Утвержден

РУСБ.30666-01-ЛУ

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

ПС РМ АБИ

Руководство оператора

РУСБ.30666-01 34 01

Листов 16

2016

Литера $О_1$

АННОТАЦИЯ

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

Структурно документ состоит из четырех разделов.

В первом разделе указаны сведения о назначении ПС РМ АБИ и информация, достаточная для понимания функций ПС РМ АБИ и его эксплуатации.

Во втором разделе указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).

В третьем разделе указана последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, приведено описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы, а также ответы программы на эти команды.

В четвертом разделе приведены тексты сообщений, выдаваемых в ходе выполнения программы, описание их содержания и соответствующие действия оператора (действия оператора в случае сбоя, возможности повторного запуска программ и т.п.).

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

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Функциональное 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. Эксплуатационное назначение программы

ПС РМ АБИ должен эксплуатироваться в профильных подразделениях на объектах заказчика. Пользователями ПС РМ АБИ должны являться сотрудники профильных подразделений объектов заказчика.

ПС РМ АБИ может эксплуатироваться в круглосуточном непрерывном режиме.

1.3. Состав функций

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).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Минимальный состав аппаратных средств

Минимальный состав и характеристики 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 .

2.2. Минимальный состав программных средств

ПС РМ АБИ предназначено для функционирования под управлением операционной системы специального назначения (ОС СН) «Astra Linux Special Edition» РУСБ.10015-01 с версией ядра не ниже 4.15.3.

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

2.3. Требования к персоналу (пользователю)

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы.

Пользователь, допущенный к работе с ПС РМ АБИ, должен сдать квалификационный экзамен на I группу электробезопасности.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Загрузка и запуск программы

Запуск ПС РМ АБИ осуществляется путем вызова исполняемого файла `rmabi`, расположенного в каталоге `\opt\nabat`.

Ярлык «ПС РМ АБИ» для запуска программы расположен в группе «Системные» раздела «Программы» главного меню операционной системы.

При запуске «ПС РМ АБИ» на рабочем столе появится окно авторизации пользователя в БД «Набат» (рис. 1). В данном окне необходимо ввести имя пользователя и пароль, затем нажать левой кнопкой мыши на кнопку **[Соединение]**.

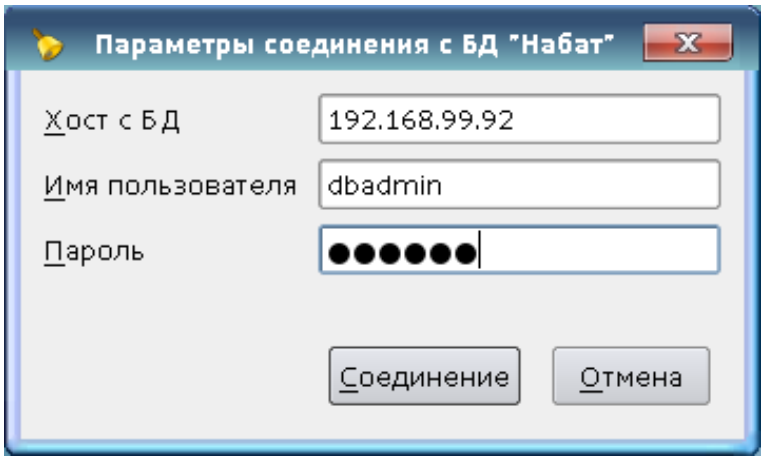


Рис. 1 – Окно авторизации пользователя в БД «Набат»

На рабочем столе появится окно оповещения (рис. 2) об успешном (или не успешном) подключении к блоку центральному процессорному (БЦП). При успешном подключении к БД на рабочем столе в окне оповещения, будет выведена следующая надпись - «Конфигурация объектов БЦП успешно обновлена. Серийный номер XXXX». Для дальнейшего запуска программы, в окне оповещения необходимо нажать на кнопку **[ОК].**

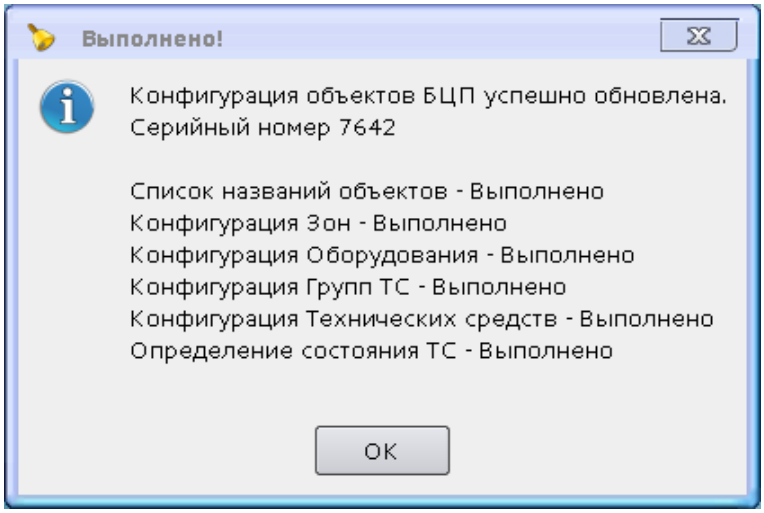


Рис. 2 – Обновление конфигурации объектов БЦП

В случае успешного запуска после завершения инициализации на рабочем столе появится главное окно программы.

3.2. Описание окон и закладок приложения

Главное окно программы, состоит из заголовка, основного меню и панели закладок.

3.2.1. В заголовке главного окна содержится информация о наименовании и версии программы.

3.2.2. Основное меню программы состоит из пунктов «Файл», «Сервис» и «Справка».

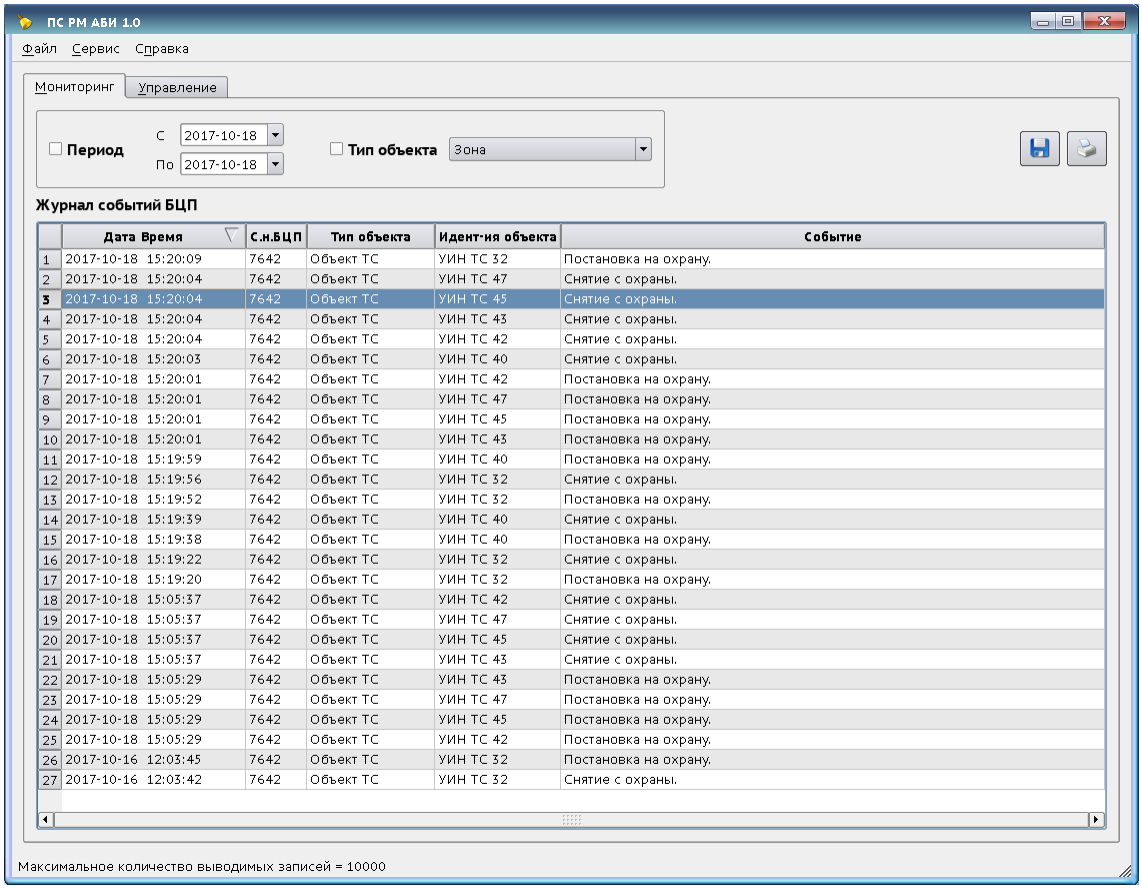
Пункт меню «Файл» содержит элементы «Скрыть окно приложения» и «Выход». При выборе элемента «Скрыть окно приложения» происходит сворачивание окна приложения в значок в правом нижнем углу рабочего стола. Для возврата окна на рабочий стол, необходимо нажать правой кнопкой мыши на указанный значок и в выпадающем меню выбрать пункт «Показать/скрыть окно приложения». При выборе элемента «Выход» в пункте меню «Файл», произойдет завершение работы с программой.

Пункт меню «Сервис» содержит элементы «Добавить БЦП», «Соединение с БЦП», «Обновить данные из БЦП» и «Удалить БЦП», служащие для проведения соответствующих действий с БЦП.

Пункт меню «Справка» содержит элемент «О программе», при нажатии на который. на рабочем столе появится окно с информацией о наименовании, версии и годе выпуска приложения.

3.2.3. Панель закладок включает в себя закладки «Мониторинг» и «Управление».

3.2.3.1. Закладка «Мониторинг» служит для отображения информации о текущих событиях, происходящих на контролируемых технических средствах охраны, просмотра, сохранения и выведения на печатающее устройство журналов регистрации событий (рис. 3). На закладке предусмотрена возможность установки фильтров событий по времени, состоянию, техническому средству охраны, группе технических средств, зоне и т.д.



	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. 3 – Закладка «Мониторинг»

Протоколирование текущих событий (включая события НСД), происходящих на контролируемых технических средствах охраны, выполняется в режиме реального времени.

3.2.3.2. Закладка «Управление» предназначена для управления состоянием (постановка/снятие с охраны) технических средств охраны, групп технических средств, зон и оборудования, отображения их текущего состояния, а также дополнительной информации (рис. 4).

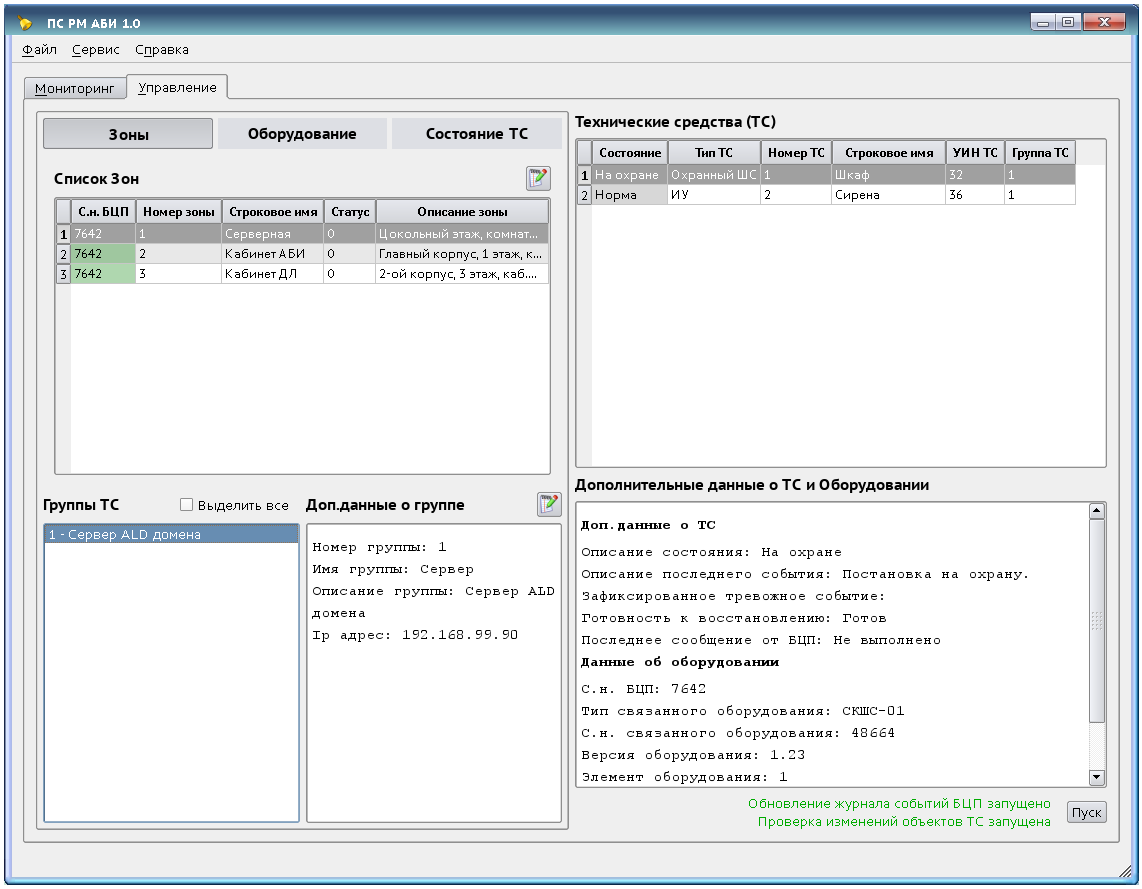


Рис. 4 – Закладка «Управление»

Окно закладки «Управление» разделено на функциональные окна. Основное окно, отображающее список «Зон», «Оборудования», а также «Состояние ТС» и дополнительные окна: «Группы ТС», «Дополнительные данные о группе», «Технические средства (ТС)» «Дополнительные данные о ТС и Оборудовании».

Панель вкладок основного окна включает в себя вкладки «Зоны», «Оборудование» и «Состояние ТС». При переходе на вкладку «Зоны» в основном окне будет выведен список «Зон», сконфигурированных на БЦП. В списке «Зон», отражены заводской номер устройства, на котором она сконфигурирована, ее номер, наименование и описание.

При нажатии левой кнопкой мыши на любую выбранную из списка «Зону» в дополнительных окнах соответственно отображаются списки «Групп ТС» и «Технических средств», привязанных к данной «Зоне». По умолчанию при выборе «Зоны» в окне «Дополнительные данные о ТС и Оборудовании» будет отображена детальная информация о ТС расположенном на первой строке списка из окна «Технические средства (ТС)». В указанном окне отражаются дополнительные данные об этом ТС — описание состояния ТС, описание последнего события, произошедшего с ТС, зафиксированное тревожное событие, готовность к восстановлению и сообщение

о физическом состоянии ТС, получаемое от БЦП, а также данные об оборудовании, к которому физически подключено ТС.

Для отображения детальной информации об выбранной «Группе ТС», необходимо в окне со списком «Групп ТС» выбрать нужную группу, нажав на нее левой кнопкой мыши. Соответственно в окне «Дополнительные данные о группе», будет выведена следующая информация о выбранной группе — номер, имя, описание и IP адрес защищаемого оборудования, к которому она привязана. Также в окне «Технические средства (ТС)», будет выведен список ТС, установленных на защищаемом оборудовании.

3.3. Выполнение функциональных задач

3.3.1. Выполнение визуальной и акустической сигнализации на АРМ нарушителя по команде АБИ. Для это необходимо выполнить следующее:

- перейти на вкладку «Управление»;

- в окне «Группы ТС», нажать правой кнопкой мыши на «АРМ нарушителя». В появившемся окне левой кнопкой мыши нажать на «Включить оповещение» (рис. 5). Для отключения, соответственно, необходимо нажать на «Выключить оповещение».

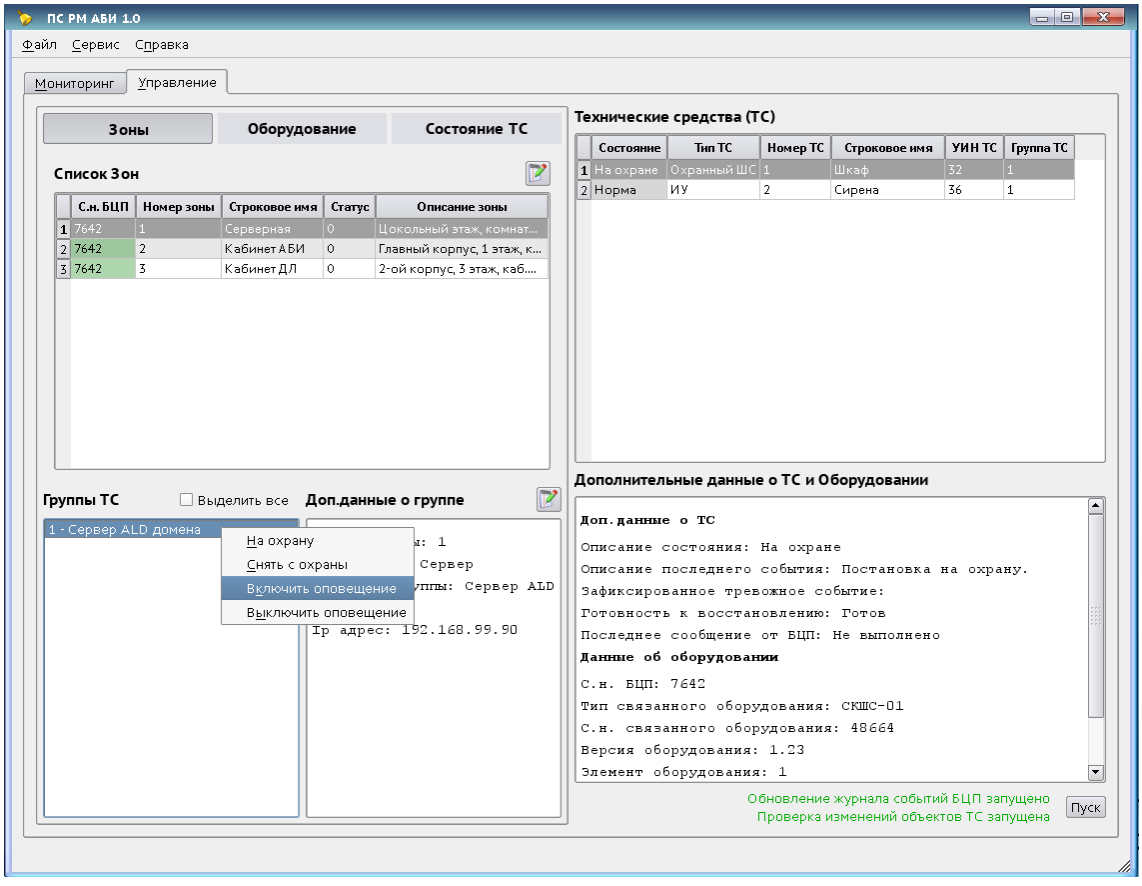


Рис. 5 – Включение оповещения для группы ТС

3.3.2. Выполнение программой отображения состояния ТС происходит в автоматическом режиме. Отображение состояния ТС отображается в окне «Технические средства (ТС)» в столбце «Состояние». Так же для детального отображения состояния, необходимо в окне «Технические средства (ТС)» левой кнопкой мыши нажать на выбранное ТС, при этом в окне «Дополнительные данные о ТС и Оборудовании» будет отображено полная информация о нем.

3.3.3. Выполнение визуального оповещения пользователя (АБИ) о наступлении события НСД по поставленным на охрану в данный момент времени выбранным «Зонам», «Группам ТС», или ТС, происходит в автоматическом режиме. При наступлении события на рабочем столе будет выведено окно оповещение. Детальное описание окна оповещения, описано в разделе 4.

После проведения анализа произошедшего события, для вывода сработавшего ТС из состояния «Тревога» оператор должен:

- перейти на закладку «Управление»;

- в окне «Технические средства (ТС)», правой кнопкой мыши нажать на ТС, отмеченное состоянием «Тревога», для его перевода в состояние «Норма» выбрать «Восстановление». Для того чтобы сбросить работу исполнительных устройств (свето звуковых оповещателей (сирен), срабатывающих на событие НСД, произошедшее с данным ТС, при нажатии правой кнопкой мыши на данном ТС, необходимо выбрать «Сбросить ШС». При этом состояние ТС останется «Тревога». В дальнейшем для восстановления нормальной работы сработавшего ТС, необходимо обязательно перевести его в состояние «Норма» и при необходимости поставить его на «Охрану».

При одновременном срабатывании нескольких ТС, описанные выше операции необходимо произвести с каждым.

3.3.4. Выполнение корректировки описаний «Зон» и «Групп ТС». Для этого необходимо выполнить следующее:

- перейти на вкладку «Управление»;

- в основном окне во вкладке «Зоны», нажать левой кнопкой мыши на выбранную зону, затем нажать на кнопку **[Редактировать]**, расположенную в правом верхнем углу окна. В появившемся окне откорректировать описание выбранной «Зоны»;

- в окне «Группы ТС», нажать левой кнопкой мыши, на выбранную «Группу», затем нажать на кнопку **[Редактировать]**, расположенную в правом верхнем углу окна. В появившемся окне откорректировать описание выбранной «Группы».

3.3.5. Выполнение постановка/снятие с охраны выбранных «Зон», «Групп ТС»

или «Технических средств». Для этого необходимо выполнить следующее:

- перейти на вкладку «Управление»;

- постановка на охрану выбранной «Зоны» производится в основном окне во вкладке «Зоны», нажатием правой кнопкой мыши на нее. В появившемся меню необходимо выбрать «Зону на охрану», при этом в окне «Технические средства (ТС)» отображается состояние «На охране» ТС с типом «Охранный шлейф». В окне «Дополнительные данные о ТС и Оборудовании» ТС с типом «Охранный шлейф», в строке описание состояния, также будет отражено состояние «На охране». Снятие с охраны, производится аналогичным образом. В меню выпадающем при нажатии правой кнопки мыши на выбранную «Зону», необходимо нажать левой кнопкой мыши «Снятие зоны с охраны»;

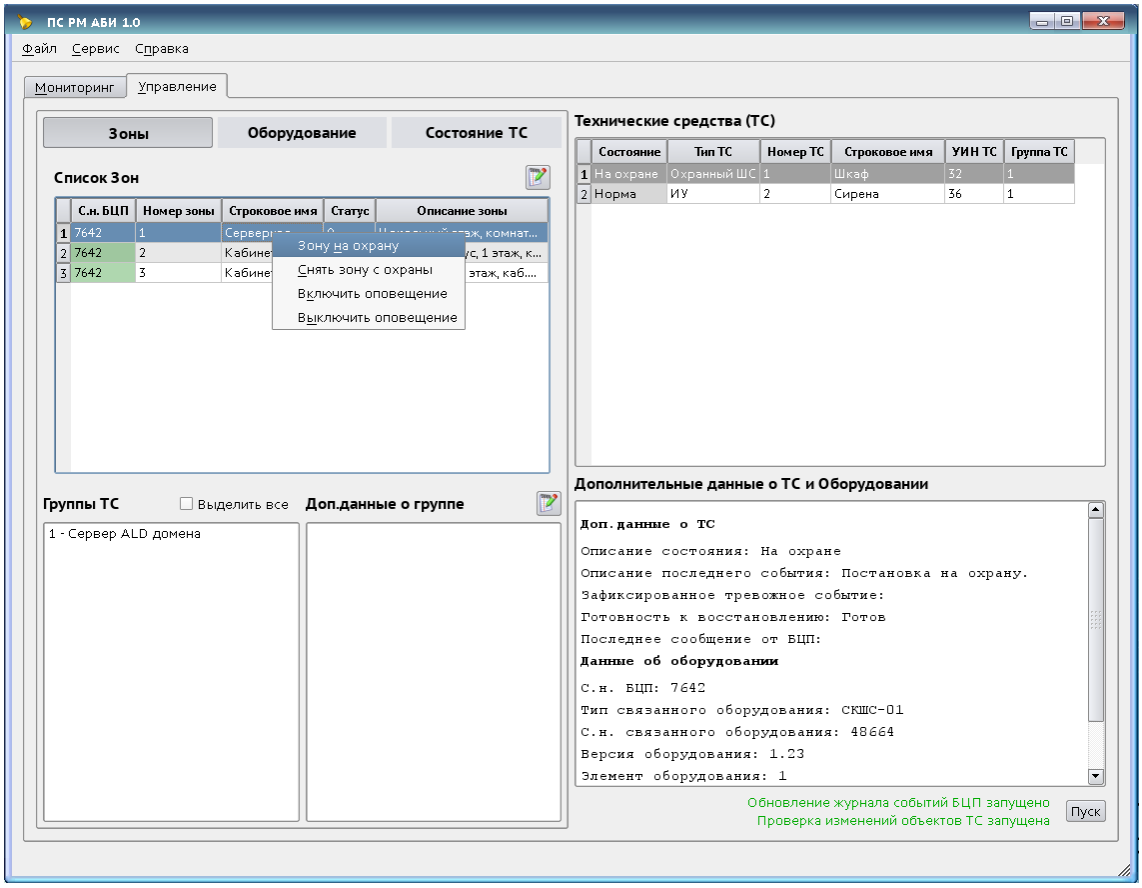


Рис. 6 – Постановка зоны на охрану

- постановка/снятие на(с) охрану(ы) «Групп ТС» и ТС производится аналогичным образом, в соответствующих окнах «Группы ТС» и «Технические средства (ТС)».

3.3.6. Выполнение программой протоколирования событий НСД, а также изменений состояний всех ТС, «Групп ТС» и «Зон» системы в БД. Происходит в автоматическом режиме. Для визуального наблюдения событий, необходимо перейти на закладку «Мониторинг». В окне закладки отображен «Журнал событий БЦП», т. е. всех событий, произошедших с начала протоколирования с оборудованием и

техническими средствами из состава изделия ПАК «Набат».

3.3.7. Выполнение управлением (сортировкой, поиском) и просмотром журнала событий, в том числе сохранение его на носители информации и выведение на печать в виде отчета (с возможностью отбора необходимой информации). Для этого необходимо выполнить следующее:

- перейти на закладку «Мониторинг»;

- в поле фильтры, ввести необходимые реквизиты поиска (даты с, по, наименование типа объекта), затем левой кнопкой мыши нажать на квадратное окно соответственно рядом со строкой «Период» и «Тип объекта». При этом в окне «Журнал событий БЦП», будет отображен журнал, отфильтрованный с учетом, введенных реквизитов;

- для сохранения журнала, необходимо нажать кнопку «сохранить», изображена в виде дискеты в правом верхнем углу окна. Во всплывающем окне, ввести имя файла, затем нажать клавишу «сохранить»;

- для проведения печати, после формирования отфильтрованного с учетом, введенных реквизитов журнала, необходимо нажать кнопку **[Печать]**, изображена в виде принтера в правом верхнем углу окна.. Во всплывающем окне, выбрать печатающее устройство, затем нажать кнопку **[Печать].**

3.3. Завершение работы программы

Для завершения работы программы необходимо выбрать в основном меню программы пункт «Файл» и далее пункт меню «Выход».

При попытке завершения программы стандартными средствами операционной системы посредством нажатия на кнопку закрытия окна приложение сворачивается в область уведомлений панели задач и отображается в виде значка  . Для отображения окна программы необходимо щелкнуть по значку левой кнопкой мыши. Для завершение работы программы необходимо щелкнуть по значку правой кнопкой мыши и выбрать пункт меню «Выход».

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. При возникновении события НСД на рабочем столе автоматически появляется окно оповещение, содержащее параметры события НСД:

- данные о ТС, на котором произошло событие, а также данные о «Группе ТС» и «Зоне», к которым оно привязано;

- наименование события.

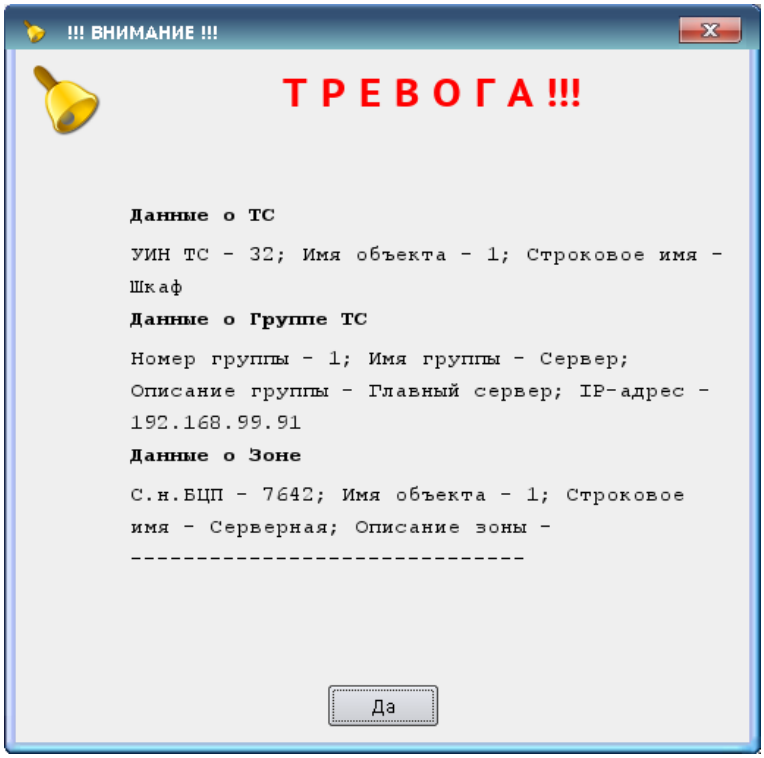


Рис. 7 – Окно сообщения о событии НСД

Окно содержит кнопку **[Да],** при нажатие на которую происходит закрытие окна оповещения.

Информация о возникновении события НСД и предпринятых оператором последующих за событием действий заносится в БД, и соответственно отражается в «Журнале событий БЦП» в закладке «Мониторинг».

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

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
	изменённых	заменённых	новых	аннулированных					