

УТВЕРЖДЕН  
ФДШИ.03618-01 34 01-ЛУ

**ПРОГРАММНЫЙ КОМПЛЕКС ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ «РЕБУС-СОВ»**

**Руководство оператора**

**ФДШИ.03618-01 34 01**

**Листов 63**

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

2024

Литера О<sub>1</sub>

## АННОТАЦИЯ

В данном документе описаны действия оператора по практическому использованию ФДШИ.03618-01 «Программный комплекс обнаружения вторжений «Ребус-СОВ» (далее – ПК «Ребус-СОВ»).

## СОДЕРЖАНИЕ

1. Назначение программы .....	5
2. Условия выполнения программы .....	6
2.1. Требования к составу технических средств .....	6
2.2. Требования к общесистемному программному обеспечению .....	6
2.3. Рекомендации по составу и квалификации обслуживающего персонала .....	6
2.4. Организация мер безопасности .....	6
3. Подготовка к работе .....	8
3.1. Состав дистрибутива .....	8
3.2. Установка ПК «Ребус-СОВ» .....	8
3.2.1. Установка ПК в ОС Windows .....	8
3.2.2. Установка ПК в ОС МСВС и ОС СН «Astra Linux Special Edition» .....	11
3.2.3. Установка ПК в ОС МСВС и ОС СН «Astra Linux Special Edition» с помощью консольного инсталлятора .....	15
3.2.4. Настройка после установки .....	17
3.2.5. Работа в режиме замкнутой программной среды ОС СН «Astra Linux Special Edition» ...	17
3.3. Удаление ПК «Ребус-СОВ» .....	18
3.3.1. Удаление в ОС Windows .....	18
3.3.2. Удаление в ОС МСВС и ОС СН «Astra Linux Special Edition» .....	19
4. Выполнение программы .....	22
4.1. Общие сведения о составе программы .....	22
4.2. Обязанности и возможности оператора .....	22
4.3. Средство настройки агентской части .....	22
4.3.1. Назначение .....	22
4.3.2. Запуск средства .....	23
4.3.3. Настройки агентской части .....	23
4.3.4. Верификация целостности модулей .....	24
4.3.5. Верификация целостности сигнатур вторжений .....	24
4.4. Консоль управления .....	24
4.4.1. Назначение .....	24
4.4.2. Запуск консоли .....	25
4.4.3. Вкладка «Текущее состояние» .....	26
4.4.4. Вкладка «Аудит» .....	28
4.4.5. Вкладка «Станции» .....	29
4.4.6. Вкладка «Параметры защиты» .....	32
4.4.7. Вкладка «Отчеты» .....	34
4.4.8. Вкладка «Управление» .....	34
4.5. Редактирование параметров средства анализа сетевого трафика с использованием сигнатур .....	36
4.5.1. Общие сведения .....	36
4.5.2. Описание формы редактирования .....	37
4.5.3. Настройка сохранения дампов сетевых пакетов .....	39
4.5.4. Вкладка «Переменные» .....	40
4.5.5. Вкладка «Правила» .....	41
4.5.6. Окно «Редактор» .....	44
4.6. Управление внешними средствами .....	45
4.6.1. Общие сведения .....	45
4.6.2. Работа со сценариями управления внешними средствами .....	47
4.6.3. Работа с шаблонами .....	51
4.6.4. Результат выполнения сценариев .....	53
4.7. Обновление БРП .....	55
4.7.1. Автоматическое обновление .....	55
4.7.2. Ручное обновление .....	56

4.8. Настройка сервера СОВ .....	56
4.9. Настройка синхронизации времени .....	56
4.10. Верификация целостности сигнатур вторжений .....	57
4.11. Использование дополнительных компонентов .....	57
5. Сообщения оператору .....	58
Перечень сокращений.....	62

## 1. НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК «Ребус-СОВ» предназначен для функционирования на уровне сети и на уровне узлов информационной системы с целью обнаружения и блокирования угроз безопасности информации, относящихся к вторжениям (атакам):

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей;

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

ПК «Ребус-СОВ» применяется в качестве элемента системы защиты информации информационных систем, функционирующих на базе вычислительных сетей и обрабатывающих информацию, содержащую государственную тайну, и (или) конфиденциальную информацию, включая персональные данные.

## 2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

### 2.1. Требования к составу технических средств

Для функционирования программы должны использоваться ЭВМ со следующими техническими характеристиками:

- ЭВМ типа IBM PC с Intel x86/x64-совместимым процессором не ниже Pentium IV 3 ГГц либо ЭВМ на базе процессора Эльбрус-8С;
- минимальный объем оперативной памяти – 2 Гбайт, рекомендуемый объем оперативной памяти – не менее 4 Гбайт;
- свободное место на системном разделе жесткого диска – не менее 1 Гбайт;
- поддержка монитором и видеоадаптером ЭВМ рабочих разрешений не менее 1024 x 768 точек при глубине цвета не менее 8 бит (для рабочего места оператора);
- клавиатура и мышь или совместимое устройство ввода;
- сетевой адаптер (поддерживающий скорость не менее 10 Мбит/с).

ЭВМ должны быть объединены в ЛВС. Сеть должна быть настроена на использование стека сетевых протоколов TCP/IPv4.

### 2.2. Требования к общесистемному программному обеспечению

В качестве операционной системы (ОС) для ПК «Ребус-СОВ» должны использоваться:

- ОС Microsoft Windows 7 SP1/8/8.1/10/Server 2008 R2 SP1/Server 2016/Server 2019/Server 2022;
- ОС MCBC 5.0 ЦАВМ.11004-01 (изменение № 7);
- ОС СН «Astra Linux Special Edition» РУСБ.10015-01 (релиз «Смоленск» версии 1.4, 1.5, 1.6, 1.7, 1.8);
- ОС СН «Astra Linux Special Edition» РУСБ.10265-01 (релиз «Ленинград» версия 8.1).

### 2.3. Рекомендации по составу и квалификации обслуживающего персонала

Эксплуатация изделия возможна только при условии наличия на объекте должностного лица, выполняющего роль администратора СОВ. Данное должностное лицо может совмещать обязанности оператора СОВ, однако рекомендуется разделить обязанности оператора и администратора. Количество должностных лиц, выполняющих роли администратора и оператора, зависит от особенностей объекта информатизации.

Администратором рекомендуется назначать специалиста, знакомого с архитектурой сетей, с принципами функционирования сетей и имеющего опыт администрирования в ОС Windows и ОС СН «Astra Linux Special Edition».

Оператором рекомендуется назначать специалиста, обладающего знаниями в области компьютерных атак.

### 2.4. Организация мер безопасности

На ЭВМ, предназначенных для эксплуатации изделия, должны функционировать средства защиты уровня ОС, обеспечивающие аутентификацию и идентификацию пользователя, а также разграничение доступа к файловым ресурсам ЭВМ.

После установки ПК «Ребус-СОВ» администратор безопасности должен настроить права доступа на файлы журнала аудита таким образом, чтобы доступ был разрешен только администраторам и операторам ПК «Ребус-СОВ». Для ОС Windows файлы журнала аудита располагаются в каталоге %ALLUSERSPROFILE%\rebus-sov\log, для ОС MCBC и ОС СН «Astra Linux Special Edition» – в каталоге /var/log/rebus-sov.

Для администраторов и операторов ПК «Ребус-СОВ» необходимо настроить разрешение на запуск и использование ПО ПК «Ребус-СОВ». Пользователям ИС, которые не являются пользователями и операторами СОВ, необходимо запретить доступ к программам настройки и управления ПК «Ребус-СОВ».

На объекте эксплуатации должна быть разработана и применена политика назначения и смены паролей пользователей СОВ. Политика назначения и смены паролей должна предусматривать использование безопасных паролей в соответствии с требованиями к паролям для класса ИС, в которой развернута СОВ. Должна быть предусмотрена процедура периодической смены паролей, а также процедура немедленной смены паролей в случае дискредитации аутентификационных данных пользователей и администраторов СОВ.

### 3. ПОДГОТОВКА К РАБОТЕ

#### 3.1. Состав дистрибутива

Дистрибутив поставляется на электронном носителе (ЭН) ФДШИ.03618-01-DE.

Состав корневого каталога ЭН:

- **Документы** – каталог, содержащий эксплуатационную документацию;
- **Программы** – каталог, содержащий дистрибутив ПК «Ребус-СОВ».

Каталог **Документы** содержит следующие документы в электронной форме в формате Portable Document Format (PDF):

- ФДШИ.03618-01 20 01 «Ведомость эксплуатационных документов»;
- ФДШИ.03618-01 31 01 «Описание применения»;
- ФДШИ.03618-01 34 01 «Руководство оператора».

Состав каталога **Программы**:

- **ФДШИ.03618-01** – каталог с дистрибутивом ПК «Ребус-СОВ»;

- **CSUM** – каталог содержит контрольные суммы дистрибутива и программу расчета контрольных сумм;

- **rebus-sov-md5-astra.txt** – контрольные суммы дистрибутива для проверки в ОС СН «Astra Linux Special Edition»;

- **rebus-sov-md5-msvs.txt** – контрольные суммы дистрибутива для проверки в ОС МСВС.

Состав каталога **ФДШИ.03618-01**:

- **AstraLinux** – каталог с дистрибутивом ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition» релиз «Смоленск»;

- **AstraLinux-Ленинград** – каталог с дистрибутивом ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition» релиз «Ленинград»;

- **Windows** – каталог с дистрибутивом ПК «Ребус-СОВ» для ОС Windows;

- **МСВС 5.0** – каталог с дистрибутивом ПК «Ребус-СОВ» для ОС МСВС 5.0;

- **Base** – каталог с сигнатурами вторжений.

#### 3.2. Установка ПК «Ребус-СОВ»

##### 3.2.1. Установка ПК в ОС Windows

Установка ПК «Ребус-СОВ» осуществляется с помощью входящего в дистрибутив модуля установки.

Перед установкой ПК «Ребус-СОВ» на ЭВМ с ОС Windows 10 (версии 1607 и более поздних) необходимо отключить механизм Secure Boot в настройках материнской платы при его наличии.

Установка осуществляется администратором ОС в следующем порядке:

- вставить дистрибутивный ЭН в устройство чтения CD/DVD-дисков;

- с помощью файлового менеджера перейти в каталог **Программы\ФДШИ.03618-01\Windows** дистрибутивного ЭН;

- запустить модуль установки **Ребус-СОВ.exe**, в результате чего появится окно установки, изображённое на рис. 1;

- в окне установки нажать кнопку «Далее», в результате чего появится окно выбора компонентов установки, изображённое на рис. 2;

- выбрать компонент установки (для сервера СОВ должны быть выбраны оба компонента), нажать кнопку «Далее», в результате чего появится окно настройки параметров соединения, изображённое на рис. 3;

- ввести IP-адрес и порт сервера СОВ, нажать кнопку «Далее». Если параметры заданы неверно, отобразится сообщение об использовании параметров по умолчанию;

- в появившемся окне (рис. 4) проверить параметры установки. Если параметры не требуется изменять, то нужно нажать кнопку «Установить», иначе – кнопку «Назад»;

- дождаться окончания процесса извлечения файлов (в процессе извлечения файлов могут появляться диалоговые окна, которые закроются автоматически) и появления окна, изображённого на рис. 5;
- в появившемся окне нажать кнопку «Готово»;
- в появившемся окне (рис. 6) на запрос о перезагрузке нажать кнопку «Да».

### Начальное окно установки

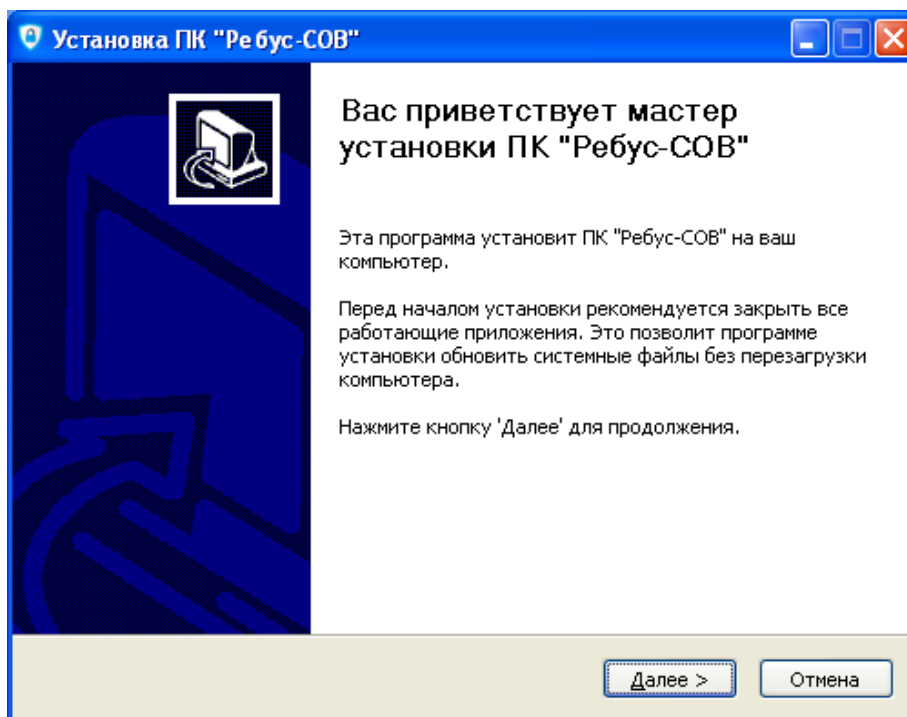


Рис. 1

### Окно выбора компонентов установки

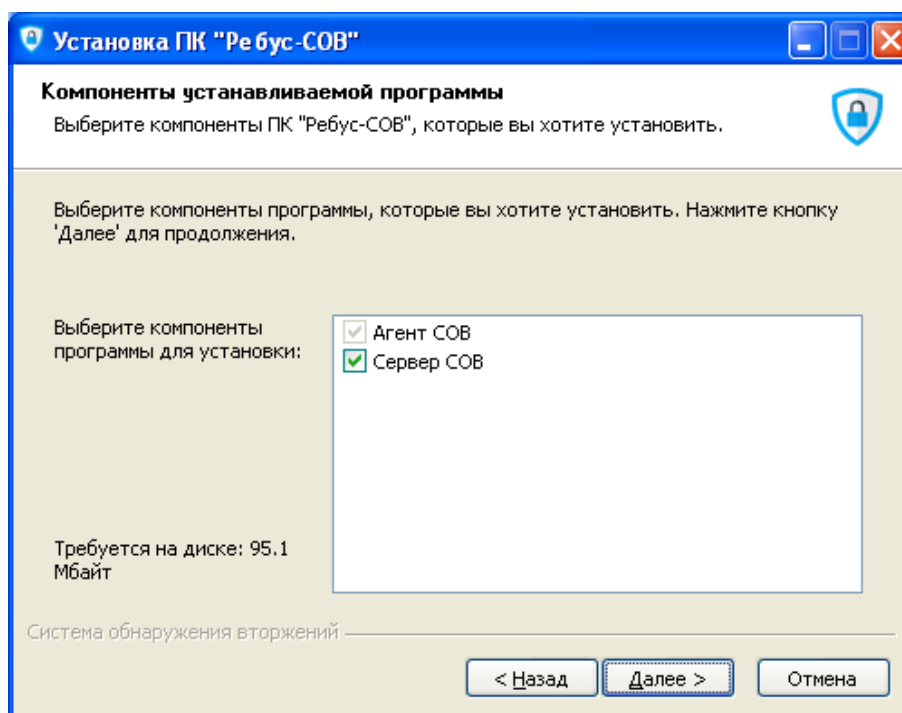


Рис. 2

Окно настройки параметров соединения

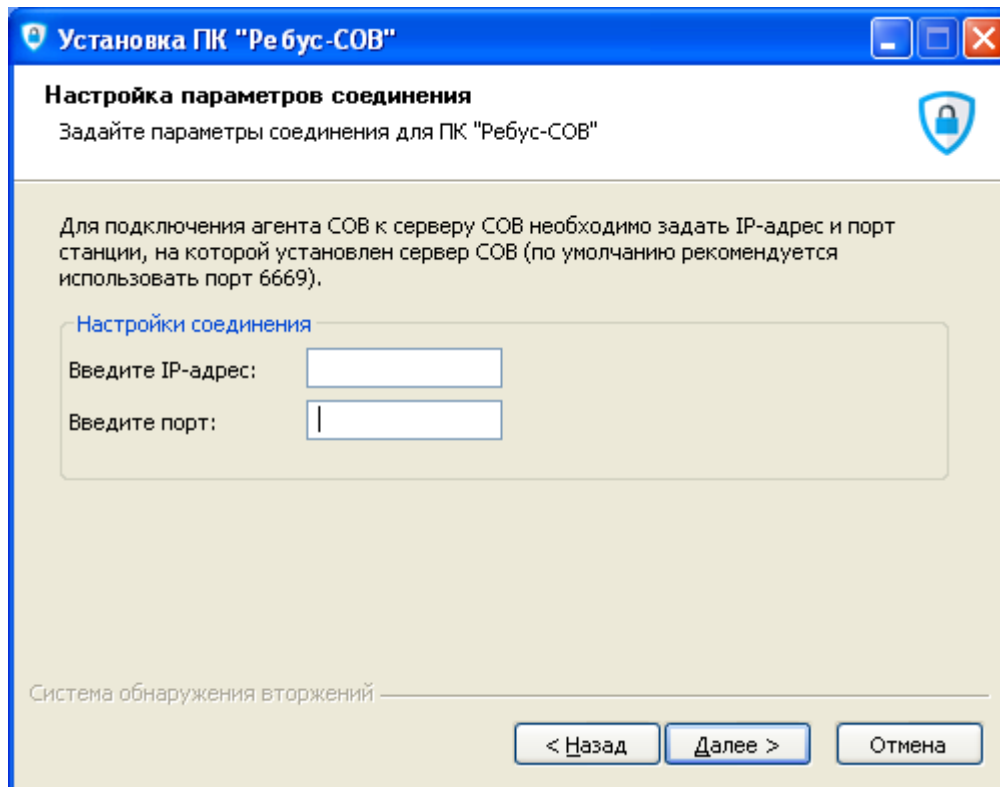


Рис. 3

Параметры установки

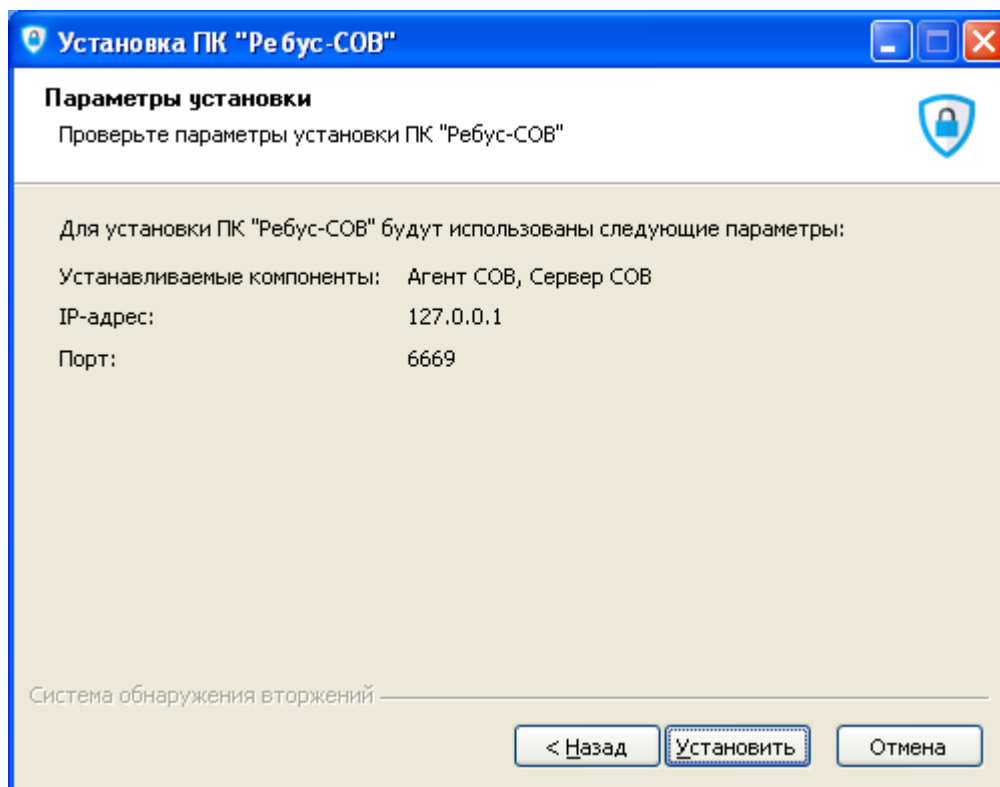


Рис. 4

### Завершение установки

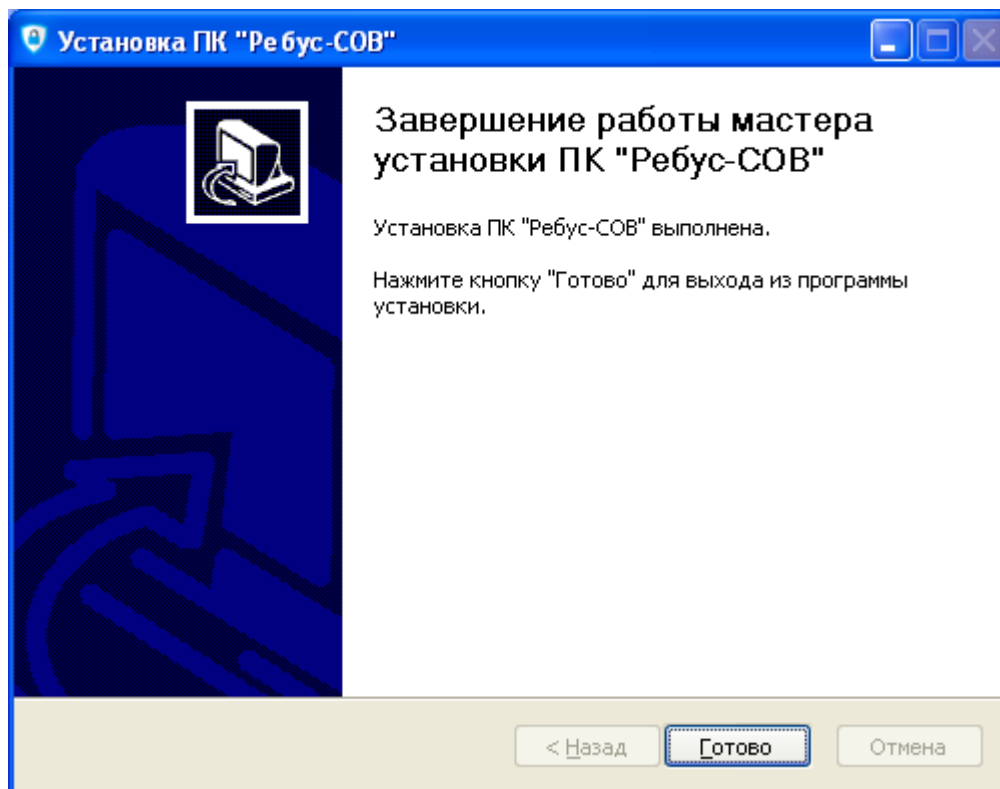


Рис. 5

### Требование перезагрузки

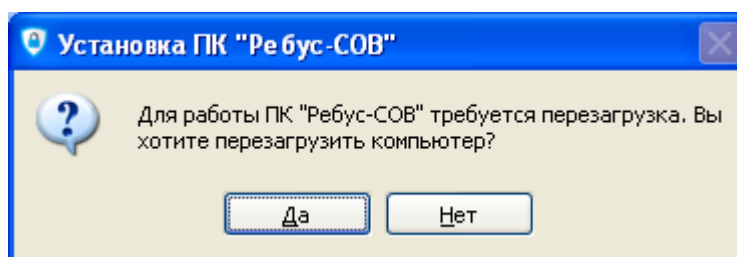


Рис. 6

### 3.2.2. Установка ПК в ОС МСВС и ОС СН «Astra Linux Special Edition»

Установка ПК «Ребус-СОВ» для ОС МСВС и ОС СН «Astra Linux Special Edition» осуществляется с помощью входящего в дистрибутив модуля установки **xinstall**.

Модуль находится на дистрибутивном ЭН в каталоге **Программы/ФДШИ.03618-01/ <тип ОС>**, где <тип ОС> принимает значение **МСВС 5.0**, **AstraLinux** или **AstraLinux-Ленинград** (в соответствии с ОС, на которую необходимо установить изделие).

Установка должна осуществляться от имени суперпользователя (пользователь должен зарегистрироваться в системе от имени **root** или запустить модуль установки с помощью команд **su** или **sudo**).

Модуль установки имеет графический интерфейс, выполненный в виде пошагового мастера из нескольких страниц. Перемещаться между страницами мастера можно с помощью кнопок «Далее» и «Назад». Кнопка «Отмена» позволяет прервать работу программы. На каждой странице требуется указать отдельный параметр установки.

Модуль установки можно запустить либо двойным щелчком на значке файла **xinstall** в файловом менеджере, либо из командной строки.

ВНИМАНИЕ! ОС МСВС и ОС СН «Astra Linux Special Edition» позволяют запретить запуск любых исполняемых файлов с внешних носителей, соответственно, запуск модуля установки с ЭН может быть невозможен, если такой запрет есть. Так по умолчанию ведет себя ОС СН «Astra Linux Special Edition», в ОС МСВС такое поведение также может быть настроено администратором. За запрет запуска файлов отвечает параметр монтирования **noexec**, который может быть задан в файле **/etc/fstab**, либо может быть передан команде **mount** в качестве аргумента командной строки. В случае если модуль установки невозможно запустить с ЭН по причине использования параметра **noexec**, администратор может осуществлять установку одним из следующих способов:

1) скопировать дистрибутив (каталог **Программы/ФДШИ.03618-01/МСВС 5.0**, **Программы/ФДШИ.03618-01/AstraLinux** или **Программы/ФДШИ.03618-01/AstraLinux-Ленинград** – в соответствии с целевой ОС, а также каталог **Программы/ФДШИ.03618-01/Base**) на жёсткий диск ЭВМ и запустить модуль установки с жёсткого диска из каталога с дистрибутивом (где находится модуль **xinstall**);

2) перемонтировать ЭН без параметра **noexec** и запустить модуль установки непосредственно с ЭН.

В первом окне мастера следует отметить переключатель «Установить» (он отмечен по умолчанию) и нажать кнопку «Далее» (рис 7).

#### Начало установки ПК «Ребус-СОВ» в ОС СН «Astra Linux Special Edition»

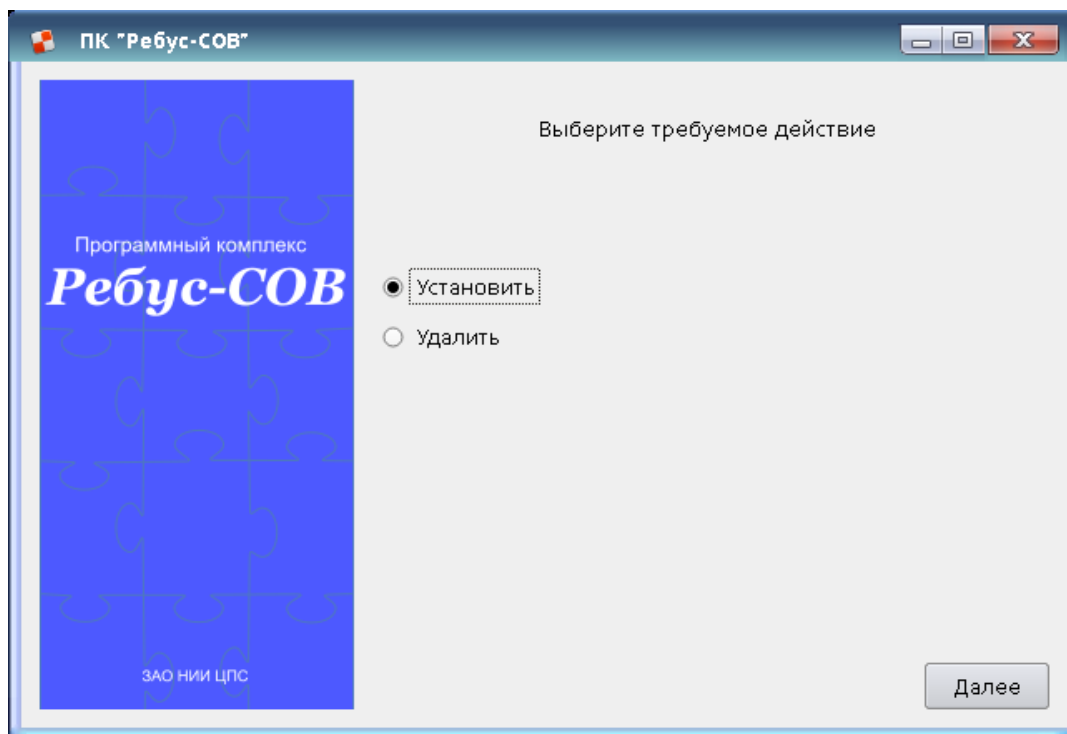


Рис. 7

Примечание. Текстовые поля в окнах мастера могут незначительно отличаться от указанных в зависимости от версии комплекса и используемой ОС.

На следующей странице выбирается тип станции (рис. 8). Типов станции два: «Сервер СОВ» или «Рабочая станция».

Окно выбора станции ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition»

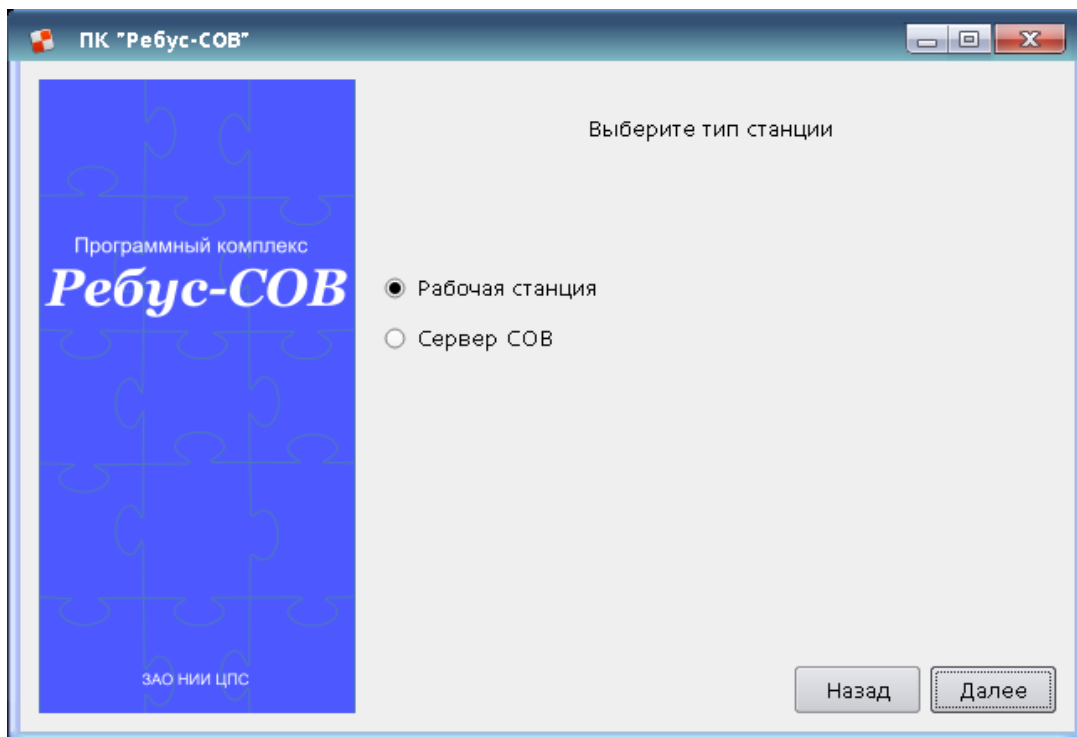


Рис. 8

После нажатия кнопки «Далее» появляется страница с запросом сетевых параметров сервера СОВ (рис. 9). На этой странице необходимо задать IP-адрес и номер сетевого порта сервера СОВ.

Установка сетевых параметров ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition»

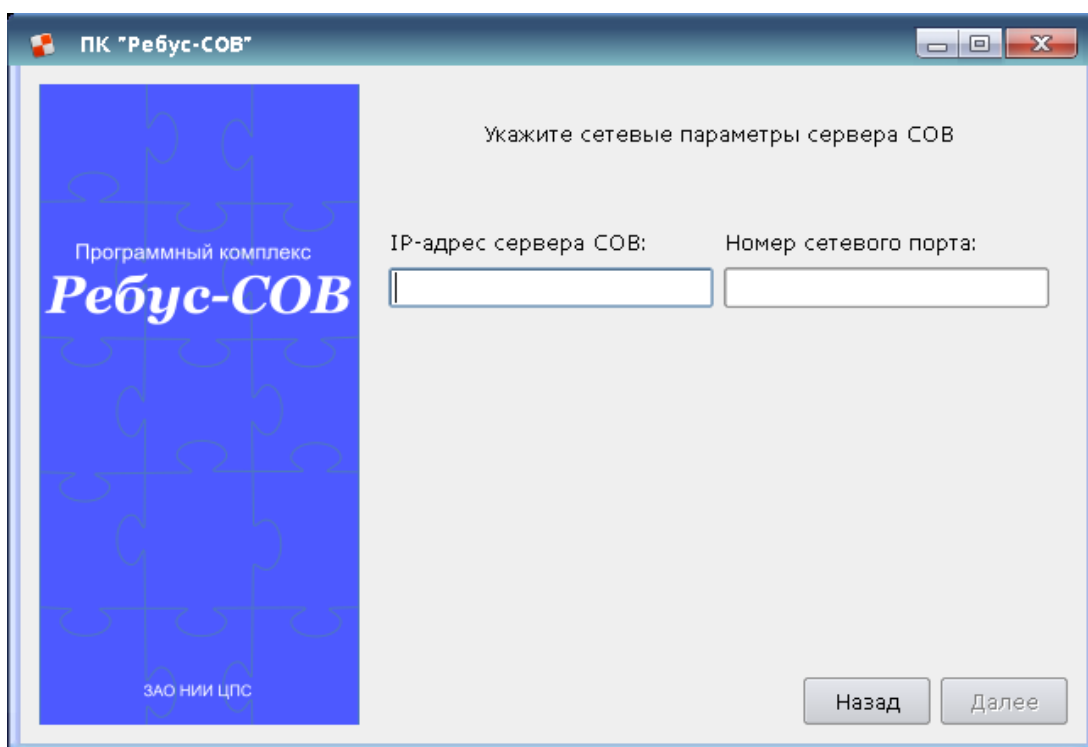


Рис. 9

В качестве номера порта рекомендуется значение 6669.

В поле IP-адреса ввести адрес станции, выделенной под сервер COB. При установке на самом сервере можно использовать 127.0.0.1.

Далее будет предложено указать путь к базам решающих правил. По умолчанию поле ввода содержит относительный путь, соответствующий расположению баз решающих правил на дистрибутивном носителе (каталог **Base** на одном уровне с каталогом для установки ПК «Ребус-COB»), и в большинстве случаев не требует модификации.

На следующей странице выводится суммарная информация об устанавливаемых компонентах и параметрах установки (рис. 10). На данном шаге можно вернуться назад и изменить какие-либо параметры.

Устанавливаемые параметры ПК «Ребус-COB» для ОС СН «Astra Linux Special Edition»

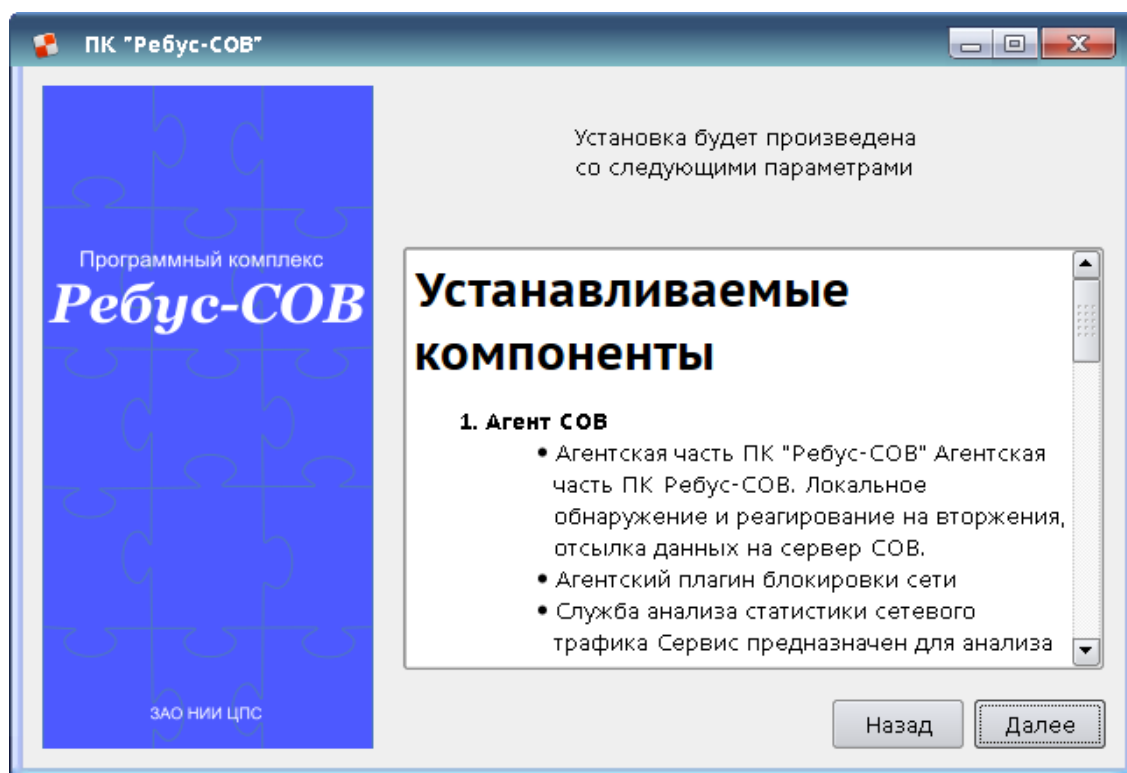


Рис. 10

После нажатия на кнопку «Далее» начинается установка, ход которой отображается с помощью индикатора прогресса.

На заключительном шаге выводится сообщение о том, что установка завершена (рис. 11).

Результат установки ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition»

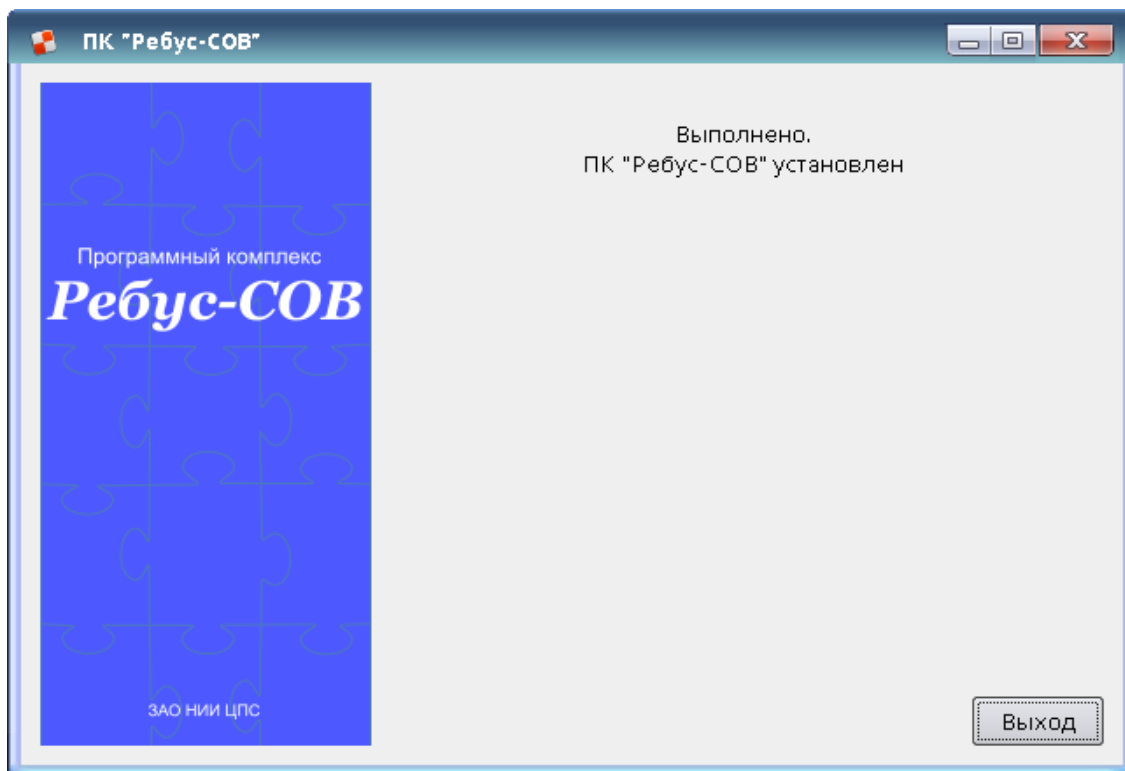


Рис. 11

3.2.3. Установка ПК в ОС МСВС и ОС СН «Astra Linux Special Edition» с помощью консольного инсталлятора

Чтобы начать установку ПК «Ребус-СОВ» с помощью консольного инсталлятора, необходимо перейти в каталог с дистрибутивом инсталлятора (где находятся модули **install** и **xinstall**) и запустить от имени администратора модуль **install**. Пример запуска приведен на рис. 12.

Запуск консольного инсталлятора ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition»

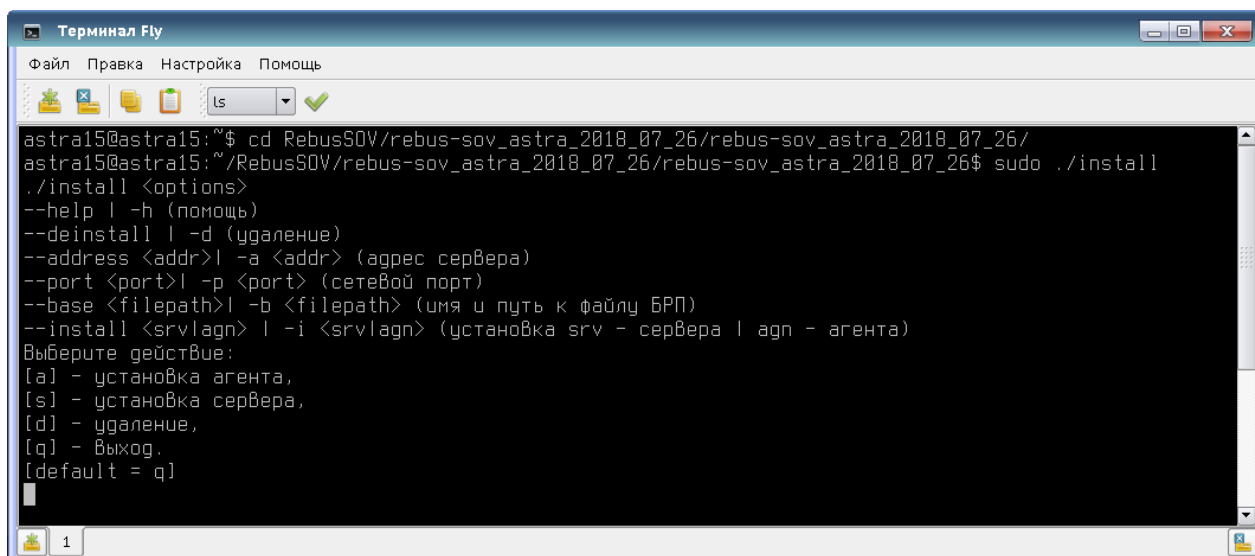


Рис. 12

После простого запуска консольного инсталлятора (без параметров) необходимо выбрать, что устанавливать: агент (a) или сервер (s). После выбора необходимо будет ввести адрес сервера и порт для подключения (рис. 13).

#### Параметры установки ПК «Ребус-СОВ» для ОС СН «Astra Linux Special Edition»

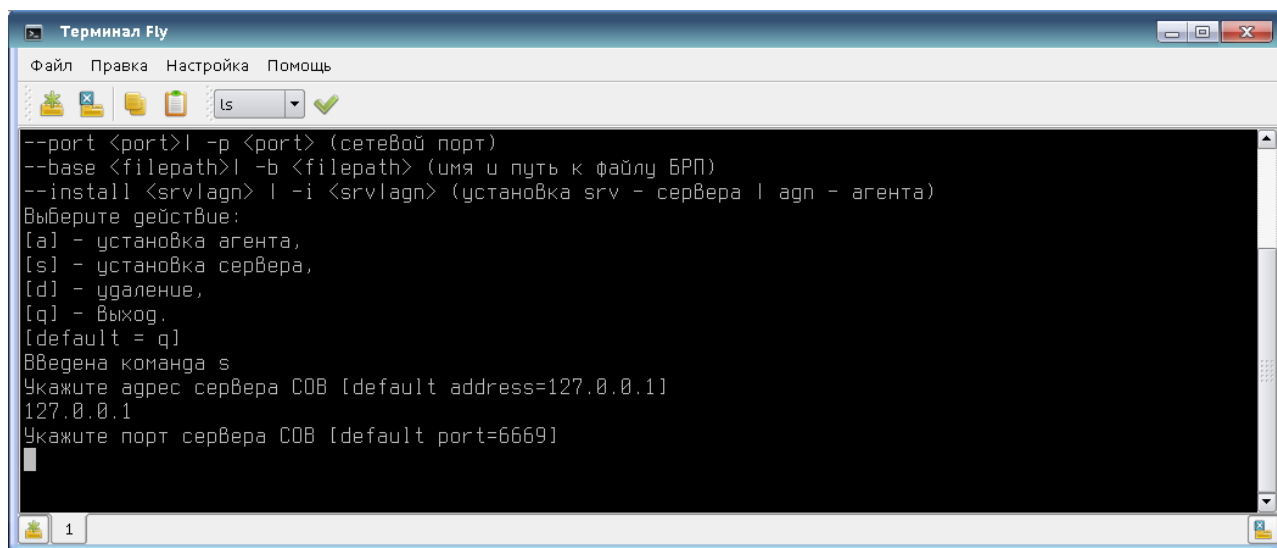


Рис. 13

Чтобы не вводить параметры позже, можно сразу задать их при запуске консольного инсталлятора (например, порт вводится с помощью опции «-p <номер порта>»). На рис. 14 указаны все параметры, необходимые для установки агента ПК «Ребус-СОВ». Все доступные параметры можно посмотреть с помощью опции -h.

#### Задание параметров при запуске консольного инсталлятора

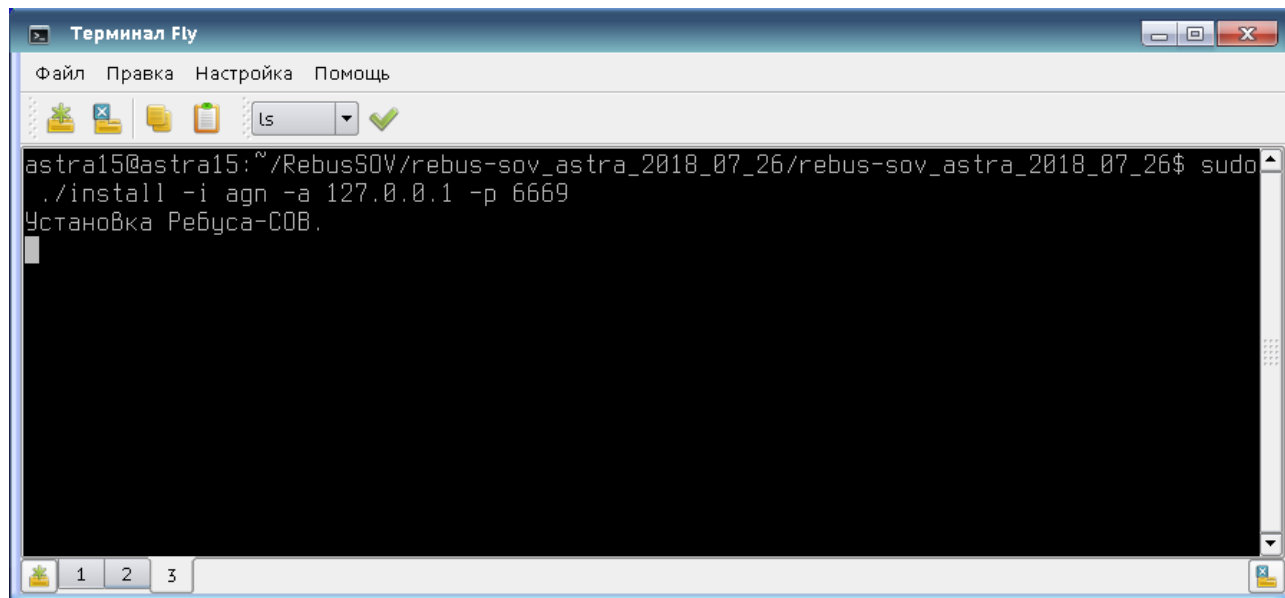


Рис. 14

Если не введён путь к базам решающих правил (БРП), тогда будет использован путь, заданный по умолчанию (каталог **Base** на одном уровне с каталогом для установки ПК «Ребус-СОВ»). После правильного ввода всех параметров начнётся установка ПК «Ребус-СОВ». Терминал вернёт управление пользователю по завершении установки ПК «Ребус-СОВ».

### 3.2.4. Настройка после установки

В случае, если на станции установлен межсетевой экран (системный, самостоятельный или входящий в состав антивирусного ПО), то в его настройках необходимо разрешить соединение по используемым ПК «Ребус-СОВ» TCP-портам. Кроме основного порта, заданного в процессе установки, ПК «Ребус-СОВ» при своей работе использует два TCP-порта, идущие непосредственно за ним. Для значения по умолчанию (порт 6669) это порты 6670 и 6671. Также в случае вывода событий ИБ в SIEM необходимо разрешить соединение сервера СОВ с сервером сбора логов по UDP-порту, указанному при настройке механизма (по умолчанию используется UDP-порт 514).

После установки ПК «Ребус-СОВ» для установления доверенного сетевого соединения между агентскими станциями и сервером СОВ используется стандартный ключ аутентификации. В целях повышения безопасности рекомендуется периодически производить смену ключа аутентификации на всех станциях с установленным ПК «Ребус-СОВ». Процедура генерации и переноса нового ключа аутентификации описана в 4.3.3 данного руководства.

Для уведомления о выявленных вторжениях по электронной почте необходимо настроить почтовый сервер. Настройка почтового сервера описана в 4.8.

Для корректной работы анализатора сетевого трафика с использованием сигнатур необходимо задать переменной HOME\_NET значение маски подсети, в которой работает анализатор. Настройка переменных анализатора сетевого трафика с использованием сигнатур описана в 4.5.

### 3.2.5. Работа в режиме замкнутой программной среды ОС СН «Astra Linux Special Edition»

Если предполагается использовать ОС в режиме замкнутой программной среды, то необходимо выполнить дополнительные настройки:

1) для ОС СН «Astra Linux Special Edition» версий 1.6, 1.7 и 1.8 релиз «Смоленск» с дистрибутивного диска ОС установить пакет **astra-digsig-oldkeys**;

2) смонтировать дистрибутивный ЭН ПК «Ребус-СОВ»;

3) для ОС СН «Astra Linux Special Edition» версий 1.4 и 1.5 релиз «Смоленск» в каталог **/etc/digsig/keys** поместить файл открытого ключа **cps.tver\_pub\_key.gpg**, находящийся в каталоге **/Программы/ФДШИ.03618-01/AstraLinux** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

4) для ОС СН «Astra Linux Special Edition» версий 1.6 и 1.7 релиз «Смоленск» в каталог **/etc/digsig/keys/legacy/keys** поместить файл открытого ключа **cps.tver\_pub\_key.gpg**, находящийся в каталоге **/Программы/ФДШИ.03618-01AstraLinux** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

5) для ОС СН «Astra Linux Special Edition» версии 1.8 релиз «Смоленск» в каталог **/etc/digsig/keys/legacy** поместить файл открытого ключа **cps.tver\_pub\_key.gpg**, находящийся в каталоге **/Программы/ФДШИ.03618-01AstraLinux** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

6) для ОС СН «Astra Linux Special Edition» релиз «Ленинград» в каталог **/etc/digsig/keys** поместить файл открытого ключа **cps.tver\_pub\_key.gpg**, находящийся в каталоге **/media/cdrom/ПДСЧ/AstraLinux-Ленинград** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

7) от имени суперпользователя выполнить команду **update-initramfs -u -k all**;

8) размонтировать дистрибутивный ЭН;

9) осуществить перезагрузку ОС.

В случае если на ЭВМ отсутствует встроенный CD/DVD-привод, необходимо использовать внешний CD/DVD-привод. Если внешний CD/DVD-привод также недоступен, необходимо копирование требуемых файлов выполнить с помощью отдельной ЭВМ, имеющей CD/DVD-привод, и USB-накопителя или локальной сети.

### 3.3. Удаление ПК «Ребус-СОВ»

#### 3.3.1. Удаление в ОС Windows

Удаление ПК «Ребус-СОВ» осуществляется администратором ОС в следующем порядке:

- открыть «Установка и удаление программ» в панели управления;
- выбрать ПК «Ребус-СОВ» и нажать кнопку «Удалить», в результате появится окно удаления, изображённое на рис. 15;
- нажать кнопку «Удалить» и дождаться окна на запрос о перезагрузке, изображенного на рис. 16;
- если требуется перезагрузить компьютер сейчас, то нажать кнопку «Да», иначе нажать кнопку «Нет»;
- если была нажата кнопка «Нет», то появится окно завершения удаления, изображенное на рис. 17;
- нажать кнопку «Заккрыть».

Окно удаления программы

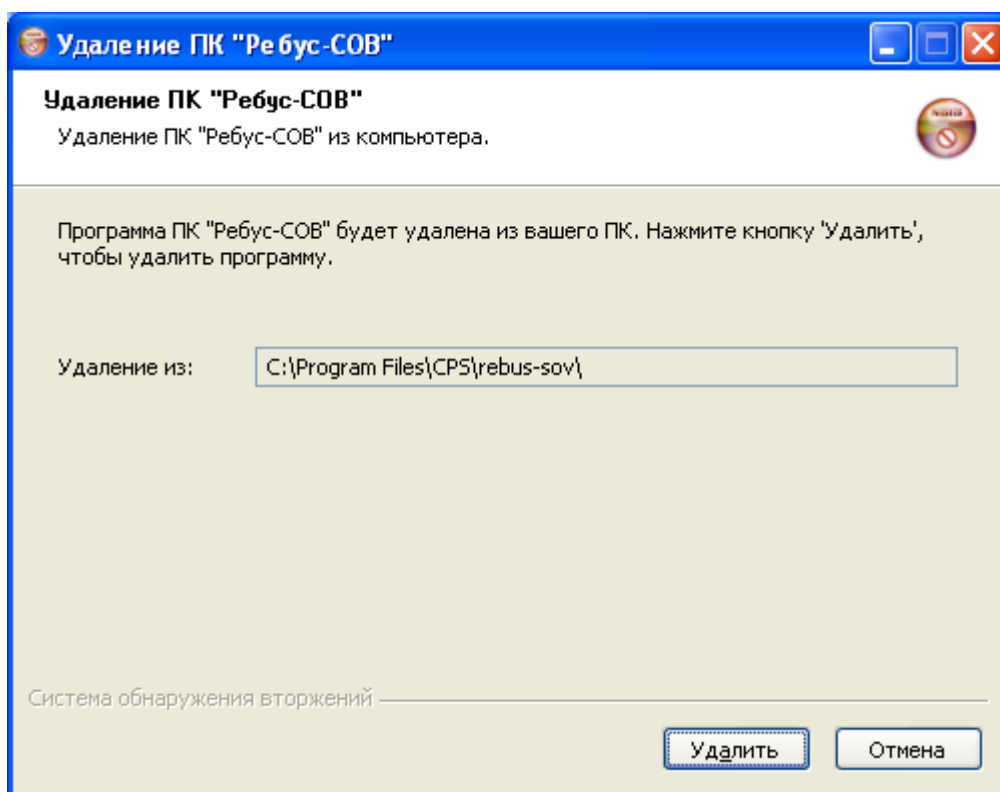


Рис. 15

Требование перезагрузки

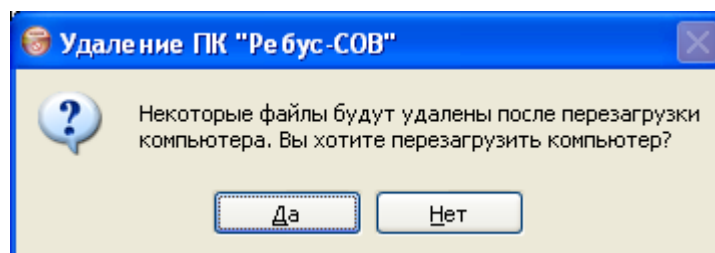


Рис. 16

### Завершение удаления программы

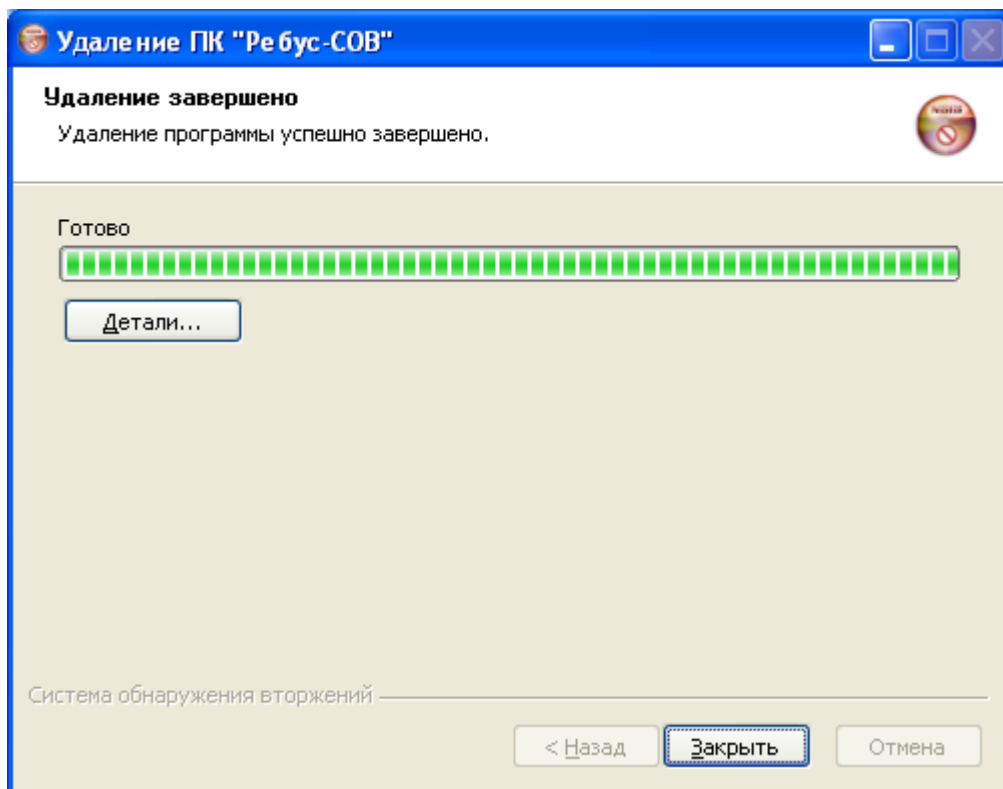


Рис. 17

#### 3.3.2. Удаление в ОС МСВС и ОС СН «Astra Linux Special Edition»

Удаление ПК «Ребус-СОВ» в ОС МСВС и ОС СН «Astra Linux Special Edition» должно выполняться от имени суперпользователя.

Для запуска удаления ПК «Ребус-СОВ» необходимо перейти в каталог с модулем **xinstall** и запустить его с правами администратора. Модуль находится на дистрибутивном ЭН в каталоге **Программы/ФДШИ.03618-01/<тип ОС>**, где <тип ОС> принимает значение **МСВС 5.0**, **AstraLinux** или **AstraLinux-Ленинград** (в соответствии с ОС, на которую установлено изделие). В результате запуска появится окно удаления, изображённое на рис. 18.

Удаление ПК «Ребус-СОВ» с помощью модуля **xinstall**  
для ОС СН «Astra Linux Special Edition»

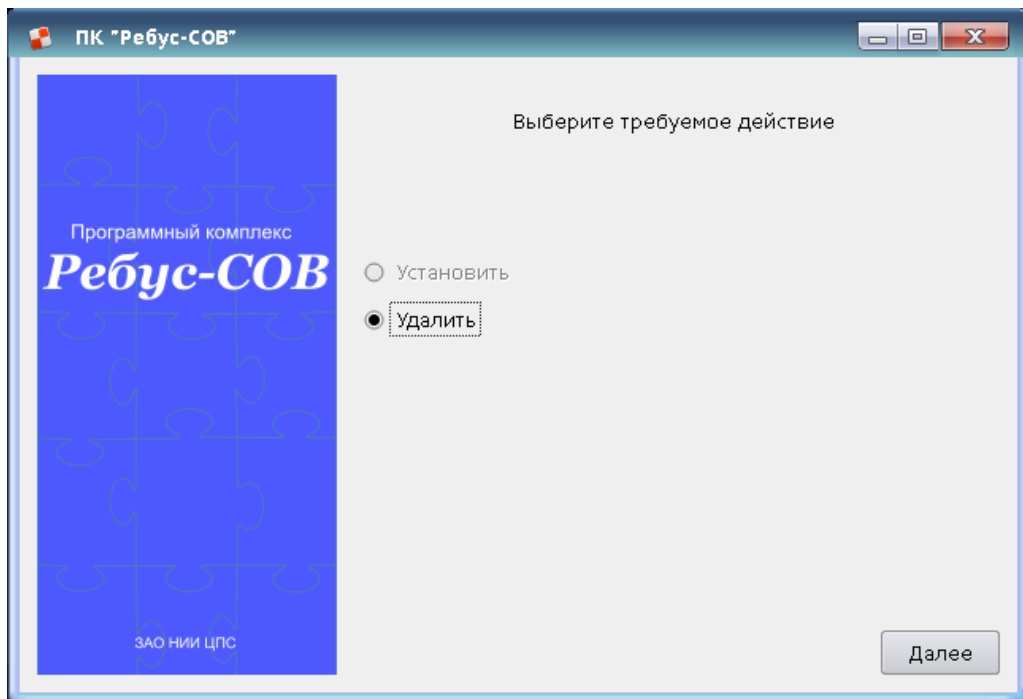


Рис. 18

Для выполнения удаления на первой странице мастера следует проверить действие переключателя, если он не на значении «Удалить», переключить его. Нажать кнопку «Далее». После этого откроется страница с суммарной информацией о параметрах удаления, изображённая на рис. 19.

Примечание. Текстовые поля в окнах мастера могут незначительно отличаться от указанных в зависимости от версии комплекса и используемой ОС.

Информация об удалении ПК «Ребус-СОВ»

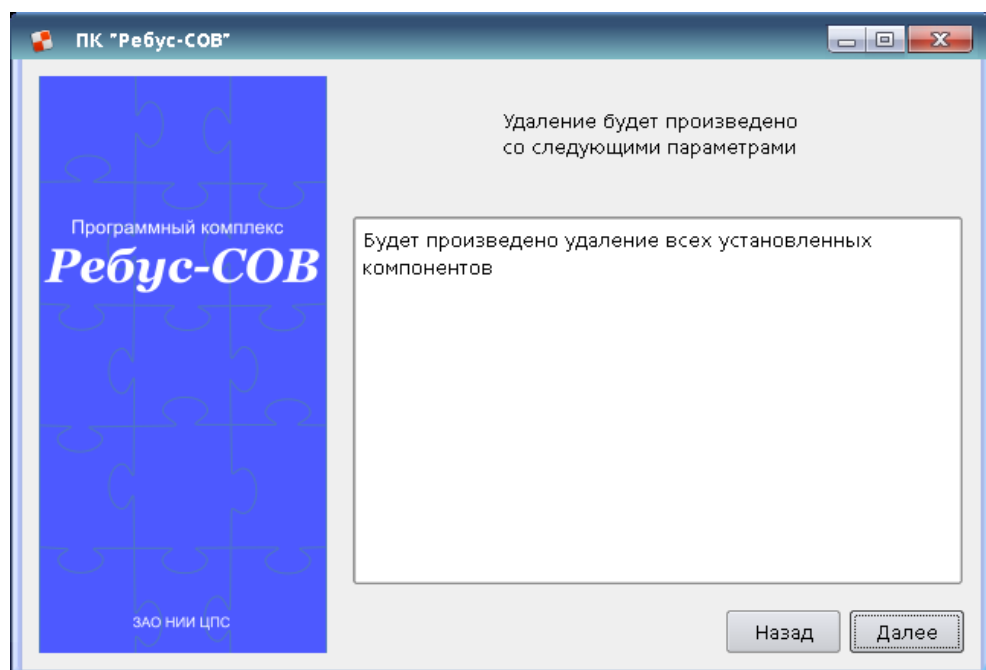


Рис. 19

Необходимо нажать на кнопку «Далее», после чего начнется удаление, ход которого отображается с помощью индикатора прогресса.

На заключительном шаге выводится сообщение о том, что удаление выполнено (рис. 20).

### Завершение удаления ПК «Ребус-СОВ»

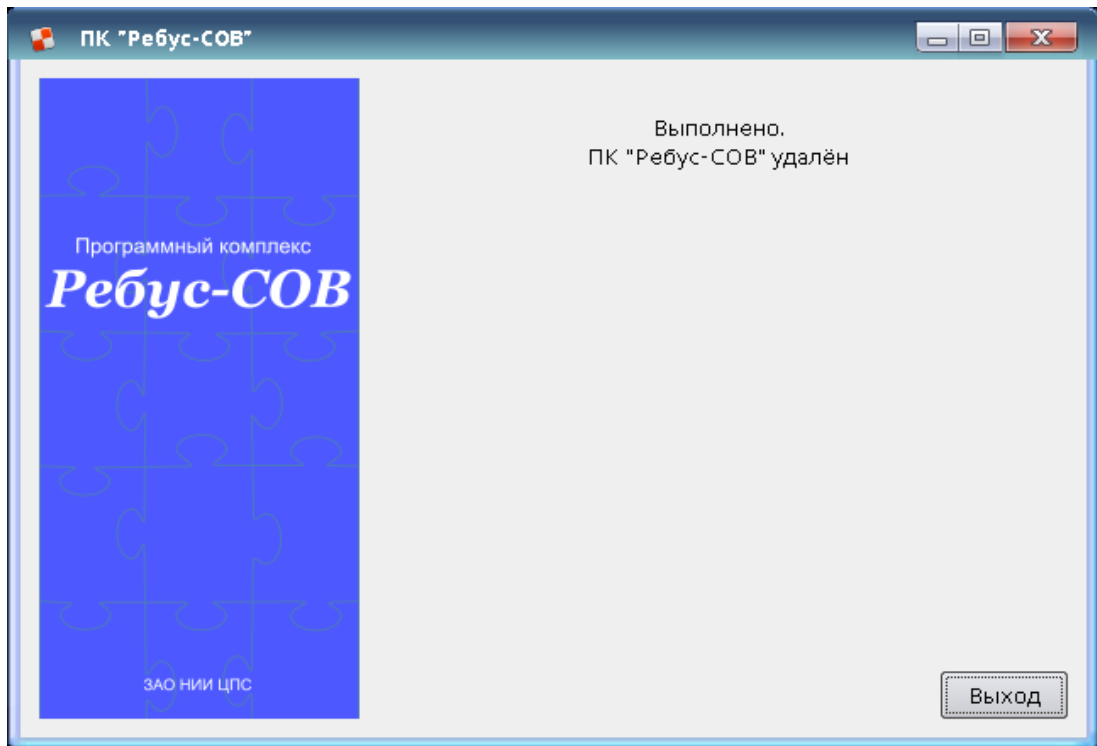


Рис. 20

## 4. ВЫПОЛНЕНИЕ ПРОГРАММЫ

### 4.1. Общие сведения о составе программы

ПК «Ребус-СОВ» работает на основе клиент-серверной архитектуры.

На каждой контролируемой станции размещается агентская часть программы (агент СОВ), которая выполняет функции локального сбора данных и анализа текущего состояния безопасности, реагирования на выявленные вторжения и передачи информации обо всех обнаруженных вторжениях на сервер. Кроме того, на каждой станции расположена консоль управления СОВ. Агент СОВ является системной службой.

Сервер СОВ размещается на выделенной станции. Сервер СОВ осуществляет централизованный сбор информации о вторжениях и оперативное оповещение администратора об обнаруженных вторжениях или нарушениях безопасности в режиме, приближенном к реальному времени.

### 4.2. Обязанности и возможности оператора

Для безопасной эксплуатации системы оператор должен:

- осуществлять обнаружение вторжений, используя консоль управления СОВ;
- выполнять анализ вторжений для обеспечения адекватной реакции, выяснения возможных последствий, а также выявления ложных срабатываний;
- осуществлять реагирование на обнаруженные вторжения. Оператор может выполнить блокировку станции либо сетевого трафика станции, используя консоль управления СОВ. Кроме того, оператор должен уведомить администратора о необходимости проведения мероприятий по устранению последствий вторжений;

- контролировать состояние СОВ. Оператор должен осуществлять аудит событий ПК «Ребус-СОВ» на предмет выявления проблем функционирования. В случае обнаружения проблем оператор должен уведомить администратора о необходимости устранения их причин.

Оператору доступны следующие функции безопасности, предоставляемые изделием:

- наблюдение за событиями, поступающими в консоль управления;
- осуществление реагирования на выявленные вторжения средствами консоли управления, а также снятие действующих блокировок;
- формирование отчетов по данным аудита ПК «Ребус-СОВ».

### 4.3. Средство настройки агентской части

#### 4.3.1. Назначение

Средство настройки агентской части предназначено для настройки функционирования агентской части СОВ.

Средство настройки агентской части позволяет решать следующие задачи:

- настройка параметров взаимодействия агентской части с сервером СОВ;
- локальное снятие установленных на станции блокировок;
- осуществление верификации целостности исполняемых модулей СОВ;
- осуществление верификации целостности сигнатур вторжений.

К параметрам сетевого взаимодействия относятся следующие настройки:

- сетевой адрес станции, на которой находится сервер СОВ;
- сетевой порт, по которому осуществляется взаимодействие сервера СОВ и агентской части СОВ;
- ключ, используемый для аутентификации агента СОВ на сервере СОВ.

#### 4.3.2. Запуск средства

Запуск средства настройки агентской части возможен только пользователем, входящим в группу администраторов данной станции. Для запуска в ОС МСВС пользователь должен входить в группу root. Для запуска в ОС СН «Astra Linux Special Edition» пользователь должен входить в группу astra-admin.

В ОС Windows запуск осуществляется выбором в меню «Пуск/Программы/ПК «Ребус-СОВ»/Средство настройки агентской части». В ОС МСВС и ОС СН «Astra Linux Special Edition» запуск осуществляется выбором в меню «Пуск/ПК «Ребус-СОВ»/Средство настройки агентской части» либо из терминала командой **ipsSettings**.

Примечания:

1. В ОС СН «Astra Linux Special Edition» версий 1.4 и 1.5 при отсутствии у пользователя прав на беспарольный запуск команд при помощи утилиты **sudo** запуск через элемент меню «Пуск/ПК «Ребус-СОВ»/Средство настройки агентской части» работать не будет. В данном случае необходимо запускать средство из терминала.

2. В ОС СН «Astra Linux Special Edition» версии 1.8 для появления раздела «Пуск/ПК «Ребус-СОВ» необходимо в контекстном меню кнопки «Пуск» выбрать опцию «Классическое меню».

Средство настройки агентской части может быть запущено только в единственном экземпляре. Модуль предоставляет однооконный интерфейс с тремя вкладками: «Настройки агентской части», «Верификация целостности модулей» и «Верификация целостности сигнатур вторжений».

#### 4.3.3. Настройки агентской части

На вкладке «Настройки агентской части» находятся настройки сетевого взаимодействия с сервером СОВ и блокировки станции, а также элементы управления агентской частью СОВ.

Элементы группы «Состояние агентской службы» служат для отображения текущего состояния службы и возможности управления службой. В группе «Настройки сетевого соединения с сервером СОВ» определяются параметры станции, на которой установлен сервер СОВ. В качестве адреса станции допустимо использовать IP-адрес сетевого интерфейса либо доменное имя. Также можно изменить основной порт, по которому производится соединение (следует помнить, что кроме основного порта ПК «Ребус-СОВ» при своей работе использует два порта, идущие непосредственно за ним – для основного порта 6669 это порты 6670 и 6671). Перед изменением настройки необходимо убедиться, что предполагаемые к использованию порты не используются другими программами. Также следует обратить внимание, что TCP-соединения с указанным адресом и используемыми портами должны быть разрешены в настройках межсетевых экранов на всех станциях.

Задание настроек сетевого взаимодействия является обязательным, так как неверное значение параметров приведет к невозможности взаимодействия с сервером СОВ. После запуска программы в полях ввода отображаются текущие настройки, некорректные данные выделяются красным цветом. После изменения поля для любой из настроек к описанию настройки добавляется символ «\*» для отображения факта изменения настройки.

Группа «Настройки аутентификации» определяет параметры аутентификации при установке соединения агентской части с серверной. Главным инструментом процесса аутентификации является ключ аутентификации, который используется при обмене сообщениями для установления доверенного соединения. Для успешной аутентификации необходимо соответствие ключей, используемых агентской службой и сервером СОВ. В поле «Текущий ключ аутентификации» отображается информация об используемом ключе.

Смена ключа аутентификации осуществляется в следующем порядке: сначала необходимо сгенерировать новый ключ на сервере СОВ, затем перенести этот ключ на агентские станции. Ключ может быть перенесен либо физически в виде файла, либо по парольной фразе.

Для генерации нового ключа на сервере необходимо запустить средство настройки агентской части на серверной станции, сгенерировать новый ключ по парольной фразе, нажать кнопку «Применить».

Для экспорта текущего активного ключа в файл необходимо нажать кнопку «Экспортировать ключ...» и в появившемся окне указать место каталога для сохранения файла ключа. Кнопка «Экспортировать ключ...» активна, только если программа запущена на сервере СОВ.

Перенос ключа на агентские станции может быть произведен двумя взаимоисключающими способами с помощью элементов группы «Подготовка нового ключа»:

1) новый ключ может быть сгенерирован по парольной фразе, которая должна соответствовать используемой сервером СОВ. Необходимо ввести парольную фразу и нажать кнопку «Генерировать»;

2) ключ сервера СОВ может быть перенесен на агентскую станцию в виде файла (по сети или при помощи внешнего носителя информации): для импорта файла ключа в программе следует нажать кнопку «Указать файл...» и в появившемся диалоге выбора файла указать файл ключа.

Для применения настроек сетевого взаимодействия и параметров аутентификации следует воспользоваться кнопкой «Применить» – будет произведен перезапуск агентской службы с новыми настройками.

Если имеются непримененные изменения настроек и будет производиться попытка закрытия программы, возникнет окно подтверждения выхода без сохранения произведенных изменений.

Нажатие кнопки «Снять блокировку» в группе «Действующие блокировки» отменяет действие всех блокировок, установленных на данной станции. Снятие блокировок доступно только при запущенной агентской службе.

#### 4.3.4. Верификация целостности модулей

На вкладке «Верификация целостности модулей» отображается контрольная сумма модулей ПК «Ребус-СОВ». Контрольная сумма должна совпадать с контрольной суммой, приведенной в документе ФДШИ.03618-01 30 01 «Формуляр», приложение 2.

#### 4.3.5. Верификация целостности сигнатур вторжений

На вкладке «Верификация сигнатур вторжений» отображается контрольная сумма сигнатур вторжений ПК «Ребус-СОВ». На сервере СОВ отображается контрольная сумма серверного хранилища сигнатур вторжений. На агентской станции отображается контрольная сумма сигнатур вторжений агентской станции. Для того чтобы выполнить верификацию сигнатур вторжений, необходимо провести расчет контрольной суммы сигнатур вторжений на серверной станции, записать полученную контрольную сумму. Далее провести аналогичный расчет на агентской станции и сравнить контрольную сумму с полученной ранее.

### 4.4. Консоль управления

#### 4.4.1. Назначение

Консоль управления предназначена для оперативного оповещения и отображения информации о вторжениях, обнаруженных на контролируемых узлах ИС (станциях). Консоль управления позволяет выполнять администратору и оператору СОВ следующие задачи:

- просмотр собранной статистики по агентам и вторжениям;
- контроль состояния агентских станций;
- блокировка/разблокировка станции и сетевого трафика;
- формирование отчетов.

Консоль управления позволяет выполнять следующие задачи администратору СОВ:

- управление задачей анализа сетевого трафика с использованием сигнатур;
- управление задачей анализа состава ЛВС;
- управление задачей анализа событий ФДШИ.469535.048 «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»));
- управление задачей анализа событий ОС и ПО;
- настройка автоматической реакции для случаев обнаружения вторжений;
- управление задачей анализа статистики сетевого трафика;
- управление внешними средствами;
- управление плагинами ПК «Ребус-СОВ»;
- управление набором сетевых интерфейсов для анализа трафика;
- управление задачей вывода событий информационной безопасности в SIEM-систему;
- управление учетными записями пользователей ПК «Ребус-СОВ»;

- управление синхронизацией времени;
- управление обновлениями сигнатур вторжений (баз решающих правил).

#### 4.4.2. Запуск консоли

Для запуска консоли управления необходимо выбрать в меню «Пуск/Программы/ПК «Ребус-СОВ»/Консоль управления» (для ОС MCBC), либо «Пуск/ПК «Ребус-СОВ»/Консоль управления» (для ОС СН «Astra Linux Special Edition»), либо «Пуск/Все программы/ПК «Ребус-СОВ»/Консоль управления» (для ОС Windows). Рекомендуется запускать консоль управления в несекретном сеансе.

**Примечание.** В ОС СН «Astra Linux Special Edition» версии 1.8 для появления раздела «Пуск/ПК «Ребус-СОВ» необходимо в контекстном меню кнопки «Пуск» выбрать опцию «Классическое меню».

Для доступа к консоли управления необходимо ввести идентификатор пользователя СОВ и его пароль. По умолчанию используются идентификатор «ОВИ» и пароль «supervis». Чтобы получить доступ к консоли управления с правами администратора в ОС MCBC, пользователь должен входить в группу root. Чтобы получить доступ к консоли управления с правами администратора в ОС СН «Astra Linux Special Edition», пользователь должен входить в группу astra-admin.

Консоль управления может быть запущена только в единственном экземпляре. Модуль предоставляет однооконный интерфейс с различным набором вкладок для оператора и администратора СОВ. Оператору доступны вкладки «Текущее состояние», «Аудит», «Станции» и «Отчеты». Администратору доступны дополнительно еще вкладки «Параметры защиты» и «Управление».

При успешном вводе идентификатора и пароля администратора СОВ на экране появляется главное окно консоли управления, изображенное на рис. 21. Главное окно консоли управления состоит из набора вкладок: «Текущее состояние», «Аудит», «Станции», «Параметры защиты», «Отчеты», «Управление».

Вкладка «Текущее состояние» при наличии новых вторжений

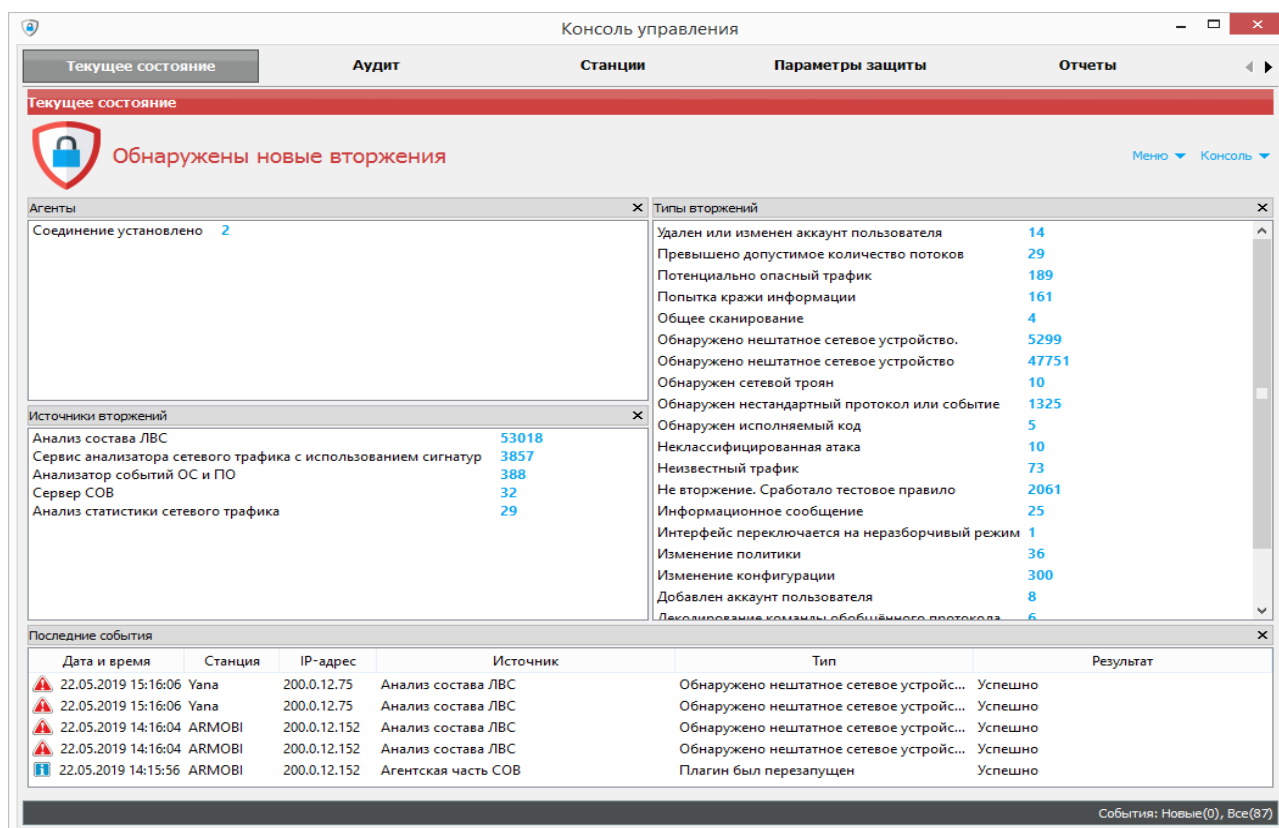


Рис. 21

#### 4.4.3. Вкладка «Текущее состояние»

Вкладка «Текущее состояние» предназначена для просмотра текущего состояния СОВ: накопленной статистики по состоянию агентов, источникам вторжений и типам вторжений, также можно просмотреть несколько событий, зарегистрированных за последнее время. Окрашивание индикатора текущего состояния красным цветом сигнализирует об обнаружении новых вторжений. При переходе на вкладку «Аудит» индикатор вторжений окрашивается зеленым цветом (рис. 22). В этом случае считается, что оператор СОВ успешно ознакомился с информацией по поступившим вторжениям и при необходимости предпринял защитные меры.

#### Вкладка «Текущее состояние» при отсутствии новых вторжений

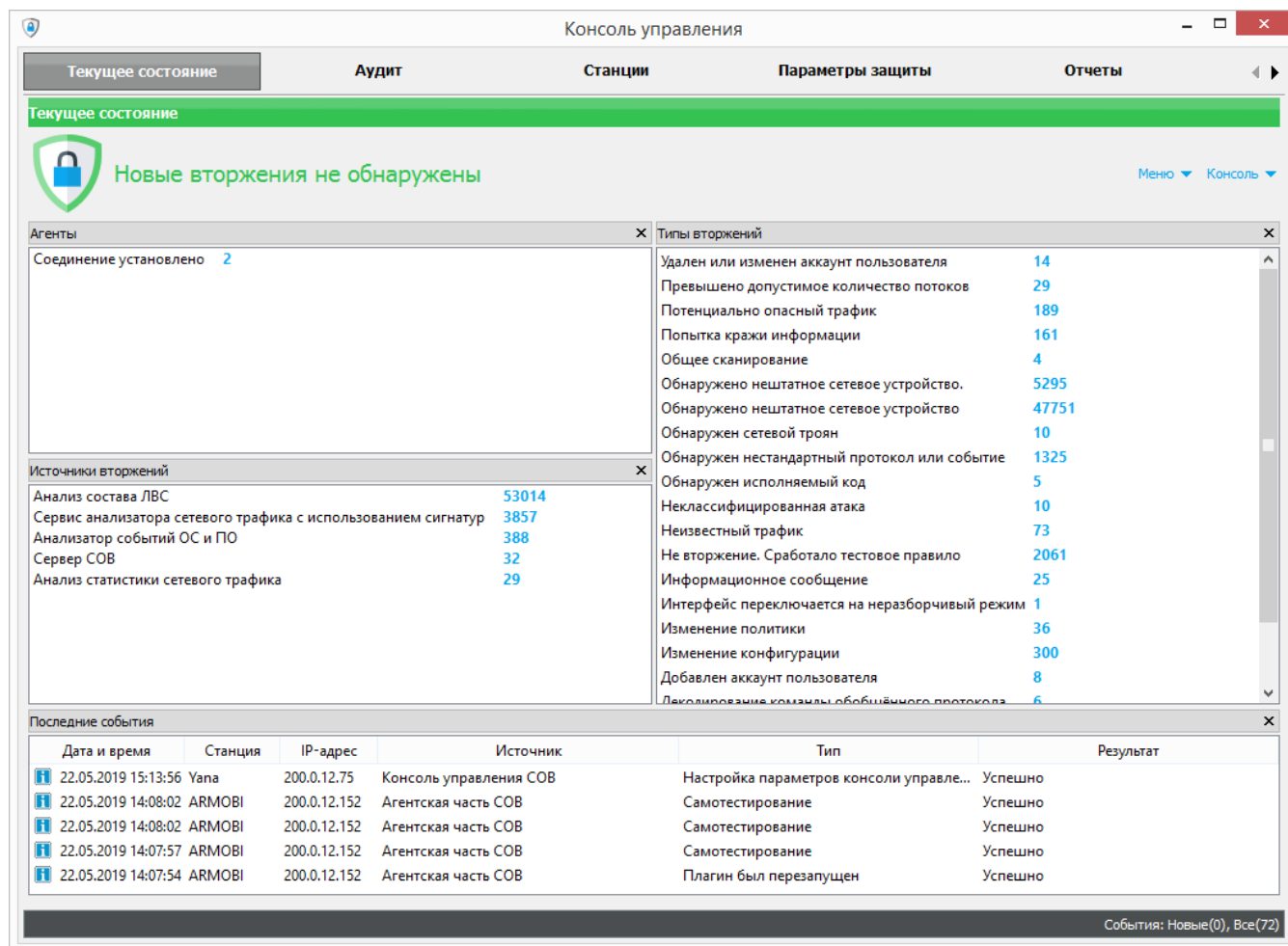


Рис. 22

Для изменения настроек отображения событий аудита и режима подключения к серверу СОВ при разрыве соединения требуется вызвать окно редактирования настроек.

Открытие окна редактирования настроек (рис. 23) производится выбором в меню на вкладке «Текущее состояние» пункта «Консоль/Настройка» или с помощью сочетания клавиш «Ctrl + K».

В группе «Отображение» можно указать количество отображаемых в консоли управления сообщений:

- вторжений и служебных сообщений во вкладке «Аудит»;
- сообщений по блокировкам во вкладке «Станции».

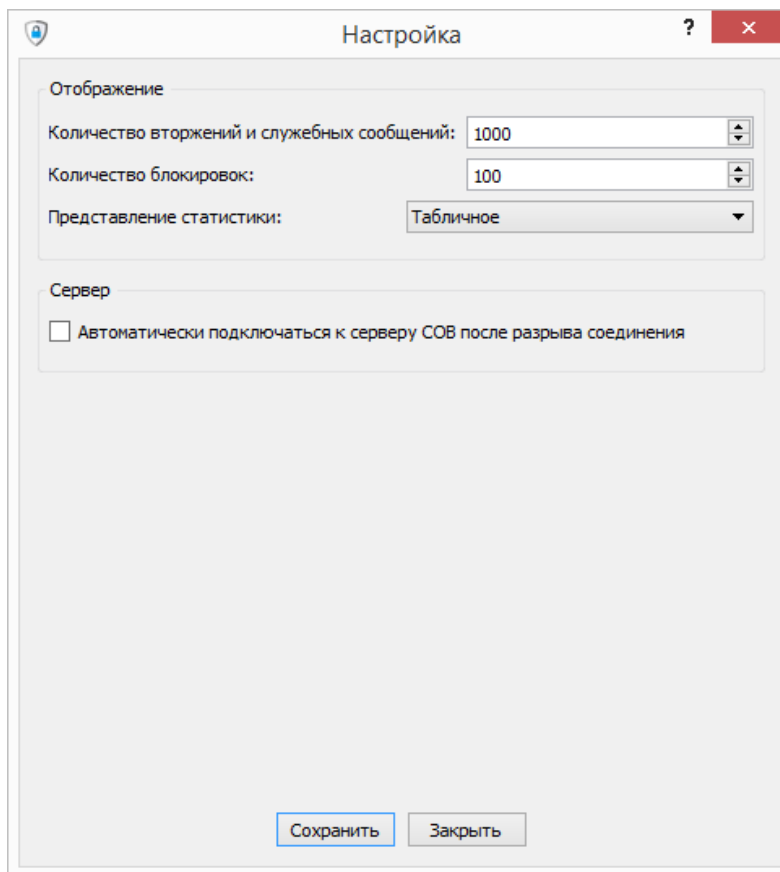
Минимально возможное количество отображаемых событий равно 10, максимально – 10000.

Отображаться будет указанное количество последних сообщений. Также в данной группе можно выбрать вид представления статистических данных: табличный или графический (рис. 24).

В группе «Сервер» можно изменить способ подключения к серверу СОВ в случае разрыва соединения.

Для вступления в силу новых настроек необходимо нажать кнопку «Сохранить».

#### Окно редактирования настроек



Настройка

Отображение

Количество вторжений и служебных сообщений: 1000

Количество блокировок: 100

Представление статистики: Табличное

Сервер

Автоматически подключаться к серверу СОВ после разрыва соединения

Сохранить    Закрыть

Рис. 23

## Графическое представление статистики

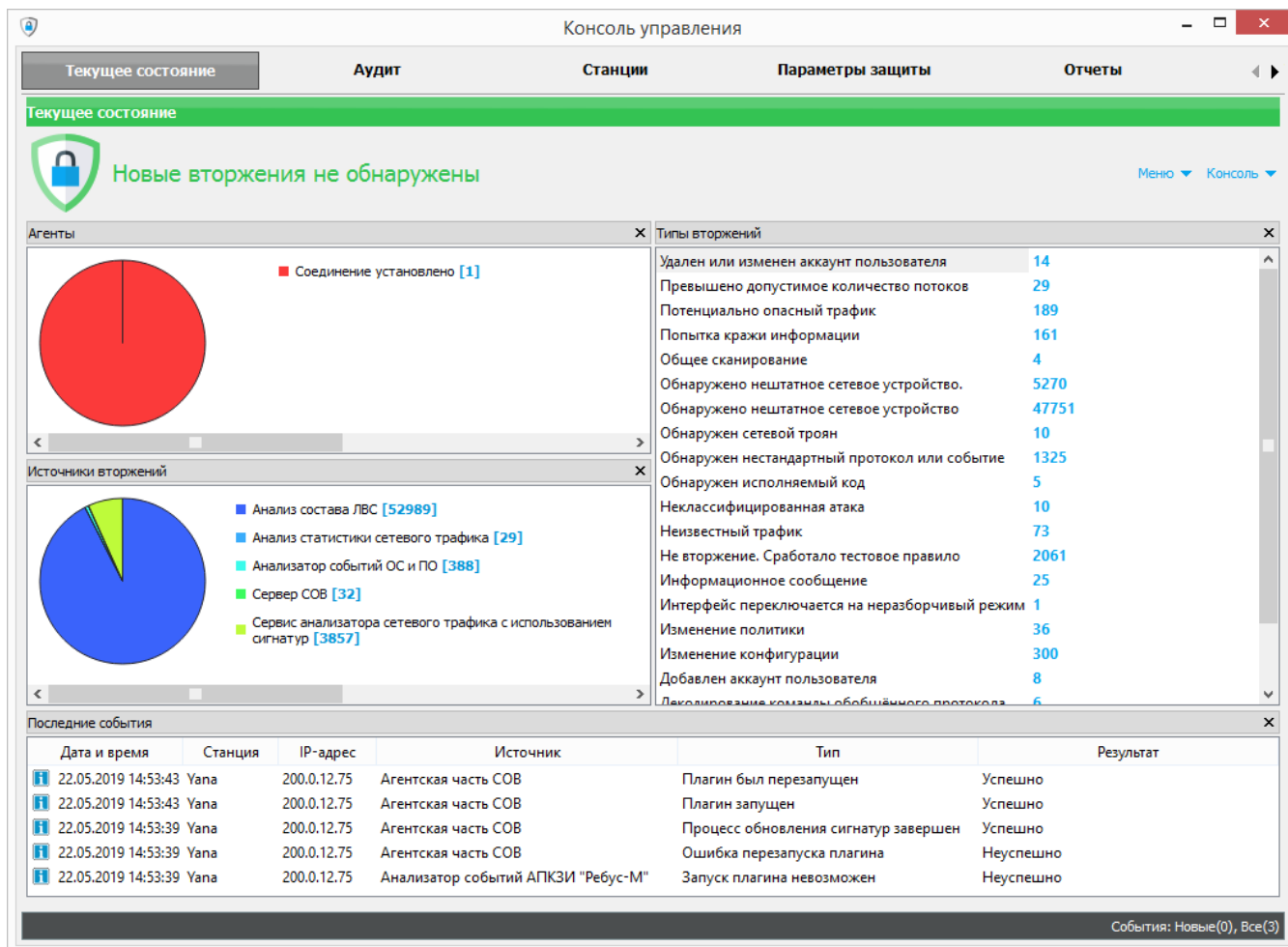


Рис. 24

### 4.4.4. Вкладка «Аудит»

Вкладка «Аудит» (рис. 25) предназначена для просмотра информации по событиям аудита. Служебная информация и информация обо всех обнаруженных на станциях вторжениях оперативно отображается в этой вкладке в таблице. По каждому событию в таблице отображаются следующие поля:

- дата и время;
- станция;
- IP-адрес;
- источник;
- тип;
- уровень важности;
- пользователь;
- результат.

Получить более подробную информацию по интересующему событию можно выделив его в таблице. Подробная информация по выбранному событию будет отображаться под таблицей событий.

Вкладка «Аудит»

Консоль управления

Текущее состояние    **Аудит**    Станции    Параметры защиты    Отчеты

Событий: 72

Фильтры    Очистить

Дата и время	Станция	IP-адрес	Источник	Тип	уровень важност	Пользователь	Результат
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Начало обновления сигнатур	Средний		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Запуск плагина	Низкий		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Успешно пройдена проверка целостности сигнатур	Средний		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Запуск агента COB	Средний		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Плагин запущен	Средний		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Плагин запущен	Средний		Успешно
22.05.2019 14:07:47	ARMOBI	200.0.12.152	Агентская часть COB	Плагин запущен	Средний		Успешно
22.05.2019 15:07:49	Yana	200.0.12.75	Сервер COB	Успешное подключение агента	Высокий		Успешно
22.05.2019 15:03:03	Yana	200.0.12.75	Агентская часть COB	Успешно пройдена проверка целостности сигнатур	Средний		Успешно
22.05.2019 15:03:03	Yana	200.0.12.75	Сервер COB	Успешно пройдена проверка целостности сигнатур	Высокий		Успешно
22.05.2019 14:57:41	Yana	200.0.12.75	Агентская часть COB	Плагин был перезапущен	Средний		Успешно
22.05.2019 14:57:41	Yana	200.0.12.75	Агентская часть COB	Плагин запущен	Средний		Успешно
22.05.2019 14:57:37	Yana	200.0.12.75	Агентская часть COB	Процесс обновления сигнатур завершен	Средний		Успешно
22.05.2019 14:57:37	Yana	200.0.12.75	Агентская часть COB	Плагин успешно остановлен	Средний		Успешно
22.05.2019 14:57:37	Yana	200.0.12.75	Агентская часть COB	Начало обновления сигнатур	Средний		Успешно
22.05.2019 14:57:29	Yana	200.0.12.75	Анализ состава ЛВС	Обнаружено нештатное сетевое устройство.	Низкий		Успешно
22.05.2019 14:57:29	Yana	200.0.12.75	Анализ состава ЛВС	Обнаружено нештатное сетевое устройство.	Низкий		Успешно
22.05.2019 14:57:29	Yana	200.0.12.75	Анализ состава ЛВС	Обнаружено нештатное сетевое устройство.	Низкий		Успешно
22.05.2019 14:57:29	Yana	200.0.12.75	Анализ состава ЛВС	Обнаружено нештатное сетевое устройство.	Низкий		Успешно

Дата и время: 22.05.2019 14:53:35, Станция: Yana

<b>Источник:</b> Сервер COB <b>Тип:</b> Обновление БП	<b>Описание:</b> Инициировано обновление базы решающий правил пользователем OBI со станции 200.0.12.75	<b>Реакция:</b> Нет
--	--	---------------------

События: Новые(0), Все(72)

Рис. 25

Над таблицей событий расположены две кнопки: «Фильтры» и «Очистить». Нажатие на кнопку «Очистить» приведет к удалению всех записей из таблицы событий.

Фильтрация событий аудита осуществляется по полям, содержащимся в таблице событий. Для вызова формы настройки фильтров необходимо нажать кнопку «Фильтры». Фильтрация событий происходит автоматически при изменении значений фильтров. Сбросить значения установленных фильтров можно нажатием на кнопку «Сбросить».

#### 4.4.5. Вкладка «Станции»

Вкладка «Станции» (рис. 26) предназначена для выполнения следующих действий:

- контроля состояния агентов COB;
- управления плагинами (доступно только администратору COB);
- выбора сетевых интерфейсов для анализа трафика (доступно только администратору COB);
- блокировки станции или сетевого трафика.

Вкладка «Станции»

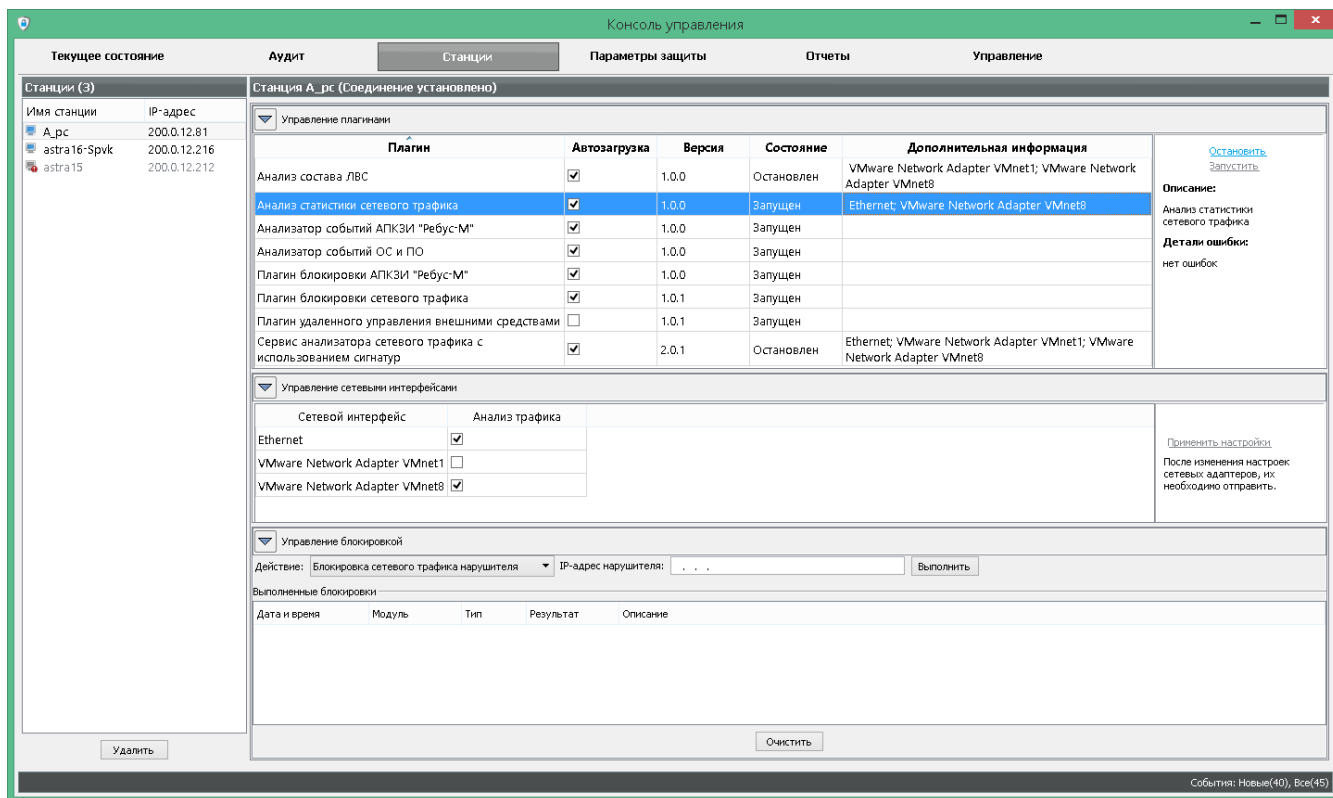


Рис. 26

В левой части вкладки содержится список станций, которые осуществляли подключение к серверу СОВ за время работы консоли управления. Для каждой станции показывается значок, содержащий о ней вспомогательную информацию в соответствии с таблицей 1.

Таблица 1 – Обозначения вспомогательной информации о станциях

Значок	Значение
	Контролируемая рабочая станция, доступная по сети в настоящий момент
	Контролируемая рабочая станция, которая при подключении к серверу СОВ не прошла аутентификацию
	Контролируемая рабочая станция, на которой установки, заданные по умолчанию, изменены (отключены агентские плагины)
	Контролируемая рабочая станция, на которой не запущена агентская часть программы
	Контролируемая рабочая станция, недоступная по сети в настоящий момент
	Контролируемая рабочая станция, которая завершила свою работу, не пройдя аутентификацию

Если в списке станций выбрать станцию, то в правой части по этой станции отобразится следующая информация:

- список установленных плагинов;
- список сетевых интерфейсов;
- список выполненных блокировок.

Имя выбранной станции и информация о соединении с ней отображаются в названии группы «Станция», например, «Станция АРМОБИ (Соединение установлено)».

Из консоли управления можно удаленно запускать и останавливать плагины, установленные на станции. Для запуска или остановки плагина на выбранной станции нужно в форме «Управление плагинами» (рис. 27) выбрать требуемый плагин и в активизированных справа от таблицы элементах управления выбрать в зависимости от задачи ссылку «Запустить»

или «Остановить». Состояние плагина на текущий момент отображается в той же таблице, где происходит выбор плагина в колонке «Состояние».

### Форма «Управление плагинами»

Плагин	Автозагрузка	Версия	Состояние	Дополнительная информация
Анализ состава ЛВС	<input checked="" type="checkbox"/>	1.0.0	Остановлен	VMware Network Adapter VMnet1; VMware Network Adapter VMnet8
Анализ статистики сетевого трафика	<input checked="" type="checkbox"/>	1.0.0	Запущен	Ethernet; VMware Network Adapter VMnet8
Анализатор событий АПКЗИ "Ребус-М"	<input checked="" type="checkbox"/>	1.0.0	Запущен	
Анализатор событий ОС и ПО	<input checked="" type="checkbox"/>	1.0.0	Запущен	
Плагин блокировки АПКЗИ "Ребус-М"	<input checked="" type="checkbox"/>	1.0.0	Запущен	
Плагин блокировки сетевого трафика	<input checked="" type="checkbox"/>	1.0.1	Запущен	
Плагин удаленного управления внешними средствами	<input type="checkbox"/>	1.0.1	Остановлен	
Сервис анализатора сетевого трафика с использованием сигнатур	<input checked="" type="checkbox"/>	2.0.1	Остановлен	Ethernet; VMware Network Adapter VMnet1; VMware Network Adapter VMnet8

Рис. 27

В консоли управления для каждой станции можно выбрать сетевые интерфейсы, на которых будет осуществляться анализ сетевого трафика. Управление сетевыми интерфейсами доступно для следующих анализаторов:

- анализ состава ЛВС;
- анализ статистики сетевого трафика;
- анализ сетевого трафика с использованием сигнатур.

Для настройки сетевых интерфейсов нужно открыть форму «Управление сетевыми интерфейсами» (рис. 28), выбрав анализатор в таблице формы «Управление плагинами». В открывшейся форме будет таблица, в которой в первой колонке будет название сетевого интерфейса, а во второй – элементы для управления состоянием адаптеров. После изменения настроек сетевых адаптеров их необходимо сохранить, нажав ссылку «Применить настройки».

### Форма «Управление сетевыми интерфейсами»

Сетевой интерфейс	Анализ трафика
Ethernet	<input checked="" type="checkbox"/>
VMware Network Adapter VMnet1	<input type="checkbox"/>
VMware Network Adapter VMnet8	<input checked="" type="checkbox"/>

Рис. 28

Анализатор «Анализ состава ЛВС» распознает и анализирует проходящий через сетевые интерфейсы VLAN-трафик. При этом для его корректного анализа доступны два подхода:

- 1) анализ трафика на основном сетевом интерфейсе (интерфейсе, поверх которого создана VLAN-сеть) включить, на VLAN-интерфейсе выключить;
- 2) анализ трафика на VLAN-интерфейсе включить, на основном интерфейсе выключить (стоит учесть, что при этом анализироваться не будет весь проходящий через основной интерфейс трафик).

При одновременном включении анализа и на основном, и на VLAN-интерфейсе сообщения анализатора будут дублироваться.

Из консоли управления можно заблокировать станцию средствами АПКЗИ «Ребус-М» (при наличии на этой станции установленного ФДШИ.01792-06 «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»). Программное обеспечение для ОС семейства Windows»), а также заблокировать или разблокировать сетевой трафик. Для выполнения блокировки выбранной станции нужно в форме «Управление блокировкой» (рис. 29) выбрать действие «Блокировка станции» и нажать кнопку «Выполнить». Результат блокировки отобразится в таблице «Выполненные блокировки». Если на станции зарегистрирован администратор, то блокировка станции не будет выполнена и в графе «Результат» отобразится «Пропуск».

Примечание. Номер издания в обозначении ПО (или редакции в обозначении программной документации) в поставленном комплекте АПКЗИ «Ребус-М» может отличаться от указанного.

### Форма «Управление блокировкой»

Управление блокировкой				
Действие: Разблокировка сетевого трафика нарушителя		IP-адрес нарушителя: 200.0.12.230		Выполнить
Выполненные блокировки				
Дата и время	Модуль	Тип	Результат	Описание
05.06.2019 11:39:25	blockNetPlugin	Консоль	Успех	Выполнена разблокировка IP-адреса 200.0.12.230
05.06.2019 11:32:48	blockNetPlugin	Консоль	Успех	Выполнена блокировка IP-адреса 200.0.12.230
05.06.2019 11:32:08	blockRebus	Консоль	Пропуск	Невозможно заблокировать станцию, т.к. текущий пользователь является администратором

Очистить

Рис. 29

Для выполнения блокировки или разблокировки сетевого трафика выбранной станции нужно в разделе «Управление блокировкой» выбрать действие «Блокировка сетевого трафика станции» или «Разблокировка сетевого трафика станции» соответственно и нажать кнопку «Выполнить». Результат блокировки/разблокировки отобразится в таблице «Выполненные блокировки».

Для выполнения блокировки или разблокировки пакетов, которые идут от IP-адреса нарушителя (с известным IP-адресом) на выбранную станцию, нужно в разделе «Управление блокировкой» выбрать действие «Блокировка сетевого трафика нарушителя» или «Разблокировка сетевого трафика нарушителя», указать IP-адрес нарушителя и нажать кнопку «Выполнить». Результат блокировки/разблокировки отобразится в таблице «Выполненные блокировки».

#### 4.4.6. Вкладка «Параметры защиты»

4.4.6.1 Вкладка «Параметры защиты» доступна только администраторам СОВ и предназначена для выполнения настроек следующих механизмов:

- контроля состава ЛВС;
- анализа событий АПКЗИ «Ребус-М»;
- автоматической реакции для случаев обнаружения вторжений;
- анализа сетевого трафика с использованием сигнатур (см. 4.5);
- анализа статистики сетевого трафика;
- управления внешними средствами (см. 4.6).

В левой части вкладки расположен список настраиваемых механизмов. При выборе в списке названия нужного механизма в правой части вкладки появляется функционал по выполнению настройки выбранного механизма.

4.4.6.2 Настройка механизма анализа состава ЛВС заключается в формировании перечня доверенных сетевых устройств.

Для формирования перечня доверенных сетевых устройств необходимо произвести следующие действия:

- во вкладке «Параметры защиты» в списке слева выбрать «Контроль состава ЛВС», в результате чего откроется окно «Настройка списка доверенных сетевых устройств»;
- включить режим редактирования данных на сервере, нажав кнопку «Включить режим редактирования»;
- нажать кнопку «Добавить», появится окно «Добавление адреса» (рис. 30);
- выбрать переключатель типа записи, в зависимости от типа записи задать IP-адрес сетевого устройства, диапазон IP-адресов или IP-адрес с аппаратным адресом, при необходимости задать примечание для устройства, нажать кнопку «ОК»;
- повторить предыдущее действие для добавления IP-адресов остальных доверенных сетевых устройств;
- нажать кнопку «Сохранить» в окне «Настройка списка доверенных сетевых устройств». Сохраненный перечень доверенных сетевых устройств будет передан на сервер СОВ.

Диалоговое окно «Добавление адреса»

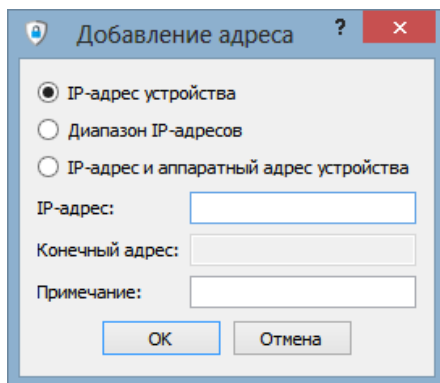


Рис. 30

4.4.6.3 Настройка механизма анализа событий АПКЗИ «Ребус-М» заключается в отнесении зарегистрированных событий АПКЗИ «Ребус-М» к атакам.

Для формирования списка событий, которые ПК «Ребус-СОВ» будет считать атаками, необходимо произвести следующие действия:

- во вкладке «Параметры защиты» в списке слева выбрать «Анализ событий АПКЗИ «Ребус-М»;

- включить режим редактирования данных на сервере, нажав кнопку «Включить режим редактирования»;

- в списке событий напротив событий, которые будут считаться атаками, поставить «галочку», в противном случае «крестик»;

- нажать кнопку «Сохранить».

Сохраненный список атак будет передан на сервер СОВ.

4.4.6.4 Чтобы сформировать правило автоматической реакции на вторжения, администратор должен перейти во вкладку «Автоматическая реакция на события» и включить режим редактирования, нажав кнопку «Включить режим редактирования». Затем нужно выбрать источник данных о вторжениях из списка «Источники», который содержит в себе пункты:

- «Анализ состава ЛВС»;

- «Анализ событий ОС и ПО»;

- «Анализ сетевого трафика».

После выбора источника становится доступным список типов событий для данного источника. Необходимо выбрать тип события. У источников «Анализ событий ОС и ПО» и «Анализ сетевого трафика» в событиях необходимо выбрать блокировку по уровню вторжения. Далее необходимо выбрать тип блокировки: «Блокировка сетевого трафика», «Блокировка станции» или «Настройка внешнего средства». При выборе типа «Настройка внешнего средства» в появившемся выпадающем списке необходимо выбрать сценарий, который будет срабатывать при автоматической реакции. Далее необходимо нажать кнопку «Создать правило» и кнопку «Сохранить». В результате правило добавится в список правил.

Для того чтобы удалить правило, необходимо перейти в режим редактирования, нажав кнопку «Включить режим редактирования», выбрать его в списке правил и нажать кнопку «Удалить».

После редактирования таблицы для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные файлы настроек автоматической реакции на вторжения будут переданы на сервер СОВ.

4.4.6.5 Настройка механизма анализа статистики сетевого трафика заключается в установке допустимого количества потоков данных. Превышение установленного количества потоков будет считаться атакой.

Для формирования настроек анализа статистики сетевого трафика, необходимо произвести следующие действия:

- во вкладке «Параметры защиты» в списке слева выбрать «Анализ статистики сетевого трафика»;
- включить режим редактирования данных на сервере, нажав кнопку «Включить режим редактирования»;
- в параметрах настройки указать допустимое количество потоков и интервал проверки;
- нажать кнопку «Сохранить».

Отредактированные параметры настройки анализа статистики сетевого трафика будут переданы на сервер СОВ.

Редактирование настроек анализа сетевого трафика с использованием сигнатур подробно рассмотрено в 4.5.

Управление внешними средствами подробно рассмотрено в 4.6.

#### 4.4.7. Вкладка «Отчеты»

Вкладка «Отчеты» предназначена для формирования по заданным фильтрам отчетов по событиям аудита и сохранения сформированных отчетов в файл формата HTML.

При формировании отчета по событиям аудита существует возможность задания условий фильтрации данных аудита по следующим критериям:

- события (вторжения или служебные сообщения);
- временной диапазон;
- станции;
- пользователи;
- источники;
- уровень важности;
- архивы.

После задания необходимых параметров фильтрации следует нажать на кнопку «Сохранить отчет». В открывшемся окне «Выбор места сохранения отчета» указать каталог, куда будет сохранен отчет, и нажать кнопку «Выбор папки». В результате будет сформирован и сохранен отчет в указанный каталог. Автоматическое открытие отчета после формирования осуществляется при установленной «галочке» в переключателе «Открыть отчет после сохранения».

#### 4.4.8. Вкладка «Управление»

4.4.8.1. Вкладка «Управление» предназначена для выполнения администратором СОВ следующих задач:

- управление учетными записями субъектов доступа (пользователей) СОВ;
- управление настройками сервера СОВ;
- настройка вывода событий ИБ в SIEM;
- настройка синхронизации времени;
- обновления БРП (баз решающих правил).

В левой части вкладки расположен список доступных для управления механизмов. При выборе в списке названия нужного механизма в правой части вкладки появляется функционал по управлению выбранным механизмом.

4.4.8.2. Для управления учетными записями пользователей СОВ необходимо в списке доступных для управления механизмов выбрать пункт «Учетные записи». Нажать кнопку «Включить режим редактирования» в правой части вкладки, после чего станет доступным список текущих пользователей с указанием их параметров и кнопок «Добавить...» – для добавления нового пользователя, «Изменить...» – для редактирования выбранного в списке пользователя и «Удалить» – для удаления выбранного пользователя. После редактирования учетных записей для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные настройки будут переданы на сервер СОВ.

В настройках учетной записи пользователя можно задать адрес электронной почты как для администратора СОВ, так и для оператора. Для всех пользователей СОВ, которым прописан

адрес электронной почты, будет осуществляться информирование о вторжениях с помощью почтовой рассылки.

4.4.8.3. Для редактирования настроек сервера необходимо в списке доступных для управления механизмов выбрать пункт «Серверы». Нажать кнопку «Включить режим редактирования» в правой части вкладки на форме «Настройка параметров локального сервера», после чего станут доступны элементы для редактирования.

В группе «Почтовая рассылка» задаются настройки почтовой рассылки: адрес почтового сервера, механизм защиты соединения, идентификатор и пароль пользователя, почтовый адрес отправителя и интервал отправки рассылки. Для отключения почтовой рассылки нужно установить интервал отправки рассылки равным нулю.

В группе «Архивирование событий аудита» задаются максимальное количество событий в архиве, интервалы смены архивов и проверки свободного места на диске, а также порог уведомления об отсутствии свободного места.

После редактирования настроек сервера для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные настройки будут переданы на сервер СОВ.

4.4.8.4. Для редактирования настроек вывода событий ИБ в SIEM необходимо в списке доступных для управления механизмов выбрать пункт «SIEM» и включить режим редактирования, нажав кнопку «Включить режим редактирования» на форме «Настройка вывода в SIEM».

В группе «Вывод в SIEM» можно настроить запись в файл, указав каталог для записи событий, или в Syslog (только для ОС СН «Astra Linux Special Edition»). После включения записи событий в Syslog можно также настроить их отправку на удалённый сервер сбора событий, указав его адрес и порт.

**Примечание.** Для исключения рекурсивной обработки сообщений не рекомендуется в качестве адреса удалённого сервера сбора событий указывать адрес сервера СОВ в комбинации с портом, который используется Syslog по умолчанию (514).

В группе «Фильтр по событиям» можно установить уровень важности для вторжений и сервисных сообщений. Все события, имеющие уровень важности, равный установленному и выше, будут записаны в SIEM.

После редактирования настроек вывода в SIEM для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные настройки будут переданы на сервер СОВ.

На сервере сбора логов для приема событий ИБ через Syslog необходимо выполнить настройки, зависящие от используемой службы журналирования – rsyslog или syslog-ng. Ниже приведены инструкции по настройке для обоих вариантов. Инструкции предполагают, что для приема событий ИБ служба журналирования использует порт по умолчанию (UDP-порт 514), при использовании другого порта настройки должны быть изменены соответствующим образом.

Если на сервере сбора событий используется служба журналирования rsyslog, то необходимо:

- дописать в конец файла **/etc/rsyslog.conf** строки (если их нет) или раскомментировать:

```
$ModLoad imudp
$UDPServerRun 514
```

- создать или отредактировать файл **/etc/rsyslog.d/events-from-rebus-sov.conf**, добавив в него строку «if \$programname startswith 'RebusIPS-SIEM' then /var/log/Rebus\_siem.log» (путь, по которому будут записываться SIEM-сообщения от ПК «Ребус-СОВ»);

- перезапустить службу, выполнив в терминале команду **sudo service rsyslog restart**.

Если на сервере сбора событий используется служба журналирования syslog-ng, то необходимо:

- создать или отредактировать файл **/etc/syslog-ng/conf.d/events-from-rebus-sov.conf**, добавив в него строки:

```
source s_rebus_udp {
    udp(ip(0.0.0.0) port(514));
};
destination d_rebus {
    file("/var/log/Rebus_siem.log");
```

```
};  
filter f_rebus_udp {  
    message("RebusIPS-SIEM");  
};  
log {  
    source(s_rebus_udp);  
    filter(f_rebus_udp);  
    destination(d_rebus);  
};
```

- перезапустить службу, выполнив в терминале команду **sudo service syslog-ng restart**.

4.4.8.5. Для редактирования настроек синхронизации времени необходимо в списке доступных для управления механизмов выбрать пункт «Синхронизация времени» и включить режим редактирования, нажав кнопку «Включить режим редактирования» на форме «Настройка синхронизации времени». Чтобы включить автоматическую синхронизацию времени с сервером СОВ, нужно отметить «галочкой» пункт «Синхронизировать время». В настройках синхронизации времени можно задать интервал проверки времени и максимально допустимую разницу во времени. Максимально допустимая разница во времени задается в секундах, интервал проверки времени – в секундах, минутах, часах, днях, неделях, месяцах.

После редактирования настроек синхронизации времени для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные настройки будут переданы на сервер СОВ.

4.4.8.6. Выполнение обновления сигнатур вторжений подробно рассмотрено в 4.7.

4.5. Редактирование параметров средства анализа сетевого трафика с использованием сигнатур

4.5.1. Общие сведения

Настройка средства анализа сетевого трафика подразумевает как задание параметров работы средства, так и редактирование правил.

Для осуществления настройки в консоли управления СОВ есть специальная форма. Ее вид приведен на рисунке 31. Интерфейс описывается в 4.5.3 – 4.5.6. Редактирование из этой формы консоли управления – единственный доступный способ настройки анализа сетевого трафика. Редактировать конфигурационные файлы из каких-либо внешних средств невозможно, т.к. ПК «Ребус-СОВ» контролирует целостность этих файлов и восстанавливает их из архива при обнаружении изменений. Только при настройке с помощью консоли управления изменения файлов рассматриваются механизмом контроля целостности как санкционированные и не перезаписываются из резервной копии.

Плагин настройки анализа сетевого трафика с использованием сигнатур

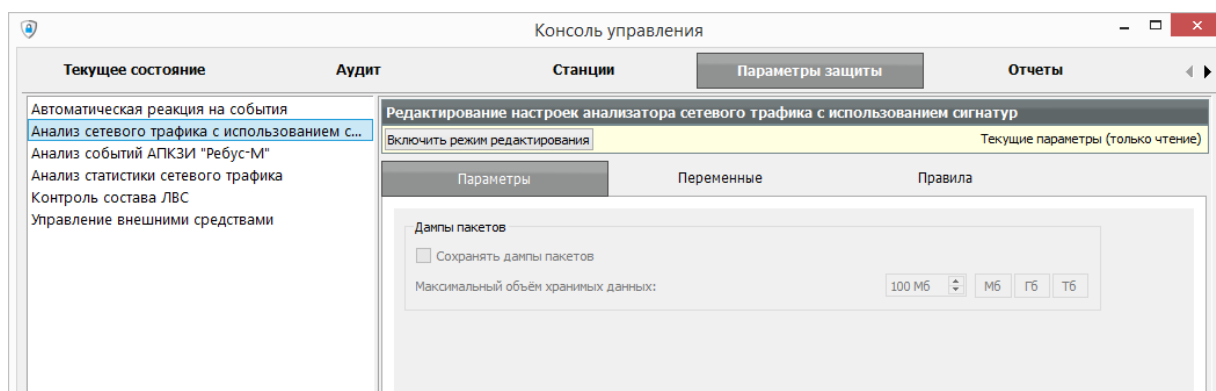


Рис. 31

Форма редактирования доступна на вкладке «Параметры защиты» консоли управления. Углубленное описание работы с плагином приведено в 4.5.3 – 4.5.6.

Предполагается, что администратор знаком с форматом конфигурационных файлов, описание которого дано в приложении к документу ФДШИ.03618-01 31 01 «Описание применения».

#### 4.5.2. Описание формы редактирования

Чтобы отредактировать настройки, необходимо в консоли выбрать вкладку «Параметры защиты» и на ней в списке слева выбрать «Анализ сетевого трафика с использованием сигнатур». После этого на вкладке отобразится форма «Редактирование настроек анализатора сетевого трафика с использованием сигнатур» (см. рис. 31).

Большую часть формы занимают три вкладки:

- «Параметры» – служит для настройки параметров средства (рассматривается в 4.5.3);
- «Переменные» – служит для работы с переменными (рассматривается в 4.5.4);
- «Правила» – служит для работы с правилами (рассматривается в 4.5.5).

Вверху формы расположена кнопка «Включить режим редактирования» и индикатор состояния. Индикатор состояния (находится справа) – это просто текстовая метка, в которой отображается состояние плагина.

БРП хранится на сервере СОВ, на рабочей же станции только текущая копия БРП. Когда пользователь переходит к форме плагина, в ней отображается текущая копия, о чём говорит текст «Текущие параметры (только чтение)» в индикаторе состояния.

Для того чтобы выполнить редактирование БРП, необходимо перейти в режим редактирования, нажав кнопку «Включить режим редактирования». При этом на сервере устанавливается признак блокировки файлов для остальных администраторов. Это нужно, чтобы в определённый момент времени только один администратор с одной ЭВМ мог редактировать настройки, т.к. одновременное редактирование несколькими людьми привело бы к несогласованности их изменений.

После перехода в режим редактирования вверху формы станут доступны кнопки управления (рис. 32). Назначение кнопок приведено в таблице 2.

Форма редактирования настроек (открыта вкладка «Правила»)

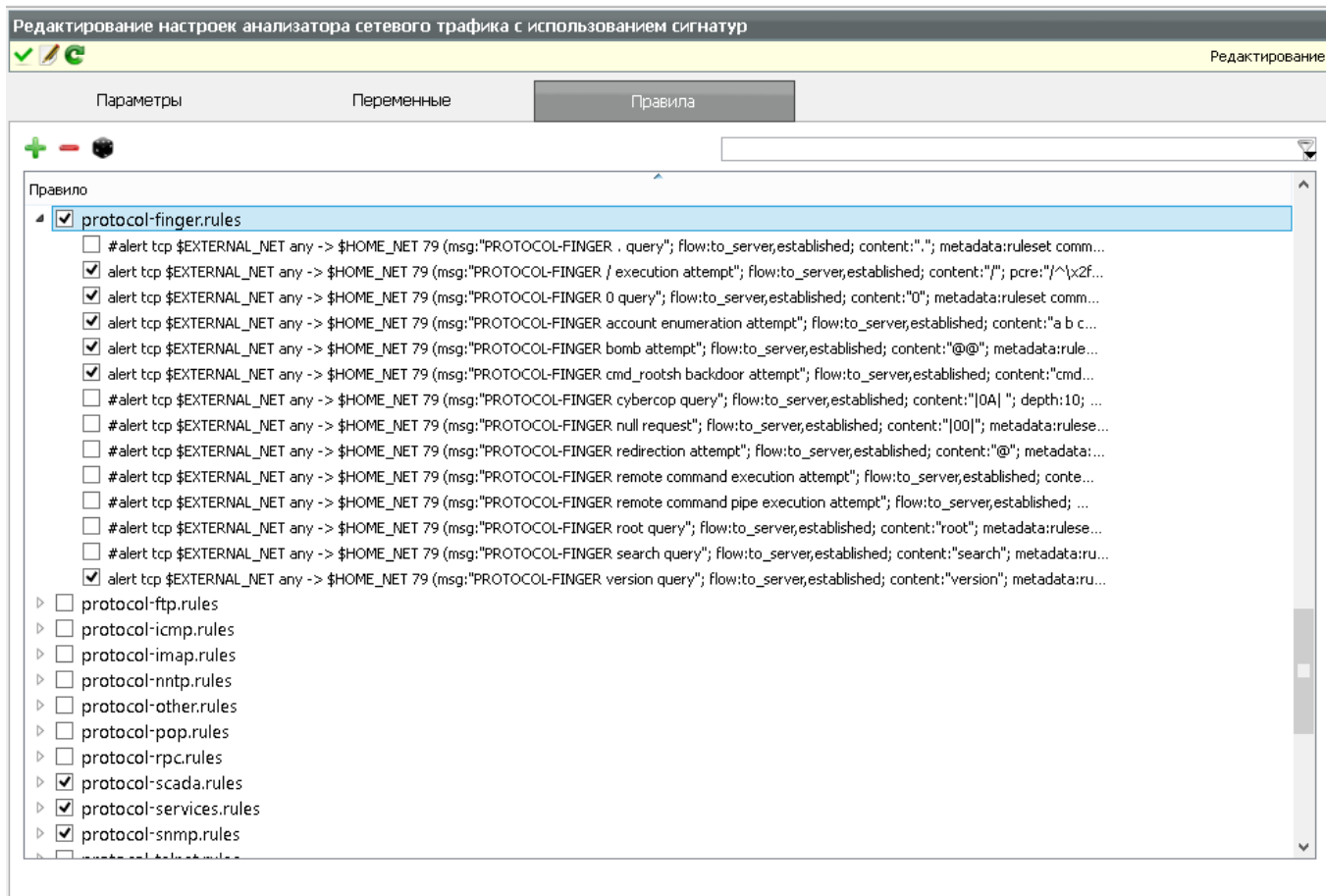


Рис. 32

Таблица 2 – Кнопки управления

Кнопка	Название	Горячая клавиша	Действие
	Открыть редактор	Нет	Вызов окна для работы с текстом конфигурационных файлов
	Отправить на сервер	Нет	Отправляет на сервер изменённые файлы и снимает признак блокировки
	Перечитать файлы	F5	Запускает повторный разбор файлов

Чтобы начать работу с редактором конфигурационных файлов, нужно нажать кнопку «Открыть редактор». Подробная работа с редактором рассматривается в 4.5.6.

В процессе скачивания файлов БРП индикатор состояния отображает текст «Скачивание настроек с сервера». Необходимо дождаться, когда он отобразит текст «Редактирование». Это означает, что файлы скачаны и на вкладках отображается уже не текущая копия БРП, а эти скачанные файлы. Когда отображён такой текст, параметры можно редактировать.

После того как администратор внёс необходимые изменения, нужно нажать кнопку «Отправить на сервер». При этом отредактированные правила и конфигурационные файлы будут отправлены на сервер СОВ и записаны в БРП. Дальше сервер СОВ произведет автоматическое тиражирование изменений в БРП по рабочим станциям.

После того как файлы будут отправлены на сервер, признак блокировки будет снят и другие администраторы смогут внести уже свои изменения.

После отправки изменений на сервер в форме опять отображается текущая копия БРП, так что появление текста «Текущие параметры (только чтение)» на индикаторе состояния говорит о том, что данные успешно переданы на сервер.

#### 4.5.3. Настройка сохранения дампов сетевых пакетов

Настройка сохранения дампов сетевых пакетов осуществляется во вкладке «Параметры». Данная вкладка представлена на рис. 33, предназначена для настройки сохранения дампов пакетов. Чтобы включить сохранение сетевых пакетов, вызвавших срабатывание правил, нужно отметить переключатель «Сохранять дампы пакетов» в группе «Дампы пакетов». Администратор также может указать максимальный объем хранимых данных, при достижении которого самые старые дампы будут удалены.

#### Вкладка «Параметры»

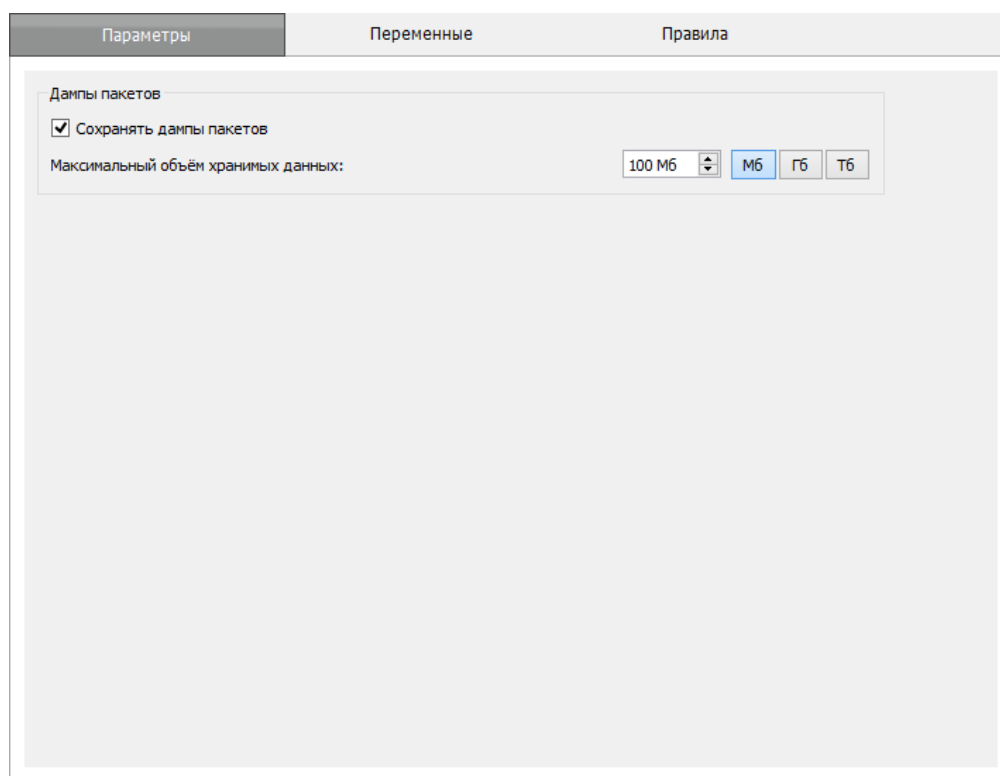


Рис. 33

Дампы пакетов будут сохраняться в каталог `/var/lib/rebus-sov/traffic-dump` в ОС СН «Astra Linux Special Edition» и ОС MCBC и в каталог `C:\ProgramData\CPS\rebus-sov\traffic-dump` в ОС Windows.

В случае, если необходимо сохранять не только сетевой трафик, непосредственно вызвавший срабатывание правил, но и предшествующий и последующий трафики, то необходимо отредактировать файл `parameters.conf` в редакторе, описанном в 4.5.6.

В этот файл необходимо добавить подключение препроцессора `netanalyzer_dump`. Необходимые параметры в файл уже занесены, но закомментированы. Нужно найти с помощью поиска строку, начинающуюся с «`preprocessor netanalyzer_dump`», и раскомментировать её.


В этой же строке после имени препроцессора перечислены параметры работы этого препроцессора в виде «<ключ> <значение>». Значения параметров администратор может менять в зависимости от потребностей. Можно также удалить любой из параметров, тогда будет использоваться значение по умолчанию. Параметры работы перечислены в таблице 3.

Таблица 3 – Параметры препроцессора netanalyzer\_dump

Назначение	Ключ	Минимальное значение	Максимальное значение	Значение по умолчанию
Количество пакетов, которое сохраняется до и после пакета, вызвавшего срабатывание правил	number_of_packet	1	100	5
Ограничение на размер файла с дампами (в байтах)	size_limit	1048576 (1 Мбайт)	4294967296 (4 Гбайт)	104857600 (100 Мбайт)
Ограничение на количество пакетов в одном файле	count_limit	3	10000	2000

Пример строки с настройками:

**preprocessor netanalyzer\_dump: number\_of\_packet 5, size\_limit 104857600, count\_limit 2000**

После внесения изменений в конфигурационный файл необходимо его сохранить и нажать кнопку  «Отправить на сервер». Настройки будут применены на всех станциях.

#### 4.5.4. Вкладка «Переменные»

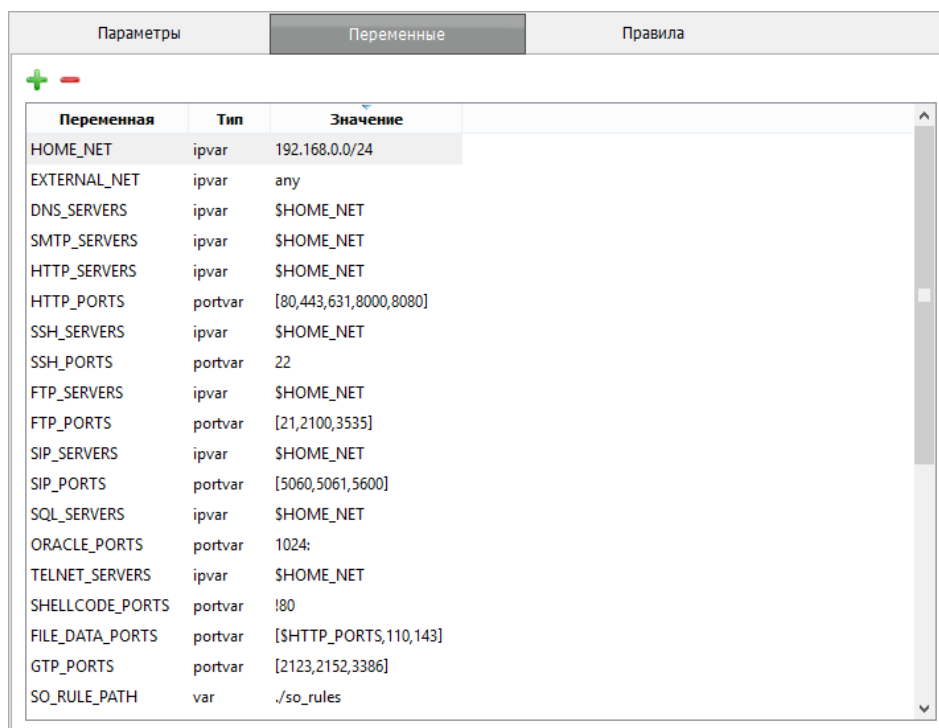
Данная вкладка, вид которой приведён на рис. 34, позволяет редактировать, создавать и удалять переменные. Описание назначения переменных, их объявления, типов и значений приведено в приложении 1 к документу ФДШИ.03618-01 31 01 «Описание применения».

Редактирование, создание, удаление переменных возможно, только если программа находится в режиме редактирования (4.5.2).

Большую часть вкладки занимает список переменных, сгруппированных по файлам, в которых они (переменные) объявляются.

Каждая переменная выводится в три колонки: в первой – идентификатор переменной, во второй – тип, в третьей – значение.

Вкладка «Переменные»




Переменная	Тип	Значение
HOME_NET	ipvar	192.168.0.0/24
EXTERNAL_NET	ipvar	any
DNS_SERVERS	ipvar	\$HOME_NET
SMTP_SERVERS	ipvar	\$HOME_NET
HTTP_SERVERS	ipvar	\$HOME_NET
HTTP_PORTS	portvar	[80,443,631,8000,8080]
SSH_SERVERS	ipvar	\$HOME_NET
SSH_PORTS	portvar	22
FTP_SERVERS	ipvar	\$HOME_NET
FTP_PORTS	portvar	[21,2100,3535]
SIP_SERVERS	ipvar	\$HOME_NET
SIP_PORTS	portvar	[5060,5061,5600]
SQL_SERVERS	ipvar	\$HOME_NET
ORACLE_PORTS	portvar	1024:
TELNET_SERVERS	ipvar	\$HOME_NET
SHELLCODE_PORTS	portvar	!80
FILE_DATA_PORTS	portvar	[\$HTTP_PORTS,110,143]
GTP_PORTS	portvar	[2123,2152,3386]
SO_RULE_PATH	var	./so_rules

Рис. 34

В верхней части вкладки расположены кнопки управления, описание которых приведено в таблице 4.

Таблица 4 – Кнопки управления вкладки «Переменные»

Кнопка	Название	Горячая клавиша	Действие
	Объявить переменную	Ins	Создаёт новую переменную
	Удалить переменную	Del	Удаляет выделенную переменную

Чтобы отредактировать переменную, необходимо дважды щелкнуть мышью на её имени в списке (можно также выделить переменную и нажать клавишу «Enter»). После этого откроется окно редактора (рис. 35). В окне редактора переменных можно изменить имя, тип и значение переменной. Для сохранения отредактированных настроек, необходимо нажать кнопку «Сохранить».

Окно редактора переменных

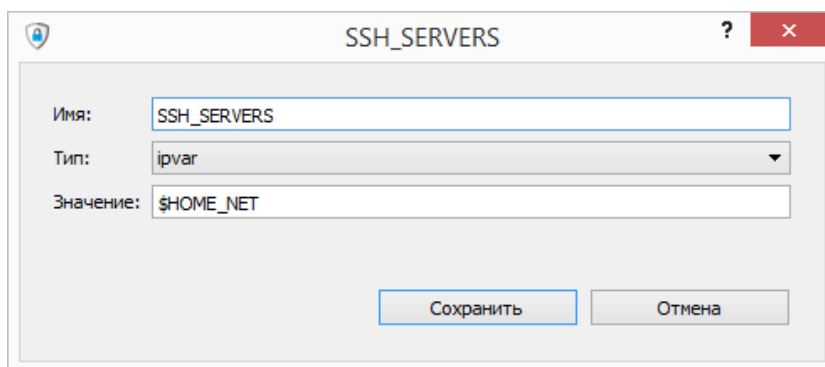




Рис. 35

Чтобы создать новую переменную, необходимо нажать кнопку  «Объявить переменную». Будет добавлен новый элемент, и откроется окно уже упоминавшееся редактора (см. рис. 34), в котором этот новый элемент нужно отредактировать. После редактирования нужно нажать кнопку «Сохранить».

Чтобы удалить переменную, необходимо выделить её мышью и нажать кнопку  «Удалить переменную».

#### 4.5.5. Вкладка «Правила»

Данная вкладка, вид которой приведён на рис. 36, позволяет редактировать, создавать и удалять правила (сигнатуры вторжений). Формат задания правил описан в приложении 1 к документу ФДШИ.03618-01 31 01 «Описание применения».

Редактирование, создание, удаление правил возможно, только если программа находится в режиме редактирования. Подробности см. в 4.5.2.

Большую часть вкладки занимает список правил, сгруппированных по файлам, в которых они (правила) объявляются.

В верхней части вкладки расположены кнопки управления, описание которых приведено в таблице 5, и поле для фильтрации правил.

Для каждой сигнатуры и файла доступен флажок, определяющий использование этой сигнатуры (файла). Если флажок установлен, сигнатура применяется при анализе. Если флажок

снят, сигнатура не применяется. Аналогично с файлами: снятый флажок означает, что данный файл не читается средством анализа сетевого трафика.

Следует помнить о некоторых нюансах:

- чтобы какая-то сигнатура применялась при анализе сетевого трафика, нужно, чтобы был установлен флажок не только для этой сигнатуры, но и для файла, в котором она содержится;
- файлы могут содержать не только сигнатуры, но и другие параметры, которые на вкладке «Правила» не отображаются. Сбрасывая флажок файла, можно отключить те параметры, которые не видны;
- файл **snort.conf** загружается средством анализа сетевого трафика всегда. Для него нельзя сбросить флажок;
- в ОС Windows запрещается включать полный набор сигнатур. Данная ОС не позволяет использовать анализатору сетевого трафика более 2 Гбайт оперативной памяти, что недостаточно для включения полного объема. Рекомендуется включать только наиболее актуальные для данного объекта сигнатуры.

### Вкладка «Правила»

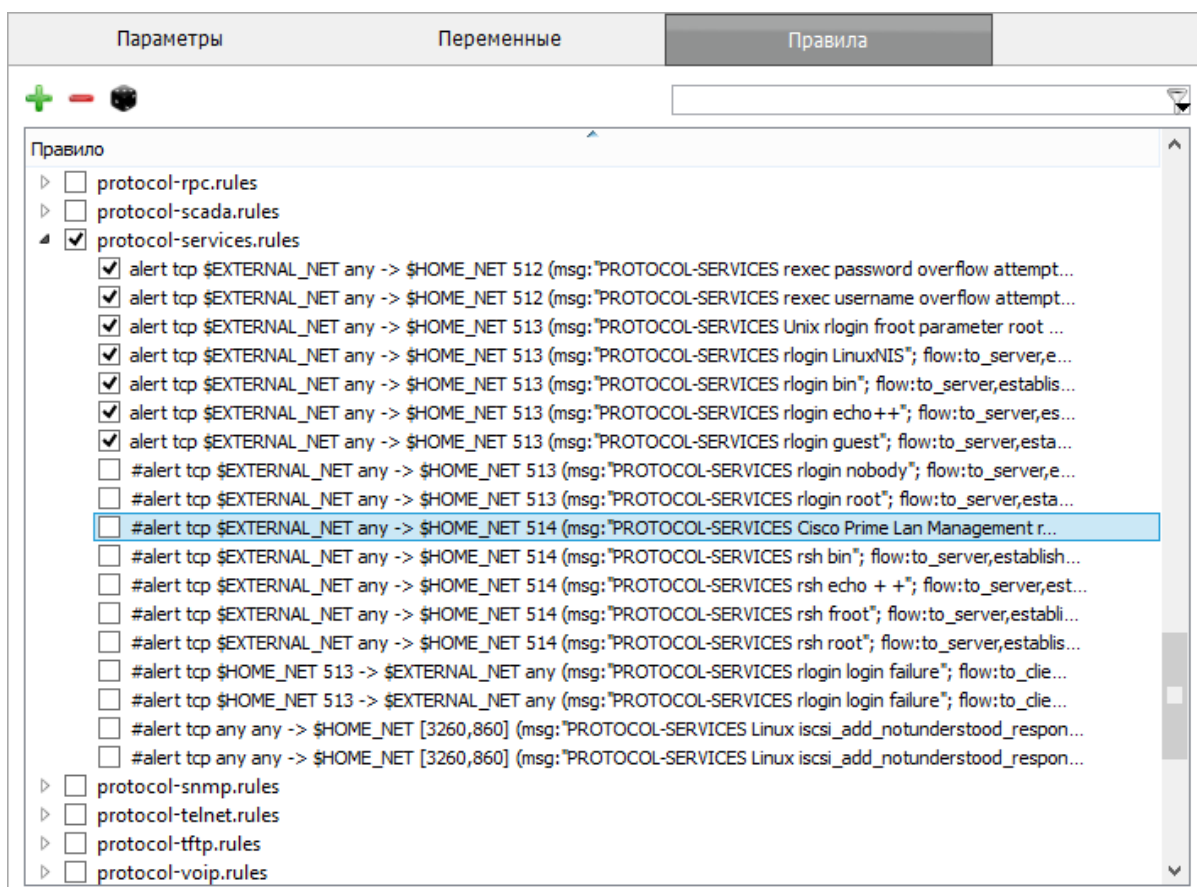


Рис. 36

Таблица 5 – Кнопки управления вкладки «Правила»

Кнопка	Название	Горячая клавиша	Назначение
	Создать правило	Ins	Создаёт новое правило
	Удалить правило	Del	Удаляет выделенное правило
	Изменить действие у группы правил	Нет	Позволяет изменить действие в правилах

Так как правил очень много и регулярно приходится искать среди них нужное, на вкладке предусмотрена возможность фильтрации по тексту правила. В верхней правой части вкладки находится поле ввода фильтра. Если ввести туда какой-либо текст, то в списке правил останутся только те правила, которые содержат этот текст.

Например, чтобы найти правило с идентификатором 1000001, нужно ввести «sid:1000001», и в списке останется только одно нужное правило. Или, если в консоли управления на вкладке «Аудит» появилось сообщение и нужно найти правило, по которому это сообщение появилось, можно скопировать текст сообщения на вкладке «Аудит» и вставить в фильтр – правило будет найдено.

Фильтрация применяется автоматически при вводе текста в поле фильтра.

Фильтрация не применяется к именам файлов, только к правилам.

При задании фильтра можно использовать подстановочные символы. Символы и их описание приведены в таблице 6. Такие же подстановочные символы используются во многих приложениях, и, скорее всего, администратор с ними уже знаком.

Таблица 6 – Подстановочные символы

Символ	Назначение	Пример
*	Замещает ноль или больше произвольных символов	Выражение «"*"» определяет любой текст, заключённый в кавычки, а также пустые кавычки без текста ("")
+	Замещает один или больше произвольных символов	Выражение «\$+» задаст любой текст, начинающийся со знака \$ (т.е. под это выражение подпадают идентификаторы переменных)
?	Замещает ноль или один произвольный символ	Выражение «flags:?AF» позволит найти правила с флагами AF или +AF
[...]	Позволяет задавать диапазон символов	Выражение «sid:[1-3]000;» позволит найти правила с идентификаторами 1000, 2000 и 3000

Чтобы отредактировать правило, нужно найти это правило в списке и дважды щёлкнуть на нём (можно также выделить его и нажать клавишу «Enter»). После этого откроется окно редактора правил (рис. 37), состоящее из поля ввода и кнопок «Сохранить» и «Отмена». Необходимо в поле ввода отредактировать правило и нажать кнопку «Сохранить».

Окно редактора правил

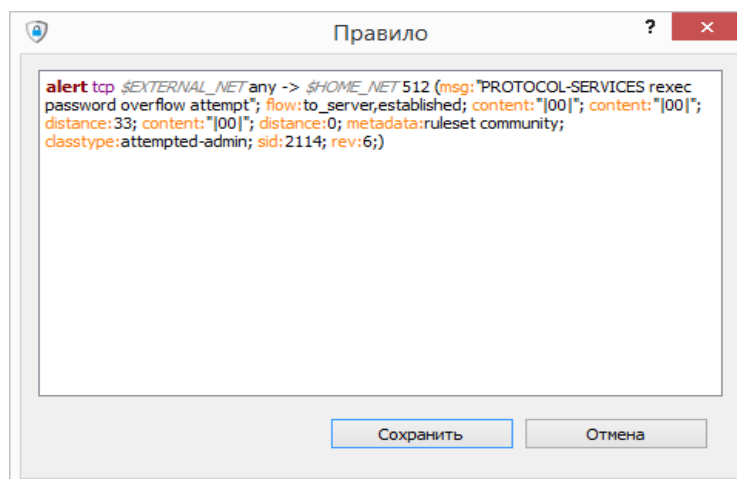





Рис. 37

Чтобы создать новое правило, необходимо нажать кнопку  «Создать правило». К файлу **localrules.rules** будет добавлен новый элемент, и откроется уже упоминавшееся окно редактора (см. рис. 37), в котором этот новый элемент нужно отредактировать. После редактирования нужно нажать кнопку «Сохранить».

Чтобы удалить правило, необходимо выделить его мышью и нажать кнопку  «Удалить правило». Если какое-либо правило больше не нужно, рекомендуется не удалять его, а только сделать неактивным, сбросив флажок. В этом случае, если правило снова понадобится, его не потребуется повторно создавать.

Чтобы изменить действие в правилах, необходимо выбрать действие из списка, который отображается после нажатия кнопки  «Задать действие для правил» (см. рис. 36). Если не задан фильтр для поиска нужных правил, то действие будет применяться для всех правил. Иначе выбранное действие будет действовать только для тех правил, которые соответствуют заданному фильтру.

#### 4.5.6. Окно «Редактор»

Окно, вид которого приведён на рис. 38, позволяет работать непосредственно с текстом конфигурационных файлов.

Окно «Редактор»

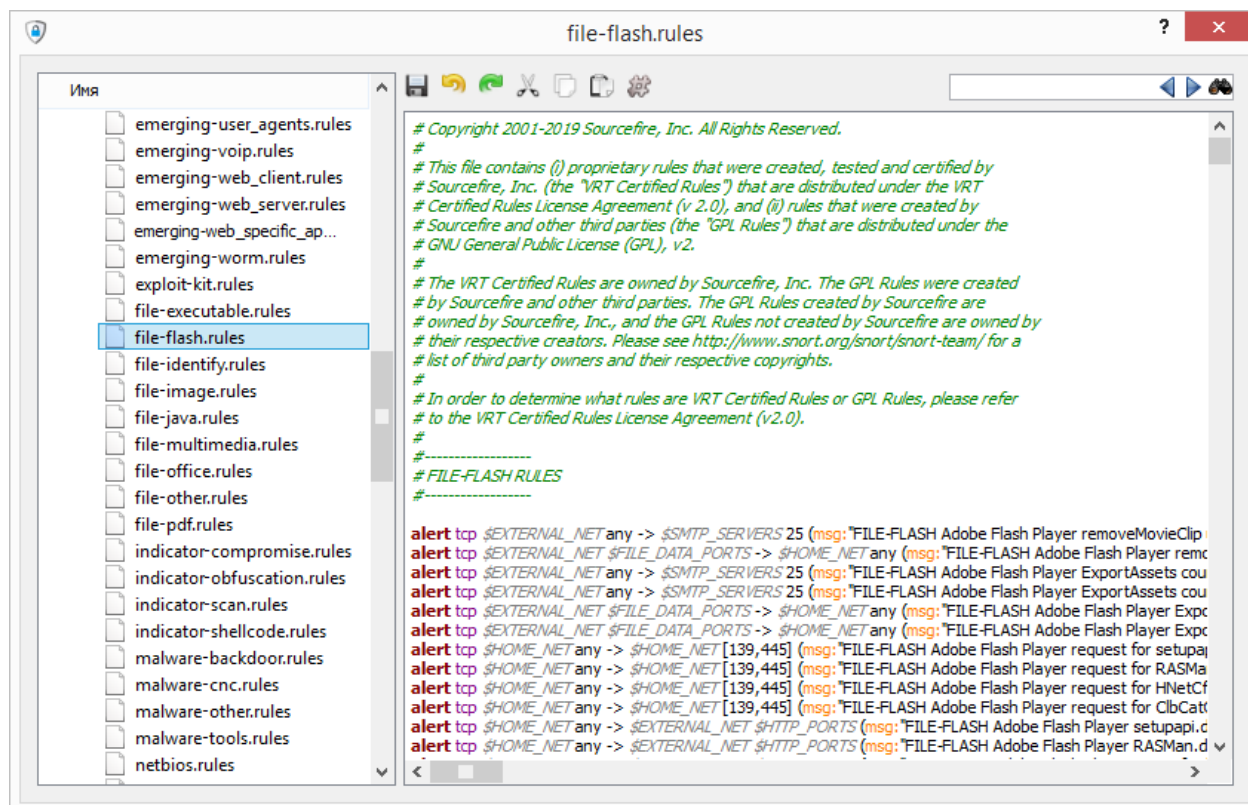


Рис. 38





Редактирование возможно, только если программа находится в режиме редактирования (см. 4.5.2).

Окно поделено на две части: слева находится список конфигурационных файлов, справа текстовый редактор.


Двойной щелчок на имени файла в списке слева открывает этот файл в редакторе. Если в редакторе уже был открыт какой-то файл, то этот файл сохраняется перед тем, как будет открыт новый.

На вкладке доступны несколько кнопок для вызова функций редактора. Все они перечислены в таблице 7.

Таблица 7 – Кнопки управления окна «Редактор»

Кнопка	Название	Горячая клавиша	Назначение
	Сохранить	Нет	Сохраняет изменения
	Отменить	Ctrl+Z	Отменяет предыдущее действие
	Повторить	Ctrl+Y	Повторяет отменённое действие
	Вырезать	Ctrl+X	Вырезает текст в буфер
	Копировать	Ctrl+C	Копирует текст в буфер
	Вставить	Ctrl+V	Вставляет текст из буфера
	Закомментировать	Ctrl+/ /	Вставляет/удаляет символ комментария

Большинство функций стандартно для текстового редактора и пояснений не требует. Рассмотрим только последнюю функцию.

Кнопка  «Закомментировать» позволяет быстро добавить (убрать) символ комментария «#» в несколько строк подряд. Формат конфигурационных файлов не поддерживает многострочные комментарии, а добавление/удаление однострочных комментариев для больших кусков теста несколько трудоёмко без этой функции.

Чтобы вызвать эту функцию, нужно выделить текст и нажать кнопку. Действие будет выполнено для каждой строки, затронутой выделением.

Будет ли символ комментария вставляться или удаляться, зависит от первой выделенной строки. Если первая строка не закомментирована, то символ комментария будет вставляться. И наоборот: если первая выделенная строка закомментирована, символ комментария будет удаляться.

## 4.6. Управление внешними средствами

### 4.6.1. Общие сведения

Управление внешними средствами осуществляется с помощью вкладки «Параметры защиты». Данная вкладка позволяет осуществлять следующие операции:

- редактирование сценариев управления внешними средствами;
- редактирование аутентификационных данных для выполнения автоматического реагирования на вторжения;
- создание сценариев по ранее заложенному шаблону.

Взаимодействие осуществляется с внешними средствами, допускающими администрирование по протоколу SSH.

Управление внешними средствами осуществляется с помощью сценариев, которые разрабатывает администратор. Каждый сценарий содержит параметры подключения к внешнему средству и набор команд, которые надо удалённо выполнить при подключении. Ниже описан формат сценария.

В первой строке указаны параметры для выполнения управления в следующем виде:

*<имя\_пользователя>@<станция>:<номер\_порта>*, где:

- *<имя\_пользователя>* – логин администратора для подключения к удалённому внешнему средству;
- *<станция>* – сетевое имя или IP-адрес внешнего средства;
- *<номер\_порта>* – номер сетевого порта, на котором принимаются подключения по SSH.

В последующих строках указываются команды для выполнения на удалённом внешнем средстве по одной команде на строку.

1) Сценарий для Дионис-NX:

- блокирующий весь трафик:

```
adm@83.220.32.66:52532
configure terminal
ip access-list rebus_deny_all
deny
do write
exit
```

- разрешающий весь трафик:

```
adm@83.220.32.66:52532
configure terminal
ip access-list rebus_permit_all
permit
do write
exit
```

2) Сценарий сервиса iptables для ОС MCBC и ОС СН «Astra Linux Special Edition», блокирующий весь трафик (где «-I» – заглавная «i», “1 -j” – единица и -j):

```
root@200.0.12.110:22
sudo iptables -I INPUT 1 -j DROP
sudo iptables -I OUTPUT 1 -j DROP
sudo iptables -I FORWARD 1 -j DROP
sudo service iptables save
```

3) Сценарий для АПК «Маршрутизатор доступа» РУЕА.465689.002(-01,-02) (изделие 83т316):

- блокирующий весь сетевой трафик:

```
rebus-ips@172.16.130.1:22
/ip/fw/violators add adm-entry subnet=0.0.0.0/0 action=deny
```

- разблокирующий весь сетевой трафик, заблокированный предыдущим скриптом:

```
rebus-ips@172.16.130.1:22
/ip/fw/violators del adm-entry subnet=0.0.0.0/0
```

- блокирующий IP-адреса источника (<attacking\_address> – это IP-адрес – параметр скрипта):

```
rebus-ips@172.16.130.1:22
/ip/fw/violators add adm-entry subnet=<attacking_address>/32 action=deny
```

- разблокирующий IP-адреса источника (<attacking\_address> – это IP-адрес – параметр скрипта):

```
rebus-ips@172.16.130.1:22
/ip/fw/violators del adm-entry subnet=<attacking_address>/32
```

- блокирующий IP-подсети источника (<attacking\_address> – это IP-подсеть в формате А.В.С.Д/М – параметр скрипта):

```
rebus-ips@172.16.130.1:22
/ip/fw/violators add adm-entry subnet=<attacking_address> action=deny
```

- разблокирующий IP-подсети источника (<attacking\_address> – это IP-подсеть в формате А.В.С.Д/М – параметр скрипта):

```
rebus-ips@172.16.130.1:22
/ip/fw/violators del adm-entry subnet=<attacking_address>
```

Переменная <attacking\_address> может использоваться только в сценариях, предназначенных для автоматической реакции. На место неё в скрипте во время автореакции на

вторжение подставляется IP-адрес атакующей стороны. К примеру, можно использовать, чтобы заблокировать станцию, от которой пришло вторжение.

Переменная *<victim\_address>* – IP-адрес «жертвы», используется для получения адреса компьютера (или устройства), который был атакован.

Переменная *<allow\_address>* – IP-адрес исключения.

#### 4.6.2. Работа со сценариями управления внешними средствами

Для выполнения управления внешними средствами необходимо на вкладке «Параметры защиты» в списке доступных для управления механизмов выбрать пункт «Управление внешними средствами» (рис. 39).

Вкладка «Параметры защиты», выбран пункт «Управление внешними средствами»

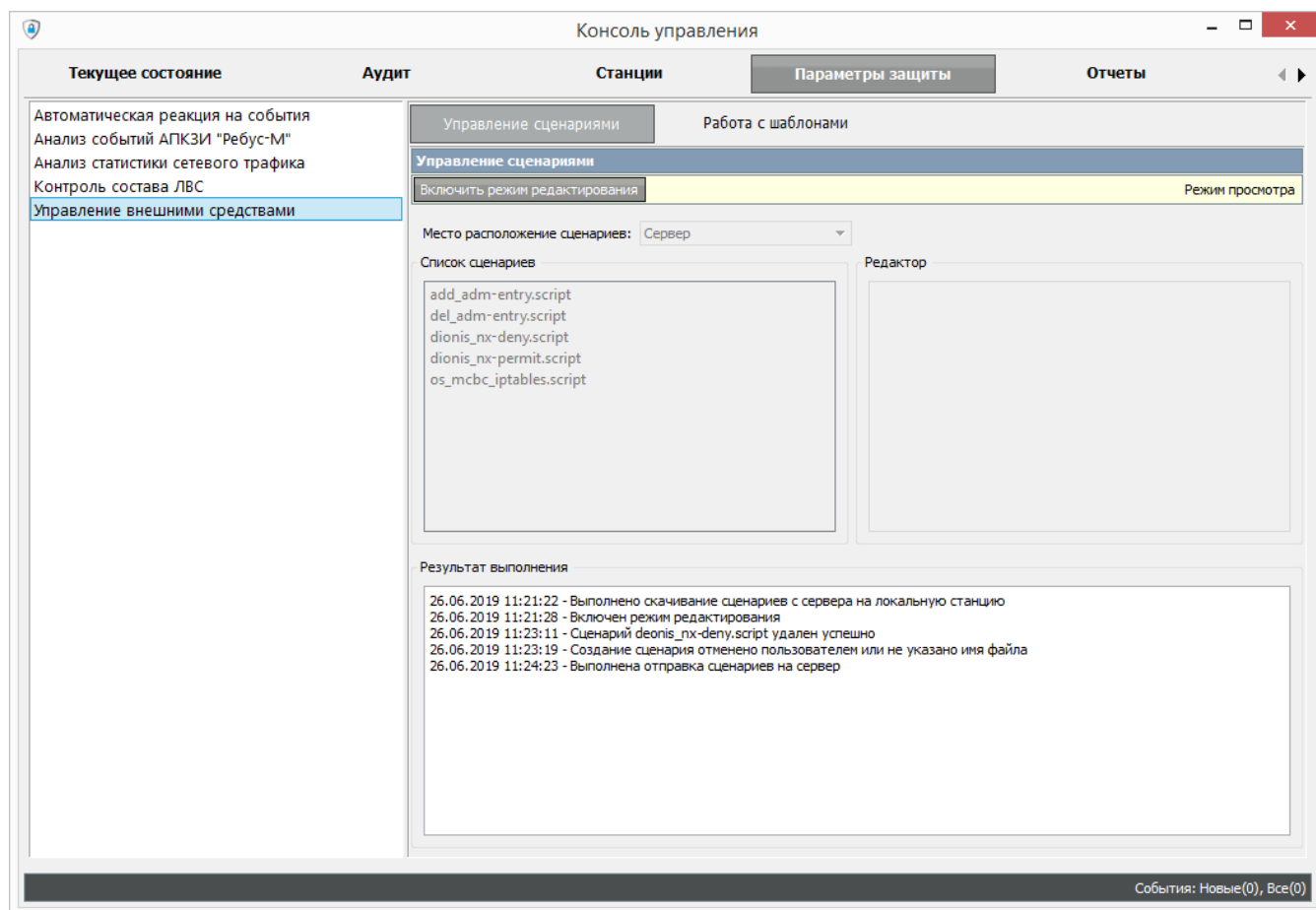


Рис. 39

Для начала работы со сценариями в верхнем левом углу формы «Управление сценариями» необходимо нажать кнопку «Включить режим редактирования». После перехода в режим редактирования станут доступны кнопки управления (рис. 40).

Для редактирования доступны два списка сценариев, различающихся по месту расположения:

- «Сервер». Сценарии будут доступны для управления всем администраторам СОВ;
- «Локальная станция». Сценарии будут доступны для управления только администратору, который их создал на своей локальной станции.

Выбор списка сценариев для редактирования осуществляется в выпадающем списке «Место расположение сценариев».

Форма «Управление сценариями» в режиме редактирования

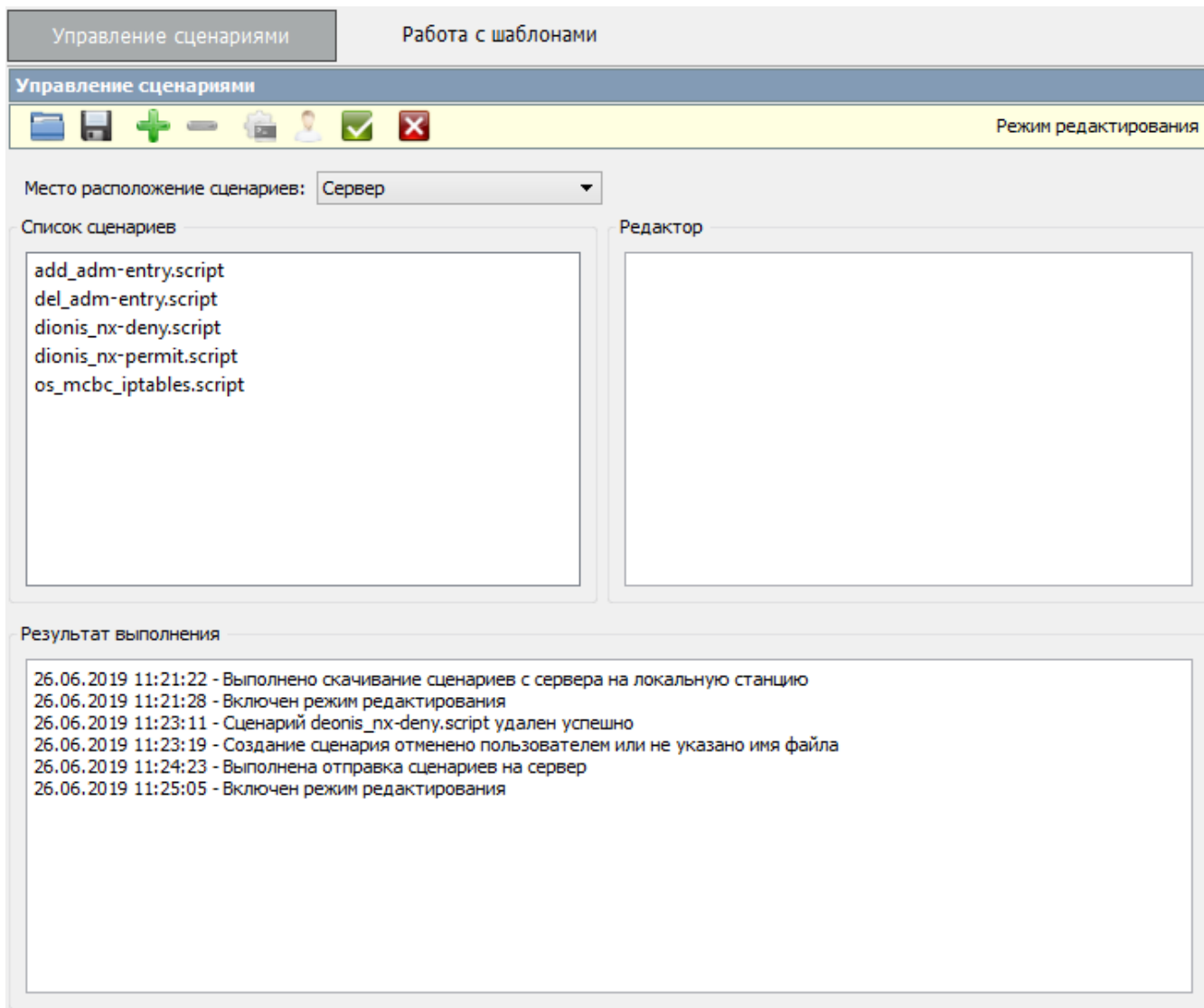




Рис. 40

При выделении сценария в поле «Редактор» появится его содержимое. После выполнения редактирования скрипта для сохранения необходимо нажать кнопку .

Для создания нового сценария необходимо нажать на кнопку . В появившемся окне нужно ввести имя нового сценария без расширения **.script** как показано на рис. 41. После ввода имени сценария необходимо нажать «Сохранить» для создания или «Отмена» для отмены создания.

Окно ввода имени нового сценария

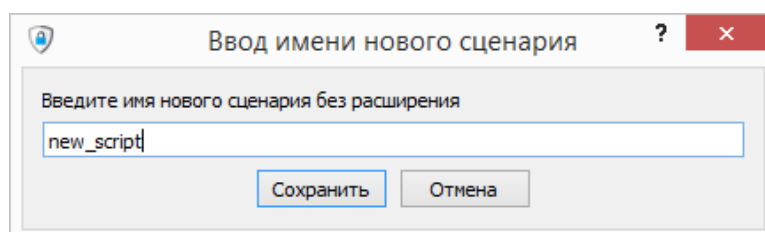


Рис. 41

При успешном создании сценарий появится в списке, как изображено на рис. 42.

Форма «Управление сценариями» после создания нового сценария

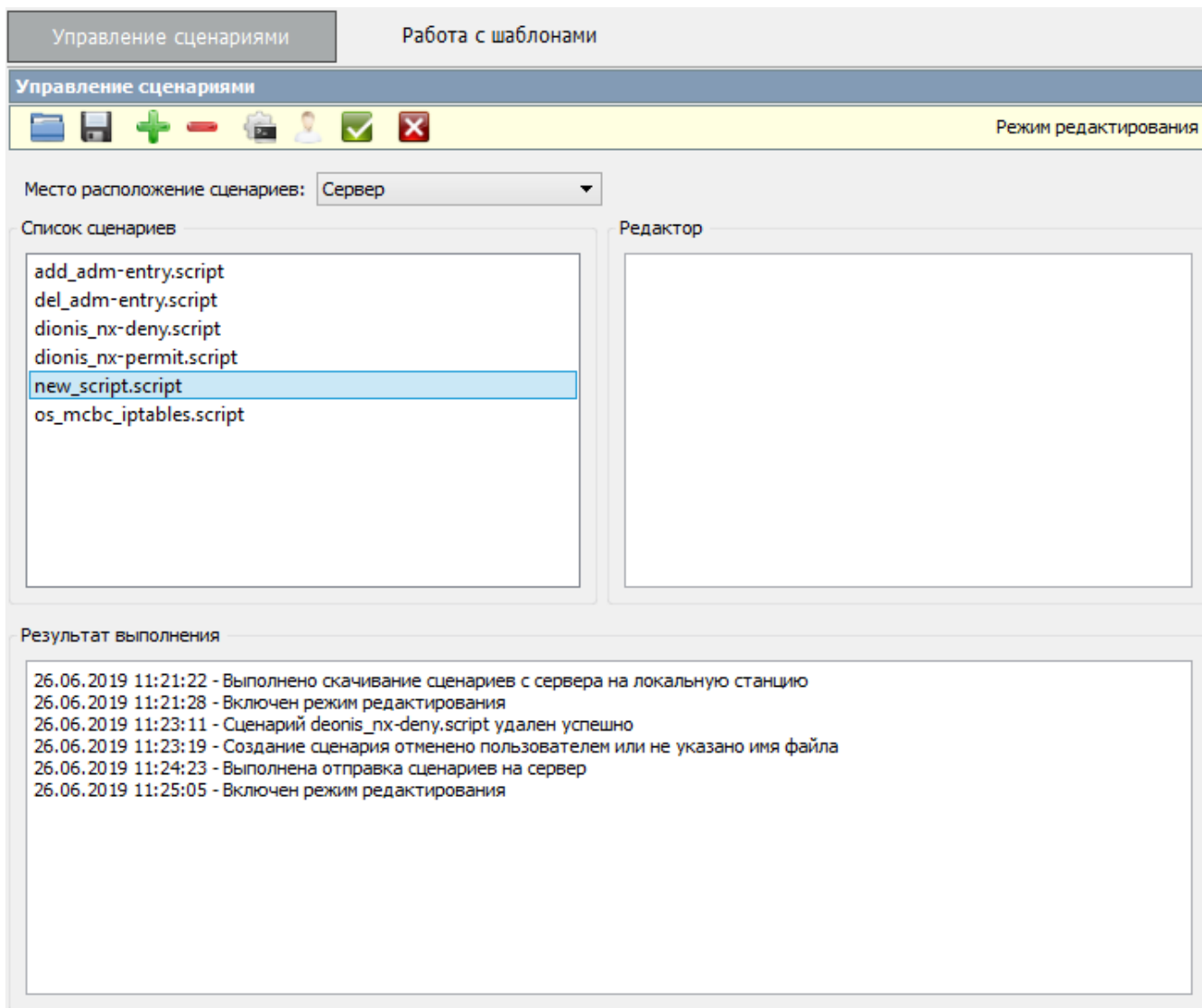


Рис. 42

Для открытия сценария, который находится в произвольном месте на локальной станции необходимо нажать . Файл сценария должен быть с расширением **.script**. В появившемся диалоговом окне выбрать необходимый сценарий. После успешного открытия сценария, его содержимое отобразится в поле «Редактор». В этом поле можно выполнять необходимое редактирование для дальнейшего использования. После редактирования сценария его можно сохранить с произвольным именем. Для этого необходимо нажать кнопку или выполнить данный скрипт нажатием на кнопку . После нажатия на кнопку сохранения появится окно для ввода нового имени сценария (рис. 43).

### Окно ввода имени нового сценария

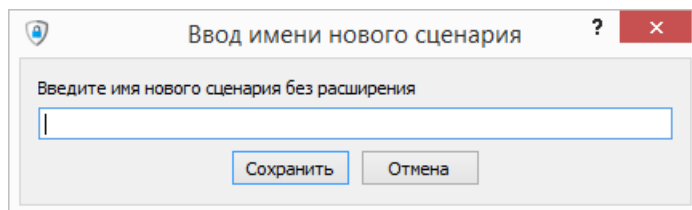


Рис. 43

Если нажата кнопка выполнения сценария, то появится окно ввода пароля для выполнения аутентификации с внешним средством (рис. 44).

### Окно ввода пароля

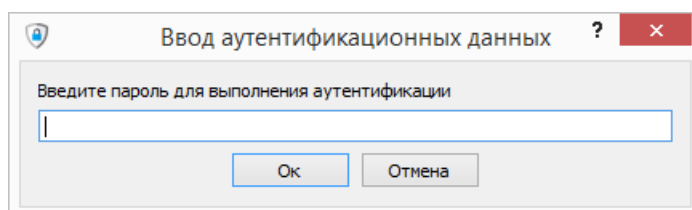





Рис. 44

Для выполнения удаления сценария необходимо выбрать его из списка сценариев и нажать кнопку . В появившемся сообщении необходимо подтвердить удаление нажатием на кнопку «Ок» или отменить удаление нажатием на кнопку «Отмена».

При необходимости можно переместить сценарий с локальной станции на сервер. Для этого нужно указать для управления список сценариев на станции. Затем выбрать сценарий из списка и нажать кнопку .

Для отправки всех изменений на сервер необходимо нажать кнопку .

Кнопка  предназначена для указания аутентификационных данных, которые будут необходимы для выполнения автоматической реакции. При нажатии на неё открывается диалоговое окно (рис. 45).

В таблице задаются следующие параметры:

- имя пользователя;
- имя/IP-адрес станции;
- пароль для данного подключения к одному из внешних средств.

### Окно редактирования аутентификационных данных

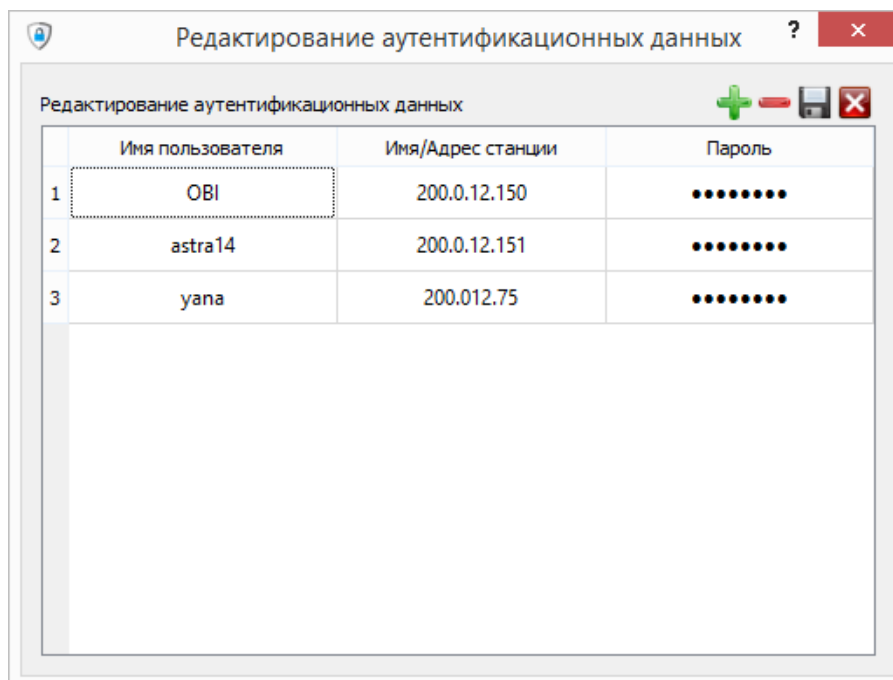


Рис. 45

При выполнении автоматической реакции, данные указанные в сценарии (имя пользователя и имя/ IP-адрес станции) будут сопоставляться с установленными в этой таблице данными. По данным, указанным в сценарии и в таблице, будет подобран пароль для аутентификации. Кнопка предназначена для добавления новой строки таблицы. Кнопка для удаления выделенной строки таблицы. Кнопка для сохранения данных. Кнопка для отмены внесенных изменений в данную таблицу. Если были заполнены не все поля строки и нажата кнопка , то эти данные не будут сохранены. Для задания значения или редактирования ячейки необходимо выполнить двойной клик левой кнопкой мыши по ней. Для сохранения и вступления в силу отредактированных данных необходимо нажать кнопку на форме «Управление сценариями».

Кнопка предназначена для отмены изменений. На локальной станции выполняется обновление сценариев со станции сервер.

#### 4.6.3. Работа с шаблонами

Для работы с шаблонами необходимо перейти во вкладку «Работа с шаблонами». В списке шаблонов выбрать необходимый шаблон. В поле «Содержимое шаблона» отображается его текст (рис. 46).

Вкладка «Работа с шаблонами»

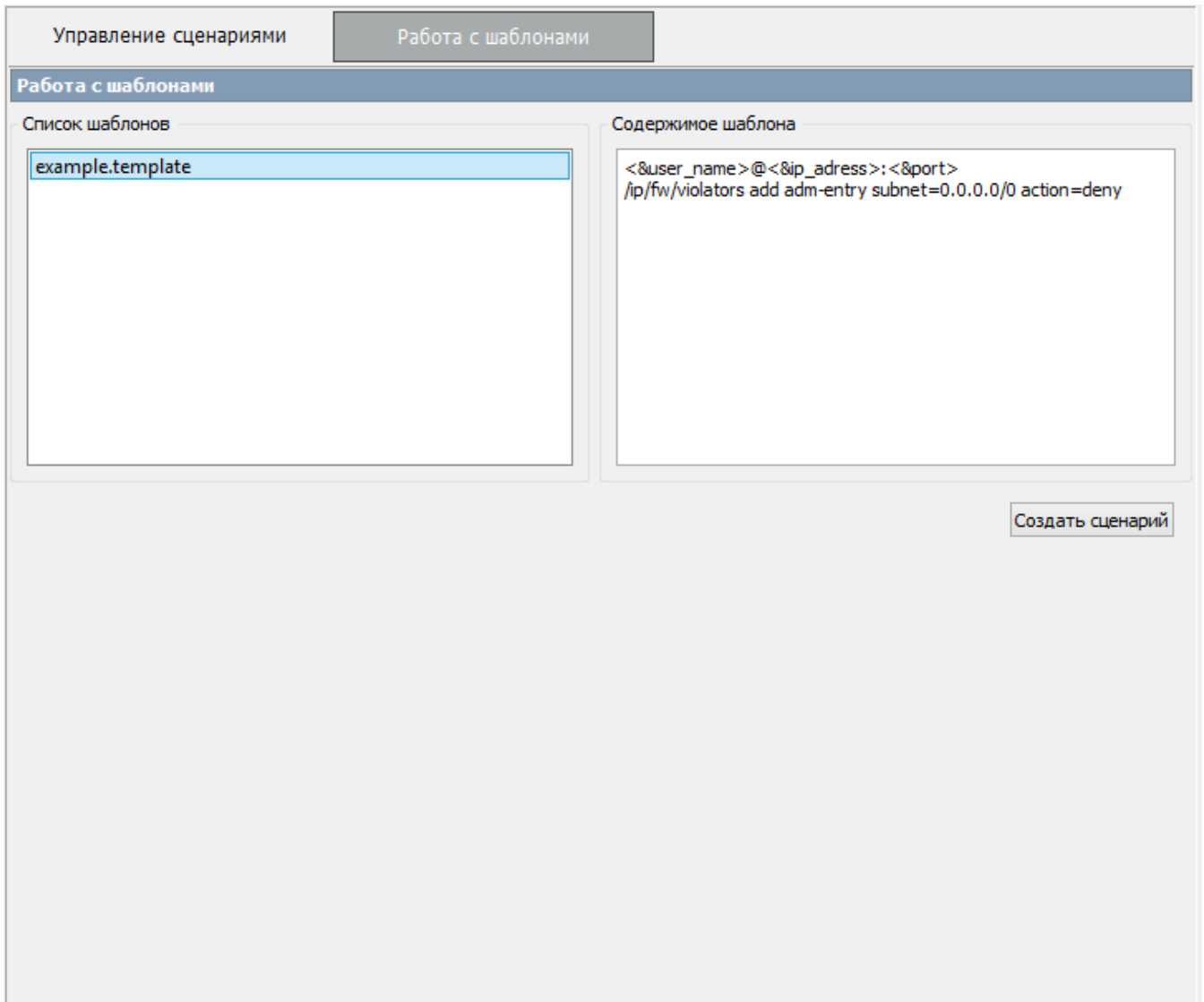


Рис. 46

После выбора шаблона необходимо нажать кнопку «Создать сценарий». В появившемся окне заполнить все доступные поля (рис. 47).

### Окно редактирования параметров сценария

Редактирование параметров

Имя пользователя (<&user\_name>)

Ip адрес межсетевого экрана (<&ip\_address>)

Порт для выполнения подключения(<&port>)

Принять Отмена

Рис. 47

Далее при нажатии кнопки «Принять» появится диалоговое окно, в котором можно ознакомиться с получившимся сценарием (рис. 48).

### Окно редактирования параметров сценария

Редактирование параметров

```
yana@200.0.12.75:22  
/ip/fw/violators add adm-entry subnet=0.0.0.0/0 action=deny
```

Сохранить Выполнить Назад

Рис. 48

При нажатии на кнопку «Сохранить» будет предложено задать имя и сценарий будет сохранен на локальной станции. При нажатии кнопки «Выполнить» появится диалоговое окно для ввода пароля и дальнейшей отправки на сервер для выполнения подключения к внешнему средству. Кнопка «Назад» позволяет вернуться к редактированию параметров.

#### 4.6.4. Результат выполнения сценариев

При выполнении сценария (нажатием кнопки «Выполнить сценарий») в поле «Результат выполнения» появится сообщение о начале выполнения сценария (рис. 49).

Просмотр результатов выполнения сценария во вкладке «Параметры защиты»

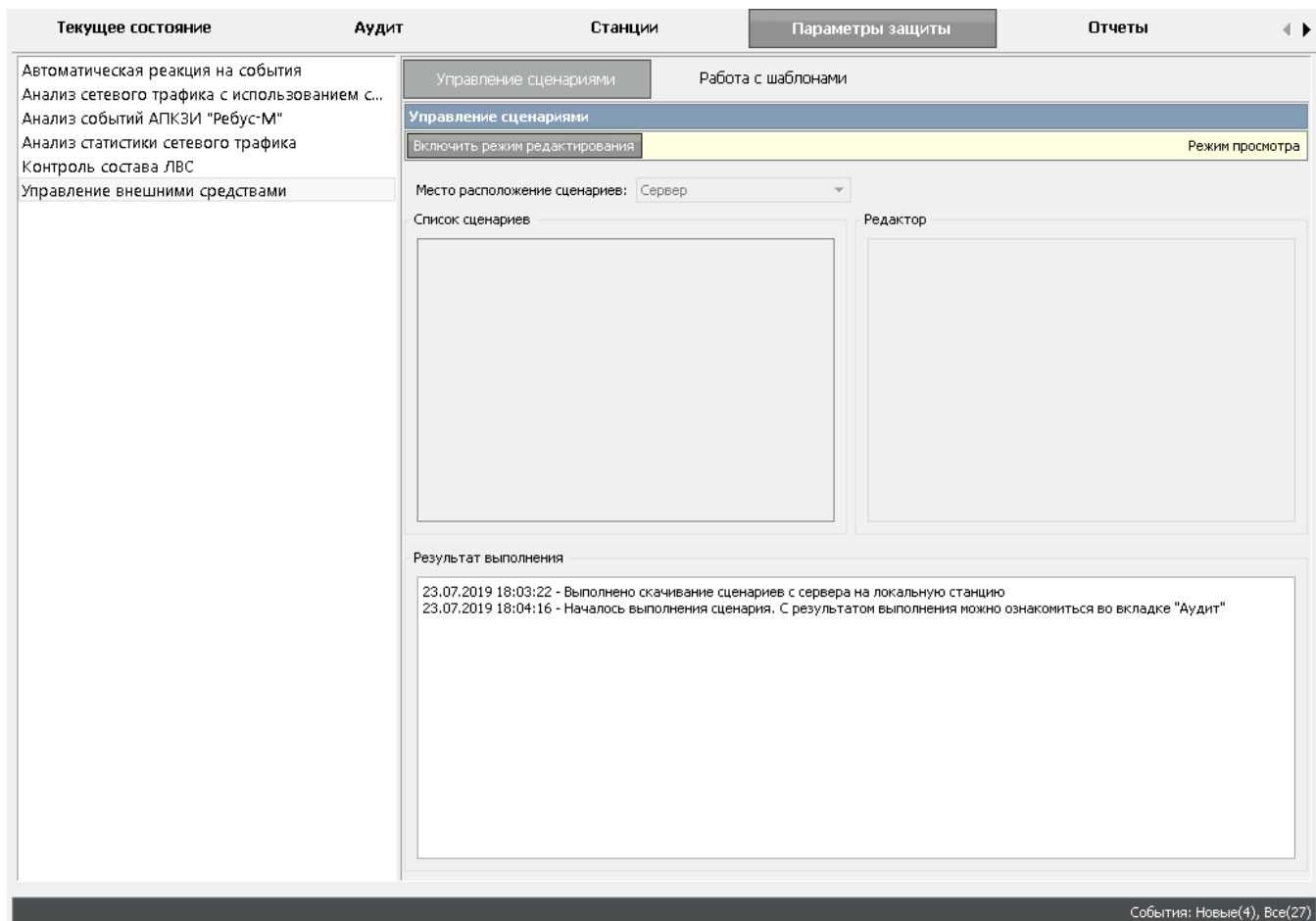


Рис. 49

После того как сценарий будет выполнен, во вкладке «Аудит» появится сообщение с результатом о выполнении и дополнительной информацией (рис. 50).

## Просмотр результатов выполнения сценариев во вкладке «Аудит»

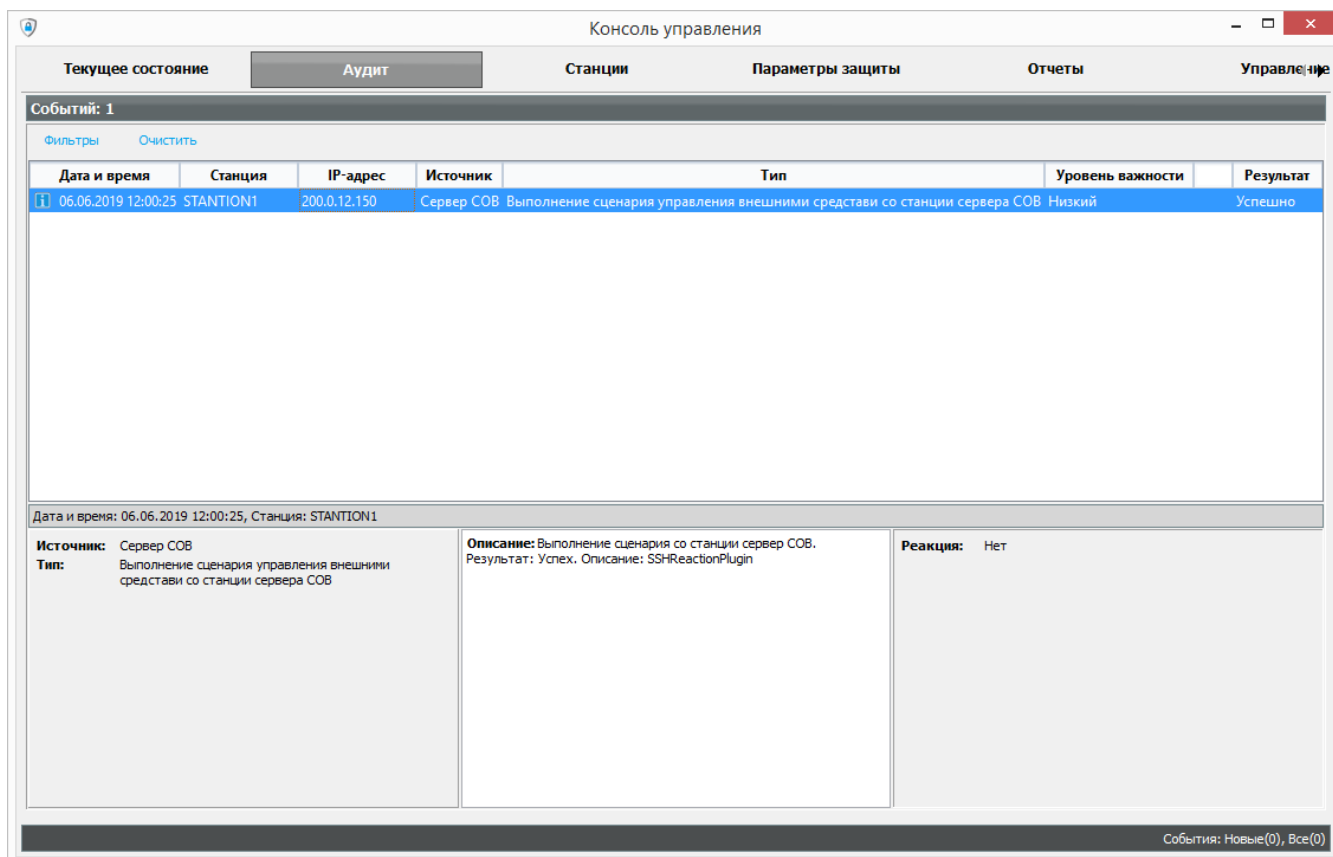


Рис. 50

### 4.7. Обновление БРП

Обновление БРП выполняется двумя способами:

- автоматически, путем проверки наличия обновления на сервере обновлений;
- вручную, путем запуска установки обновления по команде администратора COB.

#### 4.7.1. Автоматическое обновление

Для настройки автоматического обновления необходимо открыть вкладку «Управление» и в списке доступных для управления механизмов выбрать пункт «Обновление». Далее необходимо выбрать тип обновления «Автоматически».

Для доступа к параметрам обновления необходимо включить режим редактирования, нажав во вкладке «Настройка автоматического обновления» кнопку «Включить режим редактирования».

Включение и отключение автоматического обновления БРП, а также задание интервала проверки обновлений выполняется в группе «Автоматическая проверка обновлений».

В группе «Параметры подключения к серверу» задаются настройки для подключения к серверу обновлений: сетевой адрес, порт, логин и пароль.

В группе «Параметры обновления» указывается место расположения обновлений на сервере.

После ввода настроек и перед их сохранением есть возможность проверить соединение с FTP-сервером. За это отвечает кнопка «Проверить соединение». При успешном или не успешном подключении отобразится соответствующая надпись с информацией.

После редактирования настроек автоматического обновления БРП для сохранения результата необходимо нажать кнопку «Сохранить». Сохраненные настройки будут переданы на

сервер СОВ. Если автоматическое обновление включено, то после сохранения настроек сервер СОВ инициирует проверку обновления БРП.

Файлы с обновлениями должны находиться на FTP-сервере. Названия архивов с обновлениями должны иметь вид **rebus-sov-brp-update-YYYY.MM.zip**, где вместо **YYYY** должен быть год, а вместо **MM** – месяц обновления баз (например, **rebus-sov-brp-update-2019.05.zip**). Если версия последнего файла с обновлением на FTP-сервере окажется новее, чем текущая версия баз в ПК «Ребус-СОВ», будет произведена попытка обновления.

#### 4.7.2. Ручное обновление

Для запуска обновления вручную необходимо открыть вкладку «Управление» и в списке доступных для управления механизмов выбрать пункт «Обновление». В активизированных справа элементах управления нужно выбрать тип обновления «Вручную».

Далее нажать кнопку «Установить пакет». После этого в появившемся на экране диалоге выбора пакета обновления необходимо указать файл с требуемым пакетом обновления и нажать кнопку «Открыть». В результате начнется процесс обновления сигнатур вторжений на сервере СОВ. По завершении обновления на экране появится сообщение с результатом выполнения обновления.

#### 4.8. Настройка сервера СОВ

Успешное сетевое соединение агентской станции с сервером СОВ предполагает прохождение процедуры аутентификации. Для успешной установки доверенного соединения необходимо соответствие ключей аутентификации на агентских станциях и на сервере СОВ.

После установки на сервере и агентских станциях СОВ находится одинаковый ключ аутентификации. В целях повышения безопасности целесообразно проводить периодическую смену ключа аутентификации. Смена ключа производится в следующем порядке:

- запустить на сервере СОВ программу настройки агентской части и сгенерировать новый ключ по паролю средствами интерфейса данной программы;
- распространить новый ключ на каждую агентскую станцию с помощью программы настройки агентской части, используя метод генерации ключа по паролю либо импорт файла ключа (см. 4.3.3).

В случае несоответствия ключей аутентификации на агентской станции и на сервере в консоли управления на вкладке «Станции» для данной агентской станции будет отображено состояние ошибки аутентификации (см. таблицу 1).

Для уведомления о выявленных вторжениях по электронной почте необходимо настроить почтовый сервер. В почтовом сервере должны быть заданы следующие настройки: статический IP-адрес, поддержка протокола SMTP (также POP3 или IMAP если требуется читать сообщения), аутентификация входящих сообщений, поддержка шифрования (протокол SSL или TLS).

Для задания параметров почтовой рассылки необходимо:

- запустить на сервере СОВ консоль управления, войти администратором;
- настроить параметры почтовой рассылки пользователей и сервера СОВ (см. 4.4.8.3).

#### 4.9. Настройка синхронизации времени

Механизм синхронизации времени устроен следующим образом:

- сервер СОВ периодически запрашивает у агентов СОВ время, определенное на их станции;
- после получения времени от агента СОВ происходит проверка расхождения времени на серверной и на агентской станции. Если расхождение слишком большое, то сервер СОВ посылает команду на агент СОВ о коррекции времени;
- в ответ на эту команду агент СОВ посылает текущее время на сервер СОВ и ждет ответа сервера СОВ;

- как только приходит ответ от сервера СОВ, вычисляется время для установки на агентской станции.

Механизм синхронизации времени предоставляет ряд дополнительных параметров, которые прописаны в конфигурационном файле **time\_sync.conf**. Расположение файла в ОС Windows: **%ALLUSERSPROFILE%\CPS\rebus-sov\ipsCommon\time\_sync.conf**. Расположение файла в ОС MCBC/ОС СН «Astra Linux Special Edition»: **/usr/local/CPS/rebus-sov/ipsCommon/time\_sync.conf**. Вручную файл редактировать не рекомендуется. Редактирование параметров, необходимых для синхронизации времени, производится с помощью консоли СОВ (вкладка «Управление», название «Синхронизация времени»). Данная настройка описана в 4.4.8.5.

#### 4.10. Верификация целостности сигнатур вторжений

Верификация целостности сигнатур вторжений позволяет проверить целостность сигнатур вторжений, используемых на агентских станциях. Описание процесса верификации сигнатур вторжений см. в 4.3.5.

#### 4.11. Использование дополнительных компонентов

ПК «Ребус-СОВ» предусматривает возможность расширения, обеспечивающего подключение/отключение дополнительных программных компонентов (плагинов) противодействия вторжениям, сбора и анализа данных непосредственно на объекте эксплуатации без модификации исполняемых модулей изделия.

Для обеспечения возможности интеграции с ПК «Ребус-СОВ» компонент должен иметь 3 плагина – плагин агента СОВ, плагин консоли управления СОВ, плагин сервера СОВ.

Для того чтобы выполнить подключение компонента на агенте СОВ, необходимо скопировать модуль плагина в соответствующий каталог:

- **/usr/local/lib/CPS/rebus-sov/agnPlugins/** в ОС MCBC и ОС СН «Astra Linux Special Edition»;

- **%Program Files%\CPS\rebus-sov\agnPlugins\** в ОС Windows.

После этого необходимо установить дополнительные модули (в случае их наличия), взаимодействующие с плагином, и перезагрузить ЭВМ.

Для того чтобы подключить компонент в консоли управления, необходимо скопировать модуль плагина в соответствующий каталог:

- **/usr/local/lib/CPS/rebus-sov/consPlugins/** в ОС MCBC и ОС СН «Astra Linux Special Edition»;

- **%Program Files%\CPS\rebus-sov\consPlugins\** в ОС Windows.

После этого необходимо перезапустить консоль управления.

Для того чтобы выполнить подключение компонента на сервере СОВ, необходимо скопировать модуль плагина в соответствующий каталог:

- **/usr/local/lib/CPS/rebus-sov/srvPlugins/** в ОС MCBC и ОС СН «Astra Linux Special Edition»;

- **%Program Files%\CPS\rebus-sov\srvPlugins\** в ОС Windows.

После этого необходимо перезагрузить ЭВМ для перезапуска сервера СОВ.

## 5. СООБЩЕНИЯ ОПЕРАТОРУ

Сведения о сообщениях оператору, о действиях оператора при появлении данных сообщений приведены в таблицах 8, 9.

Таблица 8 – Сообщения, выдаваемые при работе со средством настройки агентской части

Содержание сообщения	Описание сообщения	Действия оператора
Имеются несохраненные изменения. Закреть программу?	В процессе работы модуля настройки агентской части некоторые настройки не были сохранены перед выходом из программы	Нажать кнопку «Отмена» для предотвращения закрытия программы. Нажать кнопку «Закреть» для закрытия программы с потерей несохраненных настроек
Отсутствует эталонный файл, необходимый для выполнения верификации модулей	При выполнении верификации целостности модулей не найден эталонный файл	Необходимо переустановить дистрибутив
Неправильный формат эталонного файла	При выполнении верификации целостности модулей содержимое эталонного файла не соответствует необходимой структуре	Необходимо переустановить дистрибутив
Программа может быть запущена только от имени администратора	Программа настройки агентской части может быть запущена только пользователем, который имеет права администратора	Выполнить вход в систему пользователем с правами администратора
Программа может быть запущена только из несекретного сеанса без категорий	Программа настройки агентской части может быть запущена только в сеансе не выше, чем несекретный	Проверить сеанс и наличие определённых мандатных меток
Не удалось запустить сервис ipsAgent	За отведенное время не удалось запустить сервис ipsAgent	Повторно запустить агент COB
Не удалось остановить сервис ipsAgent	За отведенное время не удалось остановить сервис ipsAgent	Повторно остановить агент COB
Превышено время ожидания ответа от сервиса ipsAgent	Закончилось время, отведенное на ответ сервиса ipsAgent. Сервис завис	Закреть программу настроек, открыть её снова и перезапустить агент COB
Невозможно удалить следующие объекты: .... Для корректной настройки на новый сервер необходимо вручную удалить каталог и перезапустить агентскую службу	При смене сервера не удалось очистить базу сигнатур	Необходимо проверить права на список каталогов, которые не удалось удалить. Произвести удаление вручную. Перезапустить агент COB
Ошибка инициализации базы сигнатур. Невозможно создать каталог:<Имя каталога>	При смене сервера не удалось создать необходимые каталоги	Необходимо создать вручную несозданные каталоги, описанные в сообщении, и перезапустить агент COB

Окончание таблицы 8

Содержание сообщения	Описание сообщения	Действия оператора
Программа уже запущена (идентификатор процесса) и не отвечает на запросы. Одновременный запуск нескольких экземпляров запрещен	Повторная попытка запуска экземпляра приложения. Работающий экземпляр завис	Необходимо перезагрузить станцию и выполнить запуск приложения

Таблица 9 – Сообщения, выдаваемые при работе с консолью управления

Содержание сообщения	Описание сообщения	Действия оператора
Консоль управления СОВ уже запущена. Запуск второй копии приложения невозможен	Запрещено запускать более одной копии приложения	Отменить запуск второй копии
Невозможно удалить единственного администратора СОВ	Запрещено удалять единственного администратора СОВ во избежание блокировки работы ПК «Ребус-СОВ»	Отменить операцию удаления пользователя
Пакет обновления не передан на сервер. Код ошибки: <причина ошибки>	Не удалось выполнить обновление баз решающих правил на сервере	Устранить причину ошибки и повторить операцию
Поле <наименование> задано неправильно. Укажите нужное значение	Неправильно задано поле	Задать корректное значение
Длина пароля не должна быть меньше 6 и больше 25 символов	Пароль имеет некорректную длину	Задать пароль правильной длины
Пароль не подтвержден	Подтверждение не соответствует паролю	Задать правильное подтверждение
Ошибка подключения к серверу: <описание ошибки> (<код ошибки>)	Не удалось подключиться к серверу	Проверить доступность сервера
Не удалось записать PID запущенного приложения в файл <имя файла>. Запуск приложения невозможен	Ошибка записи в файл	Проверить доступ к файлу, при необходимости настроить права доступа на файл и каталог
Произошел разрыв соединения с сервером СОВ	Сервер СОВ стал недоступен по сети	Обеспечить доступ по сети к серверу СОВ, перезапустить консоль
Не удалось установить обновление <имя файла> Причина: <описание>	Ошибка установки обновления	Устранить причину ошибки, повторить установку обновления
Не удалось получить настройки для плагина <имя плагина> Причина: <описание>	Ошибка получения настроек плагина	Устранить причину ошибки, повторить задание настроек
При передаче настроек на сервер произошла ошибка <описание ошибки>	Ошибка передачи настроек на сервер	Устранить причину ошибки, повторить передачу настроек

Продолжение таблицы 9

Содержание сообщения	Описание сообщения	Действия оператора
Не удалось скопировать настройки с сервера обмена файлами. Код ошибки: <код>	Ошибка копирования настроек с сервера обмена файлами	Устранить причину ошибки, повторить действие
Не удалось включить режим редактирования настроек. Произошла ошибка: <описание>	Ошибка включения режима редактирования настроек	Устранить причину ошибки, попытаться включить редактирование настроек
Настройки вступят в силу сразу после перезапуска консоли управления	Информационное сообщение	Перезапустить консоль управления для вступления настроек в силу
Возможно, настройки сервера были изменены. Вы хотите сохранить настройки?	Информационное сообщение об изменении настроек сервера	В случае необходимости сохранить настройки
Параметр «Адрес почтового сервера» заполнен неправильно	Параметр задан неправильно	Задать корректное значение параметра
Параметр «Почтовый адрес отправителя» заполнен неправильно	Параметр задан неправильно	Задать корректное значение параметра
Параметр «Идентификатор пользователя» заполнен неправильно	Параметр задан неправильно	Задать корректное значение параметра
Не удалось открыть справку. Причина: «Файл справки <имя файла> не найден»	Ошибка открытия справки	Переустановить ПК «Ребус-СОВ»
Не удалось заблокировать настройки на сервере. Причина: <описание>	Ошибка блокировки настроек на сервере	Устранить причину ошибки, повторить действие
Не удалось сохранить настройки на сервере <описание>	Ошибка при сохранении новых настроек на сервере	Устранить причину ошибки (ввести корректные данные), повторить действие
При распаковке обновления произошла ошибка <описание>	Ошибка распаковки обновления	Устранить причину ошибки, повторить действие
Перед передачей обновления на сервер необходимо убедиться в корректности следующих параметров безопасности: <перечень>	Информационное сообщение о необходимости проверки параметров	Проверить параметры безопасности
При передаче обновления на сервер произошла ошибка <описание ошибки>	Не удалось передать обновление на сервер	Устранить причину ошибки, повторить действие
Редактирование параметров безопасности выполнено. Вы хотите продолжить установку пакета обновления?	Сообщение после редактирования параметров безопасности	В случае необходимости продолжить установку пакета обновления
Выберите архивы для генерации отчета	Предложение выбрать архивы для генерации отчёта	Выбрать архивы

Окончание таблицы 9

Содержание сообщения	Описание сообщения	Действия оператора
Не удалось скопировать отчет с сервера. Код ошибки: <i>&lt;код&gt;</i>	Не удалось скопировать отчет	Устранить причину ошибки, повторить действие
Не удалось открыть отчет <i>&lt;путь к файлу&gt;</i>	Ошибка открытия отчета	Проверить и при необходимости настроить доступ к файлу. Проверить работоспособность программы Internet Explorer, при необходимости переустановить
Не удалось сгенерировать отчет. Причина: <i>&lt;описание&gt;</i>	Ошибка генерации отчета	Устранить причину ошибки, повторить генерацию отчета
Не удалось выполнить сохранение отчета в каталог <i>&lt;каталог&gt;</i>	Не удалось выполнить сохранение сформированного отчета по событиям в файл на диске	Проверить права доступа к каталогу и при необходимости настроить их
Ошибка агента при изменении настроек сетевых интерфейсов	При изменении настроек сетевых адаптеров произошла ошибка, возможно, файл был удален или изменен	Произвести повторную настройку сетевых адаптеров для каждого сетевого плагина выбранной станции

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АПК	– аппаратно-программный комплекс
АПКЗИ	– аппаратно-программный комплекс защиты информации
БРП	– база решающих правил
ИБ	– информационная безопасность
ИС	– информационная система
ЛВС	– локальная вычислительная сеть
МСВС	– мобильная система Вооруженных сил
ОС	– операционная система
ОС СН	– операционная система специального назначения
ПК	– программный комплекс
ПО	– программное обеспечение
СОВ	– система обнаружения вторжений
ЭВМ	– электронно-вычислительная машина
ЭН	– электронный носитель

