Утвержден

РУСБ.30666-01-ЛУ

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

ПС РМ АБИ

Руководство системного программиста

РУСБ.30666-01 32 01

Листов 20

2016

Литера $О_1$

АННОТАЦИЯ

Данный документ является Руководством системного программиста программного средства рабочего места администратора безопасности информации (ПС РМ АБИ) РУСБ.30666-01.

Структурно документ состоит из пяти разделов.

В первом разделе указаны назначение и функции ПС РМ 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 РМ АБИ, его составных частях, о связях между составными частями и о связях с другими программами.

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

В четвертом разделе приведено описание способов проверки, позволяющих дать общее заключение о работоспособности программы (контрольные примеры, методы прогона, результаты).

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 РМ АБИ.

СОДЕРЖАНИЕ

1. Общие сведения о программе....4
1.1. Назначение программы....4
1.2. Функции программы....4
1.3. Минимальный состав аппаратных средств....4
1.4. Минимальный состав программных средств....5
1.5. Требования к персоналу (системному программисту)....5
2. Структура программы....6
2.1. Сведения о структуре....6
2.2. Сведения о составных частях программы....6
2.3. Сведения о связях между составными частями программы....6
2.4. Сведения о связях с другими программами....6
3. Настройка программы....7
3.1. Настройка на состав технических средств....7
3.2. Настройка на состав программных средств....7
3.2.1. Установка ПС РМ АБИ....7
3.2.2. Настройка ПС РМ АБИ....7
4. Проверка программы....9
4.1. Описание способов проверки....9
4.2. Методы проверки целостности....9
4.2.1. Проверка целостности дистрибутивного носителя....9
4.2.2. Проверка соответствия установленных файлов дистрибутиву....9
4.3. Методы прогона....10
4.3.1. Запуск программы....10
4.3.2. Проверка работы программы....10
4.3.3. Завершение работы программы....16
5. Сообщения системному программисту....17
5.1. Сообщения об ошибках....17
5.2. Предупреждения....17
Перечень сокращений....19

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

ПС РМ АБИ предназначено для автоматизации повседневной деятельности администраторов безопасности информации (АБИ), связанной с задачами обеспечения контроля доступа к оборудованию охраняемого объекта.

1.2. Функции программы

ПС РМ АБИ обеспечивает возможность выполнения перечисленных ниже функций:

- визуальная и акустическая сигнализация на АРМ нарушителя по команде АБИ, а также из прочих программных средств АРМ АБИ с использованием интерфейса межпрограммного взаимодействия;
- отображение состояния охранных шлейфов (снят с охраны, дежурный режим, неисправность шлейфа, тревога);
- визуальное оповещение АБИ при наступлении событий НСД по выбранным охранным шлейфам;
- корректировка АБИ наименований охранных контролеров и их шлейфов, а также создание логических групп контролеров и шлейфов по принадлежности к контролируемым техническим средствам и их элементам;
- постановка/снятие с охраны выбранных технических средств и их элементов (шлейфов, контролеров и их логических групп);
- протоколирование событий НСД, а также изменений состояний всех охранных шлейфов системы в БД (в том числе удаленную БД посредством ЛВС);
- управление (сортировка, поиск) и просмотр журналов (протоколов) событий, в том числе сохранение на носители информации и выведение на печать в виде отчета (с возможностью отбора необходимой информации).

1.3. Минимальный состав аппаратных средств

Минимальный состав и характеристики используемых технических (аппаратных) средств:

- тактовая частота центрального процессора – не менее 2 Ггц;
- емкость оперативной памяти – не менее 1 Гб;
- разрешение монитора - не менее 1280 x 1024 пикселей.

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

1.4. Минимальный состав программных средств

ПС РМ АБИ предназначено для функционирования в операционной системе специального назначения (ОС СН) «Astra Linux Special Edition» РУСБ.10015-01 с версией ядра не ниже 3.16.0.

Общее программное обеспечение, необходимое для функционирования ПС РМ АБИ, включает в себя входящую в состав ОС СН «Astra Linux Special Edition» защищенную СУБД PostgreSQL.

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 ПС РМ АБИ.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Сведения о структуре

ПС РМ АБИ состоит из одной запускаемой формы.

2.2. Сведения о составных частях программы

ПС РМ АБИ состоит из одной запускаемой формы и не имеет составных частей.

2.3. Сведения о связях между составными частями программы

ПС РМ АБИ не имеет составных частей.

2.4. Сведения о связях с другими программами

В ПС РМ АБИ реализован функционал получения информации о попытках и фактах НСД из других программ использованием интерфейса межпрограммного взаимодействия.

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Настройка на состав технических средств

Настройка ПС РМ АБИ для работы с ПТК КУ РУСБ.461263.178 выполняется непосредственно из программы после ее установки и заключается в настройке соединения с БЦП.

3.2. Настройка на состав программных средств

3.2.1. Установка ПС РМ АБИ

Перед установкой программы необходимо убедиться в доступности дистрибутива ОС СН «Astra Linux Special Edition», выполнив от имени суперпользователя в окне терминала команду:

```
apt-get update
```

Для инсталляции ПС РМ АБИ необходимо

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

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

- запустить программу «Терминал Fly” перейти в каталог с установочным файлом дистрибутива командой:

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

- выполнить от имени суперпользователя в окне терминала команду:

```
./install.sh
```

В процессе установки БД требуется ввести значения следующих параметров:

- ip-адрес сервера БД ПАК «Набат»;

- имя и пароль пользователя с правами `sudo` на сервере БД ПАК «Набат»;

- имя и пароль администратора БД ПАК «Набат».

В случае успешной установки в окне программы «Терминал Fly» появляется сообщение «Установка успешно завершена», а в группе «Системные» раздела «Программы» главного меню операционной системы создается ярлык «ПС РМ АБИ» для запуска программы.

Для обеспечения работоспособности программы в условиях замкнутой программной среды в версии 1.6 ОС СН «Astra Linux Special Edition» требуется выполнить установку входящего в состава операционной системы пакета astra-digsig-oldkey, выполнив в окне терминала команду

```
apt-get install astra-digsig-oldkey
```

3.2.2. Настройка ПС РМ АБИ

После выполнения установки ПС РМ АБИ требуется выполнить настройку соединения ПС РМ АБИ с БЦП. Для этого необходимо выполнить запуск программы, открыть пункт «Управление» основного меню программы и выбрать подпункт «Добавить БЦП». В окне «Добавить БЦП» (рис. 1) требуется ввести значения полей «Серийный номер БЦП», « IP-адрес БЦП» и «Порт» и нажать кнопку **«Сохранить»**.

Значения полей «Серийный номер БЦП», « IP-адрес БЦП» и «Порт» устанавливаются при настройке БЦП в соответствии с документом «ПАК «НАБАТ» Инструкция по монтажу, пуску, регулированию и обкатке изделия» РУСБ.461263.177 ИМ.

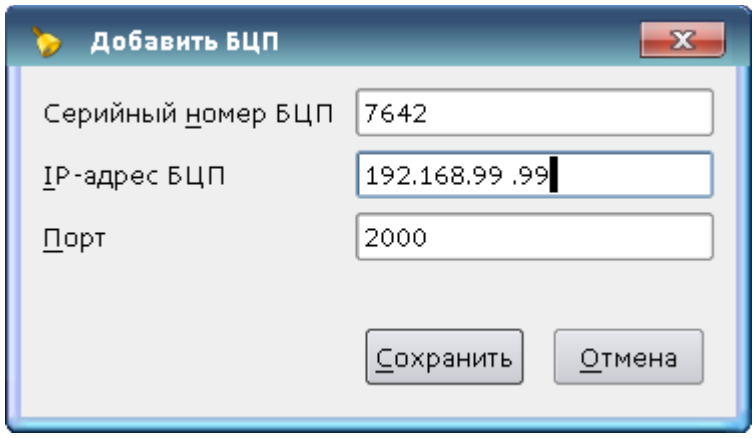


Рис. 1 – Настройка соединения с БЦП

При успешной установке соединения с БЦП происходит обновление конфигурации объектов БЦП в БД ПАК «Набат» (рис. 2).

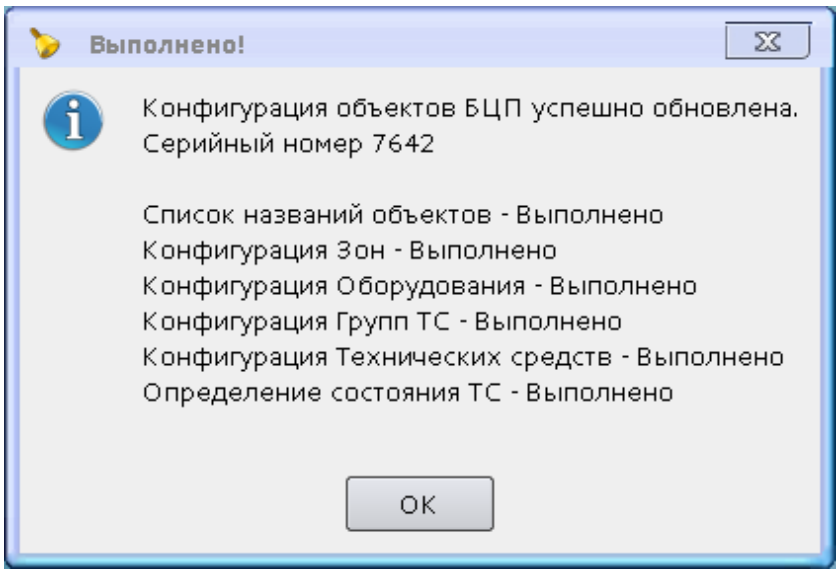


Рис. 2 – Обновление конфигурации объектов БЦП

4. ПРОВЕРКА ПРОГРАММЫ

4.1. Описание способов проверки

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

Выполнение целостности ПС РМ АБИ осуществляется посредством проверки целостности дистрибутивного носителя и проверки соответствия установленных файлов дистрибутиву.

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

4.2. Методы проверки целостности

4.2.1. Проверка целостности дистрибутивного носителя

Проверка целостности дистрибутивного носителя осуществляется посредством расчета контрольной суммы и ее сравнения со значением, указанным в Формуляре.

Для расчета контрольной суммы дистрибутива необходимо:

- установить диск с дистрибутивом в устройство чтения дисков;

- ввести в командной строке команду команду «`gostsum -d /dev/cdrom`» (для версии ОС СН 1.5 и выше команду «`gostsum --gost-94 -d /dev/cdrom`») и нажать клавишу **<Enter>**;

- дождаться завершения работы программы подсчета контрольной суммы;

- сравнить полученное значение со значением контрольной суммы, указанной в разделе 3 Формуляра РУСБ.30666-01 30 01;

- извлечь диск из устройства чтения дисков.

Проверка считается выполненной успешно в случае совпадения контрольной суммы, выданных программой подсчета, со значением контрольной суммы, указанной в разделе 3 Формуляра РУСБ.30666-01 30 01.

4.2.2. Проверка соответствия установленных файлов дистрибутиву.

Проверка соответствия установленных файлов дистрибутиву осуществляется посредством сверки контрольных сумм файлов со значениями, указанными во включенном в состав дистрибутива файле `md5sum.txt`.

Для выполнения проверки необходимо установить диск с дистрибутивом в устройство чтения дисков и выполнить в программе «Терминал» команду

```
md5sum -c md5sum.txt
```

Убедиться в отсутствии сообщений о нарушении целостности.

4.3. Методы прогона

4.3.1. Запуск программы

Запуск программы осуществляется в соответствии с Руководством оператора РУСБ.30666-01 34 01.

4.3.2. Проверка работы программы

Проверка работы программы состоит в оценке корректности выполнения ПС РМ БИ ниже перечисленных функций (при необходимости допускается проведение проверки только по выбранным зонам, группам технических средств, или отдельным техническим средствам, за исключением проверок проводимых в соответствии с разделом 7 «ПАК «Набат» Инструкция по монтажу, пуску, регулированию и обкатке изделия» РУСБ.461263.177 ИМ в ходе развертывания изделия ПАК «Набат» на объекте заказчика).

4.3.2.1. Визуальное оповещения АБИ при наступлении события НСД

Для проведения данной проверки необходимо :

- перейти на вкладку «Управление»;
- все зоны объекта охраны (выбранные зоны, группы ТС, или отдельные ТС) перевести в режим «Поставлен на охрану» (рис. 3).

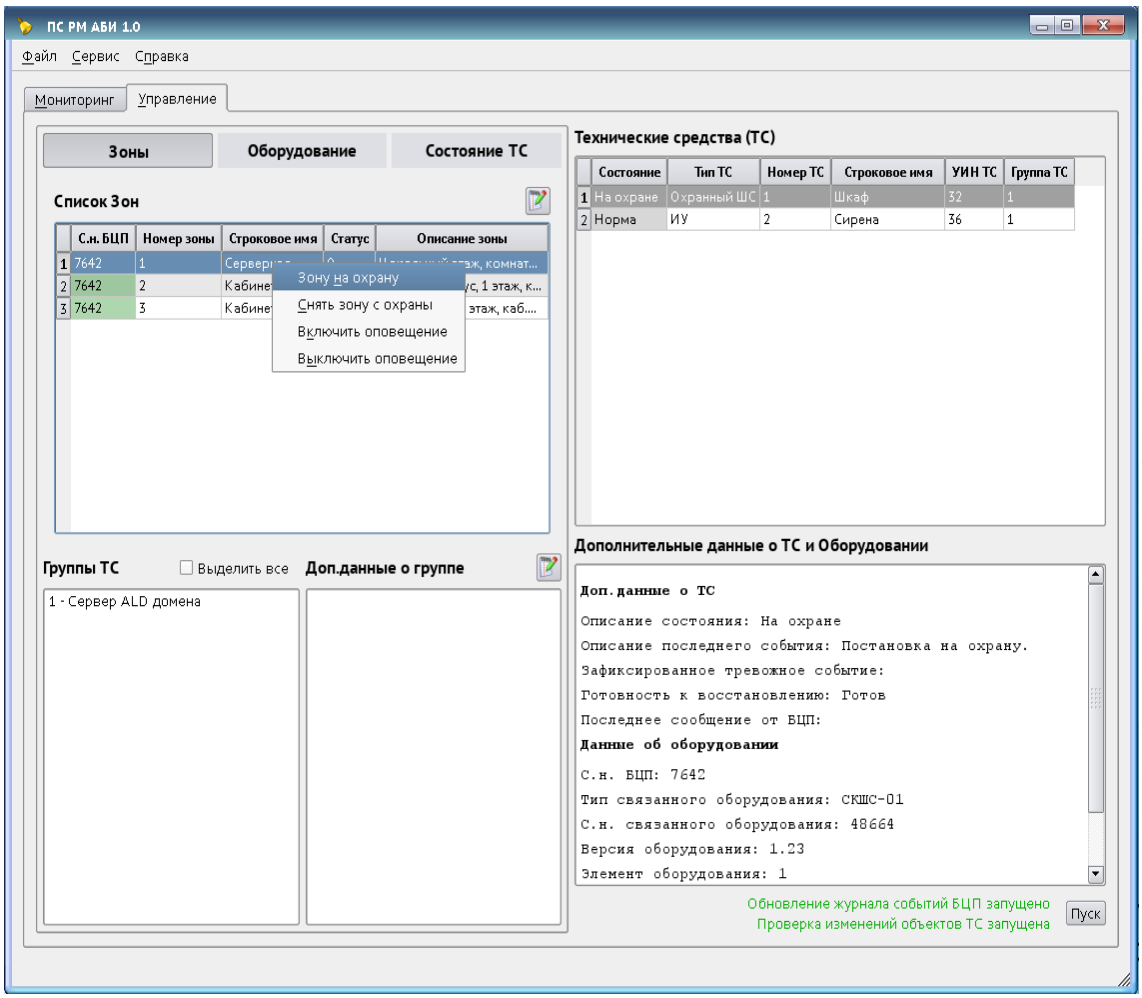


Рис. 3 – Постановка зоны на охрану

Проверка осуществляется путем принудительного создания события НСД (вскрытия системных блоков АРМ, открытия дверей серверных стоек и т.д.). При этом на экране монитора АРМ АБИ должны отображаться оповещения о событии в виде отдельного сообщения, с наименованием «ТС», «Группы ТС» и «Зоны», на которых произошло событие НСД.

4.3.2.2. Возможность визуальной и акустической сигнализации на АРМ нарушителя по команде АБИ

Для проведения данной проверки необходимо необходимо:

- перейти на вкладку «Управление»;

- в окне «Группы ТС» нажать правой кнопкой мыши на «АРМ нарушителя» и в появившемся окне выбрать пункт «Включить оповещение» (рис. 4). Убедиться в том, что по команде администратора на «АРМ нарушителя» происходит срабатывание светового и звукового оповещателей (комбинированного светозвукового оповещателя) (установленного в непосредственной близости от «АРМ нарушителя»).

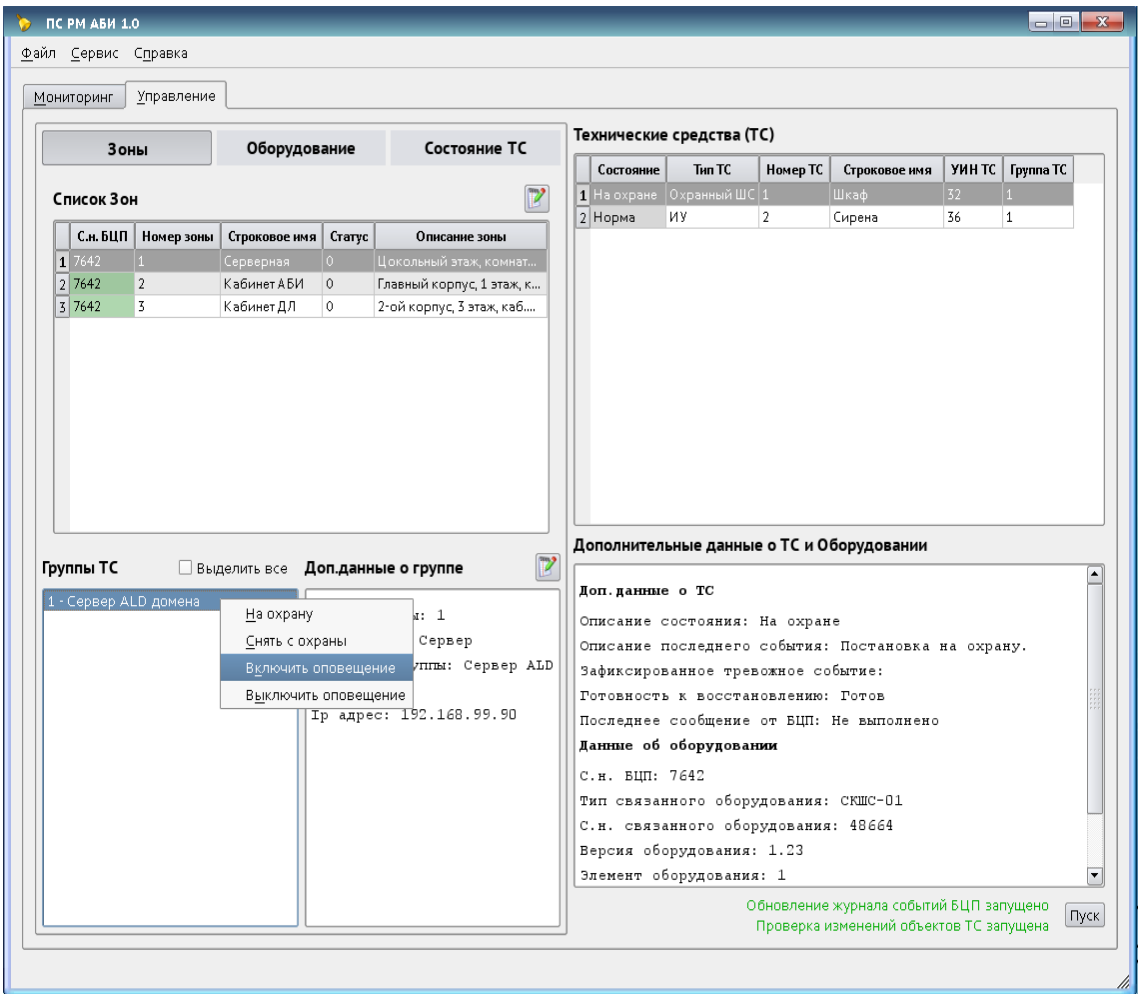


Рис. 4 – Включение оповещения

4.3.2.3. Отображение состояния охранных шлейфов (снят с охраны, дежурный режим, неисправность шлейфа, тревога);

Для проведения данной проверки необходимо

- перейти на вкладку «Управление»;

- в окне «Группы ТС» выбрать любое защищаемое устройство (ПЭВМ, стойка сервера и т.д.), нажав на него левой кнопкой мыши (проверка производится поочередно на всех защищаемых устройствах);

- в окне «Технические средства (ТС)» должны отобразиться все подключенные к выбранному устройству охранные шлейфы (извещатели (герконы и (или) микропереключатели) и оповещатели (светодиод, сирена);

- поочередно нажимая правой кнопкой мыши на все ТС, менять их состояние: поставлен «на охрану»(рис. 5), «снят с охраны» (рис. 6);

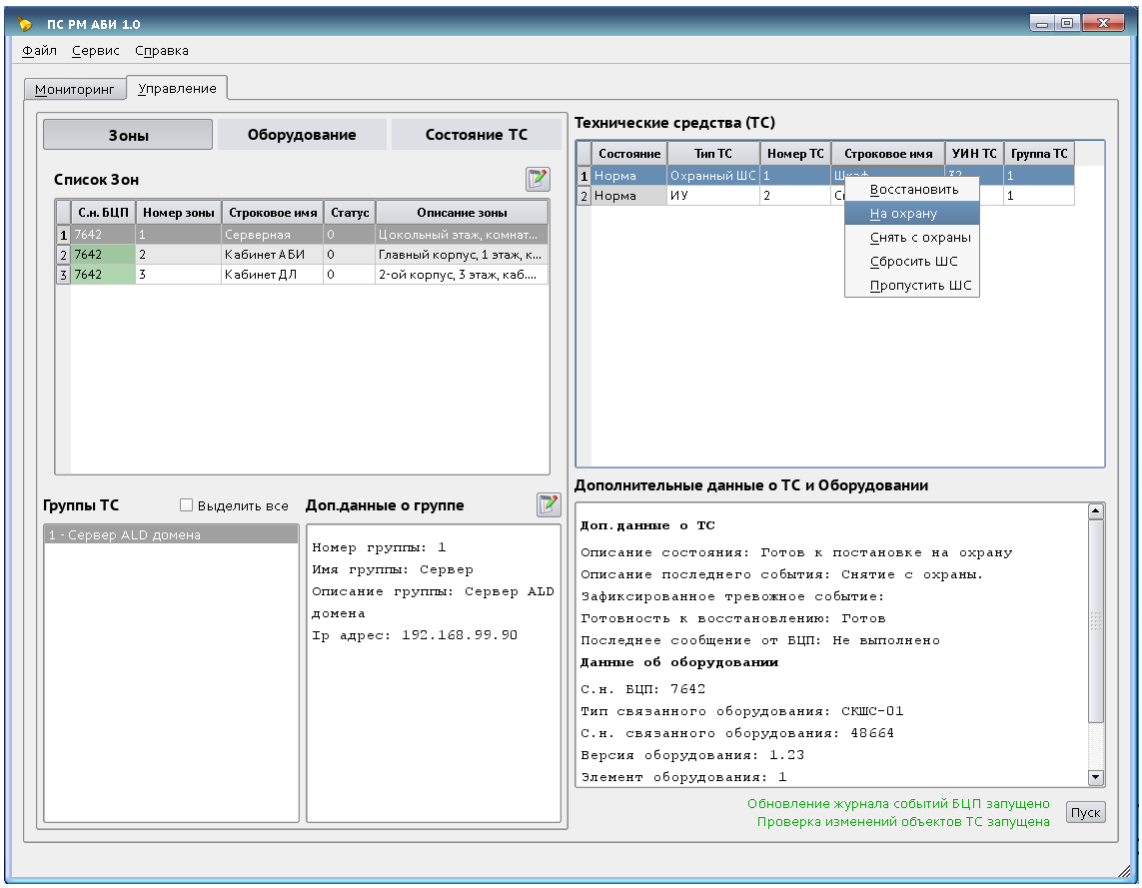


Рис. 5 – Постановка ТС на охрану

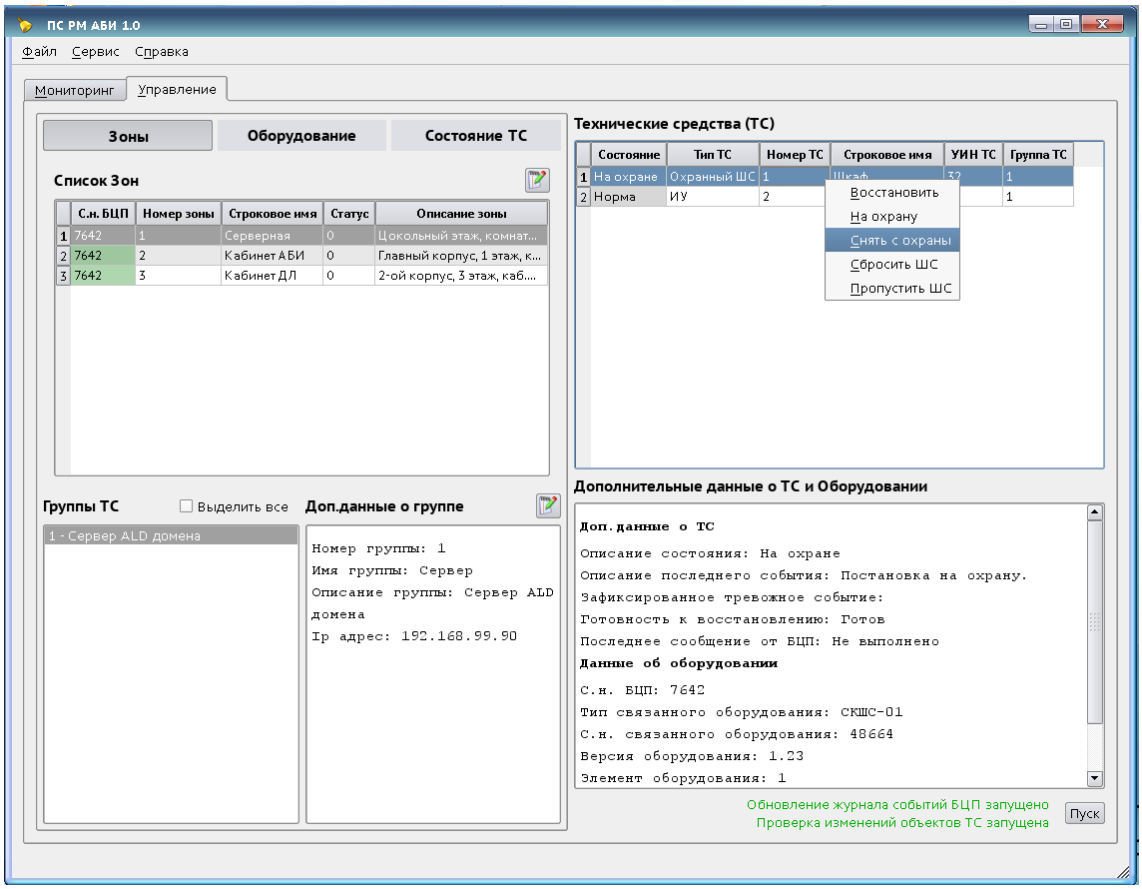


Рис. 6 – Снятие ТС с охраны

- убедиться, что в окне «Дополнительные данные о ТС» должно меняться его состояние;

- проверить отображение состояния «тревога» и «неисправность шлейфа», проводится при состоянии любого из ТС в режим «поставлен на охрану»;

- для проверки состояния «тревога», необходимо принудительно создать событие НСД (вскрыть системный блок АРМ, открыть дверь серверной стойки и т.д.), при этом в окне «Дополнительные данные о ТС», должно отобразиться состояние «тревога»;

- для проверки состояния «неисправность шлейфа», необходимо поочередно на всех извещателях (геркона и (или) микропереключатели) и оповещателях (светодиод, сирена) выбранного устройства сначала отсоединить один из контактов охранного шлейфа, затем восстановить контакт и перевести состояние ТС в «Норма», после закоротить контакты между собой. При этом каждый раз при разрыве контактов и при их закорачивании в окне «Дополнительные данные о ТС», должно отображаться состояние «неисправность шлейфа».

4.2.3.4. Возможность постановки/снятия с охраны выбранных технических средств (оборудования) и их элементов (шлейфов, контролеров и их логических групп);

Для проведения данной проверки необходимо все зоны объекта охраны (выбранные зоны, группы ТС, или отдельные ТС) необходимо:

- перейти на вкладку «Управление»;

- в окне «Группы ТС» нажать правой кнопкой мыши на любую группу (АРМ, серверная стойка и т.д.), выбрать «поставлен на охрану», при этом в окне «Дополнительные данные о ТС» должно отобразиться соответствующее состояние;

-для проверки постановки выбранного технического средства (оборудования) на охрану необходимо принудительно создать событие НСД (вскрыть системный блок АРМ, открыть дверь серверной стойки и т. д.), при этом на экран монитора АРМ АБИ, должно быть выведено сообщение о наступившем событии НСД и одновременно должны сработать соответствующие световые и звуковые оповещатели (комбинированные светозвуковые оповещатели);

- для проверки снятия с охраны технических средств (оборудования) в окне «Группы ТС» требуется нажать правой кнопкой мыши на любую группу (АРМ, серверная стойка и.т.д.), выбрать «снятие с охраны», при этом в окне «Дополнительные данные о ТС» должно отобразиться соответствующее состояние. Для проверки снятия выбранного технического средства (оборудования) с охраны необходимо принудительно создать событие НСД (вскрыть системный блок АРМ, открыть дверь серверной стойки и т. д.). При этом на экран монитора ПЭВМ не должны выводиться никакие сообщения и не должно происходить срабатывание соответствующих световых и звуковых оповещателей (комбинированных светозвуковых

оповещателей);

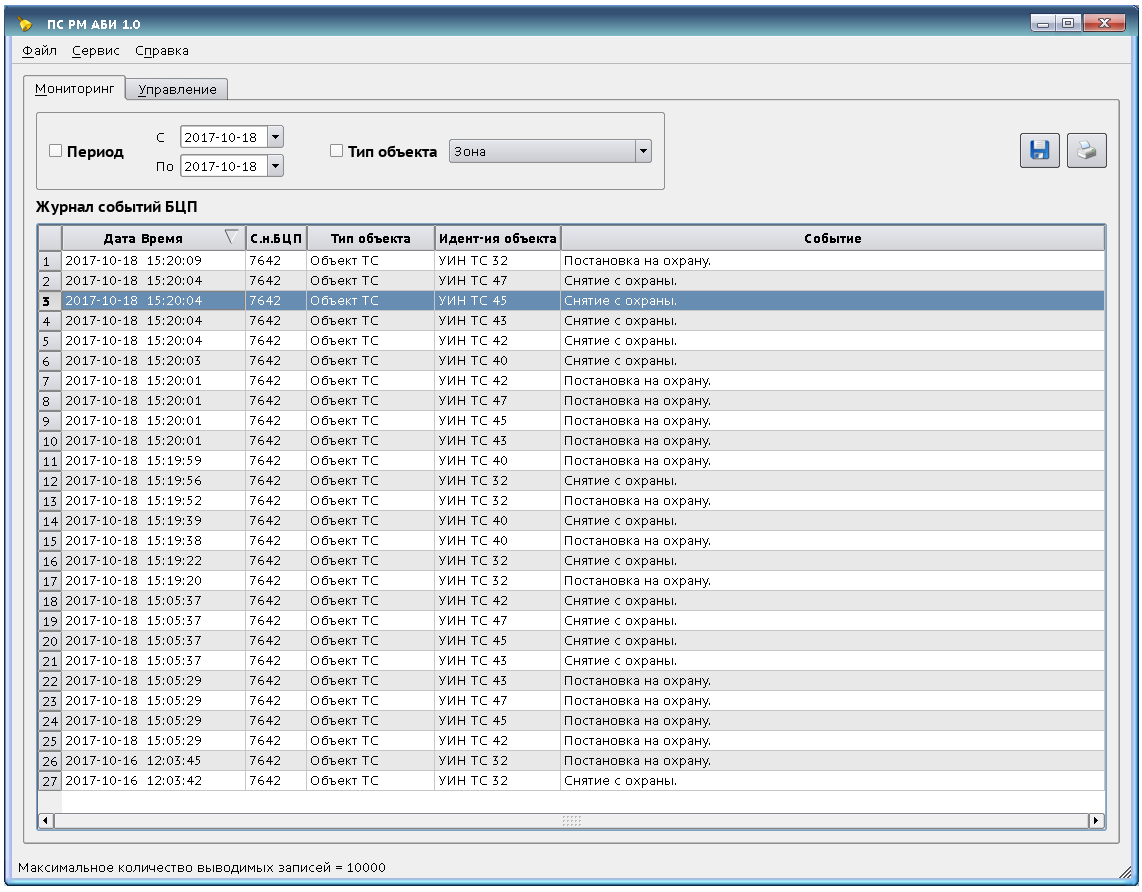
- проверка постановки/снятия с охраны элементов технического средства (оборудования) проводится аналогично, в окне «Технические средства (ТС)», нажимаем правой кнопкой мыши на выбранный охранный шлейф, сначала выбрать «постановка на охрану», проверить ее, принудительно создав событие НСД с выбранным элементом (отображение соответствующего сообщения на экране монитора ПЭВМ и срабатывание охранной сигнализации), затем выбрать «снятие с охраны», убедиться в отсутствии сообщения и срабатывания охранной сигнализации, при переводе соответствующего элемента в состояние тревоги.

4.2.3.5. Проверка протоколирования событий НСД, а также изменений состояний всех охранных шлейфов системы в БД (в том числе в удаленной БД посредством ЛВС):

Для проведения данной проверки необходимо :

- перейти на вкладку «Мониторинг» (рис. 7);

- убедиться в том, что все события, сгенерированные ранее проведенными проверками, отображены в окне «Журнал событий».



	Дата Время	С.н.БЦП	Тип объекта	Идент-ия объекта	Событие
1	2017-10-18 15:20:09	7642	Объект ТС	УИН ТС 32	Постановка на охрану.
2	2017-10-18 15:20:04	7642	Объект ТС	УИН ТС 47	Снятие с охраны.
3	2017-10-18 15:20:04	7642	Объект ТС	УИН ТС 45	Снятие с охраны.
4	2017-10-18 15:20:04	7642	Объект ТС	УИН ТС 43	Снятие с охраны.
5	2017-10-18 15:20:04	7642	Объект ТС	УИН ТС 42	Снятие с охраны.
6	2017-10-18 15:20:03	7642	Объект ТС	УИН ТС 40	Снятие с охраны.
7	2017-10-18 15:20:01	7642	Объект ТС	УИН ТС 42	Постановка на охрану.
8	2017-10-18 15:20:01	7642	Объект ТС	УИН ТС 47	Постановка на охрану.
9	2017-10-18 15:20:01	7642	Объект ТС	УИН ТС 45	Постановка на охрану.
10	2017-10-18 15:20:01	7642	Объект ТС	УИН ТС 43	Постановка на охрану.
11	2017-10-18 15:19:59	7642	Объект ТС	УИН ТС 40	Постановка на охрану.
12	2017-10-18 15:19:56	7642	Объект ТС	УИН ТС 32	Снятие с охраны.
13	2017-10-18 15:19:52	7642	Объект ТС	УИН ТС 32	Постановка на охрану.
14	2017-10-18 15:19:39	7642	Объект ТС	УИН ТС 40	Снятие с охраны.
15	2017-10-18 15:19:38	7642	Объект ТС	УИН ТС 40	Постановка на охрану.
16	2017-10-18 15:19:22	7642	Объект ТС	УИН ТС 32	Снятие с охраны.
17	2017-10-18 15:19:20	7642	Объект ТС	УИН ТС 32	Постановка на охрану.
18	2017-10-18 15:05:37	7642	Объект ТС	УИН ТС 42	Снятие с охраны.
19	2017-10-18 15:05:37	7642	Объект ТС	УИН ТС 47	Снятие с охраны.
20	2017-10-18 15:05:37	7642	Объект ТС	УИН ТС 45	Снятие с охраны.
21	2017-10-18 15:05:37	7642	Объект ТС	УИН ТС 43	Снятие с охраны.
22	2017-10-18 15:05:29	7642	Объект ТС	УИН ТС 43	Постановка на охрану.
23	2017-10-18 15:05:29	7642	Объект ТС	УИН ТС 47	Постановка на охрану.
24	2017-10-18 15:05:29	7642	Объект ТС	УИН ТС 45	Постановка на охрану.
25	2017-10-18 15:05:29	7642	Объект ТС	УИН ТС 42	Постановка на охрану.
26	2017-10-16 12:03:45	7642	Объект ТС	УИН ТС 32	Постановка на охрану.
27	2017-10-16 12:03:42	7642	Объект ТС	УИН ТС 32	Снятие с охраны.

Рис. 7 – Вкладка «Мониторинг»

4.2.3.6. Управление (сортировка, поиск) и просмотр журналов (протоколов) событий, в том числе сохранения на носители информации и выведения на печать в

виде отчета (с возможностью отбора необходимой информации).

Для проведения данной проверки необходимо :

- перейти на вкладку «Мониторинг»;

- в поле фильтры, ввести необходимые реквизиты поиска (даты с, по, наименование «ТС», или «группы ТС», тип события), затем нажать кнопку **[Применить].** В окне «Журнал событий» должен отобразиться журнал, отфильтрованный с учетом введенных реквизитов;

- для проверки сохранения необходимо нажать кнопку **[Сохранить].** Во всплывающем окне, ввести имя файла, затем нажать клавишу «сохранить». Открыть сохраненный файл в любом имеющемся текстовом редакторе и убедиться в наличии выбранных событий;

- для проверки печати после формирования отфильтрованного с учетом введенных реквизитов журнала, необходимо нажать кнопку **[Печать]**. Во всплывающем окне выбрать печатающее устройство и нажать кнопку **[Печать].** Убедиться в том, что на печать выведены выбранные события.

4.3.3. Завершение работы программы

Завершение работы программы осуществляется в соответствии с Руководством оператора РУСБ.30666-01 34 01.

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

5.1. Сообщения об ошибках

При эксплуатации ПС РМ АБИ возможно появление нижеперечисленных сообщений об ошибках:

- «Не удалось установить соединение с БД!»;

В случае появления данного сообщения об ошибке необходимо проверить доступность сервера БД ПАК «Набат», выполнив в окне терминала команду

```
ping <ip-адрес сервера БД>
```

При успешном выполнении команды `ping` необходимо проверить настройки конфигурации на сервере БД для соединения с АРМ АБИ:

- проверить в файле `etc/postgresql/9.X/main/postgresql.conf` значение параметра `listen_adress (по умолчанию 'localhost')` и разрешить соединение с АРМ АБИ, установив соответствующее значение;

- проверить наличие в файле `etc/postgresql/9.X/main/pg_hba.conf` следующих строк:

```
local nabat <логин администратора БД> pam
host nabat <логин администратора БД> <ip-адрес АРМ АБИ>:32 pam
```

При сохранении сообщения об ошибке требуется выполнить повторную установку программы в соответствии с разделом 3.

- «Не удалось установить соединение с БЦП!»;

В случае появления данного сообщения об ошибке необходимо проверить доступность БЦП, выполнив в окне терминала команду:

```
ping <ip-адрес БЦП>
```

При успешном выполнении команды `ping` необходимо открыть пункт «Управление» основного меню программы, выбрать подпункт «Соединение с БЦП» и нажать кнопку **«Выполнить»**.

При сохранении сообщения об ошибке требуется выполнить повторную установку программы в соответствии с разделом 3.

5.2. Предупреждения

При эксплуатации ПС РМ АБИ возможно появление нижеперечисленных предупреждений:

- «Найдены различия в конфигурациях в БД и БЦП»;

В случае появления данного предупреждения необходимо обновить

конфигурацию в БД. Для этого требуется открыть пункт «Управление» основного меню программы и выбрать подпункт «Загрузка конфигурации».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБИ	– администратор безопасности информации
АРМ	– автоматизированное рабочее место
БД	– база данных
БЦП	– блок центральный процессорный
КП	– комплекс программ
КУ	– контроль и управление
НСД	– несанкционированные действия
ОС	– операционная система
ПС	– программное средство
ПТК	– программно-технический комплекс
РМ	– рабочее место
СН	– специальное назначение
СУБД	– система управления базами данных
ТС	– техническое сресдтво

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного документа и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	анну-лирован-ных					
3		все			20	РУСБ.39.06-17			
4		7, 8, 10, 13, 14, 17			6	РУСБ.39.02-18			
5		7,8			2	РУСБ.39.03-19			