данных (конфигурации) управляемых доменов;

18) резервное копирование и восстановление базы данных программы;

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

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

21) тиражирование правил доступа к отчуждаемым носителям информации.

22) ведение таблицы разграничения доступа пользователей к защищаемым ресурсам;

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

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

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

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 (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 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).

1.5. Требования к персоналу (системному программисту)

Системный программист должен иметь навыки работы с ОС СН «Astra Linux Special Edition» РУСБ.10015-01 на уровне администратора операционной системы.

В перечень задач, выполняемых системным программистом, должны входить:

- задача установки (инсталляции) и настройки ПС АРМ АБИ;
- задача проверки работоспособности ПС АРМ АБИ.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Сведения о структуре

Структурно программа состоит из следующих составных частей:

- клиентская часть (агент безопасности);
- серверная часть (сервер безопасности);
- программное средство анализа событий информационной безопасности (ПС анализа событий ИБ).

2.2. Сведения о составных частях программы

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

Серверная часть устанавливается 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 функционирующих под управлением ОС СН «Astra Linux Special Edition».

Программное средство анализа событий информационной безопасности устанавливается на одном из управляемых устройств (сервер централизованного протоколирования) и функционирует как служба в фоновом режиме.

2.3. Сведения о связях между составными частями программы

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

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 ПС анализа событий ИБ.

2.4. Сведения о связях с другими программами

ПС АРМ АБИ использует компоненты, входящие в состав операционной системы 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 событий информационной безопасности, произошедших на управляемых устройствах, на сервере централизованного протоколирования используется системная служба `rsyslog`.

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

3.2.1. Предварительная подготовка

Установка ПС АРМ АБИ включает в себя следующие шаги:

- установку на всех управляемых устройствах агентов безопасности ПС АРМ АБИ;
- установку на АРМ АБИ сервера безопасности ПС АРМ АБИ;
- установку на одном из управляемых устройств (сервере централизованного протоколирования) ПС анализа событий ИБ.

Перед началом установки программы необходимо:

- убедиться в том, что 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 или FreeIPA. Подробная информация о настройке локальной сети, сетевых сервисов, службы организации домена для управления ЕПП приведена в документе «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора» РУСБ.10015-01 95 01;
- убедиться в том, что на серверах БД установлен пакет `postgresql-se-test`[1] 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;
- на устройстве, предназначенном для размещения базы данных сервера безопасности ПС АРМ АБИ, выполнить установку и настройку службы ssh для обеспечения доступа под учётной записью пользователя, имеющего права суперпользователя, на данное устройстве;
- проверить доступность на управляемом устройстве дистрибутива ОС СН «Astra Linux Special Edition», выполнив от имени суперпользователя в окне терминала команду:

```
apt-get update
```

- выполнить запуск программы «Терминал Fly»;
- получить права суперпользователя, выполнив в окне терминала команду:

```
sudo –i
```

[1] Пакет postgresql-se-test-9.6 устанавливается в ОС СН версии 1.6, пакет postgresql-se-test-11 устанавливается в ОС СН версии 1.7

- установить дистрибутивный носитель в устройство чтения компакт-дисков и смонтировать его, выполнив в окне терминала команду:

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

- перейти в каталог с установочными файлами дистрибутива:

```
cd /media/cdrom0/
```

3.2.2. Установка и настройка агентов безопасности ПС АРМ АБИ

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

Существует два варианта установки агента безопасности:

- ручная установка;

- автоматическая установка.

Для выполнения установки агента безопасности ПС АРМ АБИ необходимо:

- выполнить запуск программы «Терминал Fly»;

- получить права суперпользователя, выполнив в окне терминала команду:

```
sudo –i
```

В случае ручной установки требуется выполнить команду:

- при использовании домена ALD:

```
apt install ./armdl-ald.deb
```

- при использовании домена FreeIPA:

```
apt install ./armdl-freeipa.deb
```

Для автоматической установки требуется запустить скрипт установки, выполнив команду

```
sh ./install_PsArmAbi.sh
```

и выбрать из перечня пункт «Агент безопасности».

В процессе установки агента безопасности требуется:

- указать наличие у устройства роли контроллера домена;

- ip-адрес сервера сбора журналов событий информационной безопасности, обрабатываемых ПС анализа событий ИБ;

- в случае наличия роли контроллера домена на управляемом устройстве дополнительно требуется указать пароль администратора базы данных ПС анализа событий ИБ;

- выбрать вариант определения ip-адреса сервера безопасности ПС АРМ АБИ (автоматический поиск или ручной ввод) и указать ip-адрес;

- указать нужный интерфейс при обнаружении на устройстве нескольких сетевых интерфейсов;

- указать наличие на устройстве установленного ПС РМ АБИ из состава ПАК «Набат».

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

При наличии у устройства роли контроллера домена необходимо убедиться, что в файле /etc/armdl.conf установлено значение «1» параметра «IsDomainContr»:

```
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.

3.2.3. Установка и настройка сервера безопасности ПС АРМ АБИ

Сервер безопасности устанавливается только на АРМ АБИ.

Для выполнения установки сервера безопасности ПС АРМ АБИ необходимо:

- выполнить запуск программы «Терминал Fly»;
- получить права суперпользователя, выполнив в окне терминала команду:

```
sudo –i
```

Существует два варианта установки сервера безопасности:

- ручная установка;

- автоматическая установка.

При ручной установке требуется:

установить драйвер базы данных `libqt5sql5-psql`[1], выполнив команду:

```
dpkg –i ./<название пакета>
```

- выполнить команду:

  - при использовании домена ALD:

  ```
  apt install ./armabi-ald.deb
  ```

  - при использовании домена FreeIPA:

  ```
  apt install ./armabi-freeipa.deb
  ```

Для автоматической установки требуется запустить скрипт установки, выполнив команду

```
sh ./install_PsArmAbi.sh
```

и выбрать из перечня пункт «Сервер безопасности + Агент безопасности».

В процессе установки требуется прочитать и принять лицензионное соглашение и указать значения следующих параметров:

- логин администратора безопасности информации на АРМ АБИ (доменный пользователь);

- пароль администратора доменной службы ALD;

- пароль администратора базы данных сервера ПС АРМ АБИ.

В случае размещения установки БД ПС АРМ АБИ на удаленном хосте требуется убедиться, что на нем установлены и настроены пакеты `ssh` и `postgresql` и указать значения параметров:

- ip – адреса сервера размещения БД ПС АРМ АБИ;

- имя пользователя с правами `sudo` на сервере размещения БД;

- пароль пользователя.

После выполнения установки сервера безопасности ПС АРМ АБИ необходимо согласиться на ее продолжение и выполнить установку агента безопасности в соответствии с 3.2.1.

Значения параметров сохраняются в файле `/opt/ArmAbi/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 доменная группа «abigroup», в которую включается учетная запись администратора безопасности

[1] Пакет libqt5sql5-psql_5.11.0-0astra6_amd64.deb устанавливается в ОС СН версии 1.6, пакет libqt5sql5-psql_5.15.2+0astra4_amd64.deb устанавливается в ОС СН версии 1.7

информации[1]. 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:

- при использовании домена ALD:

```
ald-admin group-mod abigroup --add-users \
--user=<имя пользователя>
```

- при использовании домена FreeIPA:

```
ipa group-add-member abigroup --users=<имя пользователя>
```

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

3.2.4. Установка и настройка ПС анализа событий ИБ

3.2.4.1. Установка ПС анализа событий ИБ

ПС анализа событий ИБ устанавливаются в каждом контролируемом домене на одном из управляемых устройств (сервере централизованного протоколирования)

Сбор событий информационной безопасности выполняется со всех управляемых устройств контролируемого домена с использованием системного сервиса `rsyslog` с последующей ее обработкой ПС анализа событий ИБ.

Для выполнения установки ПС анализа событий ИБ требуется выполнить следующие действия:

- войти в систему под учётной записью пользователя, имеющего права суперпользователя;

- выполнить запуск программы «Терминал Fly»;

- получить права суперпользователя, выполнив в окне терминала команду:

```
sudo –i;
```

Для установки ПС анализа событий ИБ существует два варианта установки:

- ручная установка;

- автоматическая установка.

При ручной установки требуется:

- установить драйвер базы данных `libqt5sql5-psql`[2], выполнив команду:

```
dpkg –i ./<название пакета>
```

- выполнить команду:

```
apt install ./sfincs.deb
```

---

[1] Учетная запись администратора безопасности должна быть создана в домене заранее на этапе настройки домена.

[2] Пакет libqt5sql5-psql_5.11.0-0astra6_amd64.deb устанавливается в ОС СН версии 1.6, пакет libqt5sql5-psql_5.15.2+0astra4_amd64.deb устанавливается в ОС СН версии 1.7

Для автоматической установки требуется запустить скрипт установки, выполнив команду

```
sh ./install_PsArmAbi.sh
```

и выбрать из перечня пункт «ПС анализа событий ИБ + Агент безопасности».

В процессе установки требуется указать пароль администратора базы данных ПС анализа событий ИБ.

После выполнения установки ПС анализа событий ИБ необходимо согласиться на ее продолжение и выполнить установку агента безопасности в соответствии с 3.2.1.

Значения вводимых параметров сохраняются в файлах настройки ПС анализа событий ИБ располагающихся в `/etc/sfincs.conf` и СУБД PostgreSQL и могут быть отредактированы позднее в текстовом редакторе.

Статус сервиса `sfincs.service` ПС анализа событий ИБ можно проверить, выполнив от имени суперпользователя в окне терминала команду:

```
systemctl status sfincs.service
```

Для перезапуска сервиса `sfincs.service` ПС анализа событий ИБ требуется от имени суперпользователя выполнить в окне терминала команду:

```
systemctl restart sfincs.service
```

3.2.4.2. Настройка ПС анализа событий ИБ

Настройка ПС анализа событий ИБ производится изменениями файла /`etc/sfincs.conf`, а также редактированием, добавлением и удалением правил, которые представлены набором json-файлов. Каждому системному журналу присваивается свой файл правил, которых может быть несколько. Соответствия между json-файлом и журналом назначаются в конфигурационном файле.

ПС анализа событий ИБ имеет набор предварительно настроенных правил для централизованного сбора событий вида:

```
{
"id": "1",
"vars":
          [
{
         "name": "<Имя переменной>",
         "type": "<Тип переменной>",
         "template": "reg('<Выражение>')"
               }
          ],
          "conditions" : "${<Имя переменной>} != ''",
```

```
            "actions":
              [
            "alert('<Результат обработки события>',<Группа>,<Уровень
события>)"
              ]
          },
```

Для каждого правила существует свой уникальный идентификатор «id», с помощью которого, создается древовидная структура. У каждого правила может быть любое количество подправил или они могут отсутствовать.

Переменные разделены на два типа: глобальные и локальные. Глобальные и локальные переменные отличаются друг от друга областью видимости. Глобальные переменные действуют на весь json-файл, а локальные только на то правило, где переменная определена, а также на ее дочерние правила.

Структура json-файла:

- "glob_vars": [ ] - Блок, содержащий список глобальных переменных;
- "name": "varName" - Имя переменной;
- "type": "int" - Тип переменной. Переменные могут быть либо числом (**int**), либо текстом (text);
- "template": "reg('(?<=)\w+\[.*\]:')" - Шаблон, по которому будет находиться значение переменной. Данный параметр не обязательный. В шаблоне можно использовать функции reg(), concat() и column();
- "default": "0" - Значение по умолчанию. Также необязательный параметр, который указывается, если не указан шаблон. Нельзя одновременно указывать и шаблон, и значение по умолчанию;
- "lifetime": 120 - Время жизни переменной. В глобальных переменных данный параметр не указывается, так как считается, что глобальные переменные живут все время работы программы;
- "rules": [ ] - Блок, содержащий список правил, по которым будет проверяться сообщение журнала;
- "id": "1" - Номер правила;.
- "vars": [ ] - Структура аналогичная "glob_vars": [ ]. Список локальных переменных, которые существуют как в самом правиле, так и в подправилах данного правила. Если переменные в правиле не нужны, то этот блок можно не писать;

- "conditions": "${varName} != value" - Условие, указывающее на то, подходит ли нам данное правило или нет. В условии используются знаки неравенства >, <, >=, <=, ==, != и логическое И (&&) для составления более сложных условий;

- "actions": [ ] - Список функций, которые необходимо выполнить в случае выполнения условия правила. Если в правиле не нужны никакие функции, то этот блок можно опустить.

Функции в «actions» могут быть:

- let(mathExpression) - данная функция присваивает переменной результат указанной арифметической операции. Например, если в "actions" находится функция "let(varName += 1)" или "let(varName = ${varName} + 1)", то произойдет следующее: переменная varName увеличится на единицу и результат операции будет записан в базу данных;

- alert('msg', {eventGroups}, eventLevel) - данная функция содержит в себе текст сообщения, группы и уровень события, которые будут записаны в таблицу Alerts. Сообщение (msg) - сообщение, которое будет отображаться в таблице alerts, в случае выполнения правила. Группа (eventGroups) - массив групп событий. Массив должен находиться в фигурных скобках! Уровень события (eventLevel) - уровень события, должен быть от 1 до 5;

- reg('regExp', var) - функция, которая находит совпадение в сообщении журнала или переменной в соответствии с указанным регулярным выражением. regExp - регулярное выражение. var - переменная, в значении которой будет искаться то или иное совпадение. Данный параметр необязательный. Если данный параметр не указан, то все совпадения будут искаться в строке лога;

- column('delimiter', firstNum, var) - аналог функции awk, то есть выделение столбца из строки, разделенного конкретным разделителем: delimiter - разделитель, которым может быть знак, слово или переменная. firstNum - номер столбца, который необходимо получить. var - переменная, в значении которой будет находиться указанный разделитель;

- concat(someVarsOrText) — эта функция объединяет строки, которые записаны внутри функции: someVarsOrText - либо переменные, либо некий текст и переменные, которые объединятся в одну строку.

3.3. Удаление программы

Для удаления ПС АРМ АБИ требуется выполнить от имени суперпользователя в окне терминала команду:

- для удаления сервера безопасности:

```
apt remove armabi
```

- для удаления агента безопасности

```
apt remove armdl;
```

- для удаления ПС анализа событий ИБ:

```
apt remove sfincs
```

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 дистрибутивных носителей информации.

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

4.2. Проверка целостности дистрибутивных носителей информации

Проверка целостности дистрибутивных носителей информации осуществляется посредством расчета их контрольных сумм и сравнения со значениями, указанными в документе «ПС АРМ АБИ. Формуляр» РУСБ.30488-04 30 01.

Для расчета контрольной суммы носителя информации необходимо:

- установить необходимый диск в устройство чтения дисков;

- нажав комбинацию клавиш **<Alt+T>**, выполнить запуск программы «Terminal Fly»;

- ввести в командной строке команду `gostsum -d /dev/cdrom` и нажать клавишу **<Enter>**;

- дождаться завершения работы программы подсчета контрольной суммы;

- сравнить полученное значение со значением контрольной суммы, указанной в документе «ПС АРМ АБИ. Формуляр» 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 документе «ПС АРМ АБИ. Формуляр» РУСБ.30488-04 30 01.

4.3. Методы прогона

4.3.1. Запуск программы

Запуск программы осуществляется в соответствии с документом «ПС АРМ АБИ. Руководство оператора» РУСБ.30488-04 34 01.

4.3.2. Проверка работы программы

Проверка работы программы состоит в оценке корректности выполнения при работе АБИ функционала, приведенного в 1.2 настоящего документа, в соответствии с документом «ПС АРМ АБИ. Руководство оператора» РУСБ.30488-04 34 01.

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 появлении данного сообщения выполнить 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 следующие действия:

- 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
ИБ	– информационная безопасность
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					