

Утверждён  
ПМБИ.10145-01-ЛУ

**СРЕДСТВО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**  
**(САИБ «ОКО»)**  
Шифр – «ОКО»

Руководство администратора  
ПМБИ.10145-01 90 01

Листов 186

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

**Аннотация**

Настоящий документ является эксплуатационным и содержит описание основных функциональных характеристик изделия «Средство аудита информационной безопасности» (САИБ «ОКО»), руководство по установке и руководство по работе с компонентами САИБ «ОКО».

**Содержание**

1. Общие сведения .....	6
1.1. Функциональное назначение и область применения.....	6
1.2. Состав САИБ .....	6
1.3. Общее описание принципа функционирования САИБ .....	9
2. Программно-аппаратные средства, необходимые для функционирования САИБ.....	11
2.1. Требования к техническим средствам.....	11
2.1.1. ОКО-РС .....	11
2.1.2. Система управления «ОКО-КОНСОЛЬ» .....	11
2.2. Требования к программным средствам.....	11
2.3. Требования к составу и параметрам технических средств .....	12
3. Установка и начальная настройка компонентов САИБ.....	13
3.1. Установка ОПО .....	13
3.2. Установка СПО.....	13
3.2.1. Установка Сервера .....	13
3.2.2. Локальная установка Сервера.....	14
3.2.2.1. База данных MySQL.....	16
3.2.2.2. База данных Microsoft SQL Server.....	18
3.2.3. Установка графического интерфейса администратора .....	23
3.2.4. Графический интерфейс администратора.....	23
3.2.5. Настройка Сервера .....	26
3.2.5.1. Настройка сервера администрирования.....	27
3.2.5.2. Настройка сервера обновлений.....	28
3.2.6. Установка РС .....	32
3.2.6.1. Минимальные требования для установки РС.....	32
3.2.6.2. Локальная установка.....	32
3.2.6.3. Регистрация в САИБ локально установленного РС.....	36
3.2.6.4. Удалённая установка РС.....	37
3.2.7. Настройка РС .....	42

3.2.8.	Установка сетевого сенсора .....	44
3.2.9.	Подключение АГАТ .....	46
4.	Удаление СПО .....	49
4.1.	Удаление Сервера.....	49
4.2.	Удаление РС.....	49
4.2.1.	Удалённая деактивация РС .....	49
4.2.2.	Локальная деактивация РС .....	51
4.2.3.	Локальная деактивация сетевого сенсора .....	51
5.	Управление компонентами САИБ .....	53
5.1.	Управление пользователями графического интерфейса .....	53
5.2.	Ведение топологии эксплуатирующей организации .....	56
5.3.	Настройка правил мониторинга.....	61
5.3.1.	Настройка правила контроля журнала системных событий .....	65
5.3.2.	Настройка правила контроля целостности ПО .....	69
5.3.3.	Настройка правила межсетевого экрана .....	71
5.3.4.	Настройка правила контроля аппаратной конфигурации .....	75
5.3.5.	Настройка правила контроля съёма жёстких дисков.....	76
5.3.6.	Настройка правила контроля процессов.....	77
5.3.7.	Настройка правила контроля устройств USB.....	90
5.4.	Создание шаблонов правил .....	94
5.5.	Настройка сценариев опроса.....	98
5.6.	Настройка контроля датчиков и ТО .....	113
5.7.	Мониторинг и принудительное управление контролируемыми рабочими местами .....	122
5.7.1.	Системный монитор.....	123
5.7.2.	Видеотрансляция .....	125
5.7.3.	Монитор событий.....	128
5.7.4.	Менеджер задач .....	130
5.7.5.	Просмотр снимков экрана .....	137
5.7.6.	Получение локальных данных .....	139

5.7.7	Просмотр аппаратных конфигураций .....	139
5.7.8	Последний незакрытый инцидент .....	141
5.7.9	Портал администратора .....	146
5.7.10	Мнемосхема топологии САИБ.....	150
5.8.	Мониторинг САИБ.....	153
5.8.1	Журнал событий.....	153
5.8.2	Инциденты .....	156
6.	Удалённое управление ТО .....	159
6.1.	Распаковка дистрибутива организации VPN-туннеля в ОС *nix ....	160
6.2.	Формирование сертификатов и ключей OpenSSL в ОС *nix.....	161
6.3.	Запуск сервера и клиента OpenVPN в ОС *nix .....	163
6.4.	Распаковка дистрибутива организации VPN-туннеля в ОС Windows.....	166
6.5.	Формирование сертификатов и ключей OpenSSL в ОС Windows...	167
6.6.	Запуск сервера и клиента OpenVPN в ОС Windows .....	168
6.7.	Настройка АГАТ для управления ТО .....	172
6.8.	Сеанс удалённого управления ТО .....	174
7.	Аналитика событий .....	175
8.	Системные операции .....	180
8.1.	Настройка уведомлений .....	180
8.2.	Резервное копирование.....	181
	Список сокращений .....	183

## **1. Общие сведения**

### **1.1. Функциональное назначение и область применения**

Программное средство аудита информационной безопасности «ОКО» (далее по тексту – САИБ «ОКО») предназначено для получения свидетельств выполнения требований по обеспечению информационной безопасности (ИБ) в автоматизированной информационной системе (АС) на основе постоянного сбора и периодического анализа информации о событиях и инцидентах с целью выявления и предотвращения попыток несанкционированного доступа к обрабатываемой в АС информации и оценки степени выполнения установленных требований по ИБ АС администраторов безопасности.

САИБ «ОКО» реализует технологию контроля защищенности узлов АС на основе выявления и блокирования событий, происходящих в АС, их классификации с точки зрения нарушения информационной безопасности и снижения эффективности функционирования информационной системы, анализа совокупности таких событий с целью выявления возможных уязвимостей.

### **1.2. Состав САИБ**

Архитектурно САИБ «ОКО» представляет собой распределённую информационную систему модели «клиент-сервер», состоящую из компонентов, взаимодействующих по локальной вычислительной сети с использованием протоколов стека TCP/IP. Обеспечение оптимального функционирования САИБ «ОКО» может потребовать разработки топологии размещения компонентов.

В состав САИБ «ОКО» входят следующие компоненты:

- программно-аппаратный сенсор серверного оборудования и телекоммуникационных средств, устанавливаемый в телекоммуникационную стойку (АГАТ);

– программные сенсоры, устанавливаемые на серверное оборудование и рабочие станции информационной системы (ОКО-РС). ОКО-РС делятся на два типа:

- агент мониторинга событий локальной среды Windows (далее по тексту – РС или хостовой сенсор), предназначенный для сбора и систематизации данных о действиях пользователя на контролируемом рабочем месте, последующей доставки этих данных на Сервер, а также реагирования на действия пользователя;
- агент мониторинга событий сетевой среды \*nix (далее по тексту – сетевой сенсор), предназначенный для сбора и систематизации данных о событиях, возникших на объектах сетевой инфраструктуры;

– система управления программно-аппаратным средством САИБ «ОКО» (ОКО-КОНСОЛЬ), в обеспечивающая работоспособность САИБ в целом (в состав системы управления входит компонент «Сервер администрирования», компонент «Сервер обновления» и БД).

К САИБ «ОКО» подключается аппаратный агент мониторинга серверного оборудования и телекоммуникационных средств (далее по тексту – АГАТ), предназначенный для внешнего независимого мониторинга с целью оперативного выявления нештатных ситуаций и повышения уровня информационной безопасности элементов инфраструктуры, телекоммуникационного оборудования и серверов различного назначения. САИБ «ОКО» обеспечивает сбор данных мониторинга с подключенных АГАТ и управление ими из ОКО-КОНСОЛЬ.

Общая схема организации САИБ приведена на Рис. 1.

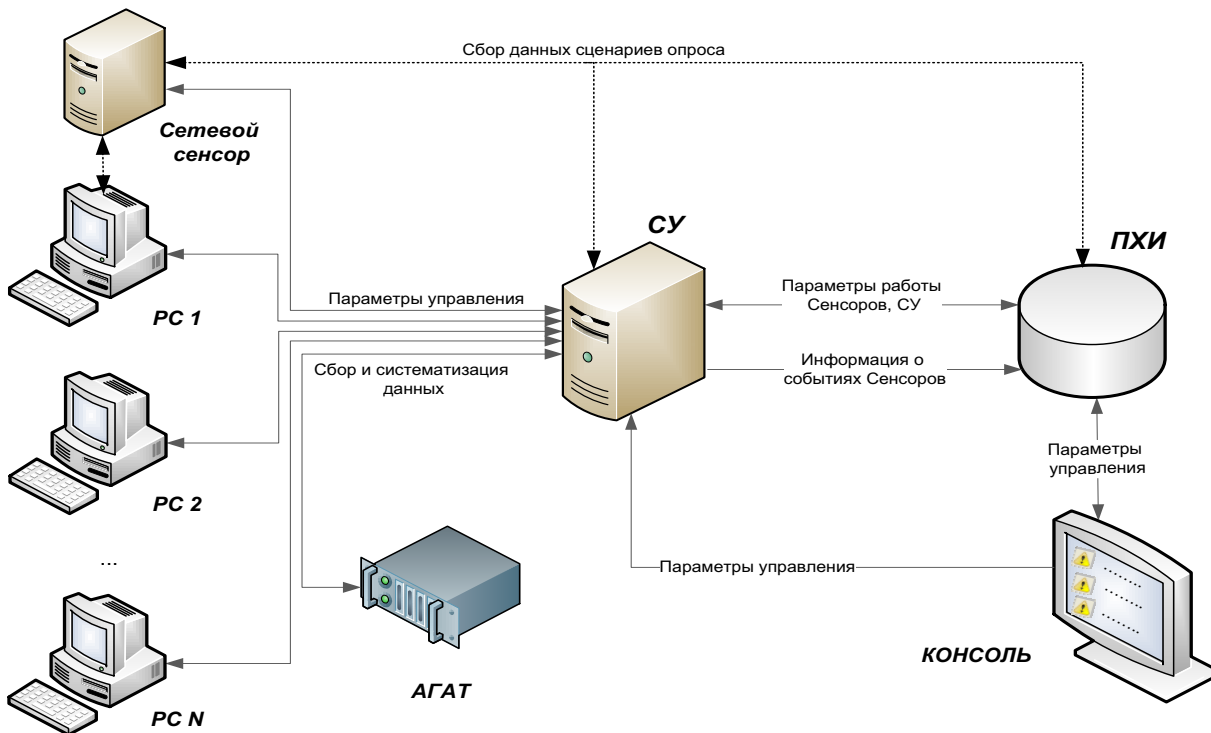


Рис. 1. Общая схема организации САИБ.

Сервер поддерживает постоянные соединения с PC всех контролируемых рабочих мест и АГАТ. Для обеспечения функционирования САИБ требуется установить по крайней мере один Сервер.

При наличии соответствующих полномочий сетевых обращений и административной политики доступ к графическому интерфейсу администратора может осуществляться с любого рабочего места эксплуатирующей организации с помощью Web-обозревателя.

Пример развёрнутого САИБ приведён на Рис. 2.



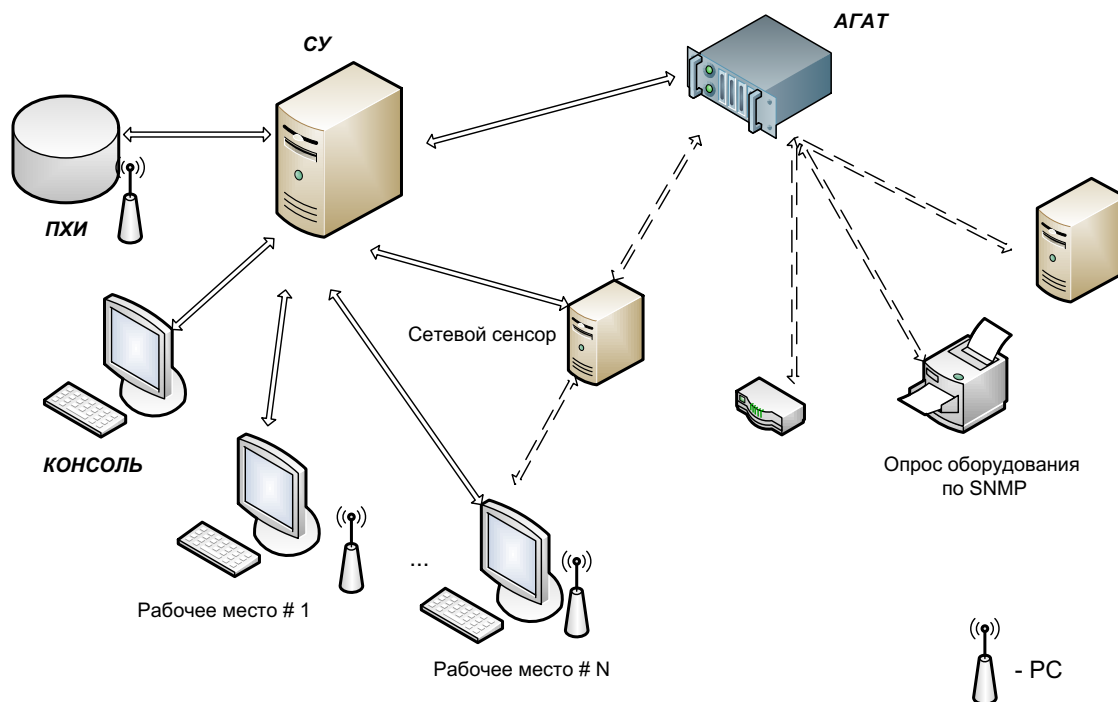


Рис. 2. Пример развёрнутого САИБ.

Количество инсталляций компонентов САИБ «ОКО» не ограничено, САИБ «ОКО» работает без участия администратора после установки и настройки.

Посредством сетевого сенсора и АГАТ САИБ «ОКО» обеспечивает контроль за устройствами, на которые установка РС (программного агента мониторинга) не представляется возможным.

### 1.3. Общее описание принципа функционирования САИБ

Осуществление функций САИБ «ОКО» основано на установке и настройке РС контролируемых рабочих мест и ТО (через АГАТ), состоящей в определении правил сбора и реагирования на типовые события, контроль которых предусмотрен возможностями САИБ «ОКО».

При загрузке ОС контролируемого рабочего места на нём запускается процесс РС (скрытно от пользователя и независимо от наличия активного сеанса пользователя). Затем РС подключается к системе управления ОКО-КОНСОЛЬ и через нее загружает из БД определённые для него правила.

Контроль ТО осуществляется АГАТ, который также загружает из БД системы управления ОКО-КОНСОЛЬ определённые для него правила.

Каждый факт нарушения правила (успешного применения РС или АГАТ условий правила контроля к событию, произошедшему на контролируемом рабочем месте или ТО) вызывает определённую реакцию РС или АГАТ. Реакция зависит от типа правила и установок, определённых для него. При этом сведения о произошедшем событии передаются в систему управления ОКО-КОНСОЛЬ и откладываются в БД для возможного последующего анализа.

В зависимости от типа правила, событиям присваиваются уровни приоритета инцидентности («информационный», «важный» или «критический»), определяющие последующие действия администратора в случае наступления события.

Средствами системы управления ОКО-КОНСОЛЬ администратор уведомляется о наступлении события с указанием его параметров и приоритета инцидентности.

## **2. Программно-аппаратные средства, необходимые для функционирования САИБ**

### **2.1. Требования к техническим средствам**

#### **2.1.1. ОКО-РС**

- ЦП не менее Intel Pentium 4 с частотой не менее 2 ГГц или аналогичного по производительности;
- ОЗУ не менее 512 Мб;
- Свободного пространства на жёстком диске не менее 200 Мб;
- Сетевая карта.

#### **2.1.2. Система управления «ОКО-КОНСОЛЬ»**

- ЦП не менее 4-ядерного процессора Intel Xeon с частотой не менее 3 ГГц или аналогичного по производительности;
- ОЗУ не менее 16 Гб;
- Свободного пространства на жёстком диске не менее 100 Гб;
- Две сетевые карты с пропускной способностью каждой не менее 1 Гбит/с.

### **2.2. Требования к программным средствам**

Установка ОКО-РС на контролируемое рабочее место или системы управления ОКО-КОНСОЛЬ требует функционирования на нём одной из следующих ОС (в зависимости):

- Microsoft Windows XP Professional SP3, x32;
- Microsoft Windows XP, x64;
- Microsoft Windows 2003 Server, x32 (Enterprise, Standard edition/SP1, SP2/R2);
- Microsoft Windows 2003 Server, x64;
- Microsoft Windows 7, x32/x64;
- Microsoft Windows 2008, x32/x64.
- Microsoft Windows 8, x32/x64.

Для функционирования системы управления ОКО-КОНСОЛЬ необходима СУБД MS SQL версии 2005/2008 или выше (при выборе данной СУБД в качестве базовой при установке).

### **2.3. Требования к составу и параметрам технических средств**

Для функционирования САИБ «ОКО» необходим сервер архитектуры IBM PC с минимальными техническими характеристиками, соответствующими ЦП Pentium IV с частотой 2800 МГц, и объёмом ОЗУ 512 Мбайт.

Для функционирования БД системы управления ОКО-КОНСОЛЬ требуется выделенный сервер, обеспечивающий ведение БД общим объёмом не менее 2 Тбайт. Уровень производительности определяется числом одновременно подключенных ОКО-РС и набора событий, контролируемых ими.

БД служит ядром САИБ «ОКО», обрабатывает и хранит данные в целях обеспечения безопасности всей организации. Поэтому следует уделить самое серьёзное внимание её защите от несанкционированного проникновения и вывода из эксплуатации. В целях предотвращения возможных атак необходимо блокировать по возможности все активные службы и сервисы, кроме СУБД (в зависимости от типа, выбранного при установке).

### **3. Установка и начальная настройка компонентов САИБ**

#### **3.1. Установка ОПО**

Все подсистемы САИБ разработаны для эксплуатации под управлением одной из ОС семейства Microsoft Windows, указанных в п. 2.1.1 настоящего документа. ОС необходимо установить и настроить в соответствии с эксплуатационной документацией на данное ОПО. Дополнительных настроек ОПО не требует.

##### **3.1.1. Особенности установки Kaspersky Antivirus (6.0, 7.0)**

Установка проводится в соответствии с эксплуатационной документацией.

Для корректного функционирования необходимо на АРМ с устанавливаемым РС исключить из проверки на наличие вирусов каталог «C:\Windows\System32\INSA» и файл «C:\Windows\System32\Drivers\Primebox.sys». Для этого в настройках антивируса в доверенную зону необходимо добавить исключения на файл 'Primebox.sys' и папку 'INSA'.

#### **3.2. Установка СПО**

Установка всех компонентов САИБ должна выполняться исключительно с правами администратора ОС того СВТ, на котором осуществляется установка, либо с правами администратора домена Windows (в случае членства целевого СВТ в домене).

##### **3.2.1. Установка Сервера**

Необходимо сделать доступными следующие административные общие ресурсы (доступны по умолчанию):

- 'ADMIN\$';
- 'IPC\$'.

В случае установки Сервера с БД MySQL на серверном СВТ должны быть свободны следующие сетевые порты (открыты по умолчанию):

- ‘5555’ (порт сервера обновлений САИБ);
- ‘5556’ (порт сервера администрирования САИБ);
- ‘444’ (порт графического интерфейса администратора САИБ);
- ‘3306’ (порт СУБД MySQL).

В случае установки Сервера с БД Microsoft SQL Server на серверном СВТ должны быть свободны следующие сетевые порты:

- ‘5555’ (порт сервера обновлений САИБ);
- ‘5556’ (порт сервера администрирования САИБ);
- ‘444’ (порт графического интерфейса администратора САИБ).

При наличии на серверной СВТ СУБД MySQL её необходимо удалить.

Если установка Сервера происходит на СВТ, находящийся в домене, то необходимо убедиться в том, что служба ‘Tomcat’ запущена от имени того пользователя, от имени которого выполняется установка.

### **3.2.2. Локальная установка Сервера**

Установка Сервера выполняется только локально. Для установки Сервера необходимо на серверной СВТ запустить файл ‘ОКО\_server\_setup.exe’ с установочного компакт-диска ПМБИ.10145-01/КД 01-03 01 и следовать инструкциям программы установки (Рис. 3).

***ВНИМАНИЕ!*** В процессе установки на серверное СВТ также устанавливаются продукты сторонних производителей: MySQL (при выборе), Tomcat, JAVA JDK. В случае наличия вышеуказанных продуктов, установщик удалит и установит заново данные продукты. При этом могут быть потеряны данные, относящиеся к данным продуктам, например, уже установленные базы MySQL. Перед началом установки рекомендуется закрыть все работающие приложения.

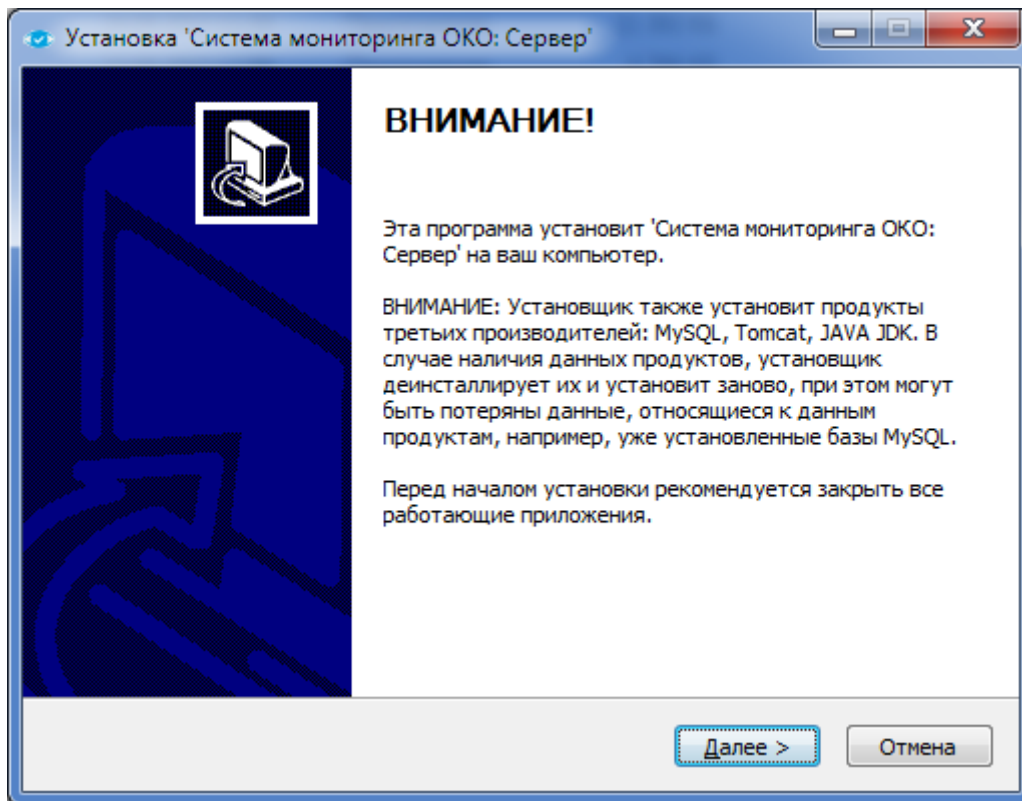


Рис. 3. Информационное окно установки Сервера.

Для продолжения установки Сервера в информационном окне следует нажать кнопку «Далее» и определить папку для установки (по умолчанию – ‘C:\Program Files\Primetech\OKOServer’). Изменение папки производится кнопкой «Обзор...» (последует стандартный диалог ОС для выбора файла).

После выбора папки для продолжения установки следует нажать кнопку «Далее» и перейти к окну выбора типа базы данных для САИБ (Рис. 4).

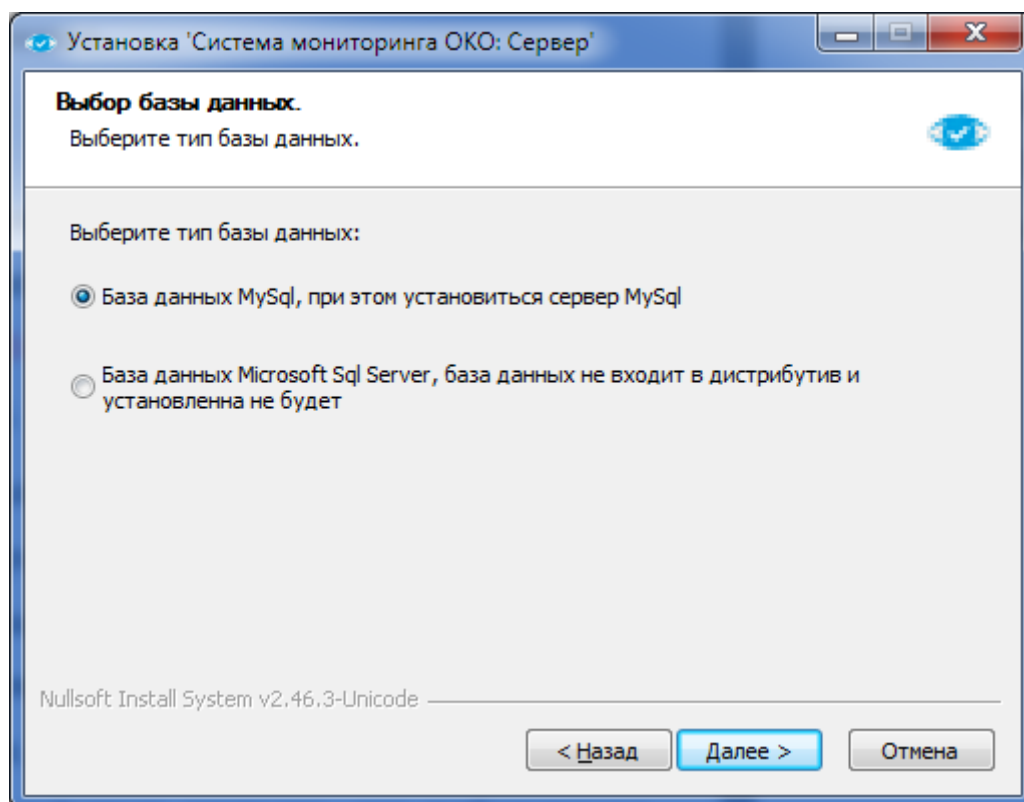


Рис. 4. Окно выбора типа базы данных.

Выбор предпочтительного типа БД для хранения данных мониторинга включает:

- «База данных MySQL» – при выборе данного варианта происходит установка Сервера с БД MySQL. Также устанавливается и запускается в эксплуатацию СУБД MySQL.
- «База данных Microsoft SQL Server» – при выборе данного варианта происходит установка Сервера с БД Microsoft SQL Server. При этом СУБД Microsoft SQL Server в состав дистрибутива Сервера не входит. Поэтому её следует предварительно установить и запустить в эксплуатацию.

### 3.2.2.1. База данных MySQL

Для установки Сервера с БД под СУБД MySQL следует выбрать первый вариант (см. рис. 2) и нажать кнопку «Далее».

Затем следует определить параметры БД MySQL (Рис. 5).



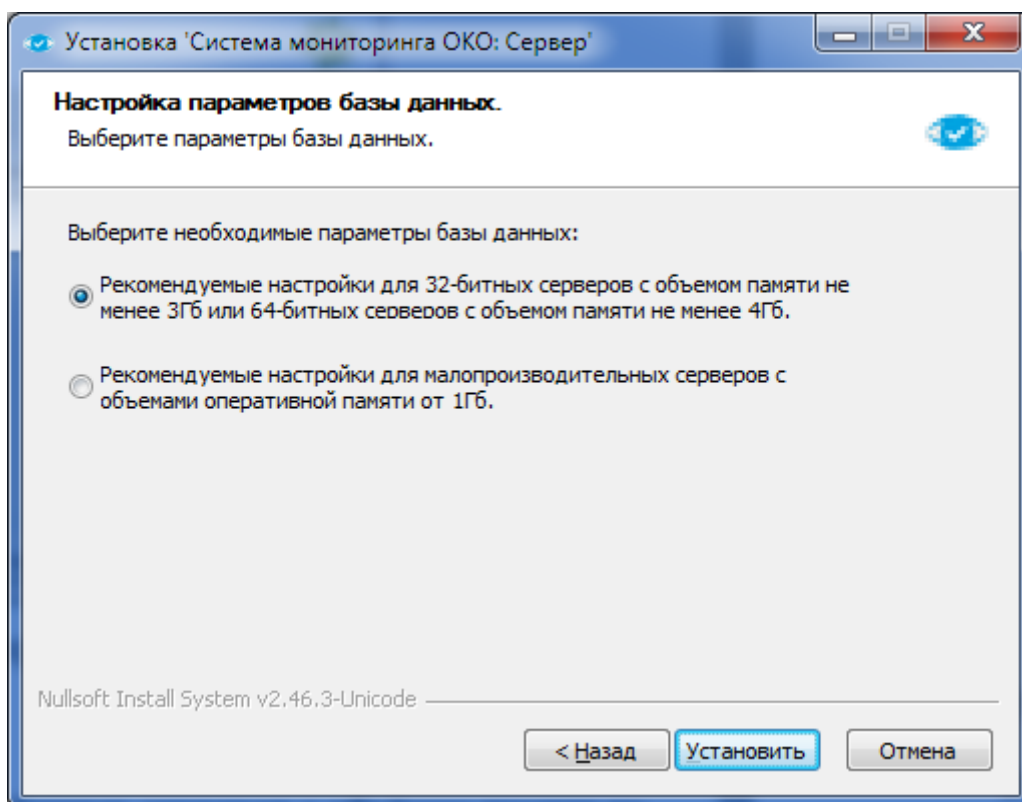


Рис. 5. Окно определения параметров БД MySQL.

Выбор параметров предусматривает:

- Рекомендуемые настройки для 32-битных серверов с объемом памяти не менее 3 Гб или 64-битных с объемом памяти не менее 4 Гб;
- Рекомендуемые настройки для малопроизводительных серверов с объемом оперативной памяти от 1 Гб.

*Примечание.* Не рекомендуется устанавливать Сервер на малопроизводительные серверные СВТ с объемом оперативной памяти от 1 Гб.

Для завершения установки Сервера с БД MySQL следует нажать кнопку «Установить».

По завершению установки Сервера с БД MySQL следует нажать кнопку «Закреть».

### 3.2.2.2. База данных Microsoft SQL Server

Для установки Сервера с БД под СУБД Microsoft SQL Server следует выбрать второй вариант (см. рис. 2) и нажать кнопку «Далее».

Затем следует определить параметры подключения к СУБД Microsoft SQL Server (Рис. 6).

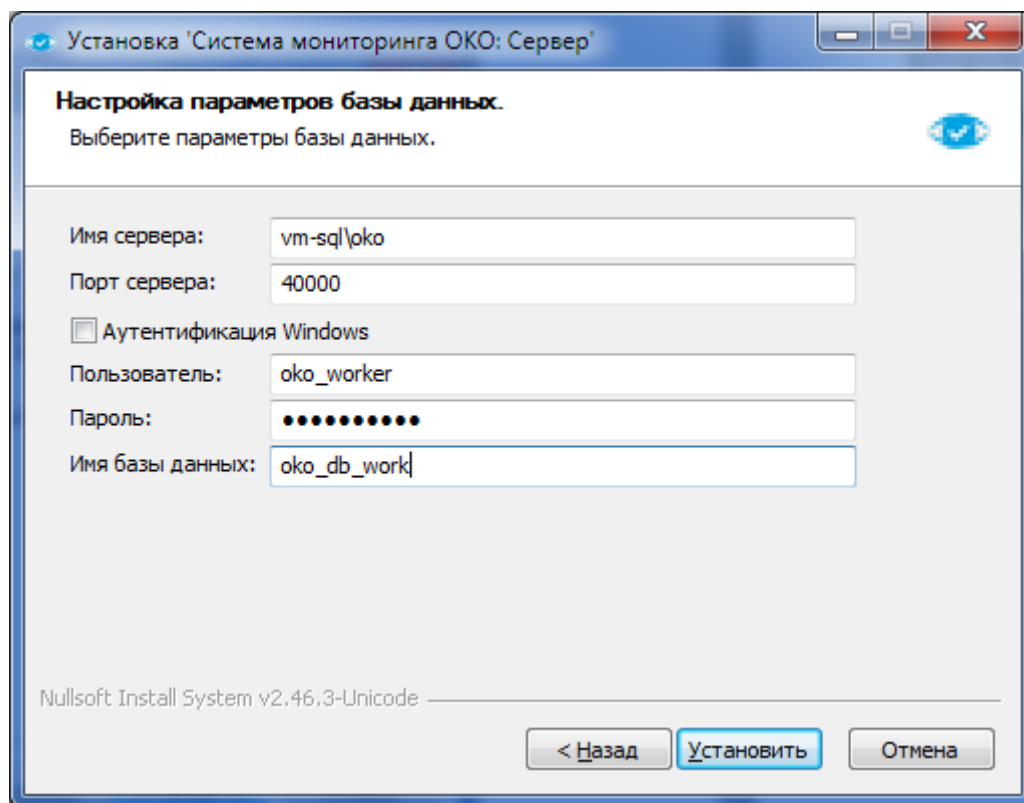


Рис. 6. Окно параметров подключения к СУБД Microsoft SQL Server.

В поле «Имя сервера» следует указать имя сервера СУБД в формате «*IP-адрес сервера*» или «*Имя сервера\имя сущности*».

*Примечание.* В поле «Имя сервера» необязательно указывать значение «Имя сущности».

В поле «Порт сервера» следует указать сетевой порт СУБД.

*Примечание.* Если поле «Порт сервера» останется пустым, то порт соединения с СУБД будет определён автоматически.

При установке флага «Аутентификация Windows» установка БД будет выполнена с применением сквозной аутентификации Windows. Флаг следует

устанавливать при использовании контроллера домена Windows для аутентификации пользователей, у которых есть учётные записи на сервере.

В полях «Пользователь» и «Пароль» следует указать реквизиты учётной записи домена Windows.

*Примечание.* Добавление учётной записи пользователя при использовании домена осуществляется в соответствии с эксплуатационной документацией на СУБД Microsoft SQL Server.

Снятый флаг «Аутентификация Windows» приведёт к использованию SQL-аутентификации. При этом в поле «Пользователь» и «Пароль» следует указать реквизиты учётной записи СУБД для проведения SQL-аутентификации.

*Примечание.* Настройка СУБД Microsoft SQL Server для проведения SQL-аутентификации должны осуществляться в соответствии с эксплуатационной документацией на СУБД Microsoft SQL Server. Также необходимо разрешить подключение к СУБД со всех СВТ с установленными Серверами.

В поле «Имя базы данных» необходимо указать имя БД, которая будет создана в СУБД для хранения данных мониторинга.

*Примечание.* Если на сервере уже имеется БД с названием, указанным в поле «Имя базы данных», БД будет удалена и установлена заново.

Для завершения установки Сервера после определения параметров настройки базы данных следует нажать на кнопку «Установить».

Если в процессе установки Сервера произойдёт сбой, администратору будут выданы следующие диагностические сообщения:

— «*Формат UPN пользователя не поддерживается*» — необходимо убедиться, что в случае установки в домене Windows имя пользователя задано в формате «domain/user»;

- «Введенный пользователь не обладает правами входа как служба» – необходимо убедиться, что у пользователя имеются необходимые права для входа в качестве службы;
- «Невозможно подключиться к серверу MS SQL» – необходимо убедиться, что заданы верные реквизиты сервиса или реквизиты пользователя;
- «Невозможно создать базу» – необходимо убедиться, что БД с таким именем не существует или у пользователя с реквизитами, указанными в полях окна (см. Рис. 6) достаточно прав для её создания;
- «Невозможно внести данные в БД» – необходимо убедиться, что на серверном СВТ достаточно места для внесения данных в БД.

В случае выбора БД Microsoft SQL Server также следует произвести установку СПО «Сервер снятия дампов для Microsoft SQL Server».

*Примечание.* Установку СПО «Сервер снятия дампов для Microsoft SQL Server» следует проводить на СВТ с установленным Microsoft SQL Server и предназначенном для размещения БД САИБ.

Для установки СПО «Сервер снятия дампов для Microsoft SQL Server» следует запустить файл ‘ОКО\_dump\_server\_setup.exe’ с установочного компакт-диска ПМБИ.10145-01/КД 01-03 01 и следовать инструкциям программы установки.

Следует определить папку для установки (по умолчанию – ‘C:\Program Files\Primetech\OKODumpServer’). Изменение папки производится кнопкой «Обзор...» (последует стандартный диалог ОС для выбора файла).

После выбора папки для продолжения установки следует нажать кнопку «Далее» и перейти к окну определения параметров подключения к СУБД (Рис. 7).

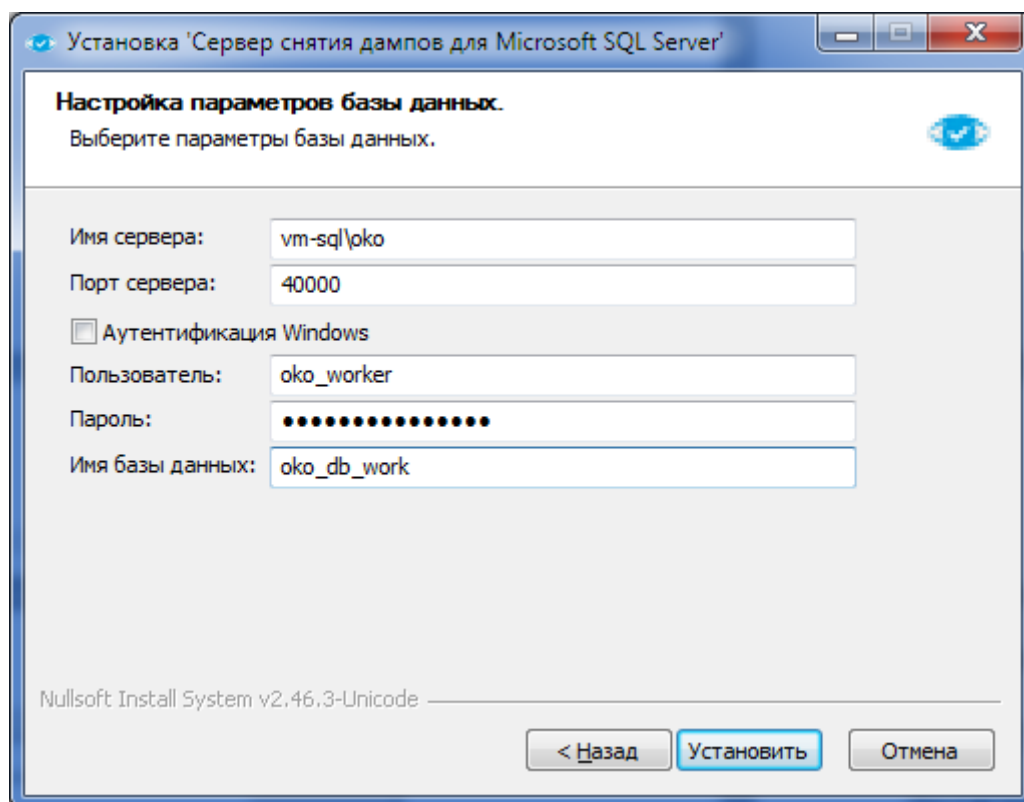


Рис. 7. Окно параметров подключения к СУБД для СПО «Сервер снятия дампов для Microsoft SQL Server»

В поле «Имя сервера» следует указать IP-адрес СУБД или сетевой путь к ней в форме «*имя\_сервера\имя\_сущности*» (имя сущности является необязательным параметром и может отсутствовать).

В поле «Порт сервера» следует указать сетевой порт СУБД. Если поле «Порт сервера» останется пустым, то порт соединения с СУБД будет определён автоматически.

При установке флага «Аутентификация Windows» установка БД будет выполнена с применением сквозной аутентификации Windows. Флаг следует устанавливать при использовании контроллера домена Windows для аутентификации пользователей, у которых есть учётные записи на сервере.

В полях «Пользователь» и «Пароль» следует указать реквизиты учётной записи домена Windows.

*Примечание.* Добавление учётной записи пользователя при использовании домена осуществляется в соответствии с эксплуатационной документацией на СУБД Microsoft SQL Server.

Снятый флаг «Аутентификация Windows» приведёт к использованию SQL-аутентификации. При этом в поле «Пользователь» и «Пароль» следует указать реквизиты учётной записи СУБД для проведения SQL-аутентификации.

*Примечание.* Параметры подключения к СУБД Microsoft SQL Server должны быть такими же, как при установке Сервера.

В поле «Имя базы данных» необходимо указать имя БД для хранения данных мониторинга САИБ.

Для завершения установки СПО «Сервер снятия дампов для Microsoft SQL Server» после определения параметров подключения к СУБД следует нажать кнопку «Установить».

«Сервер» и «сервер администрирования» являются единой сущностью САИБ. После завершения установки служба сервера администрирования запускается автоматически при загрузке ОС серверного СВТ, на котором он установлен.

Если по каким-либо причинам сервер администрирования не запустился автоматически, его запуск следует осуществить вручную из приложения «Командная строка» ('cmd') с помощью следующей команды:

```
C:\>cd C:\Program Files\Primetech\OKOServer\servers\admin\  
C:\Program Files\Primetech\OKOServer\servers\admin>net start ADMServer.exe
```

Сервер администрирования может быть запущен ручным выполнением его исполняемого модуля ('C:\Program Files\Primetech\OKOServer\servers\admin\ADMServer.exe').

*Примечание.* Записи о значимых системных событиях откладываются в текстовом журнале, который хранится на СВТ Сервера в файле 'C:\Program Files\Primetech\OKOServer\admin\ADMServer.log'.

### 3.2.3. Установка графического интерфейса администратора

Графический интерфейс администратора устанавливается в составе Сервера. Для работы с графическим интерфейсом на рабочем месте администратора необходимо установить Web-обозреватель.

*Примечание.* Для корректного функционирования графического интерфейса администратора рекомендуется использовать Web-обозреватель Mozilla Firefox.

Для загрузки приглашения на авторизацию интерфейса в строке адреса (URL) Web-обозревателя следует ввести строку

<code>https://[IP-адрес или доменное имя СВТ с установленным Сервером]:444</code>
---

и нажать клавишу 'Enter'.

При входе в графический интерфейс администратор должен пройти процедуру аутентификации. Для этого в окне авторизации следует указать имя пользователя (по умолчанию – 'admin'), пароль (по умолчанию – 'admin') и нажать кнопку «Продолжить» или клавишу 'Enter'.

**ВНИМАНИЕ!** Для повышения безопасности рекомендуется сменить заводской пароль пользователя 'admin' или создать дополнительную административную учётную запись для управления САИБ, удалив заводскую. (Подробнее об операциях над пользователями САИБ см. п. 5.1 настоящего документа.)

В случае ввода неверных данных процедуру аутентификации пользователя следует выполнить заново.

### 3.2.4. Графический интерфейс администратора

Графический интерфейс администратора САИБ устанавливается совместно с Сервером и состоит из рабочего стола и главного меню в его верхней части.

В правом нижнем углу рабочего стола отображается текущие дата и время пользователя на Сервере с учётом часового пояса по стандарту Всемирного координированного времени (Рис. 8).

*Примечание.* Часовой пояс устанавливается в учётной записи пользователя (см. п. 5.1 настоящего документа).

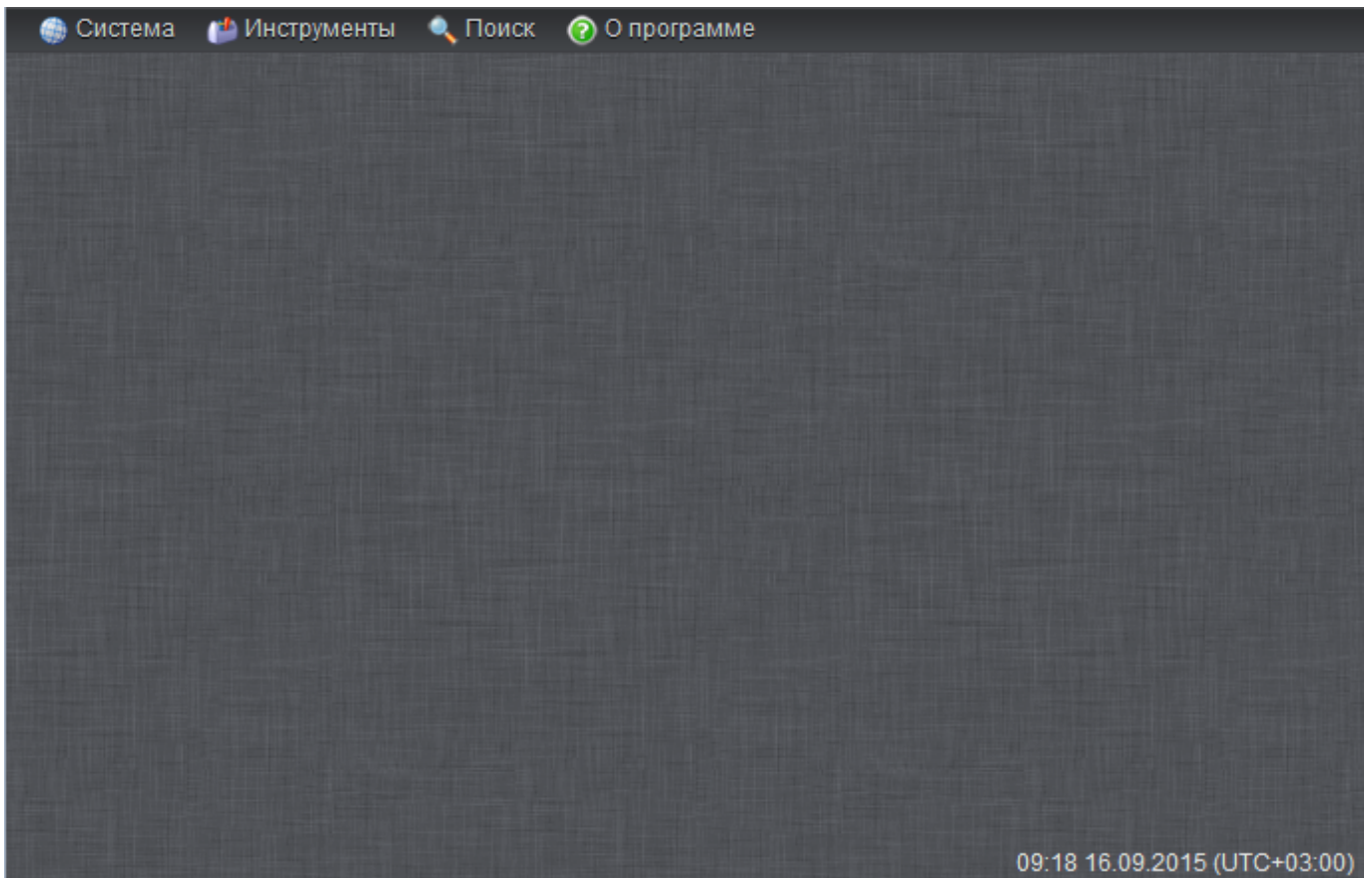


Рис. 8. Рабочий стол графического интерфейса администратора.

Графический интерфейс администратора функционирует аналогично многооконному интерфейсу ОС семейства Microsoft Windows.

С помощью системных кнопок, расположенных в правом верхнем углу, дочерние окна можно «распахивать» на всё пространство рабочего стола (кнопка '□' либо двойной щелчок левой кнопки мыши по заголовку окна) или закрывать с возможной потерей изменений, внесённых в поля ввода (кнопка '×'). Потянув за правый нижний угол любого окна можно изменить размер последнего.



Для удобства управления САИБ рабочий стол предусматривает одновременное наличие нескольких окон разных разделов главного меню, но только по одному окну от каждого из разделов. Захватывая и произвольно перетаскивая окна указателем мыши их можно свободно располагать в любой области пространства рабочего стола.

Главное меню включает следующие разделы.

***Раздел «Система»***

- а) *«Настройки»* – настройка Сервера и РС. Раздел содержит подразделы:
  - а) *«Настройка модулей»* – определение свойств модулей САИБ и правил сбора данных о событиях контролируемых рабочих мест;
  - б) *«Настройка серверов обновлений»* – определение серверов автоматического получения и применения обновлений ПО Сервера и РС;
  - в) *«Настройка уведомлений»* – управление режимами отображения системных уведомлений на рабочем столе графического интерфейса администратора (;
  - г) *«Настройка серверов администрирования»* – определение серверов управления САИБ.
- б) *«Удалённая установка»* – удалённая установка РС на контролируемые рабочие места (.
- в) *«Одобрение локальных установок»* – регистрация РС, установленных локально.
- г) *«Удаление компонент»* – удаление РС из САИБ.
- д) *«Резервное копирование»* – резервное копирование БД.
- е) *«Менеджер пользователей»* – управление пользователями САИБ.
- ж) *«Выход»* – выход из графического интерфейса администратора.

**Раздел «Инструменты»**

- а) «Портал» – мониторинг параметров САИБ в режиме реального времени;
- б) «Инциденты» – просмотр сведений о наступивших инцидентах в САИБ;
- в) «Журнал событий» – отображение информационных сообщений САИБ;
- г) «Мнемосхема» – осуществление просмотра топологии системы;
- д) «Отчёты» – построение аналитических отчётов по накопленным данным мониторинга контролируемых рабочих мест.

**Раздел «Поиск»** – контекстный поиск сущностей во всех разделах графического интерфейса администратора с возможностью ограничения области поиска отдельными разделами по выбору администратора;

**«О программе»** – просмотр сведений о версии САИБ, текущем пользователе графического интерфейса администратора, Web-обозревателе, языке пользователя и типе ОС (сведения могут потребоваться при обращении в службу технической поддержки производителя).

*Примечание.* Сведения о версии САИБ и дате её выпуска можно получить во вкладке «Быстродействие» инструмента «Системный монитор» (см. п. 5.7.1 настоящего документа).

**3.2.5. Настройка Сервера**

После установки Сервера необходимо выполнить его начальную настройку, создав хотя бы одну организационную группу и определив сервер администрирования и сервер обновлений (при необходимости).

### 3.2.5.1. Настройка сервера администрирования

Для добавления сервера администрирования следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка серверов администрирования*.

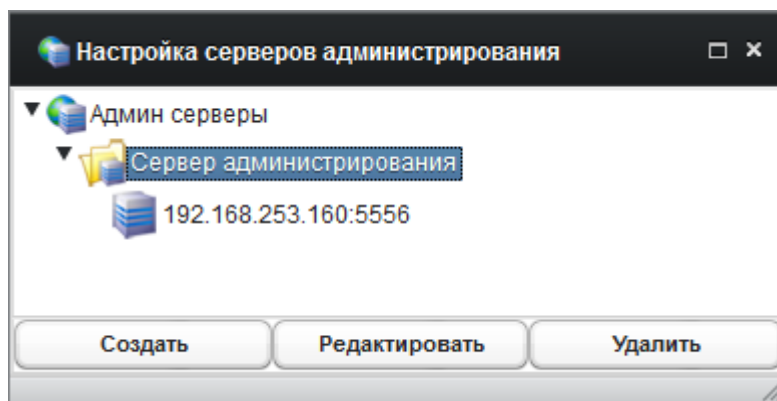


Рис. 9. Окно «Настройка серверов администрирования».

С целью удобства управления САИБ и распределения нагрузки серверы администрирования объединяются в группы, формирующие древовидную иерархическую структуру.

Если в САИБ не определена ни одна группа серверов администрирования, то сервер администрирования будет добавлен одновременно с созданием группы (пустая группа не может быть создана).

Для добавления группы следует нажать кнопку «Создать» (Рис. 9). Затем в дочернем диалоговом окне следует выбрать тип модуля «Группа» и нажать кнопку «Продолжить».

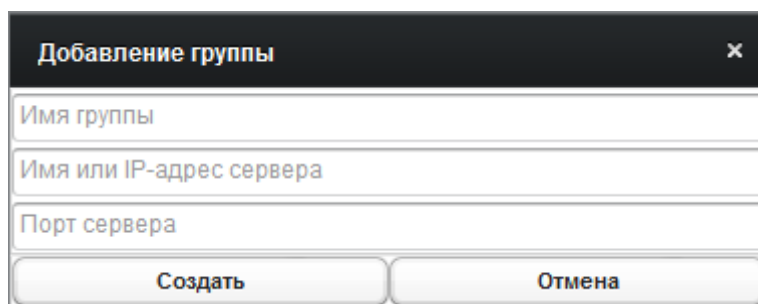


Рис. 10. Окно «Добавление группы».

Следует определить *имя группы* (произвольное наименование), *доменное имя или IP-адрес сервера администрирования* (реквизиты

серверного СВТ, на котором установлен Сервер), его *порт* (по умолчанию – ‘5556’) и нажать кнопку «Создать» (Рис. 10).

*Примечание.* В случае использования локального сервера администрирования указывается имя Сервера. В случае удалённого использования, – полное доменное имя Сервера. При запрете использования DNS, – IP-адрес Сервера.

Для добавления сервера администрирования в определённую ранее группу следует выбрать её указателем мыши или клавишами управления курсором клавиатуры и нажать кнопку «Создать», выбрав «Сервер» в качестве типа создаваемого модуля.

Для изменения реквизитов группы или сервера администрирования следует дважды щёлкнуть левой кнопкой мыши по записи искомого модуля либо выбрать нужный модуль однократным щелчком левой кнопки мыши и нажать кнопку «Редактировать».

Контекстное меню, вызываемое правой кнопкой мыши, позволяет ускорить работу с деревом серверов администрирования.

*Примечание.* Внесение изменений в реквизиты сервера администрирования необходимо осуществить **до установки РС**. После установки РС, связанных с данным сервером администрирования, внесение изменений станет невозможным.

### **3.2.5.2. Настройка сервера обновлений**

Обновление компонентов САИБ выполняется сервером обновлений. При появлении на Сервере новой версии РС производится его автоматизированное обновление на контролируемых рабочих местах. Обновление Сервера производится с Сервера, расположенного на вышележащем уровне топологии САИБ. Обновление Сервера верхнего уровня производится самим Сервером.

Обновлённые версии Сервера и РС размещаются в БД. Обновление БД производится в ручном режиме или с применением средств СУБД.

Инициализация обновлений Сервера и РС производится централизованно при помещении в БД новых версий. Обновление графического интерфейса производится в ручном режиме из дистрибутива его новой версии.

Для добавления сервера обновления в систему следует в главном меню графического интерфейса выбрать раздел *Система* → *Настройки* → *Настройка серверов обновлений*. Список серверов обновлений представлен в табличной форме (Рис. 11).

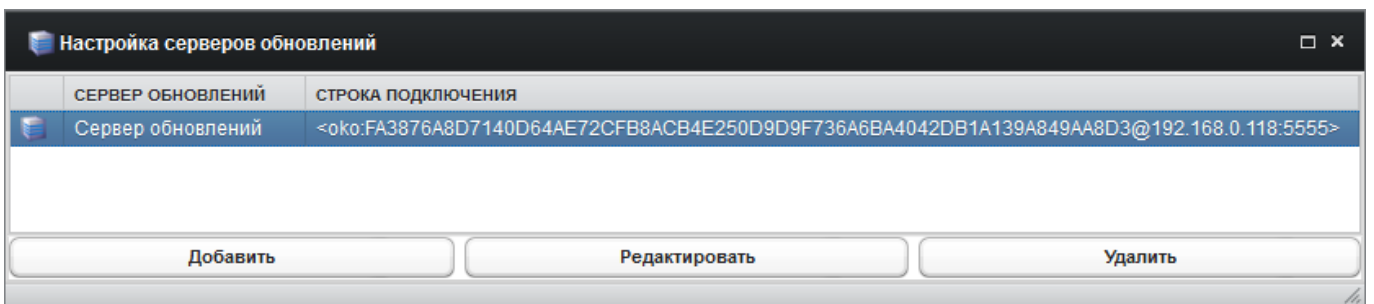


Рис. 11. Окно «Настройка серверов обновлений».

Для добавления сервера обновлений следует нажать кнопку «Добавить» и определить параметры добавляемого сервера в дочернем диалоговом окне (Рис. 12).

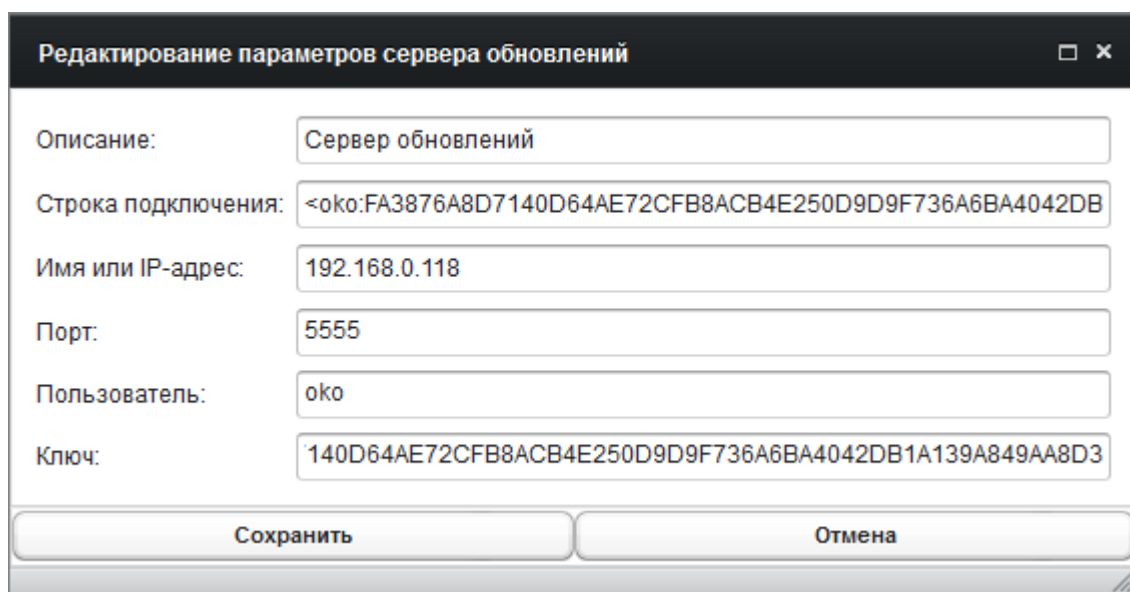


Рис. 12. Окно параметров сервера обновлений.

Следует определить «*Описание*» (произвольное наименование), «*Имя или IP-адрес*» (реквизиты серверного СВТ, на котором установлен Сервер), «*Порт*» (по умолчанию – ‘5555’). Значение поля «*Строка подключения*» сформируется автоматически по значениям прочих полей и его определять не требуется.

*Примечание.* В поля окна параметров сервера обновлений нельзя вносить символы ‘<’, ‘>’, ‘:’ и ‘@’.

Значения полей «*Пользователь*» и «*Ключ*» необходимо использовать из файла ‘%INSTALLDIR%\Servers\update\server\users.txt’ или внести свои, изменив при этом соответствующие значения в указанном файле (в формате «*идентификатор\_пользователя ключ*», через «пробел»).

В качестве значения поля «*Порт*» следует использовать значение параметра ‘port’ файла ‘%INSTALLDIR%\Servers\update\server\server\_config’ или внести значение по умолчанию (‘5555’).

В поле «*Ключ*» следует ввести 64 символа (A-F, 0-1) в шестнадцатеричной системе счисления (HEX) или взять значение ключа, сформированного для локальной установки РС (раздел главного меню *Система* → *Одобрение локальных установок*; см. п. 1.4.1.3.2.6.2 настоящего документа).

По завершению определения параметров сервера обновлений следует нажать кнопку «Сохранить».

Изменение реквизитов ранее определённого сервера обновлений осуществляется двойным щелчком левой кнопкой мыши по записи изменяемого сервера либо кнопкой «Редактировать».

*Примечания:*

1. По умолчанию система обновлений САИБ настроена на серверы ООО «ПРАЙМТЕК». В случае выпуска производителем новых модулей обновление системы произойдет в автоматическом режиме. В случае отсутствия

*необходимости в обновлениях САИБ служба ОС 'Primetech OKO Update Client' может быть остановлена и деактивирована.*

*2. Записи о работе сервера обновлений откладываются в текстовом журнале, который хранится на СВТ Сервера в файле 'C:\Program Files\Primetech\OKOServer\servers\update\server\log.txt'.*

### 3.2.6. Установка РС

РС устанавливаются на рабочие места пользователей и серверы сети, после чего они переходят в разряд контролируемых. Установка может производиться следующими способами:

- локальная установка со съёмного носителя;
- удалённая установка по локальной сети из графического интерфейса администратора.

Обновление РС осуществляется централизованно с помощью серверов обновлений (см. п. 3.2.5.2 настоящего документа).

#### 3.2.6.1. Минимальные требования для установки РС

Для работы сетевого установщика при удалённой установке на рабочих станциях должны быть открыты порты '139' и '445' по протоколу TCP (открыты по умолчанию).

Для установки РС на рабочее место:

- в домене: пользователь должен иметь права администратора домена;
- вне домена: пользователь должен иметь права администратора.

Для ОС Microsoft Vista и выше должна иметься встроенная учётная запись администратора, а контроль учётных записей пользователя (UAC) должен быть отключен.

#### 3.2.6.2. Локальная установка

Перед локальной установкой РС необходимо получить ключ установки. Для этого следует выбрать раздел главного меню *Система* → *Одобрение локальных установок*.

Если в окне «Одобрение локальных установок» (Рис. 13) ключ не определён (соответствующее поле пустое), следует нажать кнопку «Сгенерировать» для получения значения ключа, а затем – кнопку «Применить ключ» для фиксации нового значения (обновления) ключа в БД (последует запрос подтверждения принятого решения).



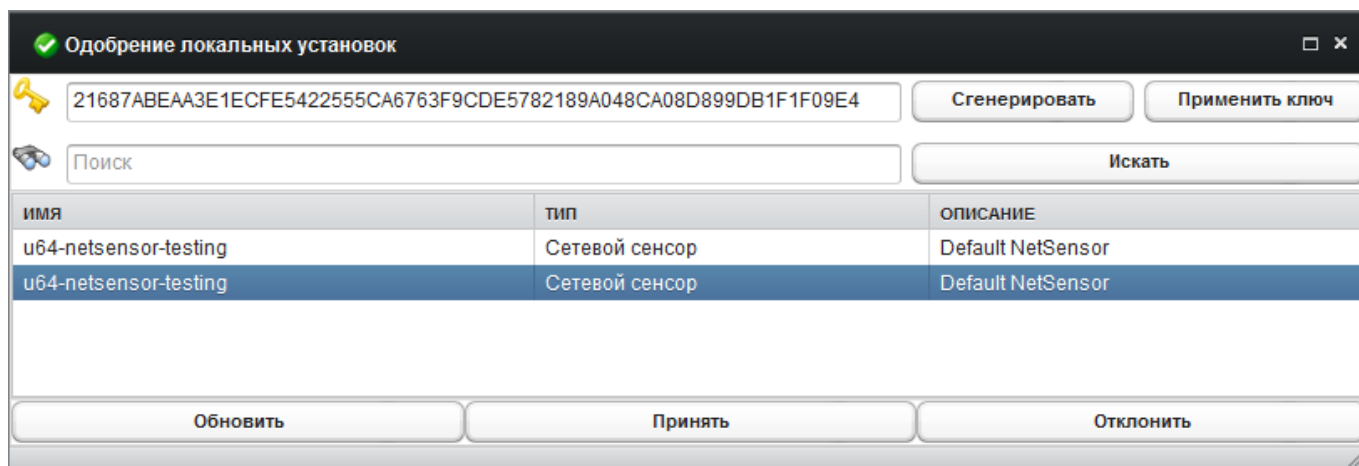


Рис. 13. Получение ключа для локальной установки.

*Примечание.* Локальная установка РС или настройка сервера обновлений проводится с единым ключом, поэтому нет необходимости генерировать и применять новый ключ многократно перед каждой новой установкой РС.

Затем следует скопировать шестнадцатеричное строковое значение ключа и сохранить его каким-либо способом для последующего использования при установке РС.

*Примечание.* Если права доступа предусматривают работу с графическим интерфейсом администратора с любого рабочего места, включая то, на котором проводится локальная установка РС, то ключ может быть скопирован и применён к установке непосредственно в ходе её процесса и предварительное сохранение значения ключа не требуется.

Для локальной установки РС на рабочем месте необходимо запустить файл 'ОКО\_host\_sensor\_setup.exe' с установочного компакт-диска ПМБИ.10145-01/КД 01-03 01 и следовать инструкциям программы установки.

При запуске установки РС появится окно активации режима сохранения снимков экрана (Рис. 14).

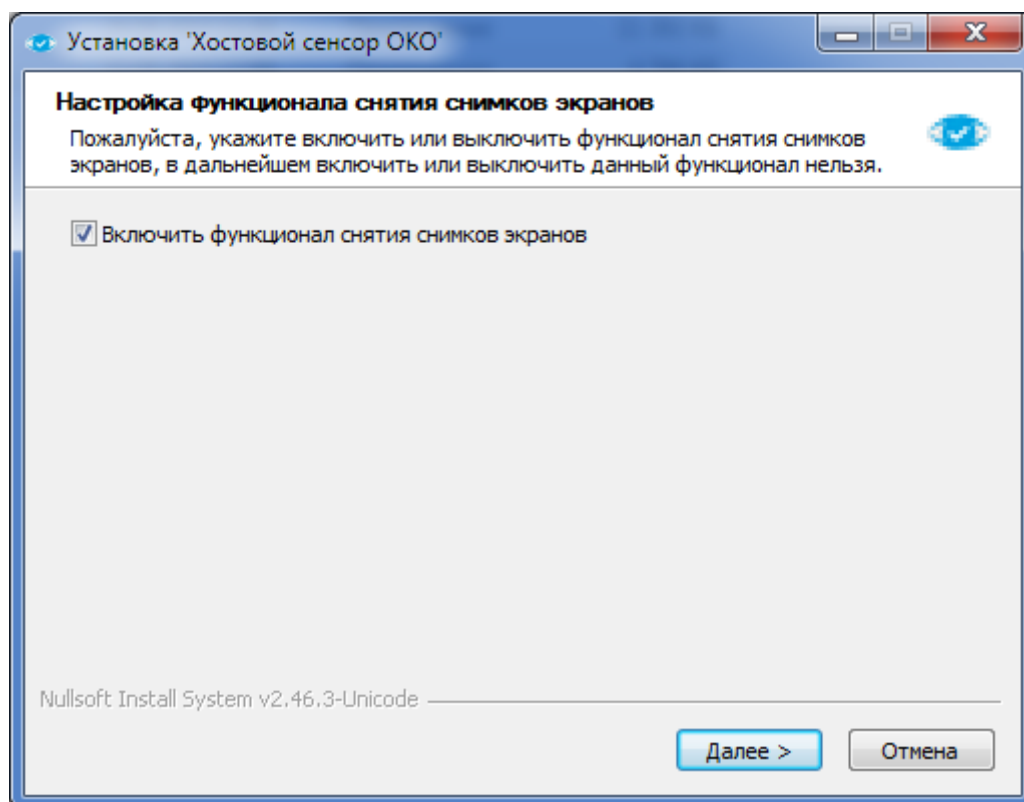


Рис. 14. Окно активации функции снятия снимков экрана.

*Примечание.* Активация функции сохранения снимков экрана осуществляется **только при установке РС**. Включить или выключить данный функционал в дальнейшем невозможно.

После установки флага включения функции сохранения снимков экрана для продолжения установки РС следует нажать кнопку «Далее» и определить параметры подключения к серверу администрирования (Рис. 15), включающие:

- «*IP-адрес/DNS-имя*» – IP-адрес или доменное имя серверного СВТ, на которое установлен Сервер;
- «*Порт*» – порт подключения к серверу администрирования (по умолчанию – ‘5556’);
- «*Ключ*» – шестнадцатеричное значение ключа, скопированное из поля «Ключ» окна «Одобрение локальных установок»;
- «*Комментарий*» – наименование рабочего места для его идентификации при последующей регистрации в САИБ данного

РС.

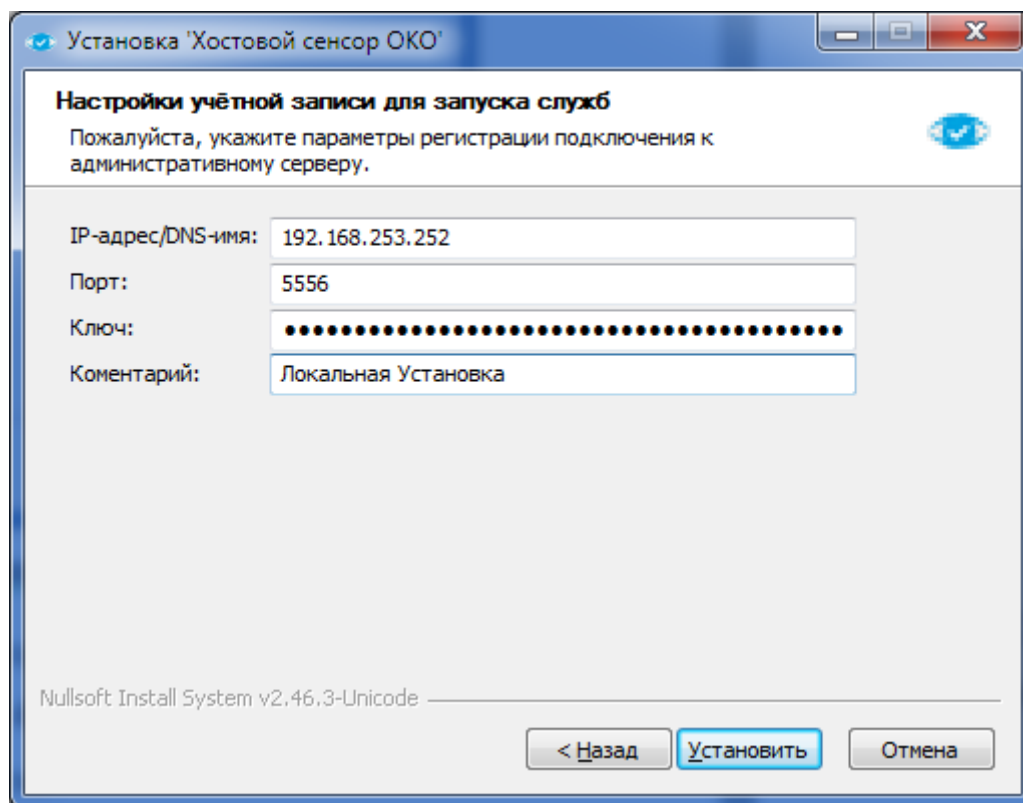


Рис. 15. Окно настройки учётной записи для запуска служб.

После определения параметров следует нажать кнопку «Установить» для перехода в окно завершения процесса установки РС на рабочем месте.

Для завершения установки необходимо выбрать один из вариантов перезагрузки рабочего места, на которое был установлен РС:

- «Да, перезагрузить ПК сейчас» – произойдет перезагрузка рабочего места для завершения установки РС и его запуска;
- «Нет, я перезагружу ПК позже» – пользователю потребуется самостоятельно произвести перезагрузку рабочего места для завершения установки РС в удобное для него время.

После ответа на запрос установщика для завершения установки РС следует нажать кнопку «Готово».

### 3.2.6.3. Регистрация в САИБ локально установленного РС

По завершению локальной установки необходимо зарегистрировать в САИБ РС нового контролируемого рабочего места (сетевой сенсор или АГАТ), выбрав раздел главного меню *Система* → *Одобрение локальных установок*. Лишь после того, как локально установленные РС (сетевые сенсоры или АГАТ) станут частью САИБ, появится возможность определения для них правил сбора событий (сценариев опроса, датчиков) и накопления их в БД.

Список РС (сетевых сенсоров или АГАТ), установленных локально и ожидающих регистрации, представлен в табличной форме (Рис. 13) и включает следующие графы:

- «*Имя*» содержит IP-адрес или доменное имя рабочего места, определённые при локальной установке РС ( сетевого сенсора или АГАТ);
- «*Тип*» содержит тип применяемого сенсора («*Хостовой сенсор 'ОКО'*» для РС, «*Сетевой сенсор*» или «*АГАТ*»);
- «*Описание*» содержит значение поля «Комментарий», определённое при локальной установке РС ( сетевого сенсора или АГАТ), и служит для его дополнительной идентификации.

Восходящая (значок '▲') / нисходящая (значок '▼') сортировка записей в таблице осуществляется щелчком левой кнопки мыши по нужной графе.

Кнопкой «Обновить» следует актуализировать список РС (сетевых сенсоров или АГАТ), установленных локально, и сведения о состоянии их установки.

Регистрация локально установленных РС (сетевых сенсоров или АГАТ) в САИБ осуществляется выбором записей о них указателем мыши или клавишами управления курсором клавиатуры и последующим нажатием кнопки «Принять».

Затем последует запрос на создание нового модуля или добавления выбранного РС ( сетевого сенсора или АГАТ) к существующему модулю.

*Примечание.* Каждый модуль может содержать как один, так и несколько РС, сетевых сенсоров или АГАТ, но на практике это может вызвать путаницу. Поэтому следует придерживаться правила: «один модуль – один компонент» (РС, сетевой сенсор или АГАТ).

При выборе действия добавления из дерева топологии (см. п. 5.2 настоящего документа) следует выбрать имеющийся модуль нужного типа, к которому будет привязан регистрируемый РС (сетевой сенсор или АГАТ) из числа установленных локально. При выборе действия создания последует запрос на создание модуля нужного типа (см. п. 5.2 настоящего документа).

Последует запрос на определение сервера администрирования и сервера обновлений для регистрируемого РС ( сетевого сенсора или АГАТ), а также интервалов обращений к ним. Проведение настроек может быть отложено (см. п. 3.2.7 настоящего документа).

Если по каким-либо причинам требуется отказаться от регистрации выбранных РС (сетевых сенсоров или АГАТ), то следует нажать кнопку «Отклонить».

После успешной регистрации РС (сетевые сенсоры или АГАТ) вносятся в топологию и становятся полноценными компонентами САИБ, готовыми к выполнению своих функций по контролю рабочих мест и ТО.

#### **3.2.6.4. Удалённая установка РС**

Для удалённой установки РС на рабочее место по локальной сети, не требующей запуска программы установки с компакт-диска, следует выбрать раздел главного меню *Система* → *Удалённая установка*.

*Примечание.* Контроль учётных записей пользователя (UAC) на удалённом рабочем месте должен быть отключен.

В окне, отображающем древовидную иерархическую структуру развёрнутых в САИБ серверов администрирования следует выбрать тот сервер администрирования, который будет взаимодействовать с устанавливаемым РС

(вид окна аналогичен изображённому на Рис. 9). После выбора следует нажать кнопку «Дальше».

На следующем этапе следует выбрать сервер обновлений и нажать кнопку «Дальше» (вид окна аналогичен изображённому на Рис. 11).

После этого следует выбрать один из вариантов удалённой установки:

- «*Использовать Active Directory*» – предполагает установку РС на рабочее место с его выбором из каталога Active Directory<sup>1)</sup>;
- «*Не использовать Active Directory*» – осуществляется установка РС на рабочее место с указанием его реквизитов вручную.

В случае выбора варианта «**Использовать Active Directory**» последует запрос на определение реквизитов сервера каталога Active Directory (Рис. 16).

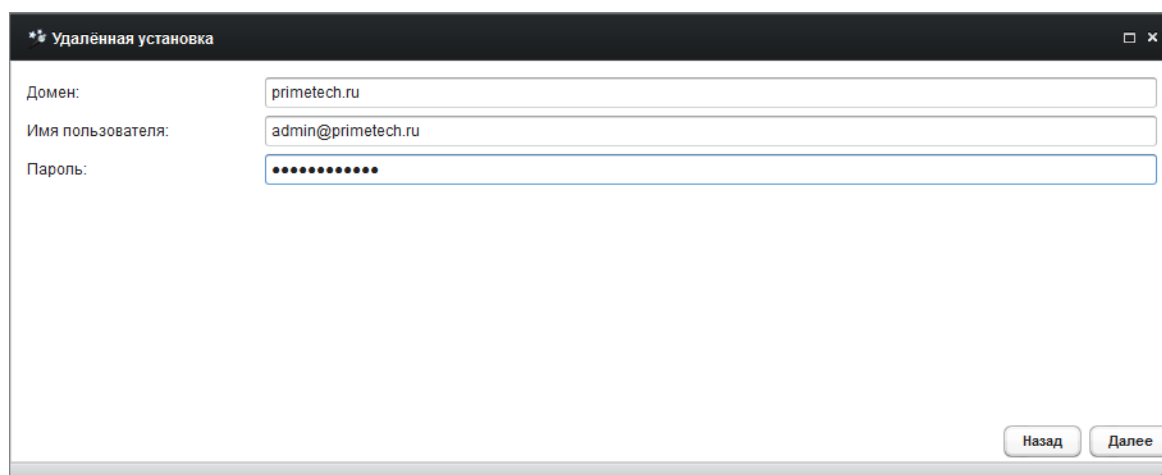


Рис. 16. Окно определения реквизитов сервера каталога.

В поле «Домен» следует указать имя того домена службы каталога, в который входит рабочее место для предполагаемой установки РС. В поле «Имя пользователя» следует указать идентификатор администратора домена в форме «*имя\_пользователя@имя\_домена*», в поле «Пароль», – его пароль. По окончании определения параметров следует нажать кнопку «Далее».

После авторизации в каталоге Active Directory появляется возможность выбора нужного рабочего места для удалённой установки РС на него.

---

<sup>1)</sup> LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows.

Следующий запрос требует подтверждения параметров установки (Рис. 17).

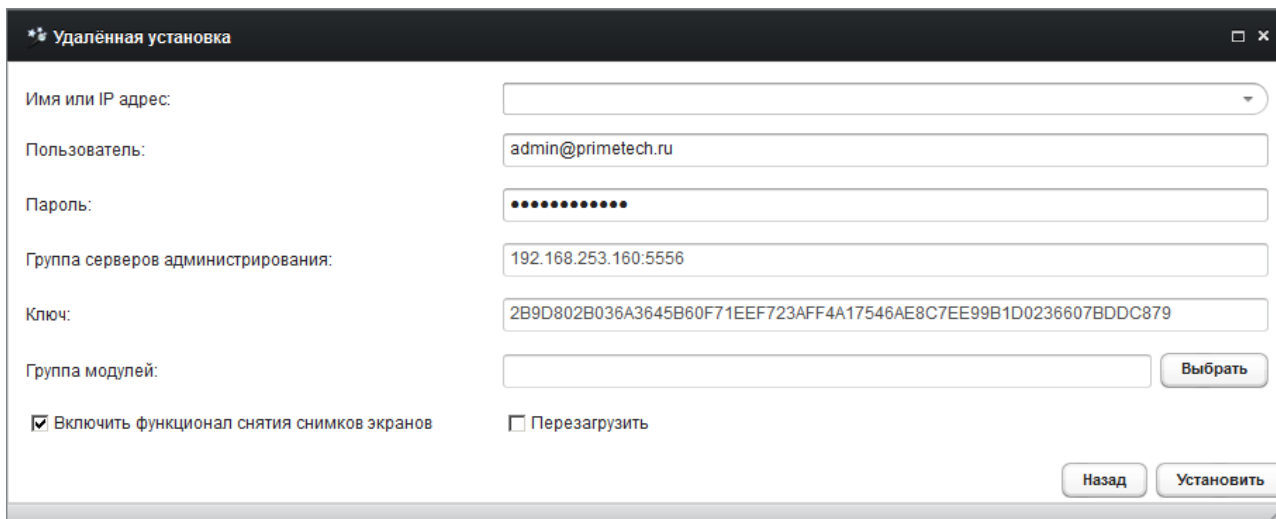


Рис. 17. Окно определения реквизитов рабочего места под РС.

Поле «Имя или IP-адрес» будет содержать реквизиты рабочего места, выбранного в каталоге Active Directory.

*Примечание.* Поля «Группа серверов администрирования» и «Ключ» заполняются автоматически. При необходимости предварительно можно выполнить смену ключа установки РС (см. п. 3.2.6.2 настоящего документа).

В поле «Группа модулей» требуется определить группу топологии, в которую РС будет включен после установки. Для выбора группы из древа топологии следует нажать кнопку «Выбрать» (Рис. 18).

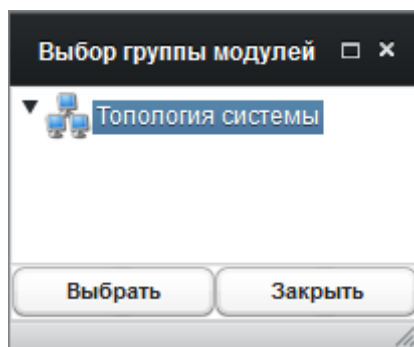


Рис. 18. Окно выбора групп модулей.

С помощью указателя мыши в окне «Выбор группы модулей» следует выбрать группу модулей, в которую предполагается поместить установленный РС и нажать кнопку «Выбрать».

*Примечание.* При отсутствии нужной группы устанавливаемый РС можно поместить в корневой уровень «Топология системы», а уже после создать нужную группу и переместить установленный РС в неё. Подробное см. п. 5.2 настоящего документа.

Установка флага «Включить функционал снятия снимков экрана» активирует режим сохранения снимков экрана в качестве одной из ответных мер на факт успешного применения правила сбора событий.

*Примечание.* Активация функции сохранения снимков экрана осуществляется **только при установке РС**. Включить или выключить данный функционал в дальнейшем невозможно.

Установка флага «Перезагрузить» приведёт к перезагрузке рабочего места для завершения установки РС и его запуска. Если флаг снят, РС будет активирован на контролируемом рабочем месте только при следующей загрузке ОС.

Для завершения удалённой установки РС следует нажать кнопку «Установить».

Установка РС на другое рабочее место по выбору из каталога Active Directory не потребует повторного ввода реквизитов и авторизации на сервере каталога.

Выбор варианта «**Не использовать Active Directory**» для установки РС предполагает авторизацию на рабочем месте с реквизитами администратора домена Windows либо пользователя рабочего места с административными полномочиями. В этом случае определение параметров установки проводится способом, аналогичном способу выполнения удалённой установки с использованием Active Directory, начиная с шага определения параметров установки (см. Рис. 17).



В поле «Имя или IP-адрес» следует вручную указать доменное имя или IP-адрес рабочего места, на которое предполагается установка РС.

В поле «Пользователь» следует указать реквизиты администратора домена Windows, либо реквизиты пользователя (в форме «*имя\_компьютера\имя\_пользователя*») рабочего места, на которое устанавливается РС. (При этом учётная запись указанного пользователя непременно должна обладать административными полномочиями.) В поле «Пароль» указываются пароль администратора домена Windows или пользователя рабочего места.

Установка флага «Перезагрузить» приведёт к перезагрузке рабочего места для завершения установки РС и его запуска. Если флаг снят, РС будет активирован на контролируемом рабочем месте только при следующей загрузке ОС.

Для завершения удалённой установки РС следует нажать кнопку «Установить».

В случае сбоя в ходе удалённой установки (например, по причине указания некорректных значений параметров) по завершению установки будет выдано сообщение об ошибке (Рис. 19). Для просмотра подробностей, облегчающих анализ создавшейся ситуации, следует нажать кнопку «Да». Кнопка «Нет» закрывает окно сообщения об ошибке.

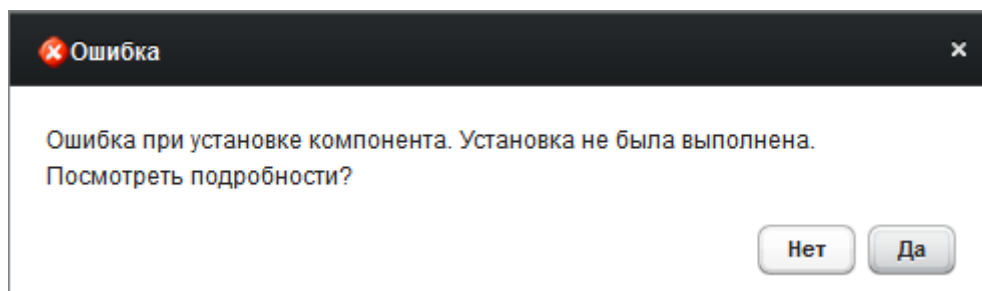


Рис. 19. Окно «Ошибка».

РС запускается автоматически после перезагрузки ОС СВТ контролируемого рабочего места, на котором он установлен.

### 3.2.7. Настройка РС

Одними из основных параметров взаимодействия РС (сетевого сенсора или АГАТ) и Сервера являются интервалы соединения с сервером администрирования и сервером обновления.

**Интервал соединения с сервером администрирования** определяет частоту передачи на Сервер событий, накопленных РС (сетевым сенсором или АГАТ). Чем короче интервал, тем чаще Сервер будет получать и анализировать данные о текущих событиях с рабочего места и обновлять настройки РС (сетевого сенсора или АГАТ).

**Интервал соединения с сервером обновлений** определяет частоту проверки наличия доступных обновлений ПО РС.

Для изменения указанных интервалов следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*, отыскать и выбрать в древе топологии нужный модуль. После этого нужно переключить окно свойств в режим отображения «Компоненты» (Рис. 20).

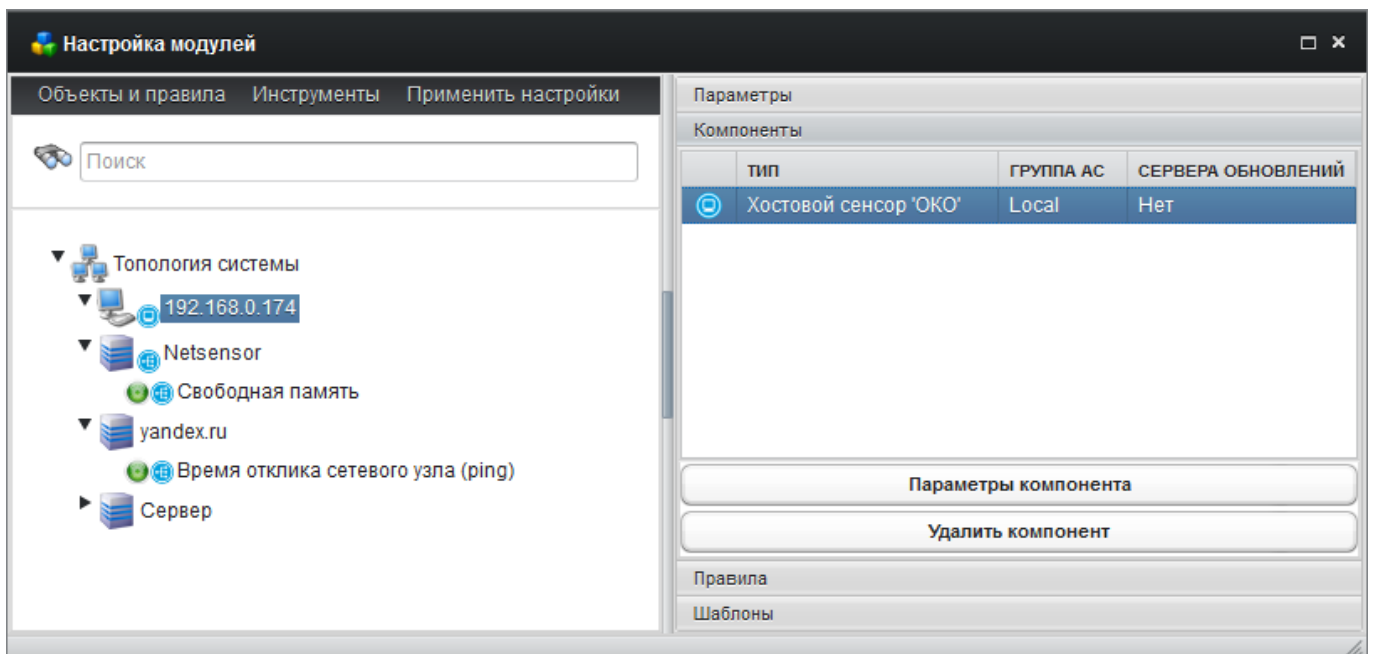


Рис. 20. Окно «Настройка модулей» в режиме «Компоненты».

Компонентами модулей в САИБ могут служить установленные на них РС, сетевые сенсоры или АГАТ. Каждый модуль может содержать неограниченное число компонентов. Неконтролируемые рабочие места

компонентов САИБ не содержат, но могут контролироваться сценариями опроса сетевого сенсора (см. п. 5.5 настоящего документа).

Для изменения значений указанных интервалов в таблице компонентов следует выбрать строку нужного компонента и нажать кнопку «Параметры компонента», либо дважды щёлкнуть левой кнопкой мыши по строке (Рис. 21).

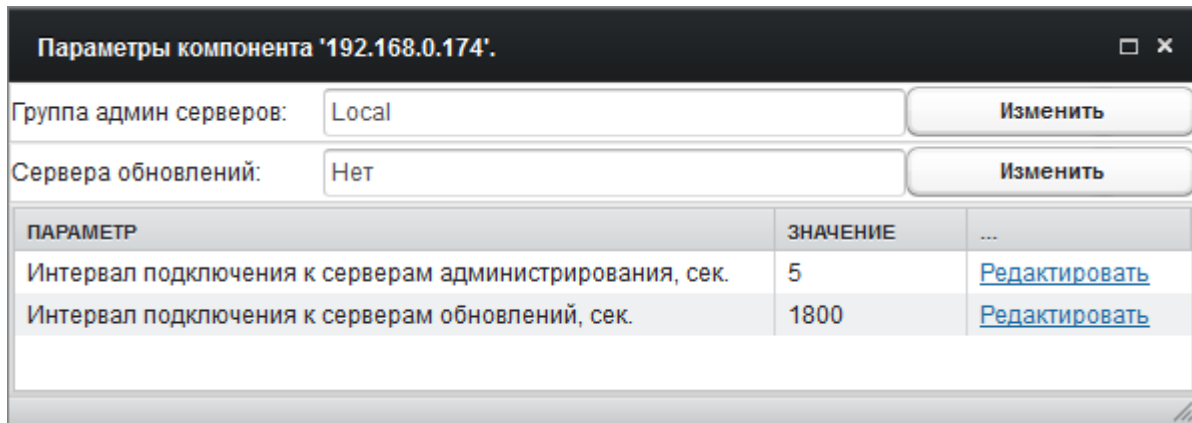


Рис. 21. Окно параметров выбранного компонента.

Определение значения интервала подключения к тому или иному серверу в секундах осуществляется выбором соответствующей ему ссылки «Редактировать» в графе «...».

Также в данном диалоговом окне можно изменить наименования серверов администрирования и обновления, нажав кнопку «Изменить», соответствующую административному серверу, либо серверу обновлений.

*Примечание.* Определение сервера обновлений при установке РС не выполняется. Поэтому следует назначить его вручную, нажав кнопку «Изменить» справа от поля «Сервера обновлений». После выбора целевого сервера обновлений указателем мыши или клавишами управления курсором клавиатуры в дочернем диалоговом окне следует нажать кнопку «Сохранить».

По завершению изменения настроек модулей следует выбрать раздел меню «Применить настройки» для их фиксации в БД и применения к компонентам.

После установки необходимо выполнить настройку РС на сбор данных о событиях, возникающих на контролируемом рабочем месте (см. п. 5.3 настоящего документа).

### 3.2.8. Установка сетевого сенсора

Установка сетевого сенсора выполняется только локально. Перед установкой необходимо получить ключ установки (см. п. 3.2.6.2 настоящего документа).

Сетевой сенсор может быть развёрнут для функционирования под управлением следующих ОС \*nix:

- Ubuntu-14.04-x86\_64 (3.13.0-63-generic, glibc 2.19);
- Debian-7-amd64 (kernel 3.2.0-4-amd64, glibc 2.13-38);
- CentOS-7-x86\_64 (kernel 3.10.0-123.el7.x86\_64, glibc 2.17).

Для установки сетевого сенсора на рабочем месте необходимо запустить файл ‘NetSensor2.sh’ с установочного компакт-диска ПМБИ.10145-01/КД 01-03 01 (самораспаковывающийся архив ‘Shar’, содержащий файлы и сценарий извлечения содержимого).

После распаковки следует выполнить следующую команду, обладая полномочиями пользователя ‘root’:

```
root@u64-netsensor-testing:~# ./NetSensor2-chroot-installer.run
```

Проверив целостность дистрибутива, установщик запросит значения нескольких параметров. В квадратных скобках указываются значения, принятые по умолчанию. Если указанные значения удовлетворяют целевым, то на запросы можно отвечать нажатием клавиши ‘Enter’, не указывая новых значений:

```
Verifying archive integrity... 100% All good.  
Uncompressing Primetech Ltd. NetSensor2 installer 100%  
-----  
Welcome to Primetech Ltd. NetSensor-2.0-x86 installer!  
Enter installation directory [/root]:
```

На запрос ‘Enter installation directory’ следует указать папку, в которую предполагается установить сетевой сенсор, и нажать клавишу ‘Enter’:

```
/root/SomeDirectory  
Enter AdminServer address [127.0.0.1]:
```

На запрос ‘Enter AdminServer address’ следует указать IP-адрес существующего и функционирующего сервера администрирования, который будет обслуживать развёртываемый сетевой сенсор, и нажать клавишу ‘Enter’:

```
192.168.0.145  
Enter AdminServer port [5556]:
```

На запрос ‘Enter AdminServer port’ следует указать номер сетевого порта сервера администрирования и нажать клавишу ‘Enter’:

```
5556  
Enter the NetSensor description [Default NetSensor]:
```

На запрос ‘Enter the NetSensor description’ следует указать произвольное наименование развёртываемого сетевого сенсора для его идентификации при последующей регистрации в САИБ и нажать клавишу ‘Enter’:

```
Testing NetSensor2-x86 installation  
Enter authentication key:
```

На запрос ‘Enter authentication key’ следует указать шестнадцатеричное значение ключа, скопированное из поля «Ключ» окна «Одобрение локальных установок», и нажать клавишу ‘Enter’:

```
E71204BFC94B1B6ABEE3F84A90C1891C23357B3AA292D0662A1EA10AEC976B9E  
Installation directory '/root/SomeDirectory' exists. Proceeding will  
wipe all this data. Proceed? (y/n):
```

Если указанная папка установки существует, то последует запрос подтверждения её очистки. В случае ответа ‘y’ существующее содержимое папки будет уничтожено, в случае ответа ‘n’ установка сетевого сенсора будет прервана. Если указанная папка отсутствует, она будет создана установщиком.

```
y  
installing...  
Installation: success.  
Use '/etc/init.d/netsensor {start|stop}' to control NetSensor2  
-----  
root@u64-netsensor-testing:~#
```

Выдача сообщения ‘Installation: success.’ сигнализирует об успешном завершении установки сетевого сенсора. В случае сбоя следует ожидать одно из следующих сообщений:

- ‘socket error[-1]’ – ошибка соединения (по какой-либо причине недоступен сервер администрирования);
- ‘authentication error[-2]’ – указан неверный ключ установки.

Для запуска сетевого сенсора в эксплуатацию следует выполнить команду:

```
root@u64-netsensor-testing:~# /etc/init.d/netsensor start
```

По завершению установки сетевой сенсор следует зарегистрировать в САИБ аналогично РС (см. п. 3.2.6.3 настоящего документа).

### 3.2.9. Подключение АГАТ

Перед подключением АГАТ необходимо получить ключ установки (см. п. 3.2.6.2 настоящего документа).

Интеграция АГАТ в САИБ выполняется через Web-интерфейс устройства АГАТ, который следует активировать в соответствии с руководством по эксплуатации АГАТ.

Затем нужно загрузить Web-интерфейс, для чего в строке адреса (URL) Web-обозревателя следует ввести строку

```
http://[IP-адрес или доменное имя АГАТ]:9000
```

и нажать клавишу ‘Enter’.

Последует запрос на авторизацию. Следует указать следующие реквизиты (возможность их изменения не предусмотрена):

- «*Пользователь*» – ‘admin’;
- «*Пароль*» – ‘J\*Ld-F@a1-dF13-80a\$’.

После авторизации в Web-обозреватель загрузится страница определения параметров подключения АГАТ к САИБ (Рис. 22).

**АГАТ: не подключен к серверу мониторинга и управления**

---

Для подключения к серверу мониторинга и управления необходимо ввести сетевые реквизиты данного сервера, а также ключ для установки

IP-адрес/имя сервера	Порт
<input type="text" value="192.168.10.10"/>	<input type="text" value="5556"/>

**Ключ установки**

Рис. 22. Окно параметров подключения АГАТ.

В правом верхнем углу интерфейса отображается обратный отсчёт времени, оставшегося до автоматического отключения Web-интерфейса (10 минут).

Следует определить параметры подключения к серверу администрирования, включающие:

- «*IP-адрес/имя сервера*» – IP-адрес или доменное имя серверного СВТ, на которое установлен Сервер;
- «*Порт*» – порт подключения к серверу администрирования (по умолчанию – ‘5556’);
- «*Ключ установки*» – шестнадцатеричное значение ключа, скопированное из поля «Ключ» окна «Одобрение локальных установок» (см. п. 3.2.6.2 настоящего документа).

После определения параметров следует нажать кнопку «Подключить».

В случае успешного подключения отобразится страница с принятыми параметрами подключения (Рис. 23).

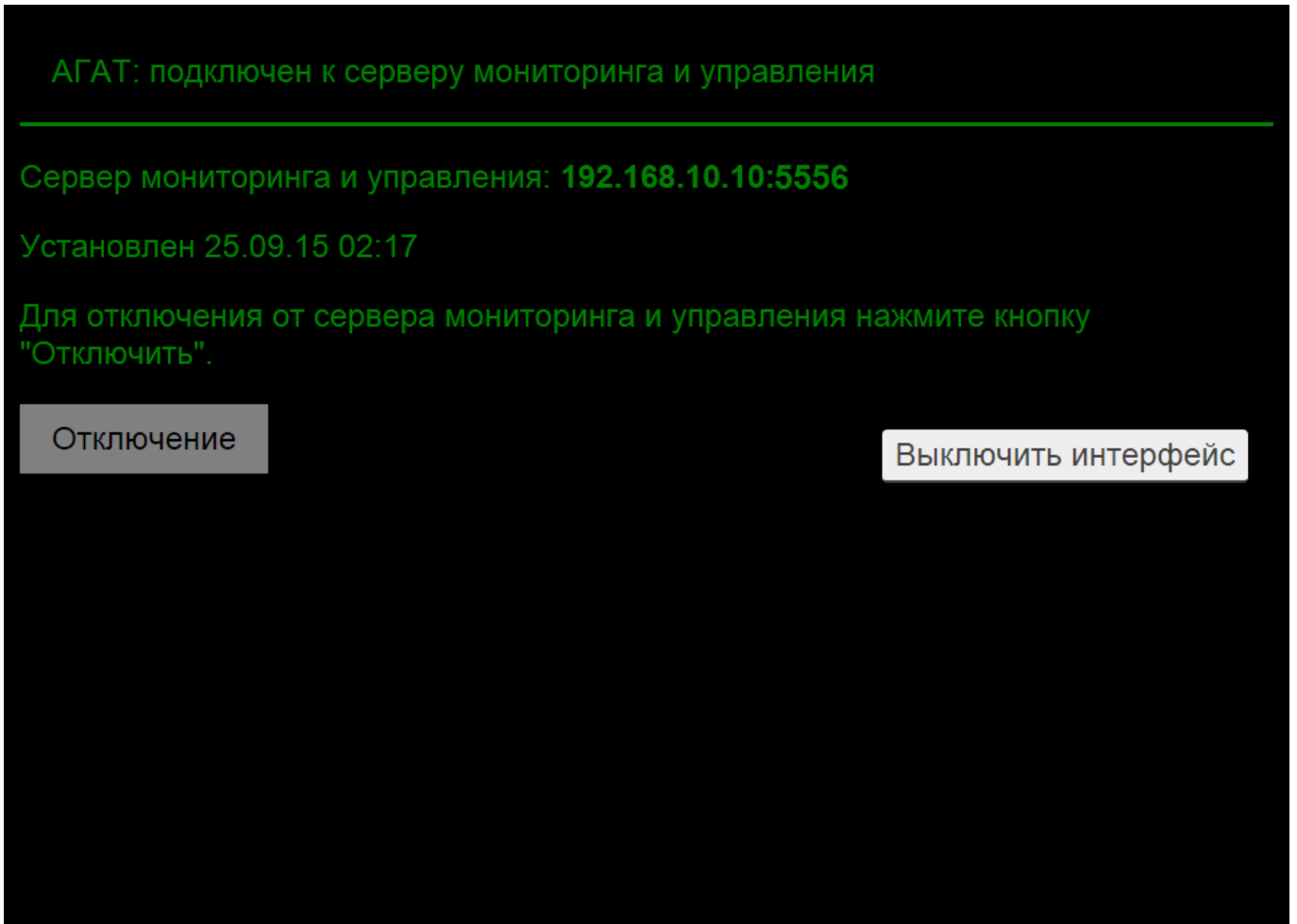


Рис. 23. Окно состояния подключения АГАТ.

По завершению подключения АГАТ следует зарегистрировать в САИБ аналогично РС (см. п. 3.9.5.3 настоящего документа).

Отключение АГАТ от САИБ осуществляется кнопкой «Отключение».

*Примечание.* Кнопка «Выключить интерфейс» производит удалённую деактивацию Web-интерфейса и соответствует аналогичной функции сенсорного экрана в настройках устройства АГАТ.



## 4. Удаление СПО

### 4.1. Удаление Сервера

Удаление Сервера производится запуском исполняемого модуля 'Uninstal.exe' из папки, в которую устанавливался Сервер: по умолчанию, – 'C:\Program Files\Primetech\OKOServer\' (см. п. 3.2.2 настоящего документа).

В окне удаления сервера администрирования необходимо указать папку, из которой будет происходить удаление Сервера и для подтверждения удаления программы нажать кнопку «Удалить».

### 4.2. Удаление РС

#### 4.2.1. Удалённая деактивация РС

Удаление сенсора (компонента) с контролируемого рабочего места и из САИБ осуществляется выбором раздела главного меню *Система* → *Удаление компонентов*.

Удалённо деактивируются и удаляются с контролируемых рабочих мест только РС. У сетевых сенсоров и АГАТ из САИБ удаляются только соответствующие компоненты. Программные модули сетевых сенсоров требуют ручного удаления. Программные модули АГАТ удалению не подлежат.

В дочернем окне (Рис. 24) компоненты САИБ представлены в табличной форме, содержащей следующие графы:

- «*Модуль*» – наименование модуля типа «Рабочая станция» или «Сервер», указанное для него в окне «Настройка модулей» в режиме «Параметры» (см. п. 5.2 настоящего документа);
- «*Тип компонента*» – содержит тип применяемого сенсора («Хостовой сенсор 'ОКО'», «Сетевой сенсор» или «АГАТ»);
- «*Имя компонента*» – IP-адрес или доменное имя контролируемого рабочего места, зафиксированное в БД при установке сенсора.

Восходящая (значок '▲') / нисходящая (значок '▼') сортировка модулей в таблице осуществляется щелчком левой кнопки мыши по нужной графе.

Кнопка «Обновить» актуализирует список компонентов.

В случае обширной топологии САИБ выбор целевого компонента можно ускорить с помощью полнотекстового поиска, для чего следует указать подстроку для поиска в текстовом поле над таблицей компонентов и нажать кнопку «Искать».

Для удаления нескольких или всех сенсоров независимо от типа одновременно следует выбрать целевые компоненты указателем мыши или клавишами управления курсором клавиатуры (с удержанием клавиши 'Ctrl' или 'Shift').

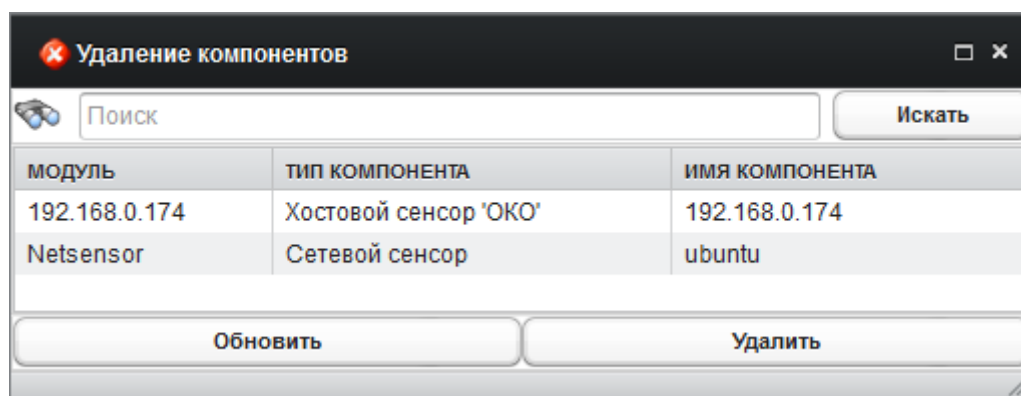


Рис. 24. Окно «Удаление компонентов».

По окончании выбора сенсоров следует нажать кнопку «Удалить» для их удалённой деактивации на контролируемых рабочих местах (последует запрос подтверждения принятого решения).

*Примечания:*

- 1. Удаление сенсоров приведёт к утрате возможности мониторинга и управления рабочими местами, на которых они были установлены.*
- 2. Деактивация компонента сохраняет соответствующий модуль топологии САИБ, который при необходимости удаляется вручную.*

#### 4.2.2. Локальная деактивация РС

В случае некорректной работы РС его удаление следует проводить вручную с контролируемого рабочего места, на котором установлен РС, предварительно удалённо деактивировав его. Затем следует:

- загрузить ОС с загрузочного диска;
- удалить файл ‘%SystemRoot%\system32\drivers\primbox.sys’;
- загрузить собственную ОС рабочего места в безопасном режиме;
- авторизоваться в ОС с полномочиями администратора;
- выполнить файл ‘%SystemRoot%\System32\INSA\uninstall.reg’ в программе управления системным реестром (‘RegEdit.exe’);
- выполнить файл ‘%SystemRoot%\System32\INSA\remove.exe’;
- перезапустить собственную ОС рабочего места;
- удалить папку ‘%SystemRoot%\System32\INSA’.

#### 4.2.3. Локальная деактивация сетевого сенсора

Для вывода из эксплуатации сетевого сенсора его следует предварительно удалённо деактивировать.

Затем следует авторизоваться с реквизитами пользователя ‘root’ в терминале СВТ, на котором установлен сетевой сенсор, и выполнить команду останова:

```
root@u64-netsensor-testing:~# /etc/init.d/netsensor stop
```

Для проверки факта завершения процессов сетевого сенсора следует выполнить команду:

```
root@u64-netsensor-testing:~# ps ax | grep NetSensor2
```

По завершению всех процессов сетевого сенсора в выводе данной команды останется только строка, содержащая ‘grep --color=auto NetSensor2’:

```
root@u64-netsensor-testing:~# ps ax | grep NetSensor2
grep --color=auto NetSensor2
root@u64-netsensor-testing:~#
```

Если в течение 10 секунд процессы всё же не завершились, можно выполнить команду аварийного останова:

```
root@u64-netsensor-testing:~# killall NetSensor2
```

После завершения всех процессов следует удалить папку установки сетевого сенсора:

```
root@u64-netsensor-testing:~# rm -rf /root/SomeDirectory
```

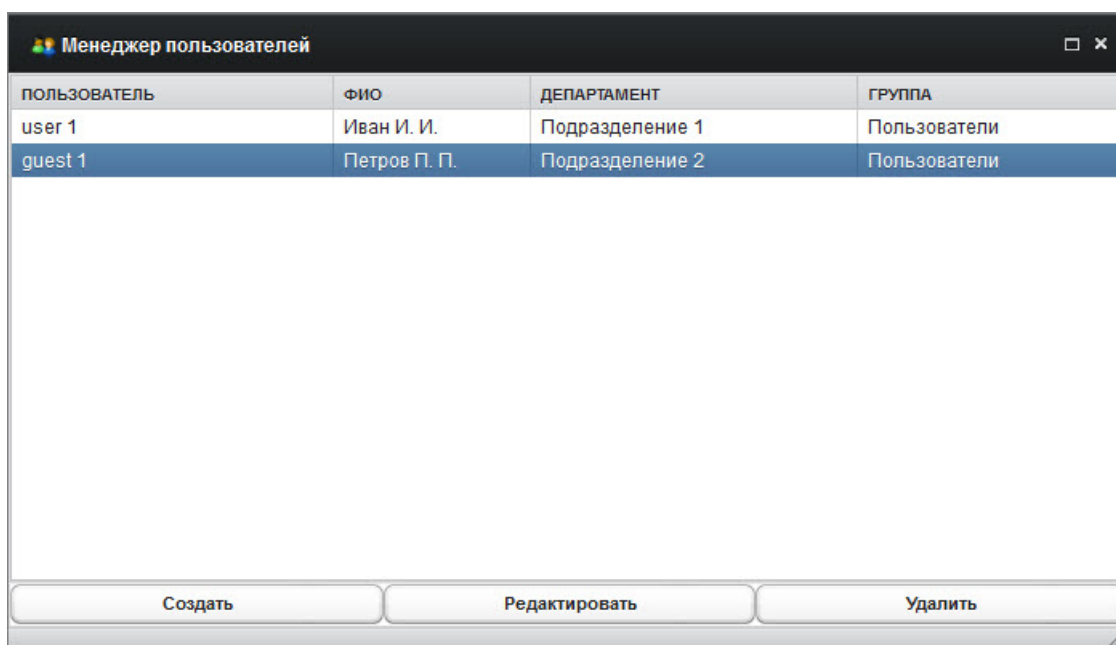
## 5. Управление компонентами САИБ

Управление компонентами САИБ реализовано с помощью графического интерфейса администратора, функционирующего в программной среде Web-обозревателя.

### 5.1. Управление пользователями графического интерфейса

Для добавления, изменения реквизитов и удаления пользователей САИБ следует выбрать раздел главного меню *Система* → *Менеджер пользователей*.

Менеджер пользователей состоит из таблицы, отображающей реквизиты пользователей (Рис. 25).



ПОЛЬЗОВАТЕЛЬ	ФИО	ДЕПАРТАМЕНТ	ГРУППА
user 1	Иван И. И.	Подразделение 1	Пользователи
guest 1	Петров П. П.	Подразделение 2	Пользователи

Создать      Редактировать      Удалить

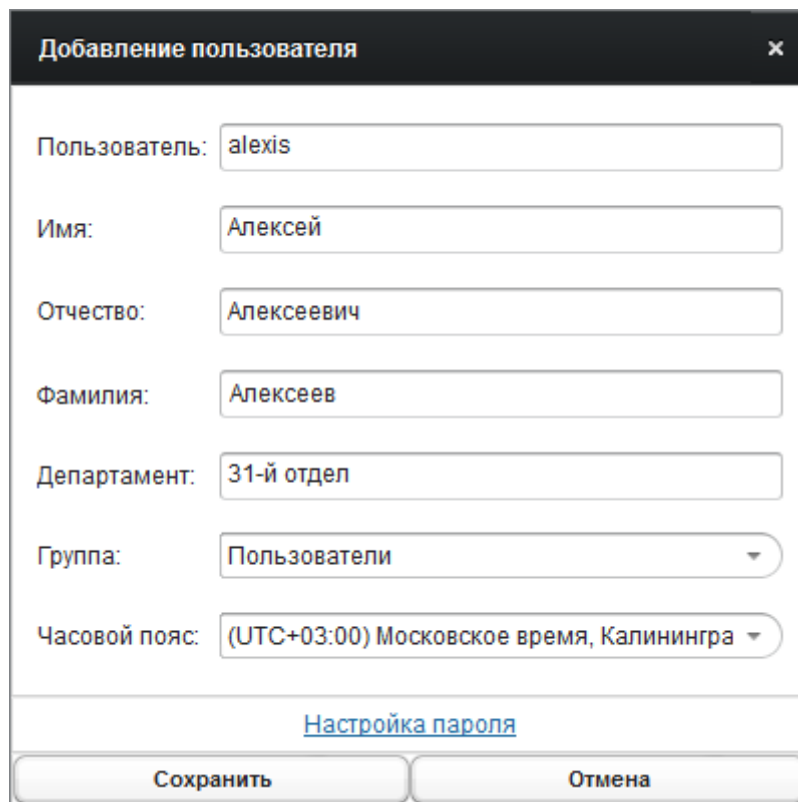
Рис. 25. Менеджер пользователей.

Восходящая (значок ‘▲’) / нисходящая (значок ‘▼’) сортировка учётных записей таблицы осуществляется щелчком левой кнопки мыши по нужной графе.

Для изменения реквизитов пользователя следует дважды щёлкнуть левой кнопкой мыши по записи искомого пользователя либо выбрать нужного пользователя однократным щелчком левой кнопки мыши и нажать кнопку «Редактировать».

Для добавления нового пользователя следует нажать кнопку «Создать».

Для удаления пользователя щелчком левой кнопкой мыши следует выбрать запись ненужного пользователя и нажать клавишу 'Delete' либо кнопку «Удалить» (последует запрос подтверждения принятого решения).



Добавление пользователя

Пользователь: alexis

Имя: Алексей

Отчество: Алексеевич

Фамилия: Алексеев

Департамент: 31-й отдел

Группа: Пользователи

Часовой пояс: (UTC+03:00) Московское время, Калинингра

[Настройка пароля](#)

Сохранить Отмена

Рис. 26. Диалог добавления/редактирования пользователя.

В САИБ предусмотрены следующие типы пользователей, объединяемые в одноимённые группы:

- «Администраторы» – члены группы наделены исключительными полномочиями (доступны все разделы главного меню графического интерфейса);
- «Пользователи» – члены группы выполняют функции исследователей инцидентов и аналитиков (см. п. 5.7.8 настоящего документа) и лишены административных полномочий (доступны разделы главного меню *Инструменты|Портал*, *Инструменты|Инциденты*, *Инструменты|Мнемосхема*, *Инструменты|Отчёты*, *Поиск*);
- «Операторы» – члены группы выполняют функции пассивного мониторинга САИБ и лишены административных полномочий

(доступны разделы главного меню *Инструменты|Портал, Инструменты|Инциденты, Инструменты|Мнемосхема, Поиск* без возможности внесения изменений).

Также члены группы «Операторы» лишены возможности работы с инцидентами, а могут лишь выполнять функции мониторинга состояния САИБ. Членам группы «Пользователи» администратор может поручать отработку зарегистрированных инцидентов (см. п. 5.7.8 настоящего документа).

Выбор операций «Добавление»/«Редактирование» откроет диалоговое окно с перечнем атрибутов, доступных для определения (Рис. 26):

- «*Пользователь*» – в обязательном к заполнению поле следует указать символьный идентификатор<sup>2)</sup>, которым пользователь будет представляться в САИБ;
- «*Имя*», «*Фамилия*» и «*Отчество*» – поля позволяют полностью персонифицировать пользователя в САИБ (необязательны к заполнению);
- «*Департамент*» – поле позволяет указать организационную принадлежность пользователя (необязательно к заполнению);
- «*Группа*» – список позволяет ввести пользователя в определённую учётную группу;
- «*Часовой пояс*» – список позволяет определить часовой пояс местонахождения пользователя (для удобства работы в САИБ с географически распределённой топологией).

*Примечание.* Отображение времени в графическом интерфейсе администратора ведётся с учётом значения параметра «*Часовой пояс*».

Определив атрибуты пользователя, следует выбрать ссылку «*Настройка пароля*». В дочернем диалоговом окне потребуется указать пароль пользователя, его подтверждение (при смене пароля пользователя также

---

<sup>2)</sup> Кодировка не имеет первостепенного значения, но латиница предпочтительнее.

потребуется указать текущий пароль) и нажать кнопку «Сохранить». Ввод значений паролей с клавиатуры скрывается.

*Примечание.* Для обеспечения безопасной эксплуатации САИБ необходимо сменить заводской пароль пользователя 'admin'.

Определив пароль пользователя следует нажать кнопку «Сохранить» для фиксации произведённых изменений в БД.

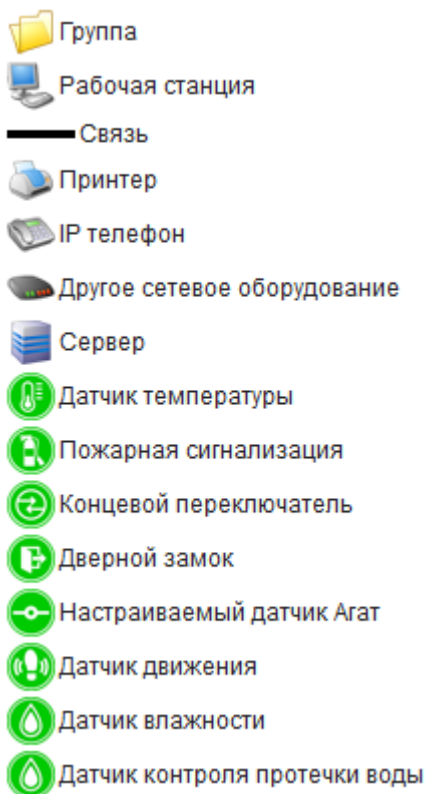
Диалоговые окна операций «Добавление»/«Редактирование» пользователей идентичны.

## **5.2. Ведение топологии эксплуатирующей организации**

После установки и начальной настройки Сервера следует уделить должное внимание полноте отражения в САИБ топологии подразделений эксплуатирующей организации. Во многом от этого зависит эффективность применения САИБ и адекватность оценки возникающих инцидентов. Для наглядности в топологию следует вносить неподконтрольные рабочие места наравне с контролируемыми.

Топология может быть одновременно построена как по организационному, так и по территориальному принципу. Поэтому перед установкой РС на контролируемые рабочие места следует разработать структуру групп топологии, в которые затем будут помещаться контролируемые рабочие места. Объектами топологии САИБ являются следующие модули:





Активную роль в САИБ выполняют любые модули, оснащённые сенсорами, либо контролируемые сценариями опроса сетевого сенсора или датчиками АГАТ. Модули остальных типов служат лишь целям полноты отражения в САИБ топологии эксплуатирующей организации.

**Модуль «Группа»** предназначен для визуального объединения модулей всех других видов по какому-либо выбранному признаку (город, организация, подразделение, комната и т.п.). Группы могут иметь подгруппы неограниченного уровня вложенности, что позволяет отобразить в топологии древовидную иерархическую структуру (например, организационную) (Рис. 27).

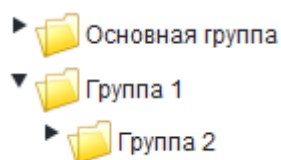


Рис. 27. Пример вложенных групп.

Значок «▶» возле изображения типа модуля показывает, что модуль имеет вложенные объекты (дочерние группы, правила и т.п.).

Развёртка/свёртка вложений осуществляется щелчком левой кнопки мыши по значку «►».

Очередность модулей, объединённых группой, может быть изменена по желанию. Модуль имеет дополнительные (необязательные) строковые параметры: «Ответственный», «Телефон» и «Электронная почта».

**Модуль «Рабочая станция» и «Сервер»** являются основными модулями САИБ, поскольку обладают возможностью установки PC, сетевого сенсора или АГАТ. Данный модуль может представлять в САИБ как сервер, так и рабочую станцию пользователя; быть контролируемым и неконтролируемым объектом. Модуль имеет дополнительные (необязательные) строковые параметры: «Адрес IPv4», «Адрес IPv6», «Имя хоста», «Ответственный», «Телефон» и «Электронная почта».

**Модуль «Принтер»** позволяет отразить в САИБ принтер или иное устройство вывода данных на твёрдых носителях. Модуль имеет дополнительные (необязательные) строковые параметры: «Адрес IPv4», «Адрес IPv6», «Ответственный», «Телефон» и «Электронная почта».

**Модули «IP телефон» и «Другое сетевое оборудование»** позволяют отразить в САИБ IP-телефон, модем и прочее периферийное оборудование, предназначенное для передачи информации. Модули имеют дополнительные (необязательные) строковые параметры: «Адрес IPv4», «Адрес IPv6», «Имя хоста», «Ответственный», «Телефон» и «Электронная почта».

**Модули «Датчик температуры», «Пожарная сигнализация», «Концевой переключатель», «Дверной замок», «Настраиваемый датчик Агат» и «Датчик движения»** (зелёного цвета) предназначены для применения совместно с АГАТ (см. п. 5.6) и отражения в топологии САИБ контролируемых датчиков соответствующих типов. Модули имеют дополнительные (необязательные) строковые параметры: «Ответственный», «Телефон» и «Электронная почта».

**Модуль «Связь»** позволяет связать между собой два других модуля для визуализации топологии на мнемосхеме (см. п. 5.7.10 настоящего документа).

Модуль имеет дополнительные (необязательные) параметры: «Источник» и «Получатель» (объектные), «Тип связи», «Ответственный», «Телефон» и «Электронная почта» (строковые).

Параметры «Источник» и «Получатель» определяют модули, объединяемые связью. Параметр «Тип связи» позволяет определить нужный тип из списка: «Связь» (по умолчанию), «Модемное соединение», «Витая пара», «Оптическое соединение», «Спутниковое соединение». Выбранное значение определяет визуальное представление связи на «Мнемосхеме»:

- Связь
- ■ Модемное соединение
- • • • Витая пара
- ※ ○ ※ ○ Оптическое соединение
- ※ ※ Спутниковое соединение

Для работы с топологией САИБ следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*.

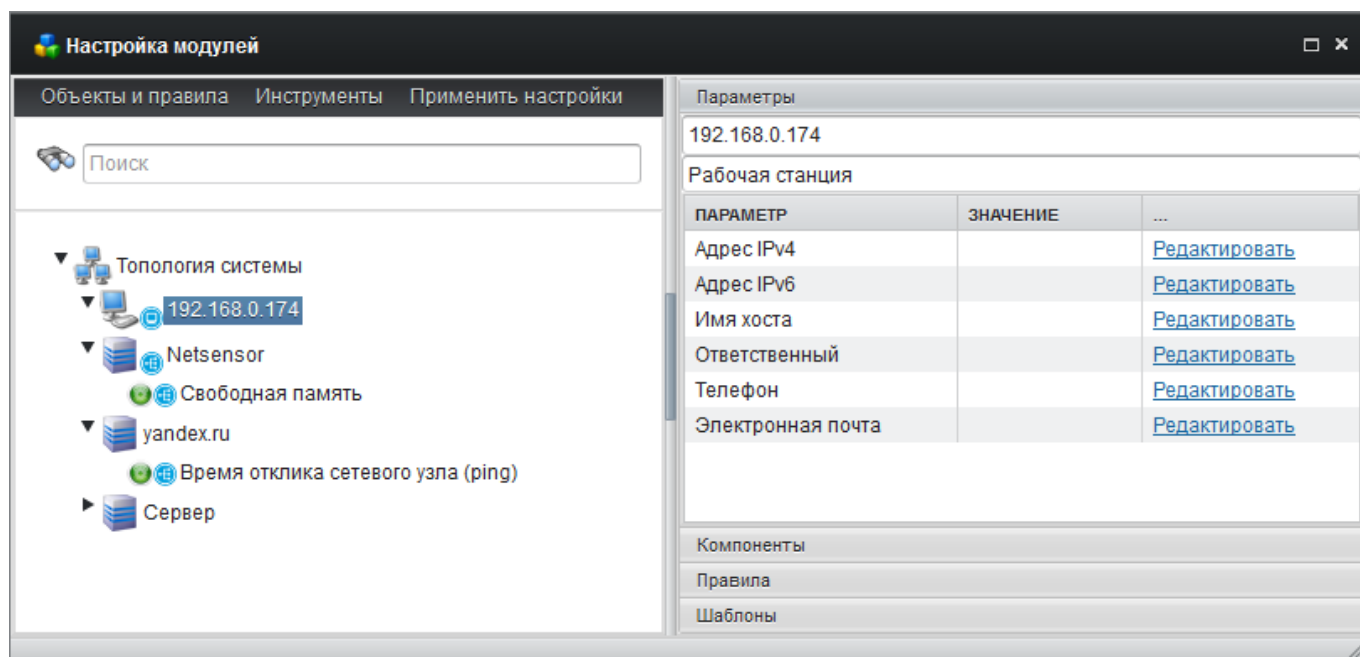


Рис. 28. Окно «Настройка модулей» в режиме «Параметры».

Окно настройки модулей состоит из навигатора по иерархическому древу топологии (слева) и контекстного окна (справа), отражающего свойства (Рис. 28). Переключение между их наборами (режимами) выполняется выбором вкладки нужных свойств. В режиме работы с топологией требуется

вкладка свойств «Параметры» (открывается по умолчанию при переходе в раздел).

Совместные размеры окон по горизонтали можно изменять, ухватив и потянув за вертикальный разделитель.

Для быстрого перемещения к нужному модулю предусмотрена строка полнотекстового поиска (вверху навигатора). Для выполнения поиска следует ввести запрос и нажать клавишу 'Enter'. При положительном результате маркёр в окне навигатора переместится к первому обнаруженному модулю, наименование которого отвечает критериям запроса.

Для добавления нового объекта (модуля) в топологию следует выбрать раздел меню *Объекты и правила* → *Добавить объект* либо выбрать одноимённый пункт контекстного меню и выбрать тип добавляемого модуля из предложенного списка.

Для изменения параметров объектов топологии в древе следует выбрать нужный указателем мыши. Набор параметров зависит от типа выбранного модуля, но непременно включает символьное наименование и текстовое описание (в верхней части окна свойств). Определение значения параметра осуществляется выбором соответствующей ему ссылки «Редактировать» в графе «...».

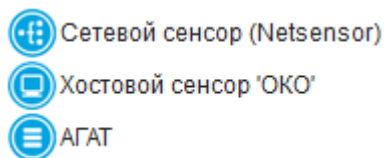
Для определения модулей, объединяемых связью, каждый модуль типа «Связь» предусматривает объектные параметры «Источник» и «Получатель», при изменении которых будет предложено выбрать соответствующие модули из древа.

Добавление вложенной группы выполняется аналогично модулю другого типа, только родительская группа должна быть выбрана в древе топологии.

*Примечание.* Для визуальной разгрузки древа топологии все связи, определённые между модулями, можно скрыть, объединив их, например, в группу «Связи».

Все типы модулей можно буксировать мышью в любую группу и менять очерёдность их расположения в древе.

Модули с установленным сенсором помечаются в топологии соответствующими признаками:



Контекстное меню, вызываемое правой кнопкой мыши при выборе определённого объекта, позволяет ускорить работу с древом топологии.

Для удаления модуля следует выбрать его в древе топологии и выбрать раздел меню *Объекты и правила* → *Удалить* либо одноимённый пункт контекстного меню либо нажать клавишу 'Delete' (последует запрос подтверждения принятого решения).

*Примечание.* Удаление модуля с установленным РС или сетевым сенсором приведёт к утрате контроля за рабочим местом, которое он представлял в топологии.

### **5.3. Настройка правил мониторинга**

После активации РС на контролируемом рабочем месте в соответствии с действующей политикой информационной безопасности АИС требуется установить правила сбора и анализа событий, возникающих на данном рабочем месте.

Правила служат основным инструментом контроля. Их набор формируется на основании экспертной оценки состояния АИС организации и действующей политики информационной безопасности. От корректности настройки правил фильтрации РС зависит адекватная работа САИБ и вероятность обнаружения различных несанкционированных действий и атак. Нарушение правила при определённых условиях порождает инцидент в САИБ (см. п. 5.8.2 настоящего документа).

Для настройки правил сбора событий с контролируемого рабочего места следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*, отыскать и выбрать в древе топологии нужный модуль, оснащённый РС. После этого нужно переключить окно свойств в режим отображения «Правила» (Рис. 29).

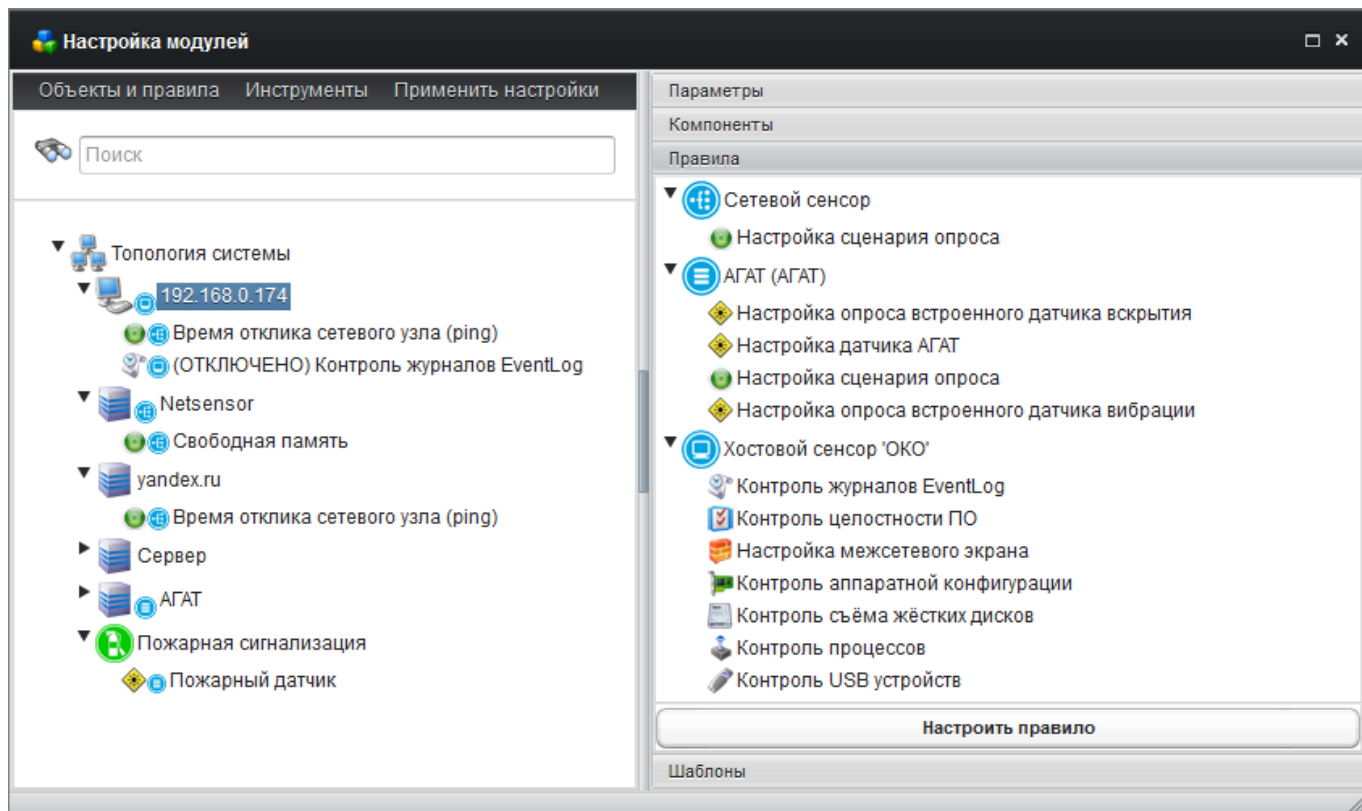


Рис. 29. Окно «Настройка модулей» в режиме «Правила».

Для сбора данных о событиях контролируемого рабочего места предусмотрены следующие типы правил (см. также раздел «Хостовой сенсор ‘ОКО’» в окне свойств на Рис. 29):

- контроль журналов системных событий ('EventLog');
- контроль целостности ПО;
- контроль входящих/исходящих сетевых пакетов с помощью межсетевого экрана;
- контроль аппаратной конфигурации;
- контроль съёма жестких дисков;
- контроль процессов;

– контроль устройств USB.

Существует возможность определения лишь одного правила каждого типа для каждого РС, кроме правила типа «Контроль процессов», которых может быть несколько.

Правила типа «Контроль процессов» являются основными средствами мониторинга активности пользователей контролируемых рабочих мест.

Для применения определённого правила контроля к РС следует выбрать его тип и нажать кнопку «Настроить правило», либо дважды щёлкнуть левой кнопкой мыши по выбранному типу. Применить правило нужного типа к выбранному в текущий момент модулю можно также методом захвата и перетаскивания мышью.

*Примечание.* Для снижения трудоёмкости применения одних и тех же правил к множеству контролируемых рабочих мест САИБ следует воспользоваться возможностью подготовки и применения шаблонов правил (см. п. 5.4 настоящего документа).

Правила, определённые для каждого контролируемого рабочего места, также отображаются в древе топологии в виде вложений в модуль (Рис. 30).

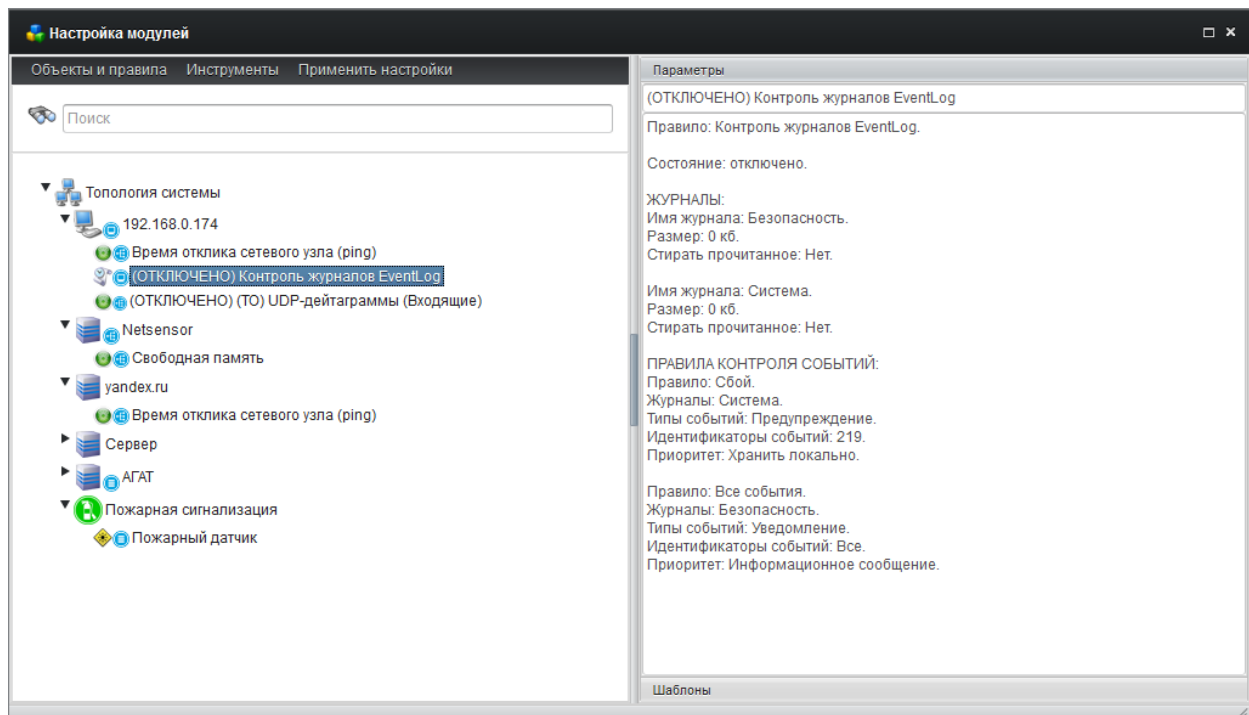


Рис. 30. Отображение в топологии правил, определённых для рабочего места.

При выборе определённого правила в окне свойств отображается его описание и установленные параметры, что позволяет текстуально оценить корректность настройки правила.

Внесение изменений в ранее определённые правила осуществляется по двойному щелчку левой кнопки мыши по нужному правилу либо выбором раздела меню *Объекты и правила* → *Редактировать правило*.

**Важно!** *Определённое правило сбора событий используется РС лишь в том случае, если в его параметрах установлен флаг «Правило активно» (для любого определяемого правила флаг устанавливается по умолчанию). Для временной приостановки применения правила РС следует снять данный флаг (в этом случае у имён приостановленных правил появляется префикс «(ОТКЛЮЧЕНО)»).*

**Важно!** *По завершению внесения изменений в настройки модулей следует выбрать раздел меню «Применить настройки» для их фиксации в БД. Применение настроек происходит массово для всех нижележащих ветвей дерева топологии при их наличии, начиная с той ветви, на которой помещается маркёр выделения.*

Применение изменений к компонентам САИБ (сенсорам) определяется интервалом подключения конкретного сенсора к серверу администрирования. Чем меньше интервал, тем быстрее сенсор получит изменения, внесённые администратором через графический интерфейс (см. п. 3.2.7 настоящего документа).

Для удаления ранее определённого правила следует выбрать его с помощью указателя мыши и нажать клавишу 'Delete' либо выбрать раздел меню *Объекты и правила* → *Удалить* либо выбрать одноимённый пункт контекстного меню.



### 5.3.1. Настройка правила контроля журнала системных событий

ОС семейства Microsoft Windows содержат журнал системных событий 'EventLog', в который добавляет записи как ОС, так и исполняемые ею приложения. По умолчанию журнал имеет три раздела: 'System' («Система» для общесистемных сообщений), 'Application' («Приложения» для сообщений от выполняемых приложений) и 'Security' («Безопасность» для сообщений подсистемы безопасности).

Все сообщения журнала по типам разделяются на следующие:

- 'Unknown' («Неизвестный»);
- 'Error' («Ошибка»);
- 'Warning' («Предупреждение»);
- 'Information' («Информация»);
- 'Success Audit' («Аудит успехов»);
- 'Fault Audit' («Аудит отказов»).

РС обладает возможностью извлечения записей из журнала системных событий. Если приложения на контролируемом рабочем месте используют журнал системных событий для протоколирования своих действий, эти сообщения будут прочитаны РС и переданы на Сервер для последующего анализа.

РС может отбирать события как по их кодам, так и по наименованию разделов журнала системных событий (обеспечивается извлечение всех имеющихся записей о событиях из выбранного раздела журнала).

Диалоговое окно определения правила для контроля журнала системных событий содержит две вкладки: «Управление журналами» и «Контроль событий» (Рис. 31).

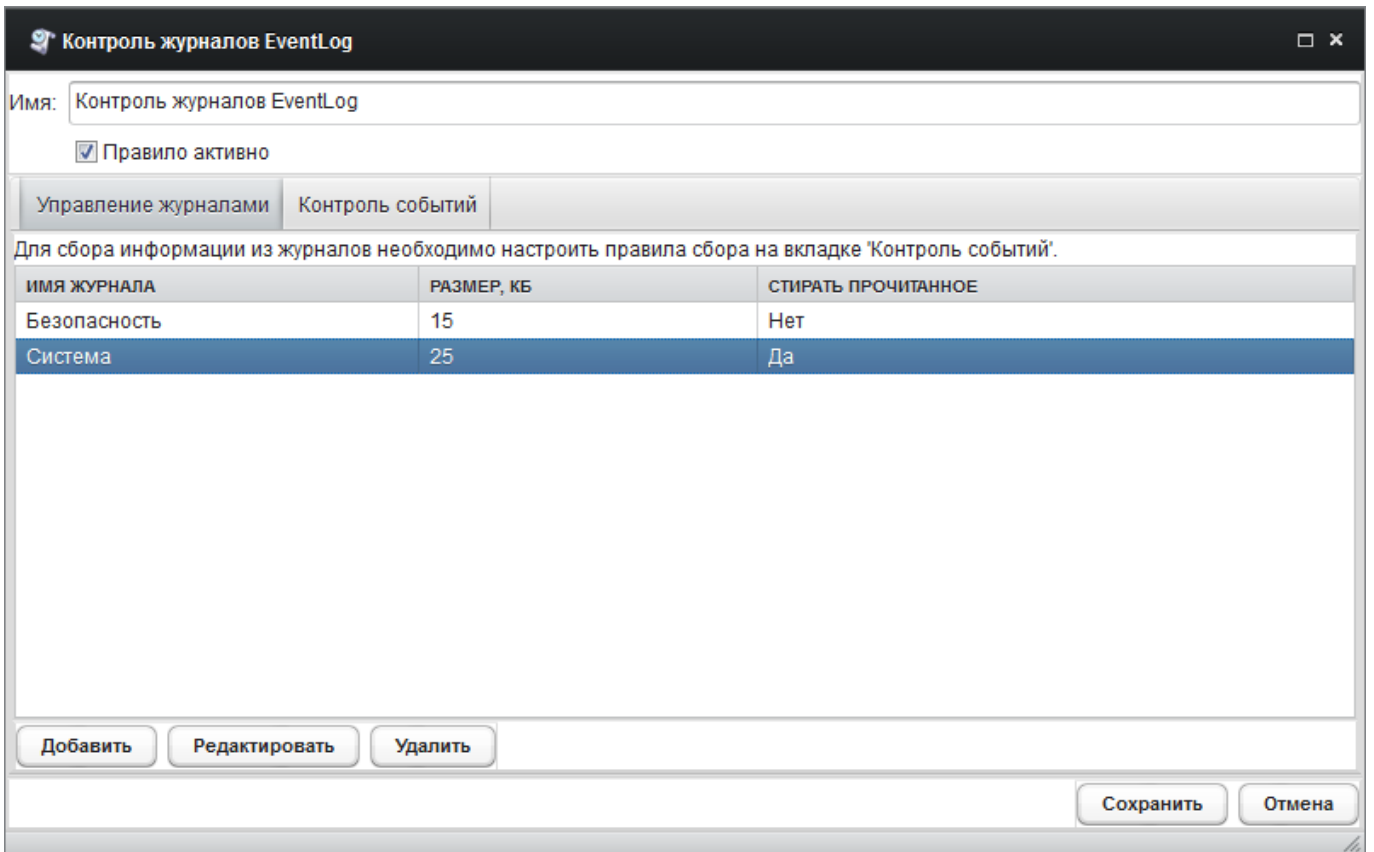


Рис. 31. Вкладка «Управление журналами».

**Вкладка «Управление журналами»** (рис. 12) позволяет определить раздел журнала, из которого требуется извлекать записи для анализа. Для добавления раздела журнала следует нажать кнопку «Добавить». Изменение ранее определённого раздела журнала осуществляется двойным щелчком левой кнопки мыши по записи изменяемого раздела либо кнопкой «Редактировать».

В дочернем диалоговом окне нужно выбрать имя журнала из списка (при выборе значения «Ввести вручную» появляется возможность определения непредусмотренного раздела, например, «Перенаправленные события»).

В поле «Размер» нужно определить объём анализируемого блока журнала в килобайтах. Ненулевое значение активирует анализ ретроспективы зарегистрированных событий необходимой длины, нулевое – только тех, что последуют после определения правила.

При установке флага «Стирать прочитанное» РС удалит обработанные записи из журнала после отбора и передачи на Сервер.

Фиксация определённых значений в БД осуществляется кнопкой «Сохранить».

**Вкладка «Контроль событий»** позволяет определить события для извлечения из журнала по их кодам (Рис. 32). Если для раздела журнала, определённого во вкладке «Управление журналами», не определить дополнительных условий, РС будет передавать на Сервер все события, записи о которых откладываются в выбранном разделе журнала.

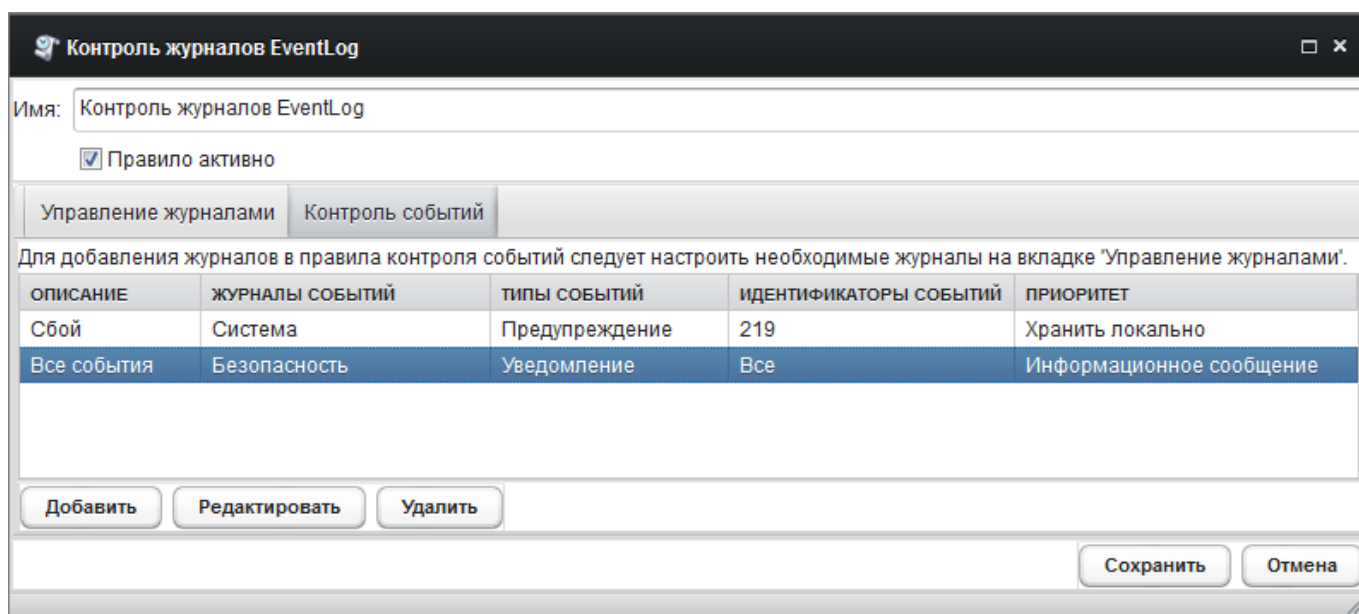


Рис. 32. Вкладка «Контроль событий».

Для установки дополнительного условия отбора события раздела журнала, определённого во вкладке «Управление журналами», следует нажать кнопку «Добавить». Изменение ранее определённого условия осуществляется двойным щелчком левой кнопки мыши по записи изменяемого условия либо кнопкой «Редактировать».

В дочернем диалоговом окне (Рис. 33) следует ввести описание (обязательное поле) и определить приоритет фиксации отобранного события в журнале инцидентов:

- «Информационное сообщение» (по умолчанию) – при нарушении правила данные о событии фиксируются Сервером с целью информирования администратора САИБ;

- «Важное сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Критическое сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Хранить локально» – при нарушении правила данные о событии не передаются на Сервер и хранятся локально на контролируемом рабочем месте до запроса данных по требованию инструментом «Получить локальные данные» (см. п. 5.7.6 настоящего документа).

ЖУРНАЛЫ EVENTLOG	ТИПЫ СОБЫТИЙ	ID СОБЫТИЙ	ИСКЛЮЧИТЬ
Система	Предупреждение	219	Нет
Безопасность	Уведомление	315	Нет

Рис. 33. Окно определения событий журнала по кодам.

Окно содержит перечни дополнительных условий по разделам журнала, типам и кодам событий. Для добавления условия в нужный перечень следует нажать кнопку «Добавить». Изменение условия выполняется двойным щелчком левой кнопки мыши или кнопкой «Изменить».

Для каждого из определённых условий доступен флаг «Исключить», установка которого позволяет исключить из обработки РС записи о событии, удовлетворяющей данному условию (операция «отрицание»).

Удаление определённых разделов журнала, условий и их наборов выполняется кнопкой «Удалить». Удаление раздела журнала приведёт к удалению и всех условий, в которых он применяется.

Для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

Реакция САИБ и фиксация в БД фактов нарушения правила выполняются в соответствии с приоритетом фиксации отобранного события в журнале инцидентов во вкладке «Контроль событий».

### **5.3.2 Настройка правила контроля целостности ПО**

Правило обеспечивает контроль отсутствия подмены или модификации исполняемого модуля приложения путём сверки контрольной суммы, определённой в качестве эталонной, с текущим значением при попытке запуска исполняемого модуля.

В дочернем диалоговом окне (Рис. 34) следует определить приоритет фиксации отобранного события в журнале инцидентов в поле «Журнал»:

- «Информационное сообщение» (по умолчанию) – при нарушении правила данные о событии фиксируются Сервером с целью информирования администратора САИБ;
- «Важное сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Критическое сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Хранить локально» – при нарушении правила данные о событии не передаются на Сервер и хранятся локально на контролируемом рабочем месте до запроса данных по требованию инструментом «Получить локальные данные» (см. п. 5.7.6 настоящего документа).

Затем с помощью календаря «Время запуска» следует определить дату и время запуска (по умолчанию установлены текущие время и дата).

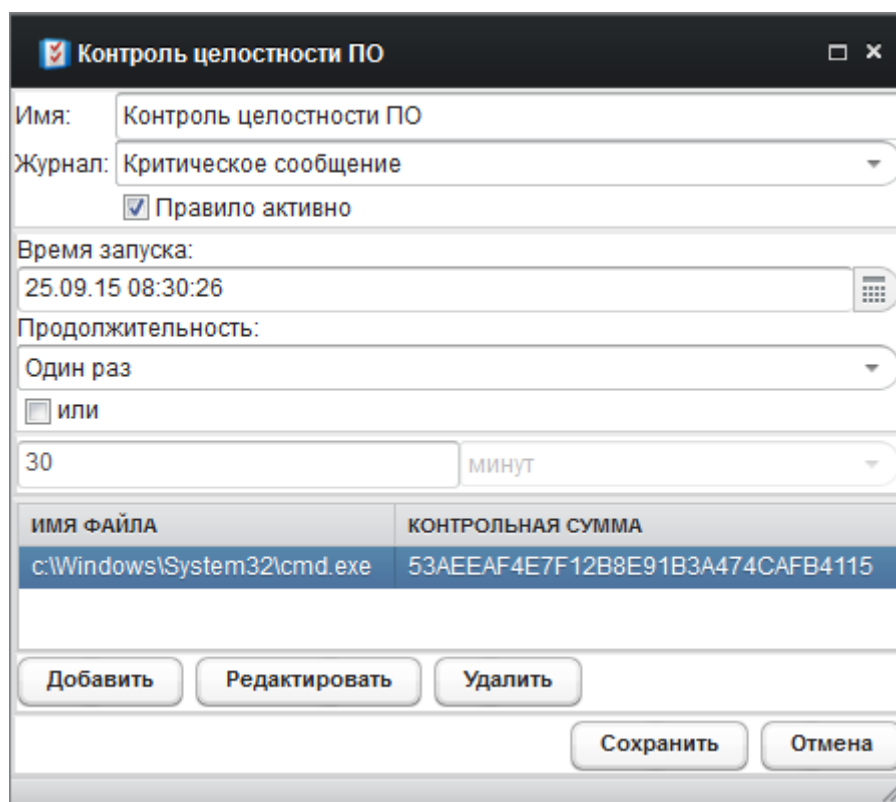


Рис. 34. Окно настройки правила контроля целостности ПО.

Группа «Продолжительность» позволяет определить периодичность применения правила (проверки соответствия контрольной суммы эталонной) значением из списка:

- «Один раз» (по умолчанию);
- «Каждые 15 минут»;
- «Каждые полчаса»;
- «Ежесечно»;
- «Ежедневно»;
- «Еженедельно».

Установкой флага «или» и заполнением дополнительного поля можно уточнить периодичность до нужного количества минут, часов или дней.

Определение списка подконтрольных файлов осуществляется кнопкой «Добавить». В дочернем диалоговом окне (Рис. 35) в поле «Имя файла» следует указать абсолютный путь (относительно контролируемого рабочего

места) к исполняемому файлу приложения и его контрольную сумму в поле «Контрольная сумма».

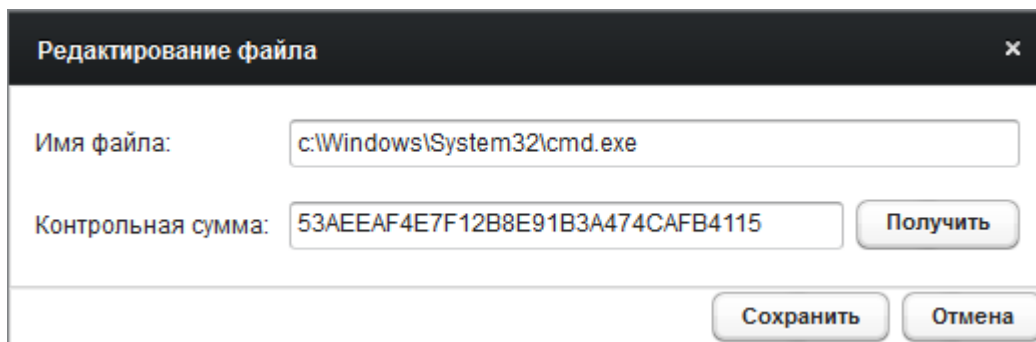


Рис. 35. Окно определения исполняемого модуля и контрольной суммы.

Кнопка «Получить» позволяет вычислить и определить контрольную сумму непосредственно в окне (при указании корректного пути к подконтрольному файлу).

*Примечание.* Исходные данные для определения контрольной суммы можно получить во вкладке «Процессы» инструмента «Менеджер задач» (см. п. 5.7.4 настоящего документа). Для определения параметров приложения, отсутствующего в списке процессов, его можно запустить в скрытом режиме.

Сохранение параметров подконтрольного файла выполняется кнопкой «Сохранить». Список может содержать неограниченное количество подконтрольных файлов.

Для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

Реакция САИБ и фиксация в БД фактов нарушения правила выполняются в соответствии с приоритетом фиксации отобранного события в журнале инцидентов.

### 5.3.3 Настройка правила межсетевого экрана

Межсетевой экран в САИБ выполняет анализ и отсев проходящих через него сетевых пакетов в соответствии с определёнными условиями с целью защиты контролируемого рабочего места от несанкционированного доступа

по сети. При этом набор определённых правил применяется к сетевому трафику последовательно.

Для определения правила работы межсетевого экрана в диалоговом окне его настройки (Рис. 36) следует нажать кнопку «Создать». Изменение ранее определённого правила осуществляется двойным щелчком левой кнопки мыши по записи изменяемого правила либо кнопкой «Редактировать».

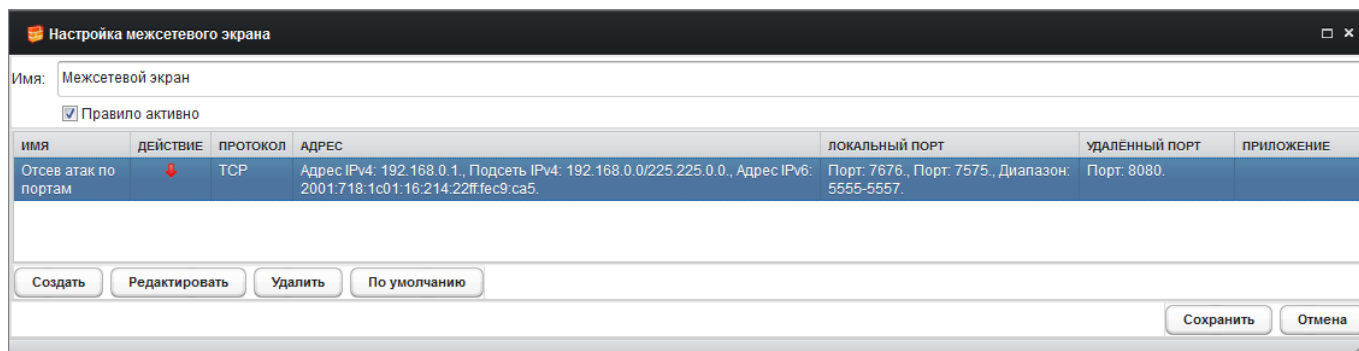


Рис. 36. Окно настройки правил работы межсетевого экрана.

В дочернем диалоговом окне (Рис. 37) следует указать имя создаваемого правила (обязательное поле) и выбрать «Направление» применения правила из списка по отношению к контролируемому рабочему месту:

- «Любое» (по умолчанию) – правило применяется как к входящему, так и к исходящему сетевому трафику;
- «Входящий» – правило применяется только ко входящему трафику;
- «Исходящий» – правило применяется только к исходящему трафику.



**Настройка межсетевого экрана** [X]

**Общая информация об этом правиле**

Имя:

Направление:

Действие:

Протокол:

**Локальный компьютер**

порт	Добавить
Порт: 7676.	Удалить
Порт: 7575.	
Диапазон: 5555-5557.	

Приложение:

**Удалённый компьютер**

удалённый адрес	Добавить
Адрес IPv4: 192.168.0.1.	Удалить
Подсеть IPv4: 192.168.0.0/225.225.0.0.	
Адрес IPv6: 2001:718:1c01:16:214:22ff:fec9:ca5.	

удалённый порт	Добавить
Порт: 8080.	Удалить

Рис. 37. Окно свойств правила работы межсетевого экрана.

Список «Действие» определяет реакцию РС на прохождение сетевого пакета, удовлетворяющего условиям правила: значение «Разрешить» предписывает ему пропустить сетевой пакет в зависимости от направления, «Блокировать» – отсеять.

Список «Протокол» определяет вид сетевого протокола, пакеты которого предполагается анализировать создаваемым правилом ('TCP', 'UDP', 'ICMP', 'IGMP', 'ICMPv6', 'RawIP').

Группа «Локальный компьютер» позволяет определить сетевые порты контролируемого рабочего места, сетевой трафик которых будет анализироваться РС. В список можно добавлять номера одиночных портов и

их диапазоны (для чего следует использовать символ '-', например, '1234-4321'). Для удаления ранее определённого значения следует выбрать нужную строку в списке и нажать кнопку «Удалить» (последует запрос подтверждения принятого решения).

В необязательном поле «Приложение» определяется абсолютный путь (относительно контролируемого рабочего места) к исполняемому файлу приложения, сетевой трафик которого подвергнется анализу РС. Если оставить поле пустым, правило будет применяться независимо от приложения – источника (адресата) сетевого трафика.

Группа «Удалённый компьютер» позволяет определить IP-адреса и сетевые порты источников/адресатов трафика контролируемого рабочего места. Для этого следует добавить нужные IP-адреса в список «Удалённый адрес».

Для определения диапазона IP-адресов следует использовать символ '-' между начальным и конечным адресами (например, '192.168.0.1-191.168.0.5'). Для определения подсети следует использовать символ '/' между адресом и маской (например, '192.168.0.0/225.225.0.0').

Может быть определён IPv6-адрес (например, '2001:718:1c01:16:214:22ff:fec9:ca5'). Для определения подсети следует использовать символ '/' между адресом и префиксом сети (например, '2002:c0a8:6301:1::1/64').

Для удаления ранее определённого значения следует выбрать нужную строку в списке и нажать кнопку «Удалить» (последует запрос подтверждения принятого решения).

Список «Удалённый порт» заполняется аналогично списку «Порт» группы «Локальный компьютер», только относительно удалённых источников/адресатов сетевого трафика.

Для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

Реакция САИБ и фиксация в БД фактов нарушения правила не предусмотрены.

### 5.3.4 Настройка правила контроля аппаратной конфигурации

Правило предусматривает сохранение эталонных профилей аппаратных конфигураций контролируемых рабочих мест с последующим отслеживанием их изменений (обеспечивается средствами графического интерфейса администратора, – см. п. 5.7.7 настоящего документа).

В дочернем диалоговом окне (Рис. 38) с помощью календаря «Время запуска» следует определить дату и время запуска (по умолчанию установлены текущие время и дата).

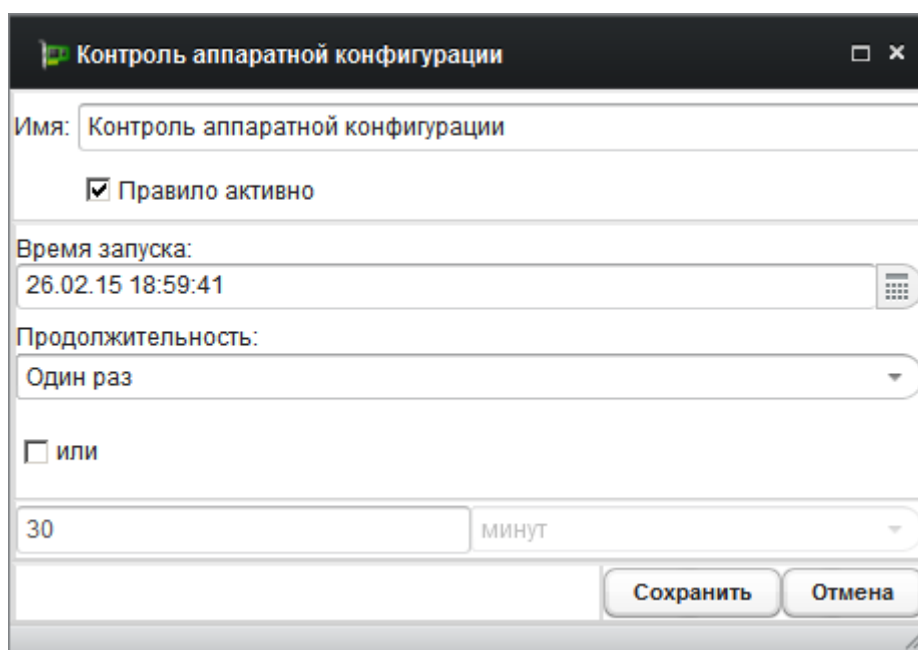


Рис. 38. Окно настройки правила контроля аппаратной конфигурации.

Группа «Продолжительность» позволяет определить периодичность применения правила (фиксации текущего профиля и проверки соответствия профиля эталонному) значением из списка:

- «Один раз» (по умолчанию);
- «Каждые 15 минут»;
- «Каждые полчаса»;
- «Ежечасно»;
- «Ежедневно»;

– «Еженедельно».

Установкой флага «или» и заполнением дополнительного поля можно уточнить периодичность до нужного количества минут, часов или дней.

Для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

*Примечание.* Для выполнения автоматической сверки профилей следует определить один из зафиксированных профилей в качестве эталонного после начала их фиксации в БД (см. п. 5.7.7 настоящего документа).

Реакция САИБ на факт нарушения правила не предусмотрена. В БД производится фиксация только факта обнаружения несоответствия текущей конфигурации эталонному профилю.

### **5.3.5 Настройка правила контроля съёма жёстких дисков**

Контроль за съёмом жёсткого диска обеспечивает невозможность его эксплуатации на стороннем компьютере, неконтролируемом САИБ.

Контроль реализован с применением технологии S.M.A.R.T.<sup>3)</sup> жёстких дисков. РС периодически (однократно в жёстко заданный промежуток времени) считывает значение атрибута DPCC<sup>4)</sup> показаний S.M.A.R.T. и сохраняет его в БД. Значением данного атрибута является количество полных циклов включения-выключения диска.

При запуске РС значение атрибута DPCC сверяется со значением, сохранённым в БД ранее. Если между двумя значениями обнаруживается разница свыше единицы, формируется сообщение об использовании диска на стороннем компьютере.

В дочернем диалоговом окне следует ввести имя правила (необязательное поле) и определить приоритет фиксации отобранного события в журнале инцидентов:

---

<sup>3)</sup> Self-monitoring, analysis and reporting technology (англ.).

<sup>4)</sup> Drive (Device) Power Cycle Count (англ.). Атрибут S.M.A.R.T. № 12.

- «Информационное сообщение» (по умолчанию) – при нарушении правила данные о событии фиксируются Сервером с целью информирования администратора САИБ;
- «Важное сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Критическое сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Хранить локально» – при нарушении правила данные о событии не передаются на Сервер и хранятся локально на контролируемом рабочем месте до запроса данных по требованию инструментом «Получить локальные данные» (см. п. 5.7.6 настоящего документа).

Правило не предусматривает настройки каких-либо свойств (в дочернем диалоговом окне лишь требуется нажать кнопку «Сохранить»).

Реакция САИБ и фиксация в БД фактов нарушения правила выполняются в соответствии с приоритетом фиксации отобранного события в журнале инцидентов.

### **5.3.6 Настройка правила контроля процессов**

Правила данного типа являются основными средствами мониторинга активности пользователей контролируемых рабочих мест. Это единственное правило, которое может быть применено к РС многократно.

Каждая из определяемых записей правила (Рис. 40) включает условия, при выполнении которых правило применяется и РС инициируется выполнение заказанного действия («Разрешить» или «Блокировать»). Условия определяют и метод реагирования САИБ (список «Дополнительное действие») на произошедшее событие, выбор которого может быть сохранён за оператором контролируемого рабочего места:

- *«Не выбрано»* (по умолчанию) – реакции не последует;

- «Снятие снимка экрана» (последующая работа с ними обеспечивается средствами графического интерфейса администратора – см. п. 5.7.5 настоящего документа);
- «Выдача сообщения пользователю» на экран компьютера контролируемого рабочего места: «Внимание! Нарушено правило контроля '[имя\_правила]'. Администратор оповещён.» (Рис. 39);
- «Блокировка компьютера»;
- «Завершение сеанса» – принудительное завершение сеанса пользователя;
- «Блокировка пользователя» – принудительное блокирование сеанса работы пользователя;
- «Перезагрузка компьютера»;
- «Выключение компьютера»;
- «Останов процесса» – происходит останов процесса, инициировавшего событие.

*Примечание.* Выполнение действия «Снятие снимка экрана» требует активации функции сохранения снимков экрана **при установке РС.** Если при установке РС режим был деактивирован, то активировать его в дальнейшем невозможно.

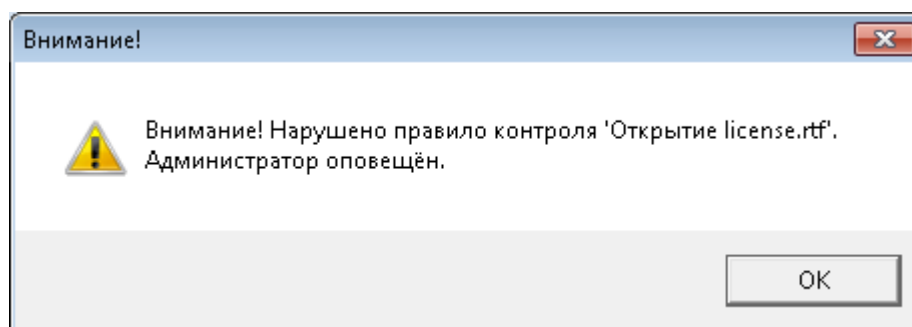


Рис. 39. Пример уведомления пользователя о нарушении правила.

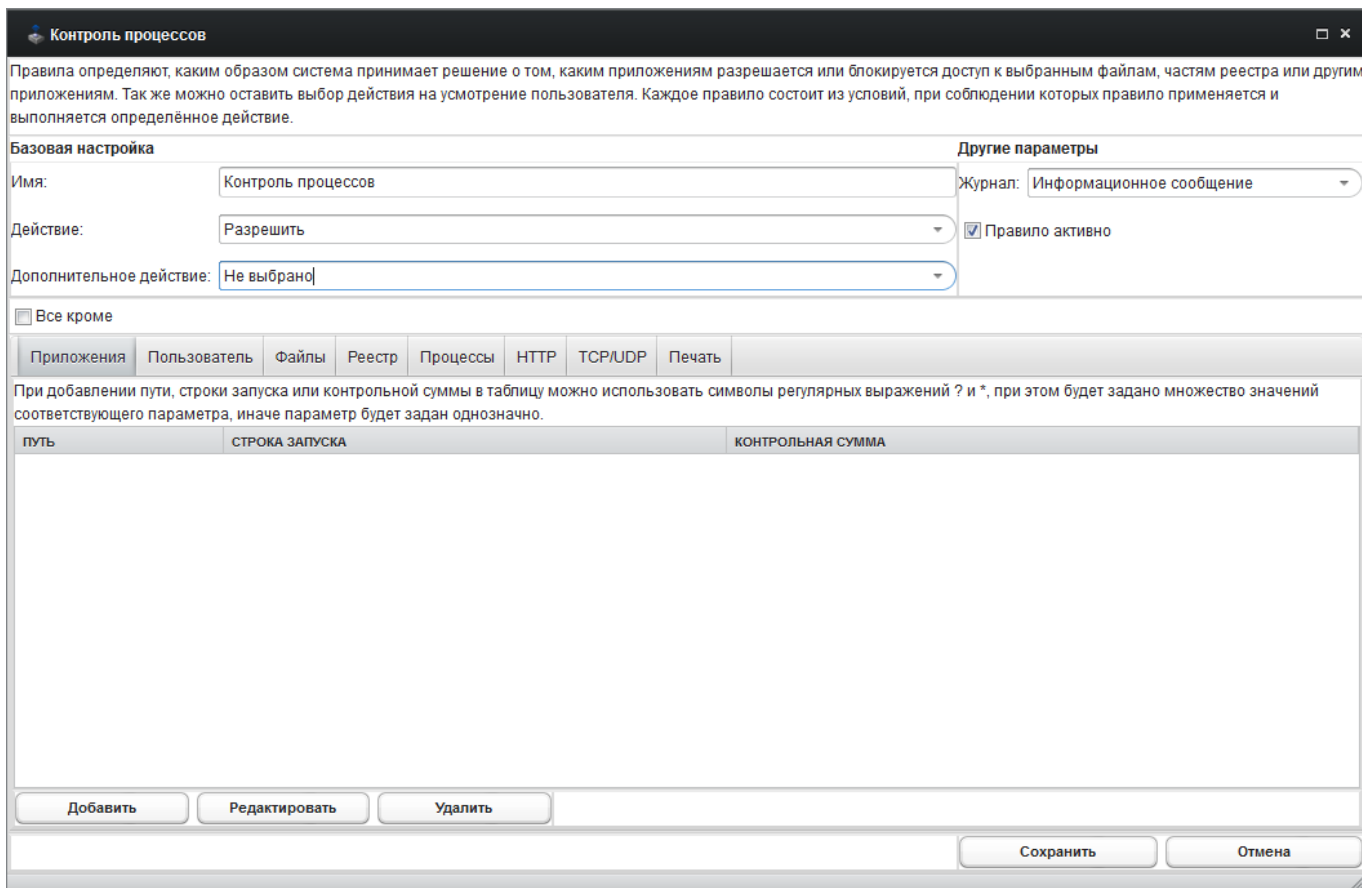


Рис. 40. Окно настройки правила «Контроль процессов».

Также факт возникновения события может быть зафиксирован в журнале событий с нужным приоритетом (список «Журнал»):

- «Не фиксировать» – при нарушении правила данные о событии не фиксируются РС и не передаются на Сервер;
- «Информационное сообщение» (по умолчанию) – при выполнении условий правила данные о событии фиксируются Сервером с целью информирования администратора САИБ;
- «Важное сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Критическое сообщение» – при нарушении правила Сервер воспримет событие как инцидент;
- «Хранить локально» – при нарушении правила данные о событии не передаются на Сервер и хранятся локально на контролируемом рабочем

месте до запроса данных по требованию инструментом «Получить локальные данные» (см. п. 5.7.6 настоящего документа).

Условия применения правила определяются во вкладках «Приложения», «Пользователь», «Файлы», «Реестр», «Процессы», «HTTP», «TCP/UDP», «Печать».

Условия вкладок оцениваются РС совместно, т.е. для применения правила (возникновения факта нарушения правила) требуется выполнение критериев всех вкладок одновременно. Например, можно определить файл, открытие которого с заданного носителя заданным приложением от имени заданного пользователя следует блокировать, выдавая при этом на экран данному пользователю информационное сообщение.

Условия вкладок «Приложения» и «Пользователь» требуют определения дополнительного условия хотя бы ещё в одной вкладке. Условия остальных вкладок могут применяться обособленно от других (для всех приложений и/или всех пользователей). Можно привести следующие мнемонические примеры комбинированного применения условий вкладок в отдельных правилах:

Правило № 1: Приложения & Пользователь & Файлы – контролируются определённые приложения, исполняемые от имени определённых пользователей, выполняющих операции с определёнными файлами.

Правило № 2: Приложения & Процессы – контролируются определённые приложения, выполняющие действия над определёнными процессами.

Правило № 3: Пользователь & Реестр – контролируются определённые пользователи, выполняющие операции над системным реестром.

Правило № 4: Приложения & HTTP – контролируются запросы HTTP, посылаемые определённым приложением.

Правило № 5: Печать – контролируется весь вывод на печать от всех приложений всех пользователей.



Установка флага «Все кроме» позволяет включить/исключить применение правила к событиям всех процессов, кроме обусловленных во вкладках.

**Вкладка «Приложения»** определяет приложения, контроль над которыми требуется осуществить на рабочем месте. Определение каждого контролируемого приложения выполняется кнопкой «Добавить».

В пустых полях нового условия следует указать путь к исполняемому файлу приложения относительно контролируемого рабочего места (графа «Путь»), строку параметров запуска (графа «Строка запуска») и шестнадцатеричную контрольную сумму (графа «Контрольная сумма»), например:

- ‘C:\Windows\System32\LogonUI.exe’ или ‘\*LogonUI.exe’ («Путь»);
- “‘LogonUI.exe’ /flags:0x0’ («Строка запуска»);
- ‘ABF555E7D98A49B992F8F5E0FBF57A65’ («Контрольная сумма»).

Параметры «Строка запуска» и «Контрольная сумма» – необязательные. При отсутствии значений выполнение условия контролируется для всех обнаруженных активных (запущенных) экземпляров указанных приложений и наоборот, – при наличии значений выполнение условия контролируется для всех приложений, у которых строка запуска и/или контрольная сумма совпадут с указанными значениями.

*Примечания:*

1. При определении данных параметров можно использовать символы регулярных выражений ‘\*’ (любая строка) и ‘?’ (любой символ) с целью определения многозначности параметра.

2. Исходные данные для определения указанных параметров можно получить во вкладке «Процессы» инструмента «Менеджер задач» (см. п. 5.7.4 настоящего документа). Для определения параметров приложения,

*отсутствующего в списке процессов, его можно запустить в скрытом режиме.*

Изменение ранее определённых параметров осуществляется двойным щелчком левой кнопки мыши по любому полю изменяемой записи либо кнопкой «Редактировать».

**Вкладка «Пользователь»** определяет пользователя, по отношению к которому применяется правило. Определение каждого пользователя контролируемого рабочего места выполняется кнопкой «Добавить».

В пустом поле нового условия следует указать имя пользователя в одной из следующих форм:

- «идентификатор\_пользователя\домен\_Windows»;
- «имя\_компьютера\идентификатор\_пользователя»;
- «\*идентификатор\_пользователя».

*Примечание.* При определении имени пользователя можно использовать символы регулярных выражений '\*' (любая строка) и '?' (любой символ) с целью определения многозначности параметра.

Если не определён ни один пользователь, условия других применяемых вкладок будут отслеживаться РС для всех пользователей без исключения.

Изменение ранее определённого пользователя осуществляется двойным щелчком левой кнопки мыши по записи изменяемого пользователя либо кнопкой «Редактировать».

**Вкладка «Файлы»** (Рис. 41) определяет список файлов, операции над которыми следует контролировать применяемым правилом. Группа «Операции» включает следующие флаги:

- «Открытие»;
- «Закрытие»;
- «Замена» – замещение данного файлового объекта иным с идентичным именем;

- «Изменение прав DACL<sup>5)</sup>»;
- «Изменение прав SACL<sup>6)</sup>»;
- «Изменение владельца файлового объекта» (смена владельца);
- «Изменение группы файлового объекта» (смена владельца);
- «Переименование файла»;
- «Переименование директории»;
- «Создание файла»;
- «Удаление файла»;
- «Удаление директории».

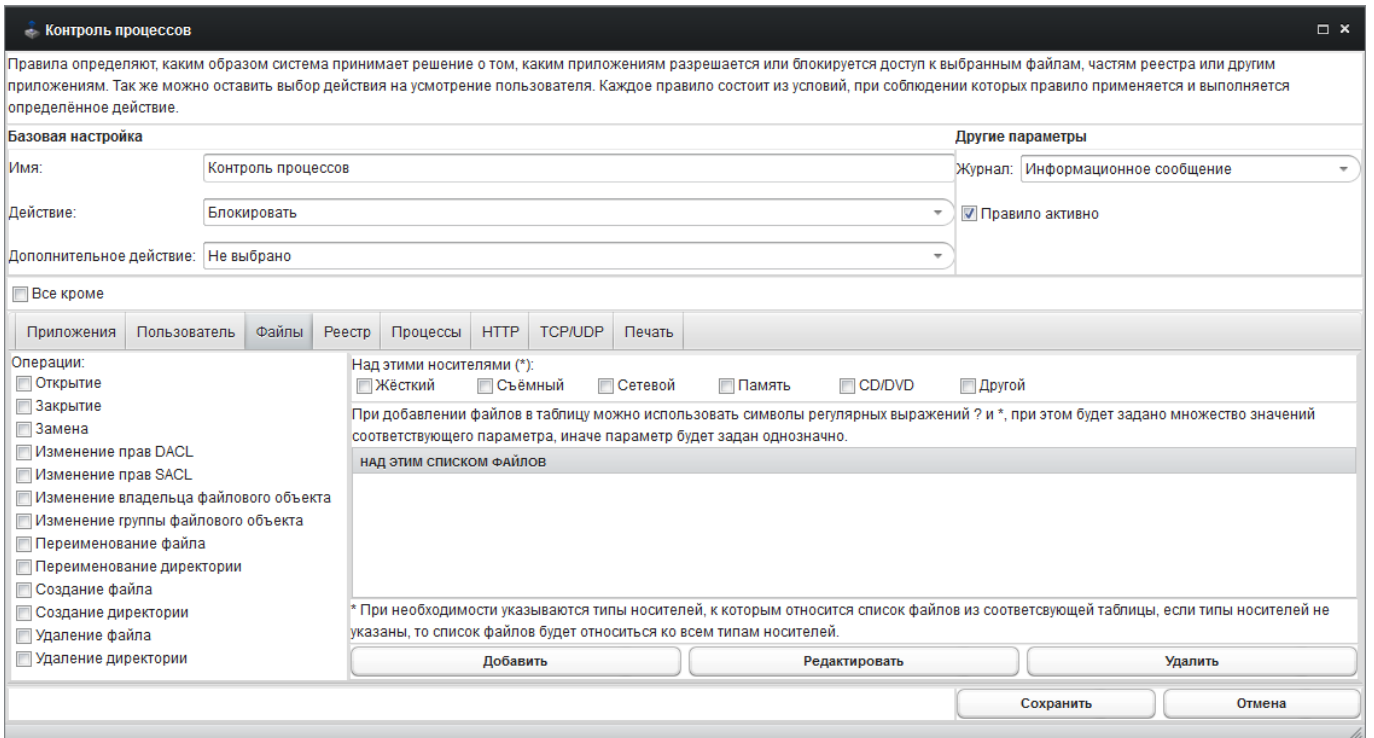


Рис. 41. Окно настройки правила «Контроль процессов». Вкладка «Файлы».

<sup>5)</sup> Discretionary Access Control List (англ.) – список избирательного доступа, контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом (чтение, запись, удаление и т. д.).

<sup>6)</sup> System Access Control List (англ.) – список управления доступом к объектам Microsoft Windows, используемый для аудита доступа к объекту. В отличие от DACL, SACL не может ограничивать доступ к файлам и папкам. Но при обращении пользователя к файлу или папке SACL отследит это событие и внесёт запись о нём в журнал системных событий (раздел 'Security').

Для определения условия контроля требуемой операции следует установить нужный флаг и добавить перечень файлов, для которых предусматривается условие. Определение каждого файла контролируемого рабочего места выполняется кнопкой «Добавить».

*Примечание.* При определении файла можно использовать символы регулярных выражений '\*' (любая строка) и '?' (любой символ) с целью определения многозначности параметра.

Например, файл может быть добавлен записями:

- 'c:\windows\system32\license.rtf' (абсолютный путь к конкретному файлу относительно контролируемого рабочего места);
- '\*system32\license.rtf' (сокращённый путь к конкретному файлу с маской);
- '\*license.rtf' (любой файл с именем 'license.rtf').

При этом запись 'license.rtf' не приведёт к применению правила для указанного файла.

Изменение значения параметра файла, определённого ранее, осуществляется двойным щелчком левой кнопки мыши по записи изменяемого файла либо кнопкой «Редактировать».

В пустом поле нового условия следует указать имя файла без указания его точного расположения (абсолютного пути), поскольку типы носителей контролируемого рабочего места определяются установленными флагами:

- «Жёсткий» – любой из жёстких дисков;
- «Съёмный» – любой из съёмных дисков, включая носители USB;
- «Сетевой» – любая из сетевых папок»
- «Память» – обнаружение файла загруженным в оперативную память;
- «CD/DVD», помещённый в дисковод;
- «Другой» – иной тип носителя, опознаваемый ОС контролируемого рабочего места в качестве такового.

Если не определён ни один из типов носителей, выбранные операции над файлом будут отслеживаться РС на носителе любого типа.

**Вкладка «Реестр»** определяет наименование ключей или ключей со значениями системного реестра, операции над которыми следует контролировать применяемым правилом. Группа «Операции» включает следующие флаги:

- «Перечисление значений»<sup>7)</sup>;
- «Перечисление ключей»;
- «Создание ключей» – запрос на создание ключа (раздела);
- «Открытие ключа реестра» – запрос на выбор указанного ключа (раздела) реестра в качестве текущего для последующих операций над вложенными ключами (значениями);
- «Удаление ключей» – запрос на удаление указанного ключа (раздела);
- «Удаление значений»;
- «Установка значений» – запрос на создание параметра любого типа с наименованием и определением его значения;
- «Чтение ключей» – запрос на чтение текущего ключа (раздела);
- «Чтение значений»;
- «Переименование ключа реестра» – запрос на переименование указанного раздела, ключа или значения.

Определение каждого наименования ключа (значения) системного реестра контролируемого рабочего места выполняется кнопкой «Добавить».

В пустом поле нового условия следует указать контролируемый ключ или значение, например:

- 'HKCU\Software\Microsoft\Command Processor';
- 'HKCU\Software\Microsoft\Command Processor\AutoRun\chcp 1251 1>nul'.

---

<sup>7)</sup> «Перечисление» – это получение имени ключа (значения) по его номеру. Нет возможности узнать, сколько ключей (значений) содержит раздел реестра. Поэтому единственным способом перечисления всех ключей (значений) является итерационный цикл получения наименований объектов с номерами '0', '1', '2' и т.д., до тех пор, пока функция не вернёт код ошибки.

Наименования корневых разделов следует указывать только в сокращённой форме:

- ‘HKCR’ для ‘HKEY\_CLASSES\_ROOT’;
- ‘HKCU’ для ‘HKEY\_CURRENT\_USER’;
- ‘HKLM’ для ‘HKEY\_LOCAL\_MACHINE’;
- ‘HKU’ для ‘HKEY\_USERS’;
- ‘HKCC’ для ‘HKEY\_CURRENT\_CONFIG’.

*Примечание.* При определении параметра можно использовать символы регулярных выражений ‘\*’ (любая строка) и ‘?’ (любой символ) с целью определения многозначности параметра.

Если не определено ни одного ключа (значения), выбранные операции будут отслеживаться РС для всех ключей (значений).

Изменение ранее определённого ключа (значения) реестра осуществляется двойным щелчком левой кнопки мыши по изменяемой записи либо кнопкой «Редактировать».

**Вкладка «Процессы»** определяет файлы модулей (процессы), действия над которыми следует контролировать применяемым правилом. Группа «Действия над процессами» включает следующие флаги:

- «*Загрузка модулей процессом*» – загрузка в оперативную память файлов модулей (библиотек DLL);
- «*Запуск процесса*» – возникновение процесса;
- «*Запуск процесса процессом*» – запуск процессом дочернего или нового внешнего процесса;
- «*Останов процесса*» – исчезновение процесса.

Определение каждого файла модуля (процесса) контролируемого рабочего места выполняется кнопкой «Добавить».

В пустых полях нового условия следует указать путь к файлу модуля процесса относительно контролируемого рабочего места или имя образа процесса (графа «Путь к файлу модуля/процессу»), а также

шестнадцатеричную контрольную сумму файла модуля или процесса (графа «Контрольная сумма модуля/процесса»), например:

- ‘C:\Windows\System32\LogonUI.exe’ или ‘\*LogonUI.exe’ («Путь к файлу модуля/процессу»);
- ‘ABF555E7D98A49B992F8F5E0FBF57A65’ («Контрольная сумма»).

Параметры «Путь к файлу модуля/процессу» и «Контрольная сумма модуля/процесса» – необязательные. При отсутствии значений выполнение условия контролируется для всех обнаруженных экземпляров указанных файлов модулей (процессов) и контрольных сумм (относящихся к приложениям, определённым во вкладке «Приложения») и наоборот, – при наличии значений выполнение условия контролируется для указанных файлов модулей (процессов), у которых контрольная сумма совпадёт с указанным значением (и относящимся к приложениям, определённым во вкладке «Приложения»).

*Примечания:*

*1. При определении данных параметров можно использовать символы регулярных выражений ‘\*’ (любая строка) и ‘?’ (любой символ) с целью определения многозначности параметра.*

*2. Исходные данные для определения указанных параметров можно получить во вкладке «Процессы» инструмента «Менеджер задач» (см. п. 5.7.4 настоящего документа). Для определения параметров процесса, отсутствующего в списке, его можно запустить в скрытом режиме.*

При определении значения лишь одного из параметров выбранные действия будут отслеживаться РС в отношении всех файлов модулей (процессов) приложений, определённых во вкладке «Приложения», и удовлетворяющих указанному значению.

Изменение значения параметра файла модуля (процесса), определённого ранее, осуществляется двойным щелчком левой кнопки мыши по изменяемой записи либо кнопкой «Редактировать».

*Примечание.* Параметры «Путь к файлу модуля/процессу» и «Контрольная сумма модуля/процесса» используются лишь для контроля дочерних процессов и совместно с установленными флагами «Запуск процесса» и «Останов процесса» группы «Действия над процессами» не применяются.

Например, требуется контролировать запуск утилиты командной строки для управления сетевыми интерфейсами ('ipconfig.exe') из интерпретатора командной строки ('cmd.exe'). Здесь приложение 'cmd.exe' запускает дочерний процесс 'ipconfig.exe', поэтому для блокирования этого действия в графе «Путь» вкладки «Приложения» следует определить '\*cmd.exe', а в графе «Путь к файлу модуля/процессу» вкладки «Процессы» следует определить '\*ipconfig.exe', установив флаг «Запуск процесса» группы «Действия над процессами».

**Вкладка «НТТР»** определяет параметры, запросы с содержанием которых по протоколу НТТР<sup>8)</sup> следует контролировать применяемым правилом. Группа «НТТР-запросы» включает следующие флаги:

- 'GET' – запрос содержимого ресурса WWW;
- 'POST' – передача пользовательских данных ресурсу WWW;
- 'CONNECT' – преобразование соединения запроса в прозрачный TCP/IP-туннель (обычно для установления защищённого SSL-соединения по открытому каналу);
- 'TRACE' – возвращает запрос с отображением изменений, внесённых в содержимое промежуточными серверами;

---

<sup>8)</sup> HyperText Transfer Protocol (англ.) – протокол передачи гипертекста. Протокол осуществляет доставку пользователю запрашиваемого им содержимого ресурса «Всемирной паутины» (WWW) для просмотра в Web-обозревателе.



- ‘*OPTIONS*’ – запрос возможностей ресурса WWW или параметров соединения;
- ‘*DELETE*’ – удаление ресурса WWW;
- ‘*HEAD*’ – аналогичен ‘GET’, но возвращает лишь заголовки содержимого ресурса WWW.

Конкретизация запросов выполняется определением их параметров. Параметры передаются<sup>9)</sup> в формате «*имя\_параметра=значение\_параметра*» и разделяются между собой символом ‘&’, например, ‘login=admin&password=qwerty’.

Определение требуемых параметров осуществляется кнопкой «Добавить». В пустом поле нового условия следует указать строку параметров запроса HTTP.

*Примечание.* При определении параметра можно использовать символы регулярных выражений ‘\*’ (любая строка) и ‘?’ (любой символ) с целью определения многозначности параметра.

При отсутствии значений параметров выбранные типы запросов будут отслеживаться РС для всех запросов HTTP, посылаемых с контролируемого рабочего места без исключения.

Изменение значения параметра запроса, определённого ранее, осуществляется двойным щелчком левой кнопки мыши по изменяемой записи либо кнопкой «Редактировать».

САИБ не обладает возможностью блокирования определённых запросов HTTP и позволяет лишь эффективно отслеживать их.

**Вкладка «TCP/UDP»** определяет параметры сетевых соединений, которые следует контролировать применяемым правилом.

Условия применения правила определяются аналогично условиям правила «Межсетевой экран» (см. п. 0 настоящего документа), но набор

---

<sup>9)</sup> Параметры ‘GET’ могут отправляться любыми методами (в строке либо в теле), а параметры ‘POST’ могут отправляться только в теле запроса ‘POST’.

контролируемых сетевых протоколов сужен до основных протоколов транспортного уровня (TCP<sup>10</sup> и UDP<sup>11</sup>).

Однако, условия вкладки не позволяют выполнять непосредственные операции над трафиком. В отличие от правила «Межсетевой экран» (применяемого обособленно от программной среды контролируемого рабочего места) условия данной вкладки могут применяться в совокупности с условиями других вкладок, точно определяя контекст возникновения ожидаемого события (например, приложение или процесс, породившие сетевой трафик).

Ещё одно отличие состоит в возможности определения списка IP-адресов локального компьютера (с целью контроля трафика через определённый сетевой интерфейс при одновременном наличии нескольких сетевых плат или нескольких IP-адресов).

**Вкладка «Печать»** определяет условия контроля событий вывода документов на твёрдые носители или псевдопринтеры применяемого правила.

САИБ не обладает возможностью блокирования событий этого типа, поэтому вкладка содержит единственный флаг «Отслеживать», установка которого активирует условие.

По завершению определения всех условий для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

Реакция САИБ и фиксация в БД фактов нарушения правила выполняются в соответствии с приоритетом фиксации отобранного события в журнале инцидентов.

### **5.3.7 Настройка правила контроля устройств USB**

Правило обеспечивает эксплуатацию на контролируемом рабочем месте зарегистрированных устройств USB согласно матрице доступа и препятствует

---

<sup>10)</sup> Transmission Control Protocol (англ.) – протокол управления передачей. Выполняет функции протокола транспортного уровня в стеке протоколов IP.

<sup>11)</sup> User Datagram Protocol (англ.) – протокол пользовательских датаграмм, один из ключевых элементов TCP/IP. UDP не гарантирует целостности передаваемых данных, контроль которой осуществляет приложение.

использованию незарегистрированных устройств. Это позволяет закрепить за сотрудником и его рабочим местом зарегистрированные устройства.

Идентификация устройств USB проводится с использованием заводского серийного номера, встроенного в устройство. Поэтому для применения правила в организации должны эксплуатироваться устройства, оснащённые производителем встроенными серийными номерами.

Одним из распространённых видов устройств, подключаемых к рабочему месту, являются накопители USB<sup>12)</sup>, работу с которыми можно контролировать с помощью данного правила. Также правило применимо для контроля подключения концентраторов USB<sup>13)</sup>.

Диалоговое окно определения правила контроля устройств USB (Рис. 42) позволяет сформировать список разрешённых (или запрещённых) к использованию устройств и определить режимы его применения.

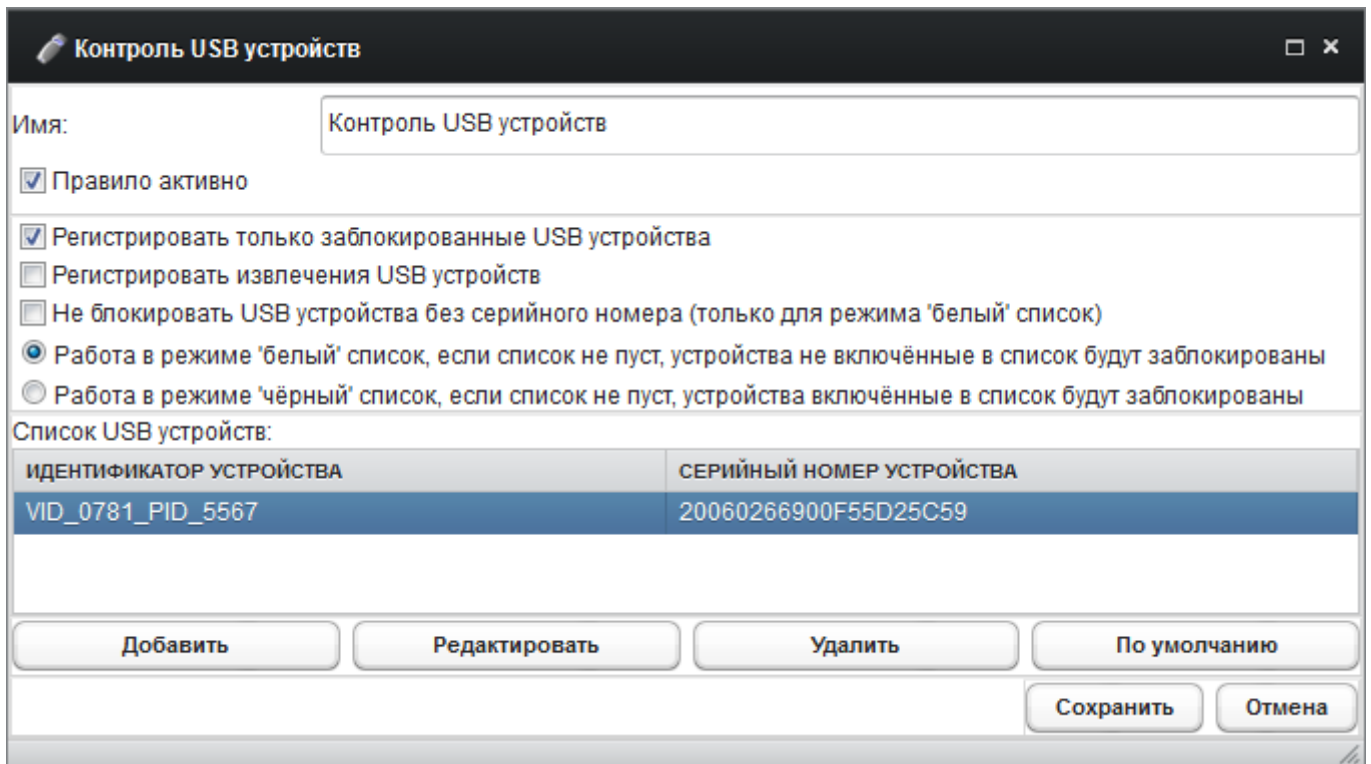


Рис. 42. Окно настройки правила «Контроль USB устройств».

<sup>12)</sup> USB flash mass storage (англ.) – накопители больших объёмов с носителями на электрически стираемых перепрограммируемых ПЗУ (ЭСППЗУ), подключаемые к СБТ или иному считывающему устройству по интерфейсу USB.

<sup>13)</sup> USB hub (англ.).

Определение каждого устройства USB, зарегистрированного к применению на контролируемом рабочем месте, выполняется кнопкой «Добавить».

Изменение реквизитов устройства, зарегистрированного ранее, осуществляется двойным щелчком левой кнопки мыши по изменяемой записи либо кнопкой «Редактировать».

В дочернем диалоговом окне (Рис. 43) следует указать реквизиты регистрируемого устройства USB:

- идентификатор производителя (Vendor ID или VID);
- идентификатор модели (Part ID или PID);
- серийный номер.

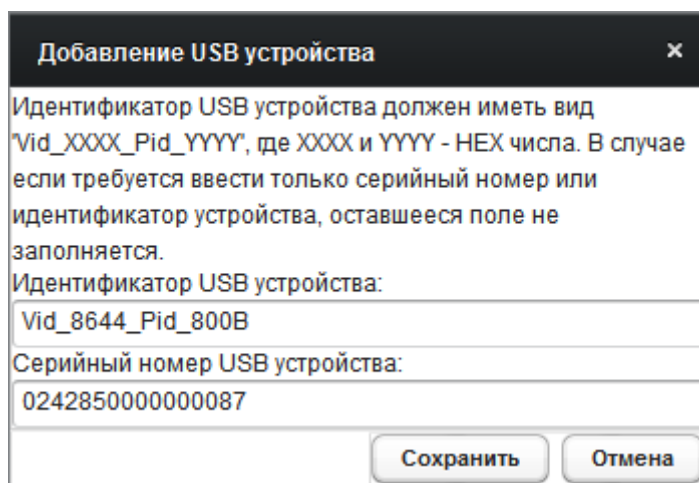


Рис. 43. Окно добавления/изменения реквизитов устройства USB».

VID и PID указываются в поле «Идентификатор USB устройства» через разделитель ‘\_’ по форме: ‘Vid\_XXXX\_Pid\_YYYY’, где ‘XXXX’ и ‘YYYY’ – соответствующие шестнадцатеричные числа.

Если требуется определить только серийный номер или только идентификатор устройства оставшееся поле не заполняется.

VID, PID и серийный номер устройств USB относительно легко можно получить средствами WMI<sup>14)</sup>, входящими в состав ОС семейства Microsoft Windows.

<sup>14)</sup> Windows Management Instrumentation (англ.).

Например, для получения сведений о накопителе USB после его подключения к порту USB из приложения «Командная строка» ('cmd') следует вызвать утилиту 'wmic', передав ей команду: 'path win32\_usbhub Where (Caption="Запоминающее устройство для USB") get DeviceID' (листинг 1).

Листинг 1

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Alexey>wmic
wmic:root\cli>path win32_usbhub Where (Caption="Запоминающее устройство для
USB") get DeviceID
DeviceID
USB\VID_0781&PID_5567\20060266900F55D25C59

wmic:root\cli>quit

C:\Users\Alexey>exit
```

Интересующие сведения о всех накопителях, подключенных к компьютеру во время выполнения команды, приведены в строках вывода после идентификатора 'DeviceID', например: 'USB\VID\_0781&PID\_5567\20060266900F55D25C59'. Здесь 'VID\_0781&PID\_5567' – идентификаторы VID и PID, объединённые через разделитель '&' (следует заменить на '\_'), '20060266900F55D25C59' – 20-символьный серийный номер устройства.

*Примечание.* При отсутствии заводского серийного номера устройства, ОС Windows выполняет генерацию 12-символьного серийного номера, уникальность которого гарантируется лишь в рамках одного рабочего места.

Для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

После регистрации всех устройств USB следует определить условия применения создаваемого правила.

Установка флага «Регистрировать только заблокированные USB-устройства» предписывает PC реагировать только на факты подключения к

контролируемому рабочему месту тех устройств USB, которые PC сочтёт незарегистрированными, и блокировать их подключение.

Установка флага «Регистрировать извлечения USB-устройств» обеспечивает фиксацию событий отключения от контролируемого рабочего места всех (как зарегистрированных, так и незарегистрированных) устройств USB без исключения.

Установка флага «Не блокировать USB-устройства без серийного номера (только для режима ‘белый’ список)» исключает блокирование PC устройств USB, внесённых в список, но не имеющих серийного номера.

Список зарегистрированных устройств USB может применяться в двух режимах в зависимости от положения переключателя (режим включается лишь в том случае, если список устройств содержит хотя бы одну запись):

- *«Работа в режиме ‘белый’ список»* (блокируются устройства, отсутствующие в списке);
- *«Работа в режиме ‘чёрный’ список»* (блокируются устройства, присутствующие в списке).

Кнопка «По умолчанию» возвращает установки условий к заводским, очищая список зарегистрированных устройств USB (состояние окна соответствует первоначальному).

По завершению определения всех условий для фиксации выполненных настроек в БД следует нажать кнопку «Сохранить».

#### **5.4. Создание шаблонов правил**

Контроль событий рабочих мест зачастую требуется осуществлять по одним и тем же типовым правилам. Трудоёмкую рутинную работу по многократному определению одних и тех же условий правил для множества контролируемых рабочих мест можно минимизировать, воспользовавшись возможностью разработки шаблонов с наборами правил нужных типов.

Количество определяемых шаблонов не ограничено, поэтому каждый шаблон может содержать полный набор правил, применяемых в

эксплуатирующей организации для контроля рабочего места определённого типа.

Механизм разработки шаблонов предусмотрен только для РС. Для настройки шаблонов правил сбора событий с контролируемого рабочего места следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей* и переключить окно свойств в режим отображения «Шаблоны» (Рис. 44).

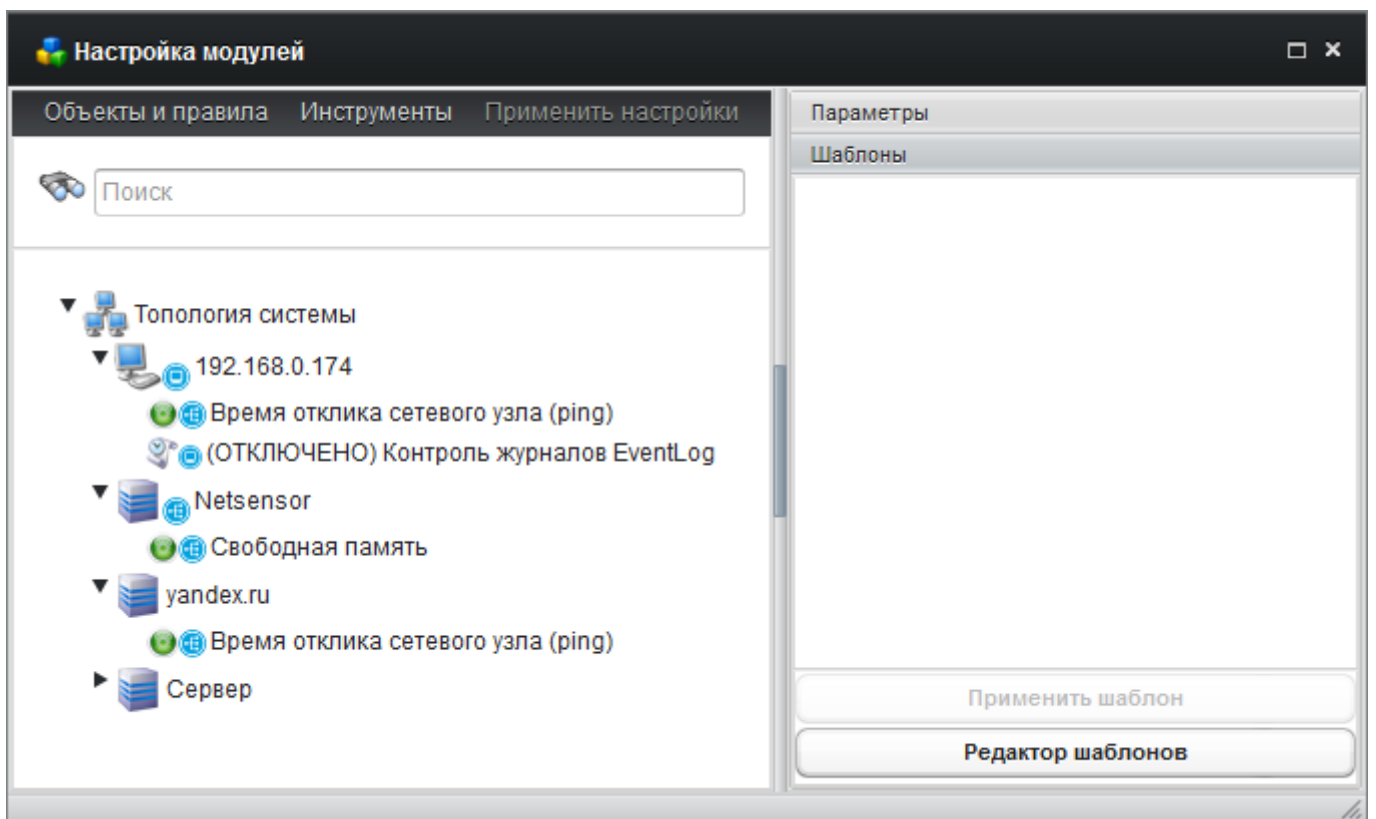


Рис. 44. Окно «Настройка модулей» в режиме «Шаблоны».

Для создания нового шаблона с набором правил следует нажать кнопку «Редактор шаблонов» в окне свойств.

Редактор шаблонов организован аналогично окну настройки модулей, только в данном случае в окне слева отображаются шаблоны с вложенными в них правилами, а справа – типы правил, доступные для добавления в шаблон (Рис. 45).

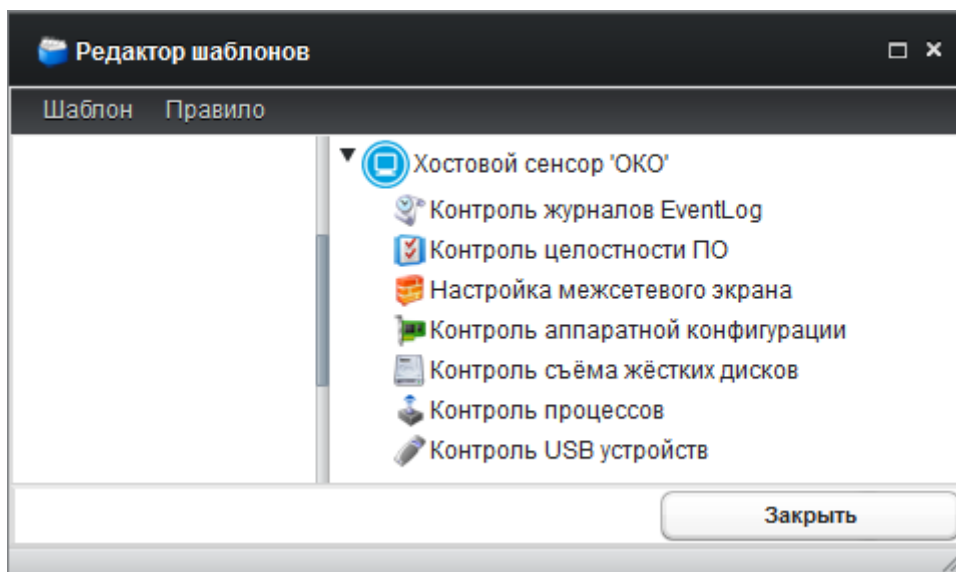


Рис. 45. Окно «Редактор шаблонов».

Для создания нового шаблона следует выбрать раздел меню *Шаблон* → *Новый*, определить имя нового шаблона и нажать кнопку «Сохранить».

Для переименования созданного шаблона следует выбрать раздел меню *Шаблон* → *Переименовать* либо одноимённый пункт контекстного меню.

Добавление в созданный шаблон правила определённого типа осуществляется буксировкой его мышью из древа в правом окне в созданный шаблон в левом окне. При этом открывается окно определения условий применения правила.

Условия правил всех типов определяются в соответствии с вышеизложенным (см. п. 5.3.1 – 5.3.7 настоящего документа).

Контекстное меню, вызываемое правой кнопкой мыши при выборе определённого шаблона, позволяет ускорить работу с шаблонами.

Внесение изменений в ранее определённые правила шаблона осуществляется по двойному щелчку левой кнопки мыши по нужному правилу либо выбором одноимённого пункта контекстного меню либо выбором раздела меню *Правило* → *Редактировать правило*.

Для удаления правила следует выбрать его в древе топологии и выбрать раздел меню *Правило* → *Удалить* либо одноимённый пункт контекстного



меню либо нажать клавишу 'Delete' (последует запрос подтверждения принятого решения).

Для применения шаблона правил к контролируемому рабочему месту следует выбрать его в древе топологии, переключить окно свойств в режим отображения «Шаблоны», выбрать нужный шаблон и нажать кнопку «Применить шаблон».

Применение шаблона правил к контролируемому рабочему месту заменяет все правила, определённые для него ранее.

### 5.5. Настройка сценариев опроса

Установка сетевого сенсора на одно из СВТ \*nix наделяет САИБ возможностями сбора и систематизации данных о событиях, возникших на объектах сетевой инфраструктуры, с помощью набора предопределённых для них сценариев опроса.

Сценарий опроса «Сетевой мониторинг» предусматривает контроль следующих параметров:

- «(ИБП) Контроль качества электропитания»;
- «(ИБП) Контроль качества электропитания по SNMP<sup>15)</sup>»;
- «(ИБП) Мониторинг параметра»;
- «(ИБП) Нагрузка на ИБП (%)»;
- «(ИБП) Нагрузка на ИБП (%) по SNMP»;
- «(ИБП) Уровень заряда (%)»;
- «(ИБП) Уровень заряда (%) по SNMP»;
- «(ТО) UDP-дейтаграммы (Входящие)»;
- «(ТО) UDP-дейтаграммы (Исходящие)»;
- «(ТО) Время работы и учет перезагрузок»;
- «(ТО) Загрузка сетевого интерфейса»;
- «(ТО) Загрузка ЦП»;
- «(ТО) Количество байт переданных через интерфейс»;
- «(ТО) Количество пакетов переданных через интерфейс»;
- «(ТО) Коллизии на интерфейсах»;
- «(ТО) Контроль статуса HSRP<sup>16)</sup> (по SNMP)»;
- «(ТО) Мониторинг BGP<sup>17)</sup>»;
- «(ТО) Мониторинг OSPF<sup>18)</sup>»;
- «(ТО) Мониторинг температуры»;

---

<sup>15)</sup> Simple Network Management Protocol (англ.).

<sup>16)</sup> Hot Standby Redundancy Protocol (англ.); разработчик – Cisco Systems, Inc.

<sup>17)</sup> Border Gateway Protocol (англ.).

<sup>18)</sup> Open Shortest Path First (англ.).

- «(ТО) Отброшенные пакеты на интерфейсах»;
- «(ТО) Ошибки на интерфейсах»;
- «(ТО) Свободная память (пулы)»;
- «(ТО) Учет настроенного статуса интерфейса (ifAdminStatus)»;
- «(ТО) Учет текущего статуса интерфейса (ifOperStatus)»;
- «(ТО) Широковещательные пакеты на интерфейсах»;
- «Вариационная задержка сетевого узла»;
- «Время отклика DHCP» (\*);
- «Время отклика DNS»;
- «Время отклика FTP»;
- «Время отклика NTP»;
- «Время отклика POP3»;
- «Время отклика SFTP»;
- «Время отклика SMTP»;
- «Время отклика SNMP»;
- «Время отклика SSH»;
- «Время отклика сетевого узла (ping)»;
- «Время получения интернет-страницы»;
- «Время работы» (\*);
- «Время с момента построения XML»;
- «Входящий сетевой трафик» (\*);
- «Загрузка ЦП» (\*);
- «Исходящий сетевой трафик» (\*);
- «Свободная память» (\*).

Сценарий опроса «Расширенный мониторинг ТО» предусматривает контроль следующих параметров:

- «(ТО) Контроль целостности BGP»;
- «(ТО) Контроль целостности загрузочной конфигурации (startup-config)»;

- «(ТО) Контроль целостности рабочей конфигурации (*running-config*)»;
- «(ТО) Контроль целостности списков доступа (*ACL*)»;
- «(ТО) Контроль целостности таблицы коммутации»;
- «(ТО) Контроль целостности таблицы маршрутизации»;
- «(ТО) Мониторинг *OSPF*»;
- «(ТО) Пользователи на линиях»;
- «(ТО) Регистрация и учет *tcp*-сессий»;
- «(ТО) Регистрация и учет *VPN*»;
- «(ТО) Регистрация и учет *xDSL*»;
- «(ТО) Состояние *ARP*-таблицы».

Сценарии могут применяться как для контроля СВТ, на котором установлен сетевой сенсор, так и для контроля любого другого модуля, как оснащённого РС, так и неконтролируемого средствами САИБ. К одному и тому же модулю может быть применено несколько различных сценариев опроса, но лишь по одному каждого типа.

Сценарии опроса источников бесперебойного питания, оборудованных сетевыми интерфейсами, обозначены префиксом «(ИБП)». Сценарии опроса телекоммуникационного оборудования обозначены признаком «(ТО)». Сценарии контроля локальных параметров, применимые исключительно к СВТ с установленным сетевым сенсором, помечены признаком «(\*)».

По своему назначению сценарии опроса аналогичны правилам, но обеспечивают реакцию САИБ не только на события, порождаемые прямыми или косвенными действиями человека, но и на события, порождаемые средствами вычислительной и телекоммуникационной техники.

Для применения сценария мониторинга сетевого сенсора к рабочему месту следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*, выбрать в древе топологии искомый модуль. После этого

нужно переключить окно свойств в режим отображения «Правила» (см. Рис. 29).

Затем в разделе свойств «Сетевой сенсор» следует выбрать пункт «Сетевой мониторинг» и нажать кнопку «Настроить правило», либо дважды щёлкнуть левой кнопкой мыши по выбранному типу. Применить сценарий к выбранному в текущий момент модулю можно также методом захвата и перетаскивания мышью пункта свойств «Сетевой мониторинг».

Последует запрос на определение средства мониторинга (Рис. 46), в котором указателем мыши или клавишами управления курсором клавиатуры из древа доступных в САИБ серверов мониторинга, оснащённых сетевыми сенсорами, следует выбрать нужный и нажать кнопку «Выбрать».

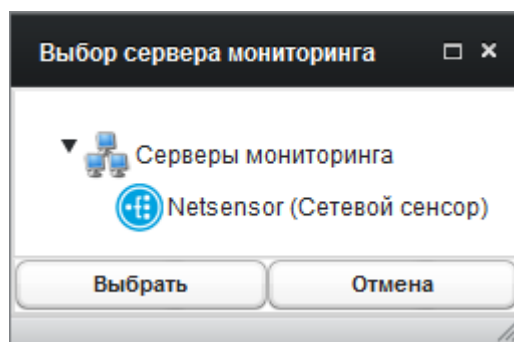


Рис. 46. Окно выбора средства мониторинга.

В целях облегчения массового применения сценариев опроса к модулям выбранное средство мониторинга будет использоваться по умолчанию (текущий выбор отражается включением имени выбранного сенсора в скобках после наименования в разделе «Сетевой сенсор» свойств «Правила»). Для отмены выбора и повторного запроса на определение средства мониторинга при последующем применении сценария сетевого мониторинга следует дважды щёлкнуть левой кнопкой мыши по текущему наименованию раздела «Сетевой сенсор».

После определения средства мониторинга последует запрос выбора и настройки параметров сценария сетевого мониторинга (Рис. 47). В окне следует определить значение «Интервал опроса» в секундах (чем короче

интервал, тем чаще актуальные данные будут поступать в САИБ для анализа) и выбрать нужное «Описание параметров» из списка.

Каждый сценарий характеризуется наборами параметров, свойственных и подконтрольных ему. После выбора описания в разделе «Параметры» следует выбрать нужные «Настройки» из соответствующего списка для отображения предопределённых параметров для выбранных настроек (раскрываются щелчком левой кнопкой мыши по ссылке «Подробные настройки»).

Сетевой мониторинг

Имя: (TO) UDP-дейтаграммы (Входящие)

Интервал опроса: 30 секунд

Описание параметров: (TO) UDP-дейтаграммы (Входящие) [Импорт описания](#)

Правило активно

▼ Параметры

Настройки

Версия SNMP протокола: 3

↓ [Подробные настройки](#)

<input type="checkbox"/>	ПАРАМЕТР	ЗНАЧЕНИЕ	...
<input type="checkbox"/>	Хост		<a href="#">Редактировать</a>
<input type="checkbox"/>	Версия SNMP протокола	3	
<input type="checkbox"/>	Имя пользователя	v3get	<a href="#">Редактировать</a>
<input type="checkbox"/>	Протокол авторизации	sha1	<a href="#">Редактировать</a>
<input type="checkbox"/>	Пароль для авторизации		<a href="#">Редактировать</a>
<input type="checkbox"/>	Ключ для авторизации		<a href="#">Редактировать</a>
<input type="checkbox"/>	Приватный протокол		<a href="#">Редактировать</a>
<input type="checkbox"/>	Приватный пароль		<a href="#">Редактировать</a>
<input type="checkbox"/>	Приватный ключ		<a href="#">Редактировать</a>
<input type="checkbox"/>	SNMP Порт	161	<a href="#">Редактировать</a>
<input type="checkbox"/>	Таймаут	30	<a href="#">Редактировать</a>
<input type="checkbox"/>	Пользовательский OID		<a href="#">Редактировать</a>
<input type="checkbox"/>	Ширина окна	10	<a href="#">Редактировать</a>
<input type="checkbox"/>	Количество ошибок в окне	6	<a href="#">Редактировать</a>

▶ Штатное состояние

[Сохранить](#) [Отмена](#)

Рис. 47. Окно определения параметров сценария сетевого мониторинга.

Список параметров представлен в табличной форме. Первая графа таблицы содержит флаг активации контроля параметра, вторая – описание параметра, третья – определённое значение параметра или значение по умолчанию, четвёртая (‘...’) – содержит ссылку «Редактировать», щелчок левой кнопкой мыши по которой позволяет изменить значение параметра, определённое в текущий момент.

Основным параметром, требующим неопременного определения для применения сценария сетевого мониторинга, является адрес сетевого узла «Хост», в котором следует указать IP-адрес или доменное имя контролируемого элемента сетевой инфраструктуры.

Если для модуля топологии определены атрибуты «Имя хоста», «Адрес IPv4» или «Адрес IPv6» (см. п. 5.2 настоящего документа), то определённые значения указанных атрибутов будут автоматически перенесены в атрибут «Хост» сценария, причём приоритетным атрибутом считается атрибут «Имя хоста». В случае определения значений всех атрибутов модуля будет предложена возможность выбора одного из трёх в качестве значения атрибута «Хост» сценария.

Параметр «Ширина окна» определяет меру накопительного анализа количества ошибок, заданных параметром «Количество ошибок в окне». Например, реакция САИБ последует, если на каждые 10 последовательных запросов ‘ping’ получено менее 6 ответов.

При изменении настроек параметров по умолчанию в список «Настройки» вносится новое значение «Пользовательская установка», которая позволяет вновь вернуться к заводским установкам выбором значения «Настройки по умолчанию».

Предусмотрена реакция САИБ на факт нарушения штатного состояния элемента сетевой инфраструктуры. Это достигается определением пороговых значений контролируемых параметров в разделе «Штатное состояние» (раскрывается щелчком левой кнопки мыши по заголовку раздела и

повторным щелчком левой кнопки мыши по ссылке «Подробные настройки»).

Набор порогов включает следующие (см. Рис. 48):

- «Критическое значение ([единица\_измерения])»;
- «Затруднительное значение ([единица\_измерения])»;
- «Нормальное значение ([единица\_измерения])».

Превышение значений порогов «Затруднительное значение» и «Критическое значение» приведёт к реакции САИБ в виде инцидента. Атрибут '[единица\_измерения]' отражает наименование единицы измерения, характерной для значения порога применяемого типа (например, «количество», «байт», «мегабайт» и т.п.).



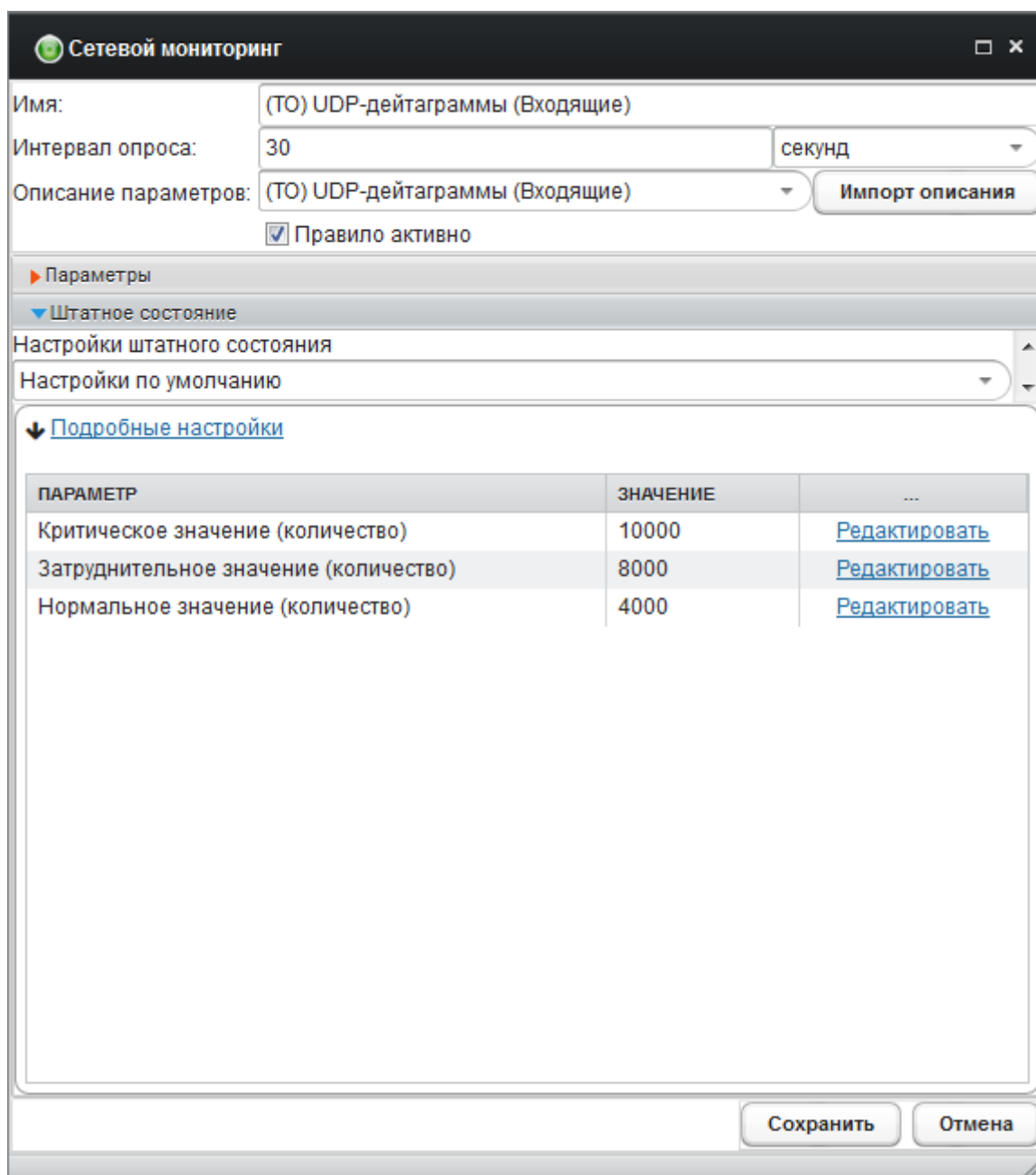


Рис. 48. Окно определения порогов сценария сетевого мониторинга.

При изменении настроек по умолчанию в список «Настройки штатного состояния» вносится новое значение «Пользовательская установка», которая позволяет вновь вернуться к заводским установкам выбором значения «Настройки по умолчанию».

Определив все необходимые параметры сценария, следует нажать кнопку «Сохранить» для фиксации настроек в БД.

Сценарии, определённые для каждого модуля, также отображаются в древе топологии в виде вложений в модуль (см. Рис. 30).

При выборе определённого сценария в окне свойств отображается его описание и установленные параметры, что позволяет текстуально оценить корректность настройки сценария.

Внесение изменений в ранее определённые сценарии осуществляется по двойному щелчку левой кнопки мыши по нужному сценарию либо выбором раздела меню *Объекты и правила* → *Редактировать правило*.

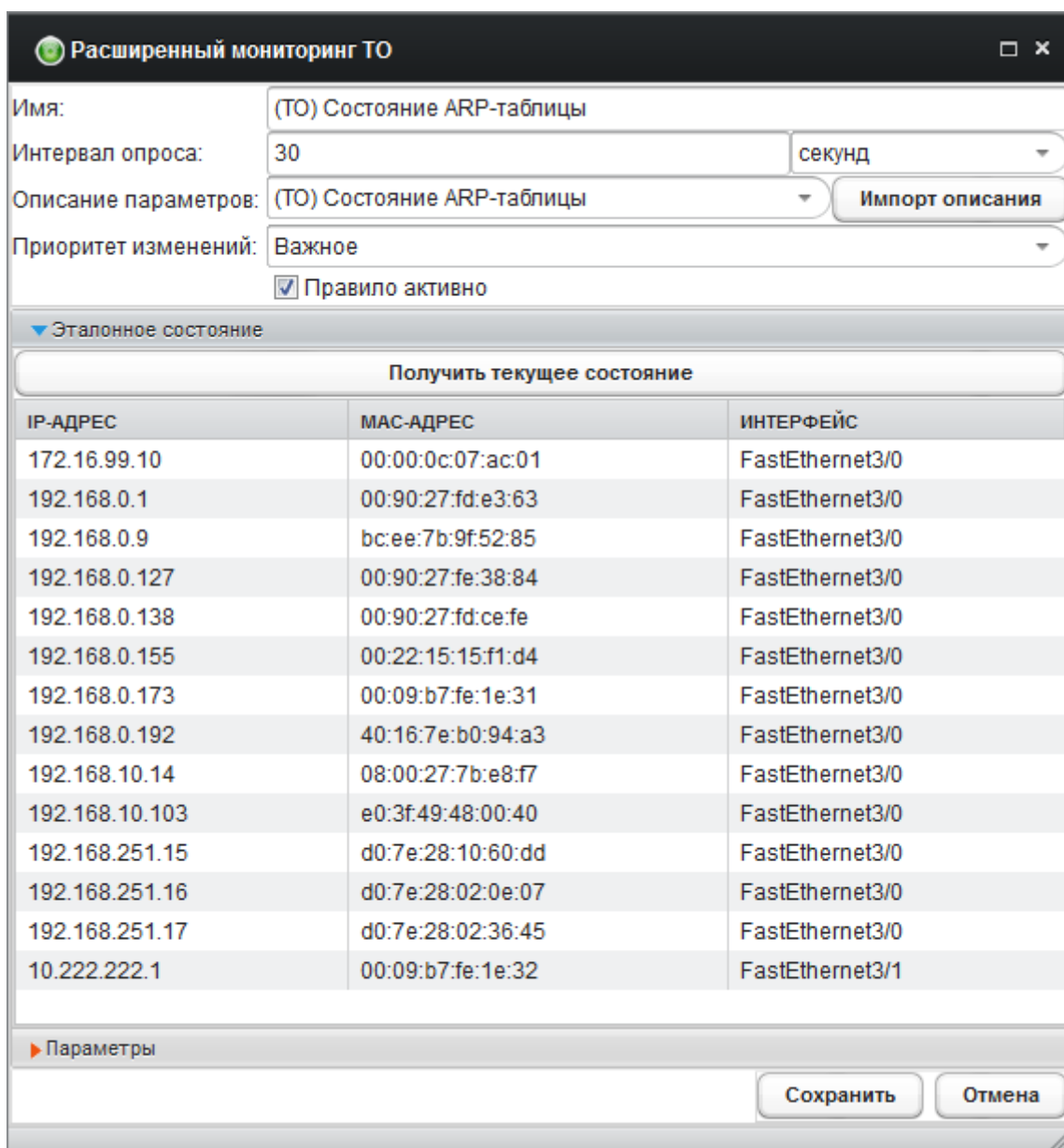
**Важно!** *Определённый сценарий опроса работает лишь в том случае, если в его параметрах установлен флаг «Правило активно» (для любого определяемого сценария флаг устанавливается по умолчанию). Для временной приостановки применения сценария следует снять данный флаг (в этом случае у имён приостановленных сценариев появляется префикс «(ОТКЛЮЧЕНО)»).*

**Важно!** *По завершению внесения изменений в настройки модулей следует выбрать раздел меню «Применить настройки» для их фиксации в БД. Применение настроек происходит массово для всех нижележащих ветвей древа топологии при их наличии, начиная с той ветви, на которой помещается маркёр выделения.*

Применение сценария «Расширенный мониторинг ТО» (Рис. 50) предусматривает определения приоритета фиксации события выбором значения списка «Приоритет изменений»:

- «Информационное»;
- «Важное» (порождает инцидент);
- «Критическое» (порождает инцидент).

Контроль параметров основан на сравнении эталонного и текущего состояний. Для получения и фиксации текущего состояния контролируемого параметра в качестве эталонного с целью последующего сравнения с ним следует нажать кнопку «Получить текущее состояние». По завершению определения остальных параметров сценария и его применения следует нажать кнопку «Сохранить».



Имя: (ТО) Состояние ARP-таблицы

Интервал опроса: 30 секунд

Описание параметров: (ТО) Состояние ARP-таблицы Импорт описания

Приоритет изменений: Важное Правило активно

▼ Эталонное состояние

Получить текущее состояние

IP-АДРЕС	MAC-АДРЕС	ИНТЕРФЕЙС
172.16.99.10	00:00:0c:07:ac:01	FastEthernet3/0
192.168.0.1	00:90:27:fd:e3:63	FastEthernet3/0
192.168.0.9	bc:ee:7b:9f:52:85	FastEthernet3/0
192.168.0.127	00:90:27:fe:38:84	FastEthernet3/0
192.168.0.138	00:90:27:fd:ce:fe	FastEthernet3/0
192.168.0.155	00:22:15:15:f1:d4	FastEthernet3/0
192.168.0.173	00:09:b7:fe:1e:31	FastEthernet3/0
192.168.0.192	40:16:7e:b0:94:a3	FastEthernet3/0
192.168.10.14	08:00:27:7b:e8:f7	FastEthernet3/0
192.168.10.103	e0:3f:49:48:00:40	FastEthernet3/0
192.168.251.15	d0:7e:28:10:60:dd	FastEthernet3/0
192.168.251.16	d0:7e:28:02:0e:07	FastEthernet3/0
192.168.251.17	d0:7e:28:02:36:45	FastEthernet3/0
10.222.222.1	00:09:b7:fe:1e:32	FastEthernet3/1

► Параметры

Сохранить Отмена

Рис. 49. Окно определения параметров сценария расширенного мониторинга ТО.

Осуществление контроля событий системного журнала 'Syslog' ТО производства Cisco Systems, Inc. с помощью сценария «Мониторинг syslog'a ТО» требует от системного администратора ТО, подключенного к АГАТ, настройки сбора событий на IP-адрес АГАТ по протоколу UDP на порт '514' (значение, принятое по умолчанию для всех устройств Cisco).

Параметры контроля этого сценария представлены в табличной форме, организованной аналогично представлению параметров сценария «Сетевой мониторинг» (Рис. 50).

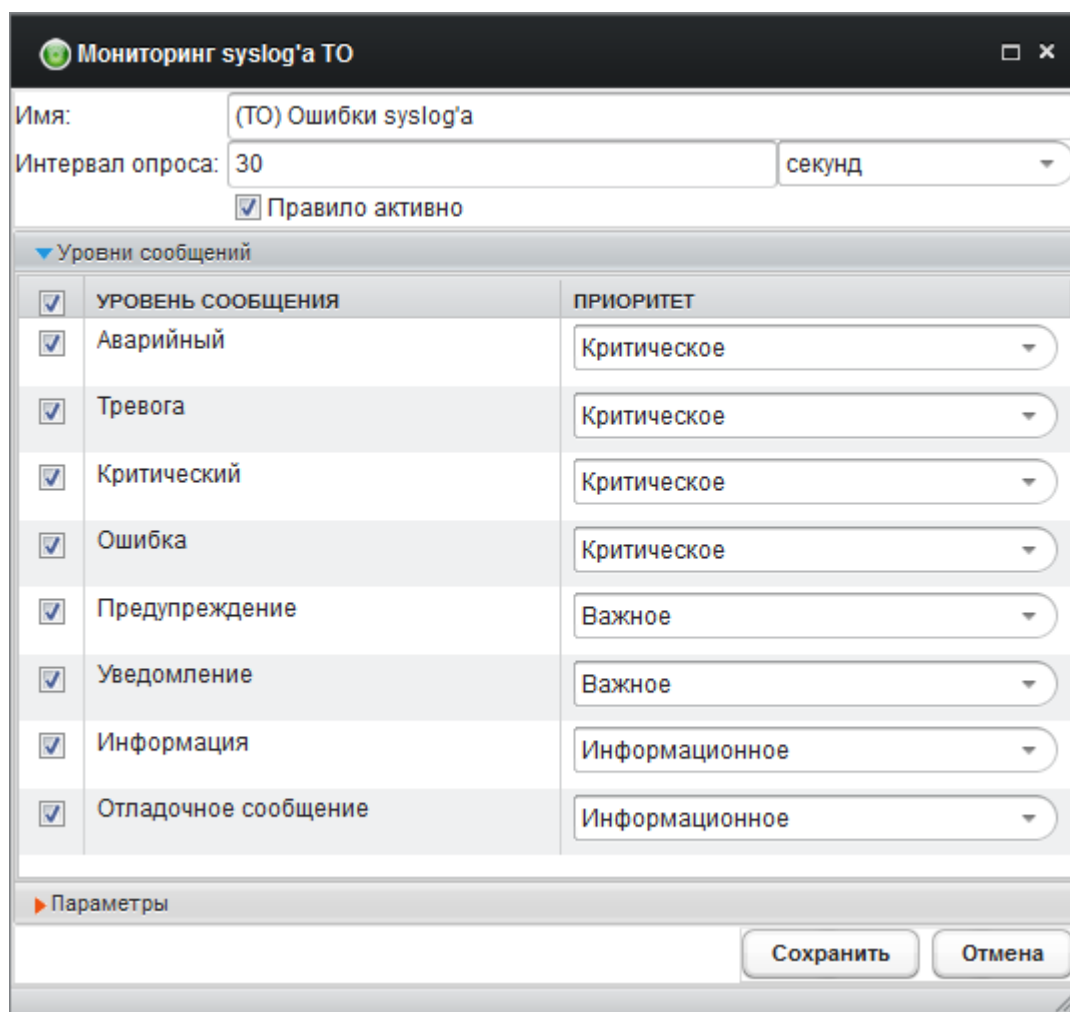


Рис. 50. Окно определения параметров сценария мониторинга 'Syslog'.

Список «Уровень сообщения» определяет набор видов сообщений, требующих контроля и управляется соответствующими флагами первой графы. Список включает следующие виды сообщений:

- «Аварийный» ('Emergencies', уровень '0');
- «Тревога» ('Alerts', уровень '1');
- «Критический» ('Critical', уровень '2');
- «Ошибка» ('Errors', уровень '3');
- «Предупреждение» ('Warning', уровень '4');
- «Уведомление» ('Notifications', уровень '5');
- «Информация» ('Informational', уровень '6');
- «Отладочное сообщение» ('Debugging', уровень '7').

Каждый уровень сообщения снабжён списком «Приоритет», определяющим уровень приоритета фиксации события в журнале инцидентов:

- «*Информационное*»;
- «*Важное*» (порождает инцидент);
- «*Критическое*» (порождает инцидент).

В САИБ предусмотрена возможность динамического контроля работы сценариев опроса в реальном времени с помощью инструмента «Трансляция». Его удобно применять, например, для выбора порогов штатного состояния при деактивированном сценарии во избежание возникновения ложных инцидентов.

Отображение осуществляется в виде графика (Рис. 51) или таблицы (Рис. 52) отражающих текущее состояние на основе определённых параметров штатного состояния.

По достижению пороговых значений цвет фона графика меняется (белый – «нормальное значение», жёлтый – «затруднительное значение», розовый – «критическое значение»).

Для вызова инструмента следует выбрать сценарий, определённый для нужного модуля в древе топологии, и активировать контекстное меню, выбрав пункт *Трансляция*.

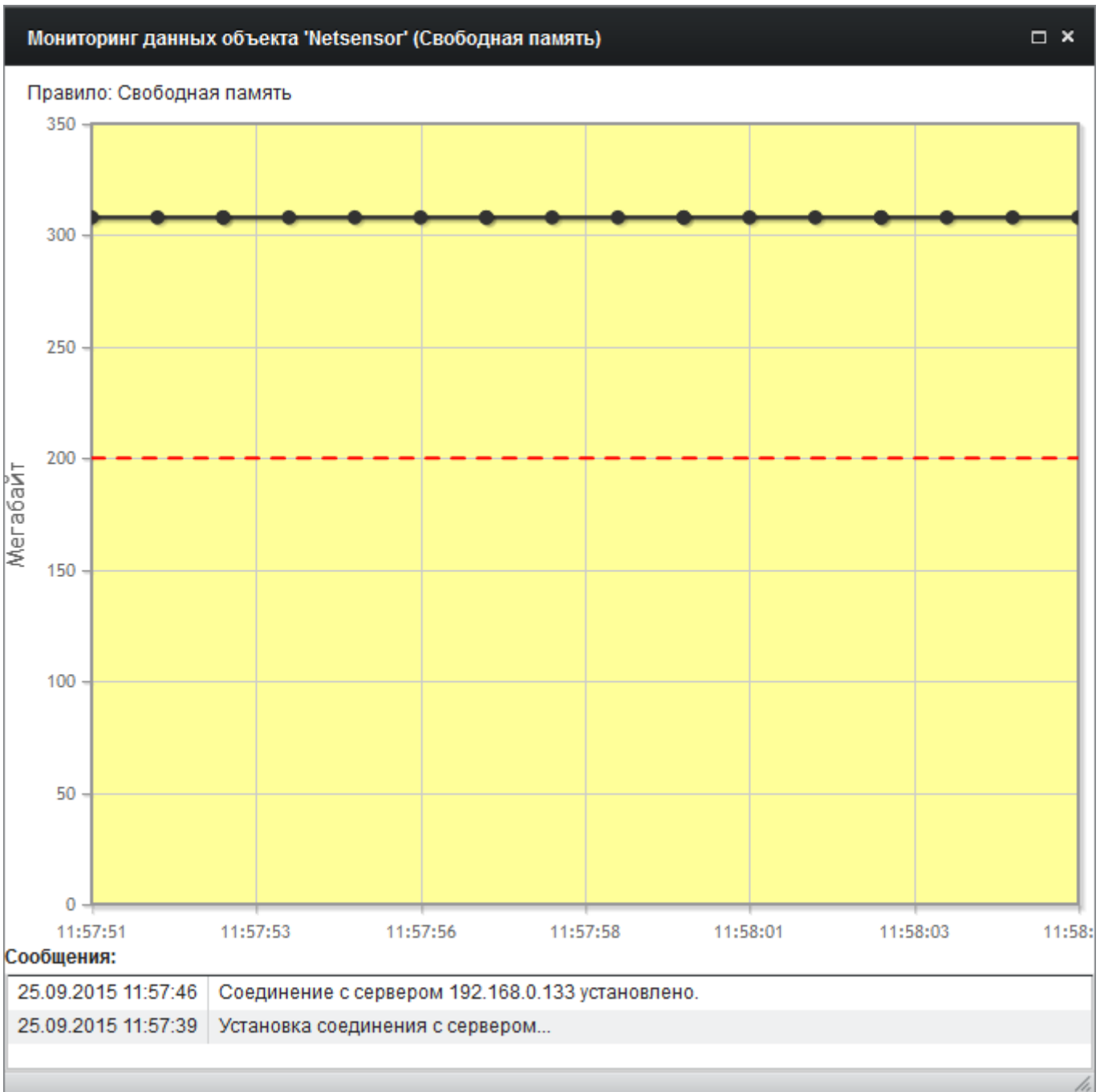


Рис. 51. Окно динамической трансляции сценария сетевого мониторинга (график).

Мониторинг данных объекта 'CISCO' ((ТО) Контроль статуса HSRP (по SNMP))

Правило: (ТО) Контроль статуса HSRP (по SNMP)

Задержка в секундах:

Сообщения трансляции:

ДАТА	СООБЩЕНИЕ
30.09.2015 13:20:18	[1 (active/down/100)]
30.09.2015 13:20:15	[1 (active/down/100)]
30.09.2015 13:20:13	[1 (active/down/100)]
30.09.2015 13:20:10	[1 (active/down/100)]
30.09.2015 13:20:08	[1 (active/down/100)]
30.09.2015 13:20:05	[1 (active/down/100)]

Сообщения:

30.09.2015 13:20:04	Соединение с сервером 192.168.253.178 установлено.
30.09.2015 13:19:58	Установка соединения с сервером...

Рис. 52. Окно динамической трансляции сценария сетевого мониторинга (таблица).

Список «Задержка в секундах», предусмотренный для отдельных видов трансляций, позволяет определить задержку обновления данных с целью снижения нагрузки на СУ и ТО. Предусмотрен выбор из значений '1', '2' (по умолчанию), '5', '10', '15' и '30' секунд.

Список трансляций всех сценариев, определённых для выбранного модуля, можно получить во вкладке «Сетевой сенсор» инструмента «Панель

мониторинга», который вызывается из раздела меню *Инструменты* → *Панель мониторинга* окна «Настройка модулей» (Рис. 53). Выбрав указателем мыши нужную трансляцию следует выбрать раздел меню *Действия над трансляциями* → *Открыть трансляцию в новом окне*.

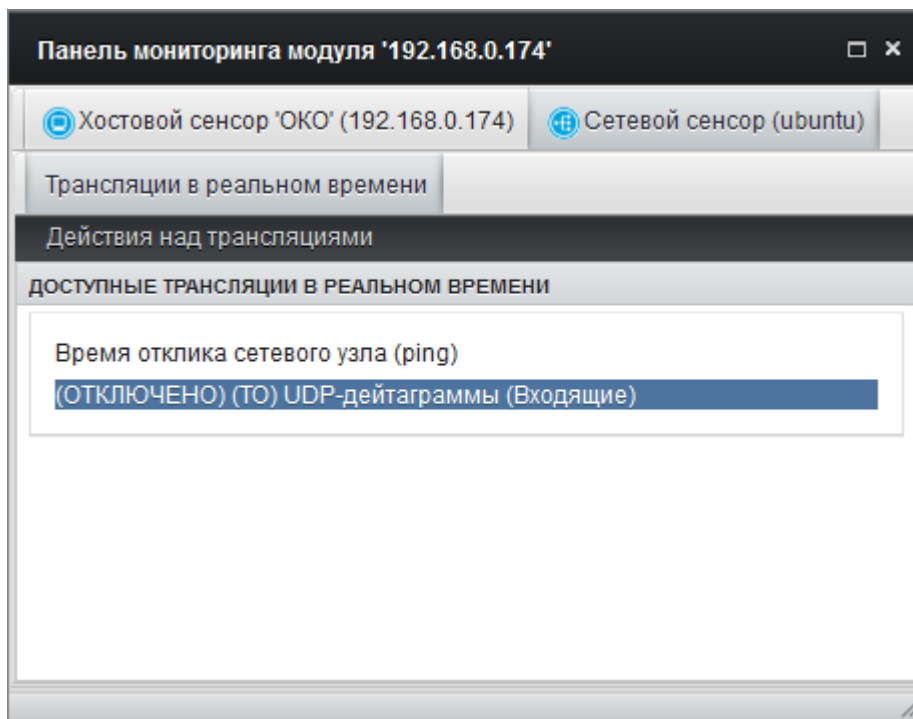


Рис. 53. Трансляции сценариев опроса в инструменте «Панель мониторинга».

Также из раздела контекстного меню «Сетевой сенсор» модуля доступен вызов инструмента «Последний незакрытый инцидент» (см. п. 5.7.8 настоящего документа).



## 5.6. Настройка контроля датчиков и ТО

Если к САИБ подключен аппаратный агент мониторинга серверного оборудования и телекоммуникационных средств АГАТ, то в дополнение к функциональным возможностям, предоставляемым сетевым сенсором, появляется возможность сбора данных мониторинга внешних датчиков и ТО, подключенных к АГАТ. Набор правил для АГАТ включает:

- *«Расширенный мониторинг ТО»* (расширен по сравнению с набором для сетевого сенсора);
- *«Настройка датчика АГАТ»*;
- *«Сетевой мониторинг»* (расширен по сравнению с набором для сетевого сенсора);
- *«Мониторинг syslog'a ТО»* (аналогично сетевому сенсору);
- *«Настройка опроса встроенного датчика вибрации»*;
- *«Настройка удаленного управления ТО»*.

АГАТ включает все сценарии сетевого мониторинга, предусмотренные для сетевого сенсора, а также два дополнительных сценария, применимых для мониторинга состояния устройства АГАТ («Сетевой мониторинг»):

- *«(Агат) Входящий сетевой трафик»*;
- *«(Агат) Исходящий сетевой трафик»*;
- *«(Агат) Свободное место для хранения журнальных файлов»*.

Также к устройству АГАТ применимы сценарии контроля локальных параметров, помеченные признаком ‘(\*)’ в п. 5.5 настоящего документа.

Сценарий опроса «Расширенный мониторинг ТО» включает контроль всех параметров, предусмотренных для аналогичного сценария сетевого сенсора, но по сравнению с последним расширен возможностями контроля параметров ТО при его подключении к одному из интерфейсов RS-232 АГАТ:

- *«(ТО) Контроль целостности IOS по RS-232»*;
- *«(ТО) Контроль целостности загрузочной конфигурации (startup-config) по RS-232»*;

- «(ТО) Контроль целостности памяти по RS-232»;
- «(ТО) Контроль целостности рабочей конфигурации (*running-config*) по RS-232»;
- «(ТО) Контроль целостности списков доступа (ACL) по RS-232»;
- «(ТО) Контроль целостности флеш-диска по RS-232»;
- «(ТО) Регистрация и учет tcp-сессий по RS-232»;
- «(ТО) Регистрация и учет VPN по RS-232»;
- «(ТО) Регистрация и учет xDSL по RS-232».

Для контроля данных параметров ТО следует подключить к одному из интерфейсов RS-232 (порту COM) АГАТ и указать его номер в качестве значения параметра «Номер порта» раздела «Подробные настройки» сценария «Расширенный мониторинг ТО» (см. Рис. 47).

АГАТ оборудован встроенным датчиком вибрации, который настраивается сценарием «Настройка опроса встроенного датчика вибрации» аналогично «Сетевому мониторингу» сетевого сенсора.

В отличие от сценария «Сетевого мониторинга» сетевого сенсора, аналогичные настройки для АГАТ содержат дополнительную возможность отображения результатов исполнения сценария на сенсорном экране устройства АГАТ выбором одного из режимов списка «Скринсейвер»:

- «Не отображать» (по умолчанию);
- «Отображать как график» (аналогично инструменту «Трансляция» сетевого сенсора);
- «Отображать как текст» (в форме таблицы с параметрами и значениями);
- «Отображать как график за сутки».

Циклическая демонстрация выполняется в динамическом режиме в виде графиков и таблиц наравне с демонстрацией диагностических параметров устройства АГАТ. При достижении пороговых значений цвет отображения графика меняется.

Также сенсорный экран устройства АГАТ может отобразить произвольный текст, определённый в САИБ (например, уведомление о проведении регламентных работ). Для определения текстового сообщения следует выбрать раздел главного меню *Система → Настройки → Настройка модулей*.

Затем в древе топологии следует выбрать нужный модуль АГАТ с помощью левой кнопки мыши и открыть контекстное меню, выбрав пункт *АГАТ → Сообщение для скринсейвера* (то же осуществляет выбор раздела меню *Инструменты → АГАТ → Сообщение для скринсейвера*).

В дочернем диалоговом окне следует установить флаг «Отобразить текст» и в поле «Текст» ввести текст для отображения на сенсорном экране АГАТ. По окончании определения параметров следует нажать кнопку «Сохранить». После применения настроек сообщение будет отображаться в наборе экранов циклической демонстрации. Снятие флага «Отобразить текст» позволяет отменить отображение сообщения без необходимости его удаления.

АГАТ осуществляет взаимодействие со следующими типами датчиков и соответствующих им модулей САИБ:

- Датчик вибрации (встроенный, отдельным модулем не представлен и настраивается правилом «Настройка опроса встроенного датчика вибрации», применимым к модулю «АГАТ»);
- «Датчик температуры» (правило «Настройка датчика АГАТ»);
- «Пожарная сигнализация» (правило «Настройка датчика АГАТ»);
- «Концевой переключатель» (правило «Настройка датчика АГАТ»);
- «Дверной замок» (правило «Настройка датчика АГАТ»);
- «Настраиваемый датчик Агат» (правило «Настройка датчика АГАТ»);
- «Датчик движения» (правило «Настройка датчика АГАТ»);

- «Датчик влажности» (правило «Настройка датчика АГАТ»);
- «Датчик контроля протечки воды» (правило «Настройка датчика АГАТ»).

Для контроля в САИБ датчика, подключенного к АГАТ, следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*, а затем выбрать раздел меню *Объекты и правила* → *Добавить объект*. В списке «Тип модуля» дочернего диалогового окна следует выбрать датчик нужного типа и нажать кнопку «Создать» (см. также п. 5.2 настоящего документа).

После создания следует выбрать датчик в древе топологии и переключить окно свойств в режим отображения «Правила» (см. Рис. 29).

Затем в разделе свойств «АГАТ» следует выбрать пункт «Настройка датчика АГАТ» и нажать кнопку «Настроить правило», либо дважды щёлкнуть левой кнопкой мыши по выбранному типу. Применить сценарий к выбранному в текущий момент модулю можно также методом захвата и перетаскивания мышью пункта свойств «Настройка датчика АГАТ».

После этого следует запрос на определение средства мониторинга (Рис. 54), в котором указателем мыши или клавишами управления курсором клавиатуры из древа доступных в САИБ серверов мониторинга типа «АГАТ» следует выбрать нужный и нажать кнопку «Выбрать».

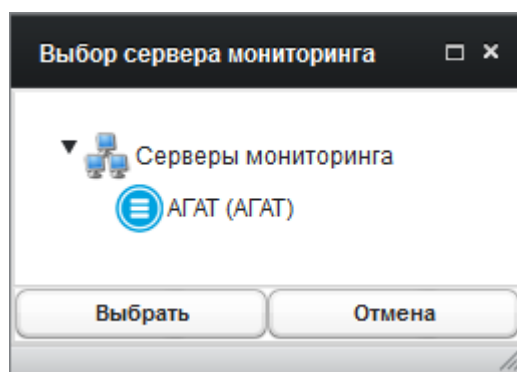


Рис. 54. Окно выбора средства мониторинга.

В целях облегчения массового применения сценариев опроса к модулям выбранное средство мониторинга будет использоваться по умолчанию (текущий выбор отражается включением имени выбранного сенсора в скобках

после наименования в разделе «АГАТ» свойств «Правила»). Для отмены выбора и повторного запроса на определение средства мониторинга при последующем применении сценария опроса следует дважды щёлкнуть левой кнопкой мыши по текущему наименованию раздела «АГАТ».

После определения средства мониторинга последует запрос настройки параметров датчика (Рис. 47).

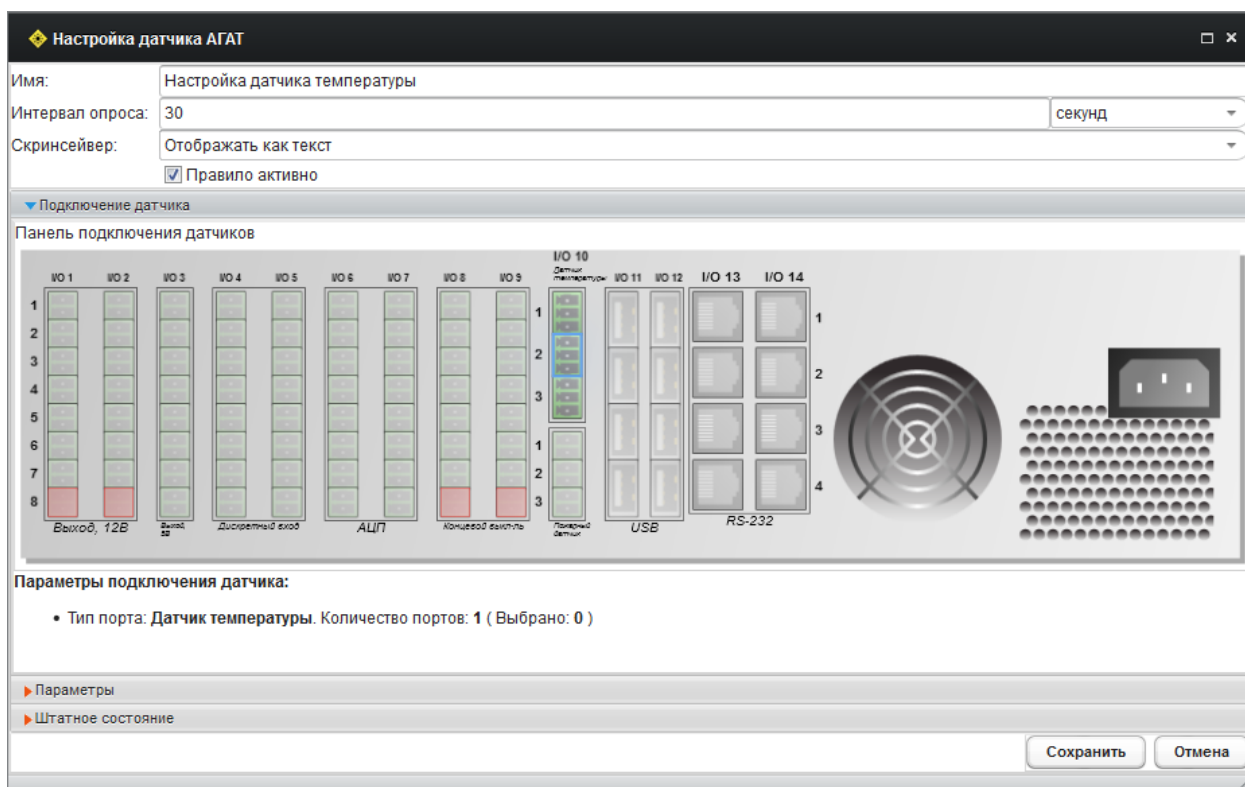


Рис. 55. Окно настройки датчика АГАТ.

В окне следует определить значение «Интервал опроса» (чем короче интервал, тем чаще актуальные данные будут поступать в САИБ для анализа). Значение может быть определено в единицах, выбираемых в дополнительном списке:

- «миллисекунд»;
- «секунд» (по умолчанию);
- «минут»;
- «часов»;
- «дней».

При необходимости следует выбрать из списка «Скринсейвер» нужный режим отображения состояния датчика на сенсорном экране устройства АГАТ (см. выше).

Затем в разделе «Подключение датчика» на схеме задней панели АГАТ следует визуально указать физический интерфейс (разъём), к которому подключен добавленный датчик. При этом в зависимости от типа датчика доступными для выбора будут лишь группы интерфейсов (подсвечиваются зелёным цветом), предназначенные для подключения датчика указанного типа.

*Примечание.* С целью упрощения выбора нужного разъёма на схеме в разделе «Параметры подключения датчика» указывается тип и количество портов, требуемые для подключения датчика выбранного типа. Также раздел позволяет проконтролировать подключение всех разъёмов датчика по количеству портов.

Цифра, отображаемая на интерфейсе при наведении на него указателя мыши, обозначает номер контакта, обеспечивающий корректность подключения датчиков, требующих подключения нескольких разъёмов к разным функциональным группам интерфейсов.

Занятые интерфейсы (подсвечиваются красным цветом), по которым в САИБ уже зарегистрировано подключение датчиков, для новых подключений недоступны вплоть до изменения настроек соответствующих датчиков.

Для выбора интерфейса подключаемого датчика следует щёлкнуть левой кнопкой мыши по изображению нужного интерфейса на задней панели (выбранный интерфейс будет подсвечен синим).

*Примечание.* С целью упрощения процедуры физического подключения внешних датчиков к АГАТ целесообразно сперва подключить их в графическом интерфейсе администратора САИБ (виртуально), затем получить отчёт «По подключению датчиков» (см. п. 7 настоящего документа), а уже после этого выполнять физическое подключение датчиков

*к разъёмам коммуникационных интерфейсов задней панели АГАТ в соответствии с данными полученного отчёта.*

Назначение разделов «Параметры» и «Штатное состояние» аналогично описанным для сценариев опроса сетевого сенсора, но с учётом специфики датчиков (отдельные их типы требуют определения нестандартных нормальных и/или критических значений).

Определив все необходимые параметры датчика, следует нажать кнопку «Сохранить» для фиксации настроек в БД.

Настройки, определённые для каждого из датчиков АГАТ, также отображаются в древе топологии в виде вложений в модуль (см. Рис. 30).

При выборе настроек определённого датчика в окне свойств отображается его описание и установленные параметры, что позволяет текстуально оценить корректность настройки.

Внесение изменений в ранее определённые настройки осуществляется по двойному щелчку левой кнопки мыши по нужным настройкам либо выбором раздела меню *Объекты и правила* → *Редактировать правило*.

***Важно!*** *Определённый сценарий опроса (профиль настройки датчика) работает лишь в том случае, если в его параметрах установлен флаг «Правило активно» (для любого определяемого сценария или профиля флаг устанавливается по умолчанию). Для временной приостановки применения сценария (профиля настроек) следует снять данный флаг (в этом случае у имён приостановленных сценариев или профилей появляется префикс «(ОТКЛЮЧЕНО)»).*

***Важно!*** *По завершению внесения изменений в настройки модулей следует выбрать раздел меню «Применить настройки» для их фиксации в БД. Применение настроек происходит массово для всех нижележащих ветвей древа топологии при их наличии, начиная с той ветви, на которой помещается маркёр выделения.*

Предусмотрена возможность динамического контроля работы сенсоров в реальном времени с помощью инструмента «Трансляция». Его удобно применять, например, для выбора порогов штатного состояния при деактивированном датчике во избежание возникновения ложных инцидентов.

Для вызова инструмента следует выбрать настройки, определённые для нужного датчика в древе топологии, и активировать контекстное меню, выбрав пункт «Трансляция».

В дополнение к видам отображения трансляции сетевого сенсора, трансляция состояний датчиков АГАТ осуществляется в виде сигнализатора «светофор» (Рис. 56), отражающего текущее состояние на основе определённых параметров штатного состояния.

По достижению пороговых значений сигналы «светофора» переключаются (зелёный – «нормальное значение», жёлтый – «затруднительное значение», красный – «критическое значение»).



Рис. 56. Окно трансляции состояния датчика («светофор»).

Для модуля АГАТ доступна панель мониторинга (Рис. 57), отображающая трансляции всех встроенных датчиков при их определении (вкладка «Трансляции в реальном времени»), а также вид задней панели



устройства АГАТ с возможностью просмотра интерфейсов и подключенных к ним датчиков.

Инструмент вызывается из раздела меню *Инструменты* → *Панель мониторинга* окна «Настройка модулей». Выбрав указателем мыши нужную трансляцию следует выбрать раздел меню *Действия над трансляциями* → *Открыть трансляцию в новом окне*.

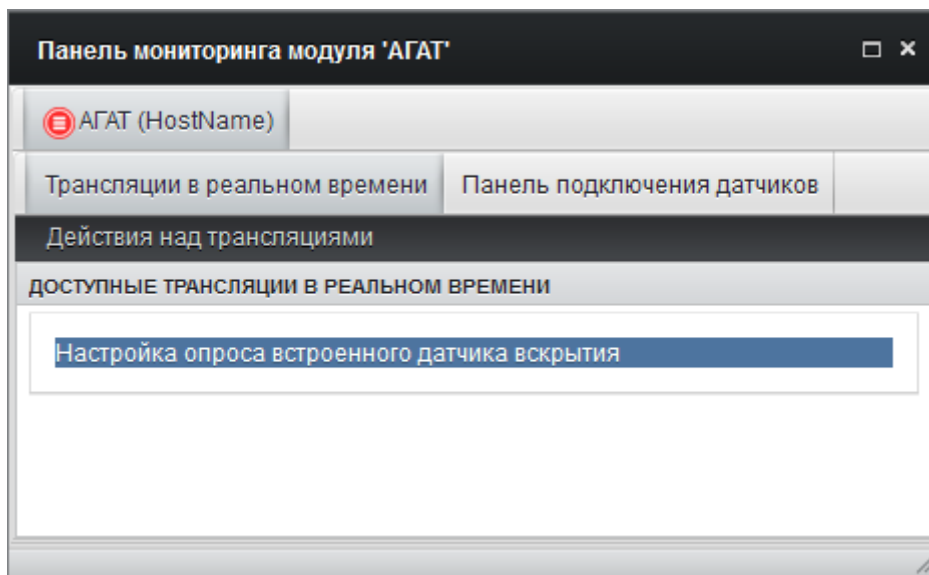


Рис. 57. Трансляции датчиков АГАТ в инструменте «Панель мониторинга».

Также из раздела контекстного меню «АГАТ» модуля доступен вызов инструмента «Последний незакрытый инцидент» (см. п. 5.7.8 настоящего документа).

### **5.7. Мониторинг и принудительное управление контролируемыми рабочими местами**

РС, установленные на контролируемых рабочих местах, обеспечивают не только сбор, анализ и реагирование на определённые события программной среды, но и позволяют осуществлять непосредственный контроль за функционированием рабочих мест и действиями пользователя в реальном времени.

Для этого в САИБ предусмотрены следующие инструменты:

- *«Системный монитор»* служит для оценки производительности контролируемого рабочего места;
- *«Видеотрансляция»* осуществляет непрерывную трансляцию снимков экрана выбранного сеанса пользователя контролируемого рабочего места;
- *«Монитор событий»* отражает текущие события, в отношении которых произошли нарушения правил, определённых для контролируемого рабочего места;
- *«Менеджер задач»* отражает текущие процессы, все службы, учётные записи пользователей, профиль аппаратной конфигурации контролируемого рабочего места, а также позволяет физически выключить или перезагрузить компьютер удалённо;
- *«Просмотр снимков экрана»* обеспечивает доступ к снимкам экрана, собранным при срабатывании условий правила типа «Контроль процессов» в случае определения соответствующего значения в списке «Дополнительное действие» (см. п. 5.3.6 настоящего документа);
- *«Просмотр аппаратных конфигураций»* обеспечивает доступ к результатам проверки аппаратной конфигурации контролируемого рабочего места при определении для него

правила типа «Контроль аппаратной конфигурации» (см. п. 5.3.4 настоящего документа);

- «*Последний незакрытый инцидент*» отображает последний инцидент, зафиксированный РС на контролируемом рабочем месте (см. п. 5.7.8 настоящего документа).

Для применения выбранного инструмента мониторинга следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей*, отыскать и выбрать в древе топологии нужный модуль, оснащённый РС. После этого нужно выбрать раздел меню *Инструменты* → *Хостовой сенсор 'ОКО'* и из подраздела выбрать один из инструментов мониторинга, перечисленных выше.

Контекстное меню, вызываемое правой кнопкой мыши при выборе определённого объекта мониторинга, позволяет ускорить работу с инструментами.

### **5.7.1 Системный монитор**

Инструмент служит для оценки производительности контролируемого рабочего места и по своим функциям схож с вкладкой «Быстродействие» Диспетчера задач ОС семейства Microsoft Windows. В САИБ инструмент содержит две вкладки.

**Вкладка «Быстродействие»** (Рис. 58) отображает сведения о версии САИБ и дате её выпуска, а также о наименовании ОС и её версии.

Данные о процентной загрузке ЦП и хронологии загрузки ЦП представлены в динамике реального времени. На панели «Память» отображается общий объём доступной оперативной памяти и объём памяти, используемый в текущий момент времени. На панели «Диски» отображается доступный и свободный объём дискового пространства.

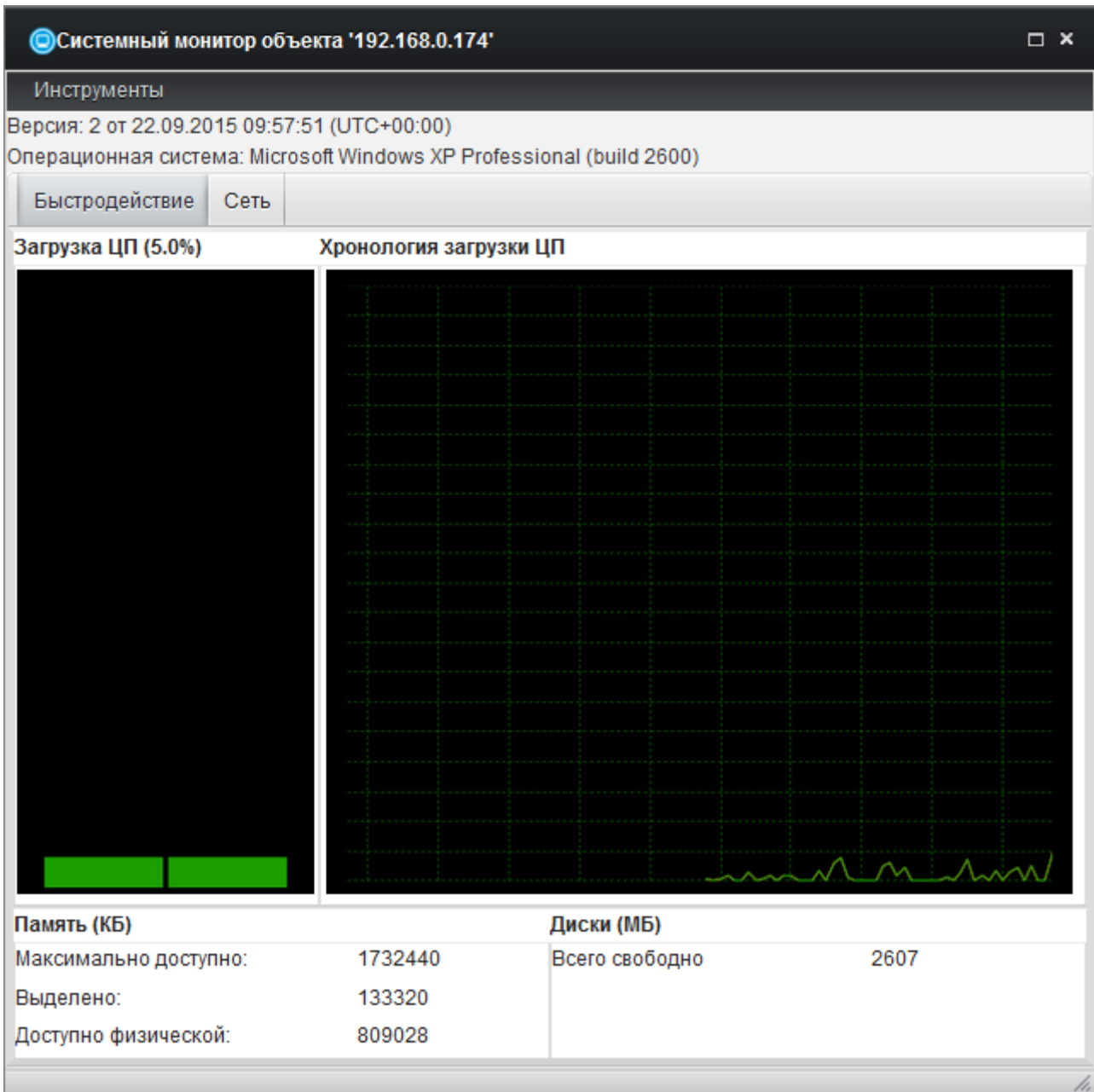


Рис. 58. Вкладка «Быстродействие» инструмента «Монитор ресурсов».

**Вкладка «Сеть»** (Рис. 59) позволяет наглядно контролировать текущий суммарный сетевой трафик в разрезе отдельных сетевых адаптеров, входящих в аппаратную конфигурацию контролируемого рабочего места.

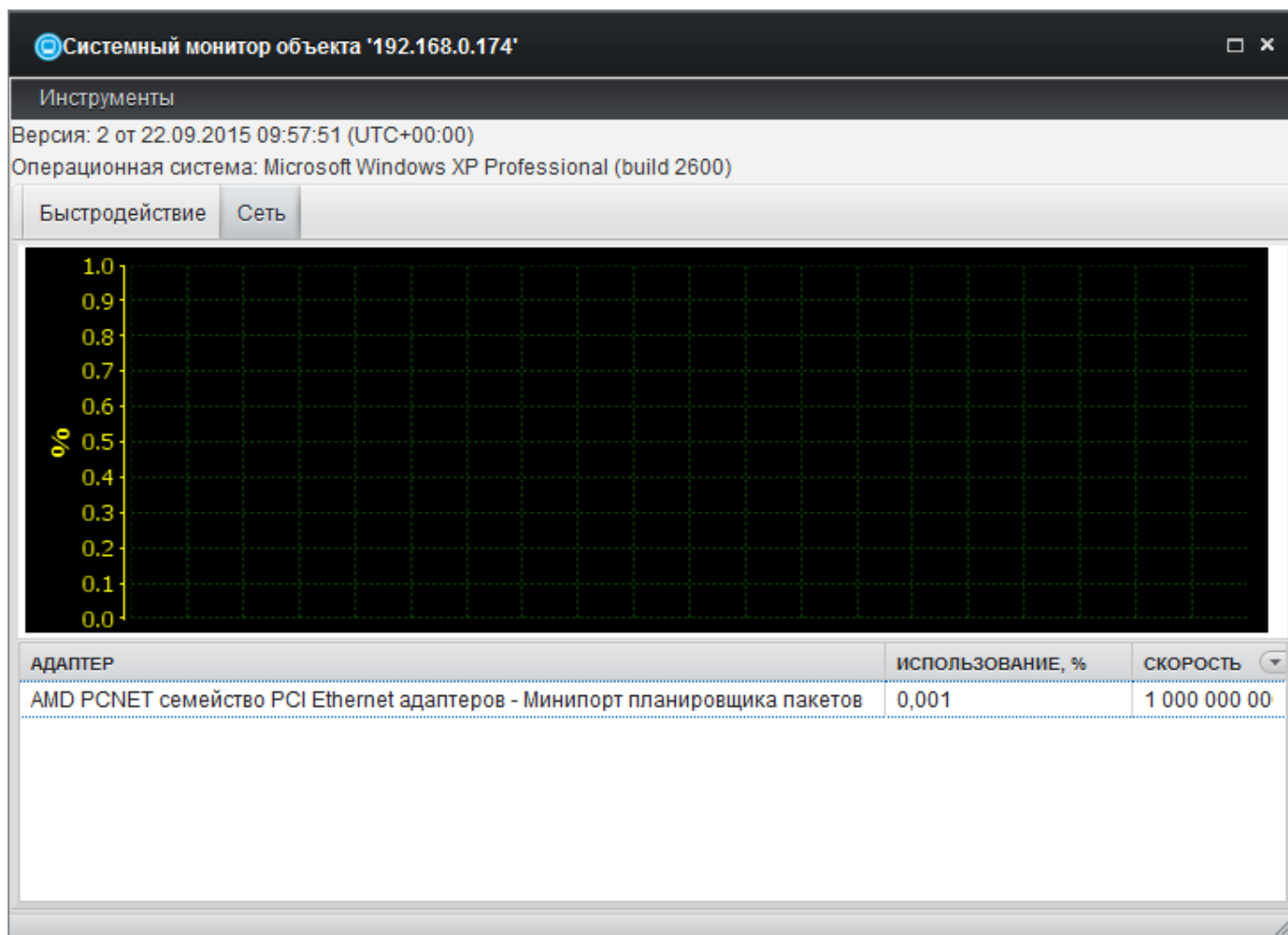


Рис. 59. Вкладка «Сеть» инструмента «Монитор ресурсов».

Единственный раздел меню *Инструменты* → *Менеджер задач* открывает инструмент «Менеджер задач» (см. п. 5.7.4 настоящего документа) непосредственно из «Монитора событий».

*Примечание.* Инструмент применим лишь в период работы компьютера контролируемого рабочего места (требуется активный PC, передающий данные на Сервер для отображения в инструменте).

### 5.7.2 Видеотрансляция

Инструмент служит для трансляции в графический интерфейс администратора текущих действий пользователя контролируемого рабочего места в режиме реального времени.

В окне инструмента (Рис. 60) с помощью списка «Сессия» доступен выбор сеанса, который требуется транслировать для просмотра администратором.

*Примечание.* Если список «Сессия» включает единственное значение 'Nobody' (выбирается по умолчанию), то на контролируемом рабочем месте отсутствуют активные сеансы пользователей.

Установка флага «Соблюдать пропорции» обеспечивает трансляцию с сохранением пропорций экрана контролируемого рабочего места независимо от настроек рабочего места, на котором эксплуатируется графический интерфейс администратора.

Ползунок «Качество» позволяет управлять степенью сжатия при непрерывной трансляции потока снимков экрана (кадров) во избежание их потерь и снижения нагрузки на Сервер. Значение по умолчанию – 50 %.

Ползунок «Задержка» определяет задержку между захватом двух отдельных снимков экрана, т.е. скорость смены кадров: чем дольше задержка, тем реже обновляется вид экрана в окне трансляции. Значение по умолчанию – 2 сек.

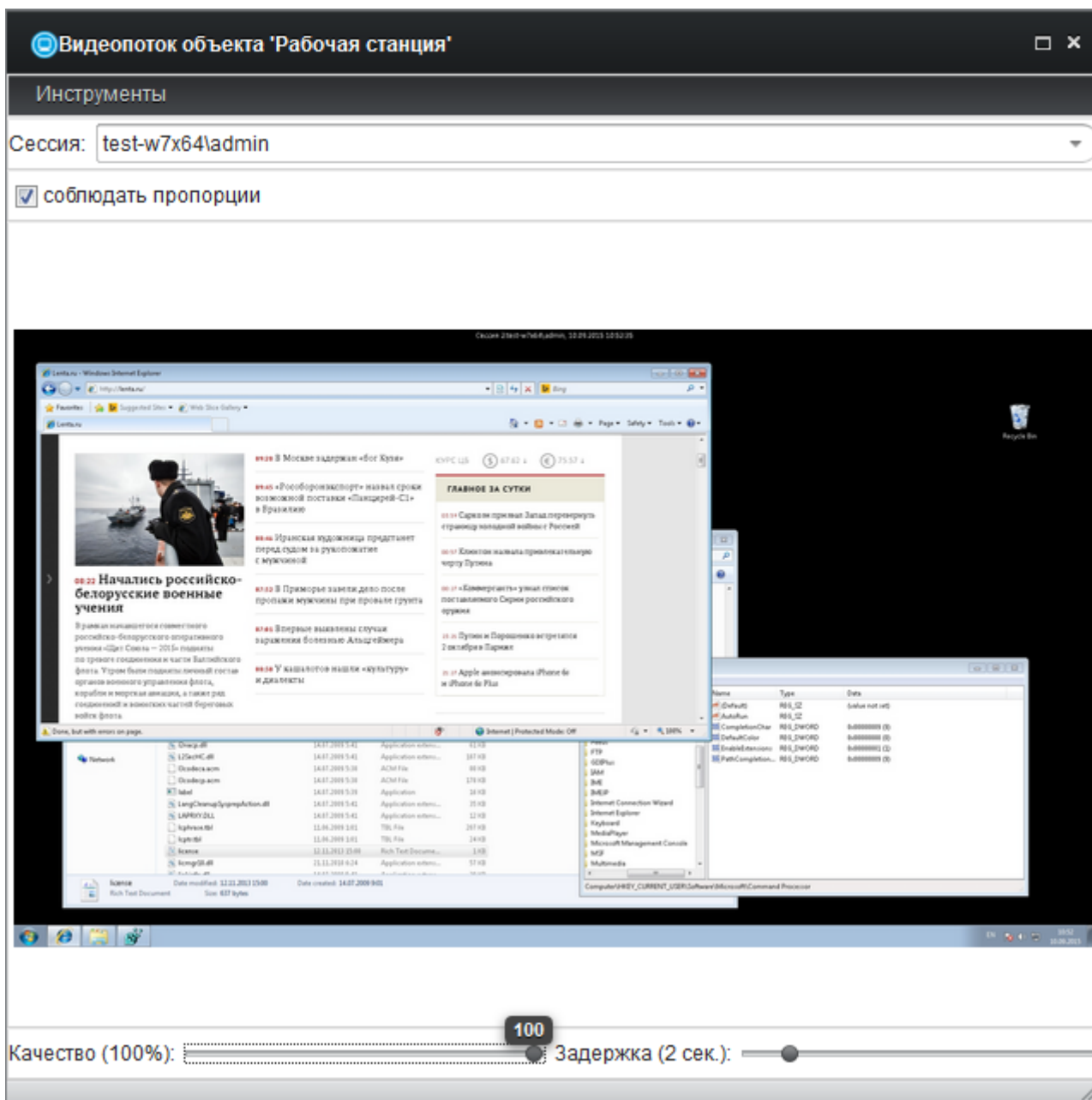


Рис. 60. Инструмент «Видеотрансляция».

Единственный раздел меню *Инструменты* → *Менеджер задач* открывает инструмент «Менеджер задач» (см. п. 5.7.4 настоящего документа) выбранного рабочего места непосредственно из «Монитора событий».

*Примечание.* Инструмент применим лишь в период работы компьютера контролируемого рабочего места (требуется активный PC, передающий данные на Сервер для отображения в инструменте).

### 5.7.3 Монитор событий

Инструмент (Рис. 61) отражает текущие события программной среды, а также события, нарушившие правила, определённые для контролируемого рабочего места.

Список в верхней части окна позволяет установить режим отображения событий в мониторе:

- «Показывать все события» (по умолчанию);
- «Критические события» (расцениваются инцидентными);
- «Критические и важные события» (расцениваются инцидентными).

Хронология событий, отвечающих заданному критерию отбора, отображается в таблице, содержащей параметры фиксации события по графам:

- «Дата» содержит дату и время наступления события;
- «Событие» отражает вид наступившего события (нарушенное условие или правило контроля);
- «Уровень» указывает уровень приоритета инцидентности события, определённое параметром нарушенного правила: «Информационное событие», «Важное событие» или «Критическое событие»;
- «Сообщение» приводит атрибуты события с указанием статуса операции и реакции САИБ, определённой параметром нарушенного правила.

Фон записей о событиях подкрашивается цветом в зависимости от приоритета инцидентности (информационный – зелёный, важный – жёлтый, критический – розовый).



ДАТА	СОБЫТИЕ	УРОВЕНЬ	СООБЩЕНИЕ
04.09.2015 13:37:53	Запуск процесса	Критическое событие	Реакция: Выведение сообщения пользователю Путь к файлу процесса: C:\Program Files\Windows NT\Accessories\wordpad.exe Контрольная сумма процесса: 715BFF236158F61C042928A53C0D5AA8 Размер файла процесса в байтах: 4583424 Строка запуска процесса: "C:\Program Files\Windows NT\Accessories\WORDPAD.EXE" "C:\Windows\System32\license.rtf" PID процесса: 2724 Пользователь процесса: test-w7x64\admin Идентификатор сессии процесса: 2 Путь к файлу родительского процесса: C:\Windows\explorer.exe Контрольная сумма родительского процесса: AC4C51EB24AA95B77F705AB159189E24 Размер файла процесса родителя в байтах: 2872320 Строка запуска родительского процесса: C:\Windows\Explorer.EXE PID родительского процесса: 2736 Пользователь родительского процесса: test-w7x64\admin Идентификатор сессии родительского процесса: 2 Статус операции: Блокирована Реакция: Выведение сообщения пользователю
04.09.2015 13:28:06	Запуск процесса	Важное событие	Путь к файлу процесса: C:\Program Files\Windows NT\Accessories\wordpad.exe Контрольная сумма процесса: 715BFF236158F61C042928A53C0D5AA8 Размер файла процесса в байтах: 4583424 Строка запуска процесса: "C:\Program Files\Windows NT\Accessories\WORDPAD.EXE" "C:\Windows\System32\license.rtf" PID процесса: 1164 Пользователь процесса: test-w7x64\admin Идентификатор сессии процесса: 2 Путь к файлу родительского процесса: C:\Windows\explorer.exe Контрольная сумма родительского процесса: AC4C51EB24AA95B77F705AB159189E24 Размер файла процесса родителя в байтах: 2872320 Строка запуска родительского процесса: C:\Windows\Explorer.EXE PID родительского процесса: 2736 Пользователь родительского процесса: test-w7x64\admin Идентификатор сессии родительского процесса: 2 Статус операции: Блокирована Реакция: Выведение сообщения пользователю

Рис. 61. Инструмент «Монитор событий объекта».

Перемещение по хронологии осуществляется с помощью страничного навигатора, расположенного над таблицей.

Восходящая (значок ‘▲’) / нисходящая (значок ‘▼’) сортировка хронологии событий осуществляется щелчком левой кнопки мыши по нужной графе. Управление отображением отдельных граф осуществляется по щелчку левой кнопки мыши на значке ‘▼’ с правой стороны строки заголовков граф.

Единственный раздел меню *Инструменты* → *Менеджер задач* открывает инструмент «Менеджер задач» непосредственно из «Монитора событий».

*Примечание.* Инструмент применим как в период работы компьютера контролируемого рабочего места, так и в период его бездействия (в этом случае отображается хронология событий, накопленная в БД к моменту вызова инструмента).

#### 5.7.4 Менеджер задач

Инструмент отражает текущие процессы, все службы (независимо от их текущего состояния), учётные записи всех пользователей, текущий профиль аппаратной конфигурации, а также обеспечивает принудительное управление контролируемым рабочим местом (позволяет физически выключить или перезагрузить компьютер удалённо).

Скрытый	Имя образа	PID	Имя пользователя	Строка запуска	Размер, Б	Сессия	Контрольная сумма
	C:\Windows\System32\svchost.exe	840	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k DcomLaunch	27 136	0	C78655BC80301D76ED4FEF1C1EA40A7D
	C:\Windows\System32\LogonUI.exe	180	NT AUTHORITY\SYSTEM	"LogonUI.exe" /flags:0x0	27 648	1	715F03B4C7223349768013EA95D9E5B7
	C:\Windows\System32\lsass.exe	712	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe	31 232	0	9262D6E2C239EDD6D87B080F2BCCEC9I
	C:\Program Files\Primetech\JaguarServer\Tomcat\bin\Tomcat7.exe	1 684	NT AUTHORITY\SYSTEM	"C:\Program Files\Primetech\JaguarServer\Tomcat\bin\Tomcat7.exe" //RS//Tomcat7	109 696	0	F0EC67A5280737765805614DB4B72355
	C:\Windows\System32\smss.exe	416	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe	112 640	0	DA5EF2CC0764BE7097BAFA9CAF903FE8
	C:\Windows\System32\wininit.exe	576	NT AUTHORITY\SYSTEM	wininit.exe	129 024	0	94355C28C1970635A31B3FE52EB7CEBA

Рис. 62. Вкладка «Процессы» инструмента «Менеджер задач».

Инструмент содержит вкладки «Процессы», «Службы», «Пользователи», «Аппаратная конфигурация» и «Управление» (Рис. 62).

**Вкладка «Процессы»** отражает текущие процессы контролируемого рабочего места. Список процессов представлен в табличной форме и содержит следующие графы:

- «Скрытый» отображает флаг процесса, скрытого от глаз пользователя;
- «Имя образа» содержит символьное наименование образа процесса (обычно – абсолютный путь к исполняемому файлу);

- «PID» содержит цифровой идентификатор процесса;
- «Имя пользователя» содержит идентификатор пользователя, от имени которого выполняется процесс;
- «Строка запуска» содержит абсолютный путь к исполняемому файлу с перечнем параметров запуска;
- «Размер, б» содержит текущий объём памяти, занимаемой образом процесса в байтах;
- «Сессия» содержит цифровой идентификатор сеанса ('0' – системный, '1' – пользовательский);
- «Контрольная сумма» содержит шестнадцатеричную строку контрольной суммы процесса.

*Примечание.* Параметры процессов можно использовать при определении шаблонов и правил контроля событий типа «Контроль процессов» для определения условий вкладки «Приложения» и «Процессы» (см. п. 5.3.6 настоящего документа).

Восходящая (значок '▲') / нисходящая (значок '▼') сортировка списка процессов осуществляется щелчком левой кнопки мыши по нужной графе. Управление отображением отдельных граф осуществляется по щелчку левой кнопки мыши на значке '▼' с правой стороны строки заголовков граф.

Для удалённого запуска на контролируемом рабочем месте нового процесса следует нажать кнопку «Новая задача». Дочернее диалоговое окно запросит имя исполняемого файла, которое следует определить в поле «Путь к файлу запускаемого процесса»: следует указать абсолютный путь относительно программной среды контролируемого рабочего места, например 'C:\WINDOWS\system32\calc.exe'.

Также необходимо выбрать режим исполнения процесса:

- 'Explorer Account' (запуск в консольном режиме – пользователь сеанса наблюдает ход выполнения процесса);

- ‘System Account’ (запуск в скрытом режиме – пользователь сеанса не имеет возможности наблюдать ход выполнения процесса).

Владелец процесса, от имени и в сеансе которого осуществляется его исполнение, определяется выбором значения в списке «Сессия», включающем все активные сеансы пользователей.

*Примечание.* Если список «Сессия» включает единственное значение ‘Nobody’, то на контролируемом рабочем месте отсутствуют активные сеансы пользователей и новый процесс инициировать нельзя.

По завершению определения параметров старт процесса осуществляется кнопкой «ОК».

*Примечание.* Процессы, запущенные с помощью «Менеджера задач», получают привилегии системы и могут предоставлять пользователю дополнительные права.

Для завершения процесса указателем мыши или клавишами управления курсором клавиатуры следует выбрать запись ненужного процесса и нажать кнопку «Завершить процесс» (последует запрос подтверждения принятого решения).

*Примечание.* Завершение работы процесса приложения может привести к утрате не сохранённых данных. Завершение работы процесса системной службы может нарушить функционирование отдельных компонент ОС контролируемого рабочего места.

**Вкладка «Службы»** (Рис. 63) отражает все службы контролируемого рабочего места, независимо от их текущего состояния и позволяет управлять их работой. Список служб представлен в табличной форме и содержит следующие графы:

- «Имя» содержит символьный идентификатор службы;
- «Описание» содержит наименование службы;

- «Состояние» отражает текущее состояние службы («Остановлен» или «Запущен»).

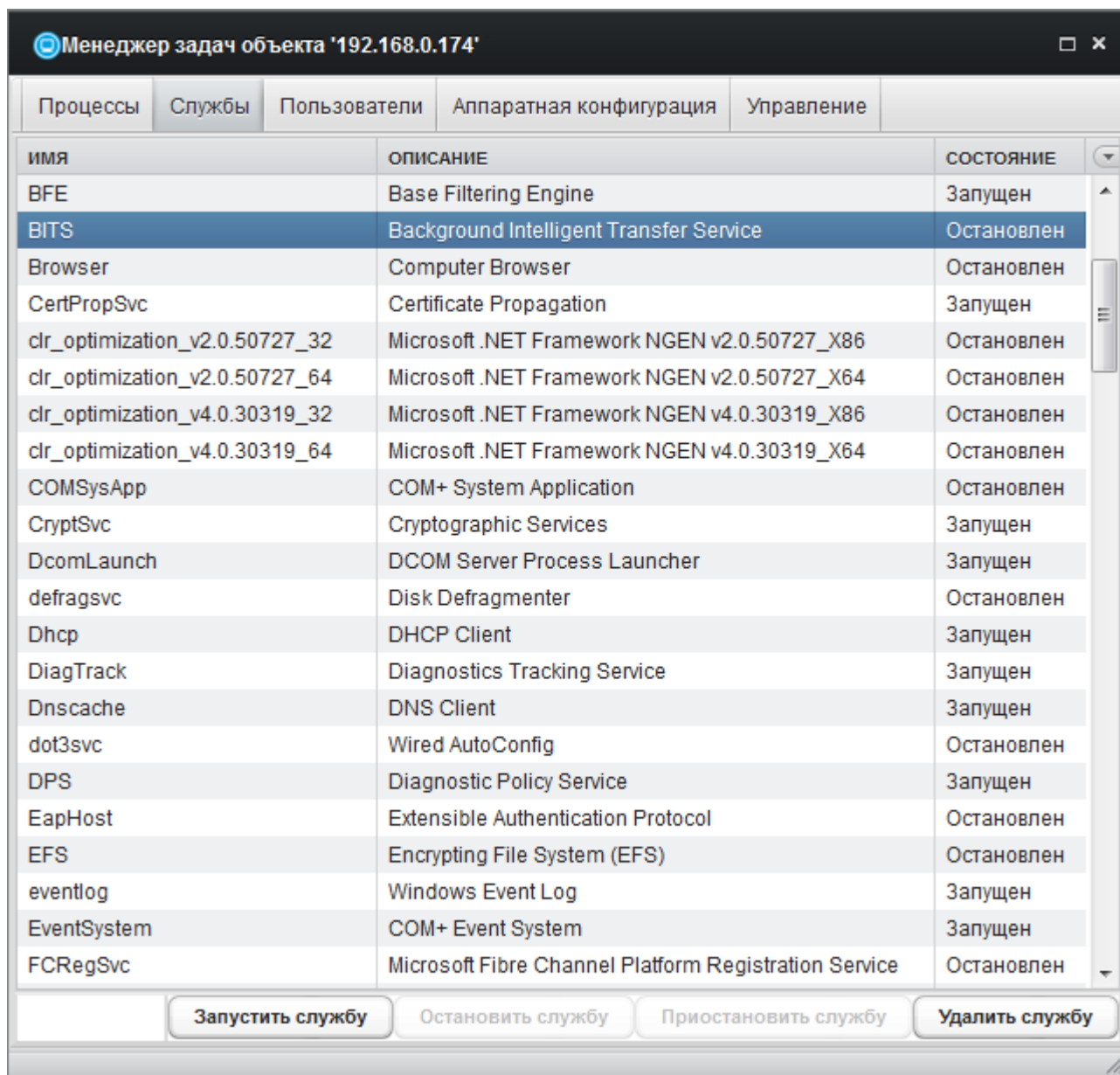


Рис. 63. Вкладка «Службы» инструмента «Менеджер задач».

Например, штатное функционирование САИБ обеспечивают следующие службы Сервера:

- ‘Primetech ОКО Admin Server’ (исполняемый модуль ‘%INSTALLDIR%\servers\admin\ADMServer.exe’) – компонент «Сервер администрирования»;

- ‘Primetech ОКО Web Server’ (исполняемый модуль ‘%INSTALLDIR%\tomcat\bin\tomcat7.exe’) – служба графического интерфейса администратора САИБ;
- ‘Primetech ОКО Report System’ (исполняемый модуль ‘%INSTALLDIR%\ReportSystem\ReportSystem.exe’) – служба системы отчётности САИБ;
- ‘Primetech ОКО Update Server’ (исполняемый модуль ‘%INSTALLDIR%\servers\update\server\UpdateServer.exe’) – компонент «Сервер обновлений».

Клиентская служба ‘Primetech ОКО Update Client’ (исполняемый модуль ‘%INSTALLDIR%\servers\update\client\UpdateClient.exe’) обеспечивает обновление ПО Сервера.

На контролируемом рабочем месте РС представлен службой ‘Primetech ОКО Sensor’ (запускается скрытно).

Управление работой служб осуществляется кнопками «Запустить службу», «Остановить службу», «Приостановить службу» и «Удалить службу». Для выполнения требуемого действия указателем мыши или клавишами управления курсором клавиатуры следует выбрать запись целевой службы и нажать соответствующую кнопку (в зависимости от этого может последовать запрос подтверждения принятого решения).

*Примечание. Останов службы ‘Primetech ОКО Admin Server’ или ‘Primetech ОКО Web Server’ приведёт к выводу из эксплуатации графического интерфейса администратора.*

Восходящая (значок ‘▲’) / нисходящая (значок ‘▼’) сортировка списка служб осуществляется щелчком левой кнопки мыши по нужной графе. Управление отображением отдельных граф осуществляется по щелчку левой кнопки мыши на значке ‘▼’ с правой стороны строки заголовков граф.

Вкладка «Пользователи» (Рис. 64) отражает учётные записи всех пользователей и позволяет управлять ими. Список пользователей представлен в табличной форме и содержит следующие графы:

- «Пользователь» содержит идентификатор пользователя;
- «Группы» содержит список групп, членом которых является данный пользователь;
- «Состояния» содержит текущее состояние пользователя («пусто» для активного пользователя, «Заблокирован» – для пользователя, чья запись временно заблокирована администратором сервера либо администратором САИБ).

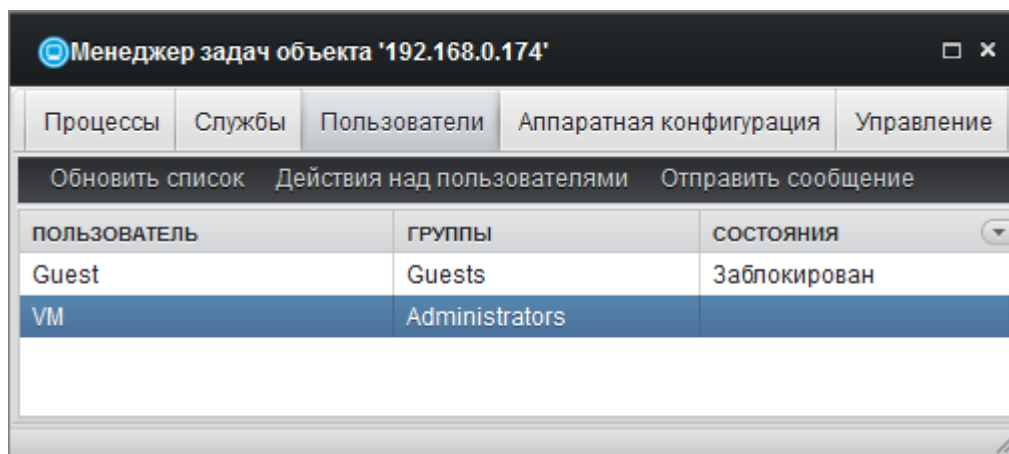


Рис. 64. Вкладка «Пользователи» инструмента «Менеджер задач».

Для просмотра свойств пользователя следует дважды щёлкнуть левой кнопкой мыши по соответствующей записи списка.

Инструмент позволяет выполнять различные действия над учётными записями пользователей контролируемого рабочего места. Для этого следует выбрать соответствующий пункт раздела меню «Действия над пользователями»:

- «Создать» – для создания нового пользователя (последует запрос его идентификатора);
- «Удалить» – для удаления существующего пользователя (последует запрос подтверждения принятого решения);

- «Свойства» – для просмотра свойств существующего пользователя, добавления его учётной записи в группы и блокировки;
- «Задать пароль» – для изменения текущего пароля пользователя (последует запрос нового пароля).

Дочернее окно свойств пользователя (Рис. 65) позволяет заблокировать учётную запись выбранного пользователя, а также добавить её в нужные группы пользователей.

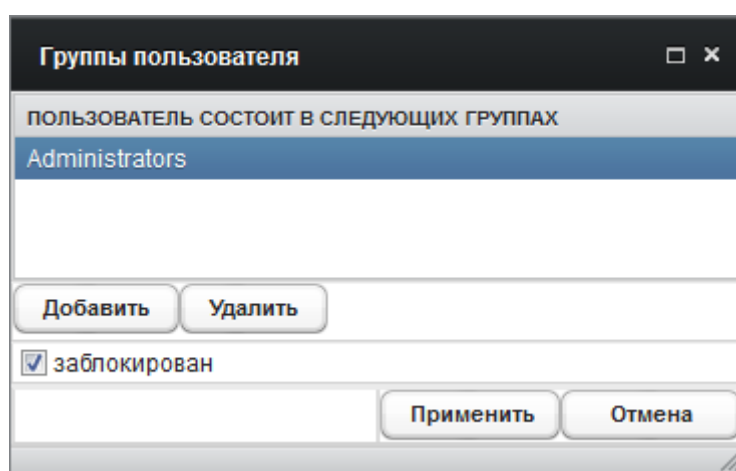


Рис. 65. Окно свойств пользователя.

Блокировка учётной записи осуществляется установкой флага «Заблокирован».

Для добавления учётной записи в группу пользователей следует нажать кнопку «Добавить» и выбрать требуемую группу из списка.

По окончании работы со свойствами пользователей и фиксации выполненных изменений на контролируемом рабочем месте следует нажать кнопку «Применить».

Раздел меню «Обновить список» осуществляет принудительное обновление списка пользователей контролируемого рабочего места.

Раздел меню «Отправить сообщение» позволяет отправить короткое текстовое сообщение пользователю выбранного сеанса (кроме сеанса 'Nobody').



**Вкладка «Аппаратная конфигурация»** обеспечивает обзор текущей аппаратной конфигурации контролируемого рабочего места. Просмотр и актуализация текущего профиля осуществляется кнопкой «Обновить».

*Примечание.* Все обозначения и значки в профиле аппаратной конфигурации аналогичны используемым в ОС семейства Microsoft Windows.

**Вкладка «Управление»** обеспечивает принудительное управление контролируемым рабочим местом (позволяет физически выключить или перезагрузить компьютер удалённо) с помощью предусмотренных кнопок (последует запрос подтверждения принятого решения).

Следует заметить, что удалённое выключение питания контролируемого рабочего места не лишает пользователя физической возможности включить свой компьютер вновь.

*Примечание.* Инструмент применим лишь в период работы компьютера контролируемого рабочего места (требуется активный РС, передающий данные на Сервер для отображения в инструменте).

### **5.7.5 Просмотр снимков экрана**

Инструмент (Рис. 66) обеспечивает доступ к снимкам экрана, собранным при срабатывании условий правила типа «Контроль процессов» в случае определения соответствующего значения в списке «Дополнительное действие» (см. п. 5.3.6 настоящего документа).

Для актуализации представления полученных снимков экрана следует выбрать раздел меню «Обновить». В результате загрузятся снимки экрана контролируемого рабочего места с указанием даты и времени получения каждого снимка.

Загрузка выбранного снимка экрана в формате JPG на компьютер пользователя графического интерфейса администратора САИБ осуществляется выбором пункта контекстного меню Web-обозревателя «Сохранить изображение как...».

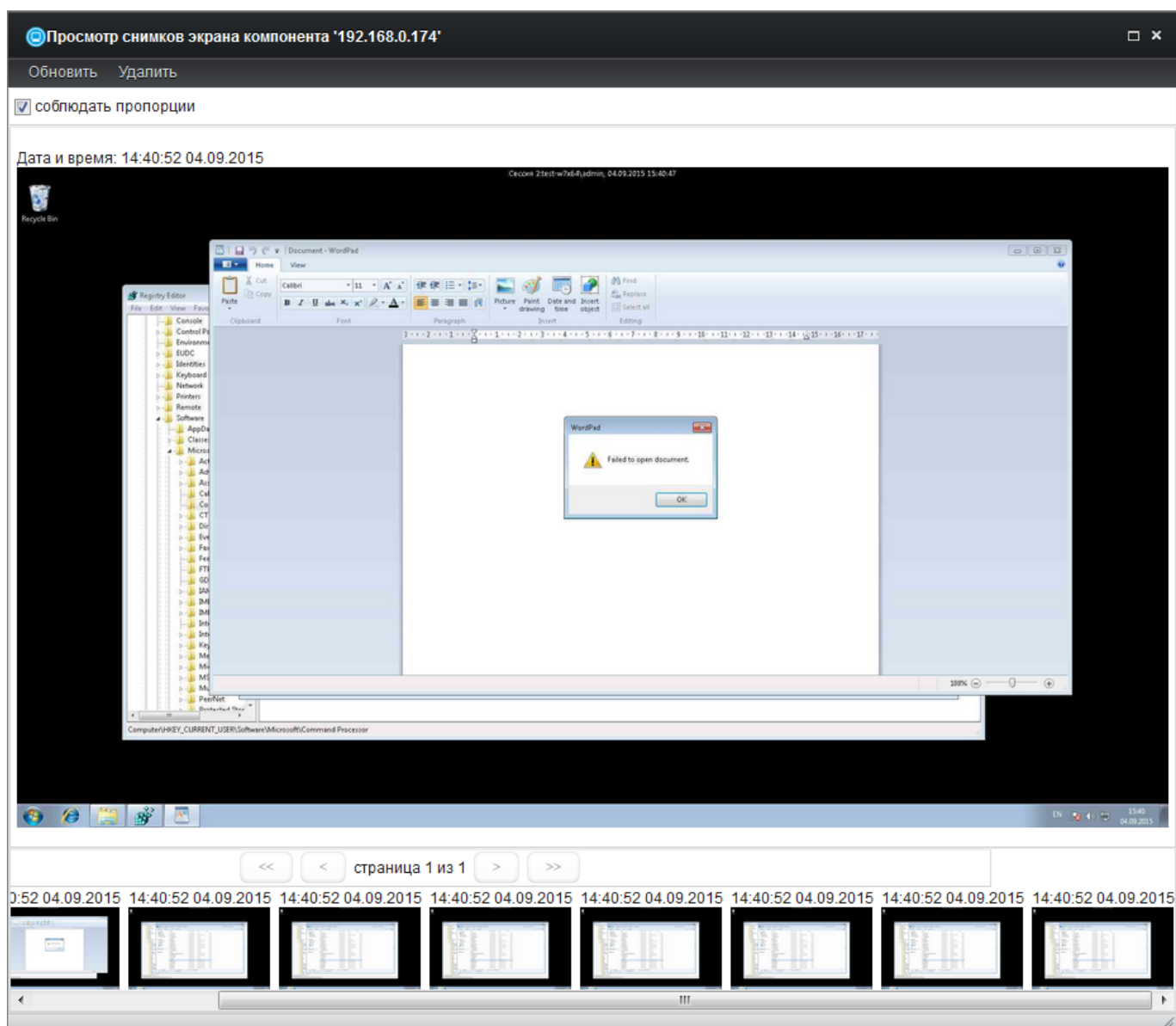


Рис. 66. Инструмент «Просмотр снимков экрана».

Для удаления текущего снимка экрана следует выбрать раздел меню «Удалить».

Установка флага «Соблюдать пропорции» обеспечивает демонстрацию снимка с сохранением пропорций экрана контролируемого рабочего места независимо от настроек рабочего места, на котором эксплуатируется графический интерфейс администратора.

Перемещение по представлению осуществляется с помощью страничного навигатора, расположенного под ним.

*Примечание.* Инструмент применим как в период работы компьютера контролируемого рабочего места, так и в период его бездействия (в этом случае отображаются снимки экрана, накопленные в БД к моменту вызова инструмента).

### **5.7.6 Получение локальных данных**

В случае выбора в качестве значения приоритета фиксации отобранного события в журнале инцидентов «Хранить локально» данные о событии при нарушении правила не передаются на Сервер и хранятся локально на контролируемом рабочем месте до запроса данных по требованию.

Для принудительной передачи локально накопленных данных РС в БД следует выбрать раздел главного меню *Система → Настройки → Настройка модулей*. После определения объекта мониторинга следует выбрать раздел меню *Инструменты → Хостовой сенсор 'ОКО' → Получить локальные данные*.

Затем в дочернем диалоговом окне следует определить временной интервал, локально накопленные данные за который следует передать в БД, и нажать кнопку «Отправить запрос». После формирования запроса работу с инструментом можно продолжить (по желанию).

### **5.7.7 Просмотр аппаратных конфигураций**

Инструмент (Рис. 67) обеспечивает доступ к результатам фиксации и проверки соответствия эталонной аппаратной конфигурации контролируемого рабочего места при определении для него правила типа «Контроль аппаратной конфигурации» (см. п. 5.3.4 настоящего документа).

Фиксация профилей аппаратной конфигурации выполняется в соответствии с параметрами, определёнными правилом, но инструмент отражает лишь факты зафиксированных несоответствий между эталоном и текущим состоянием.

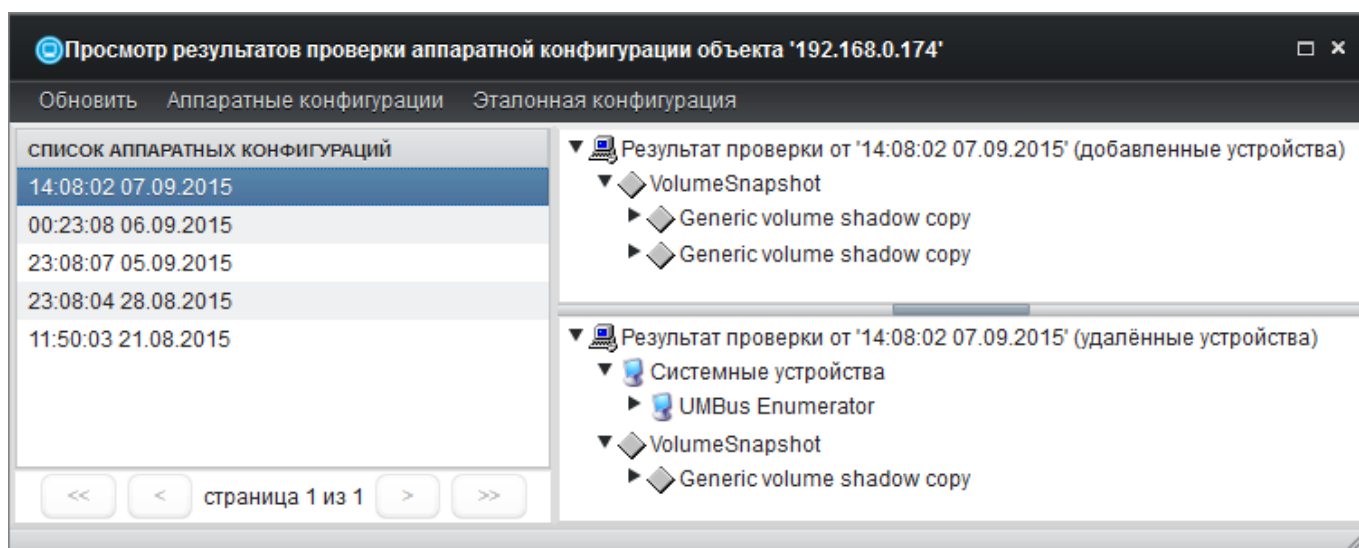


Рис. 67. Инструмент «Просмотр результатов проверки аппаратной конфигурации».

**Важно!** Для выполнения автоматической сверки профилей следует определить один из зафиксированных профилей в качестве эталонного после начала их фиксации в БД.

Для этого в «Списке аппаратных конфигураций» по дате применения правила «Контроль аппаратной конфигурации» следует выбрать профиль, фиксируемый в качестве эталонного. Фиксация выбора выполняется с помощью раздела меню *Аппаратные конфигурации* → *Сохранить как эталон*.

Обзор установленной эталонной конфигурации выполняется выбором раздела меню *Эталонная конфигурация* → *Посмотреть*.

Удалить установленный эталон можно, выбрав раздел меню *Эталонная конфигурация* → *Удалить*. При этом зафиксированный профиль удалён не будет, а лишь лишится статуса эталонного. Непосредственное удаление зафиксированного профиля выполняется выбором раздела меню *Аппаратные конфигурации* → *Удалить*.

Актуализация списка зафиксированных профилей выполняется выбором раздела меню *Обновить*.

Восходящая (значок ‘▲’) / нисходящая (значок ‘▼’) сортировка «Списка аппаратных конфигураций» осуществляется щелчком левой кнопки мыши по нужной графе.

При выборе в «Списке аппаратных конфигураций» любого профиля он автоматически будет сверяться с эталонным. Результат проверки выводится в двух окнах справа. Верхнее окно содержит перечень устройств, добавленных с момента фиксации эталонного профиля, нижнее, – перечень устройств, удалённых с момента фиксации эталонного профиля.

*Примечание.* Все обозначения и значки в профилях аппаратной конфигурации аналогичны используемым в ОС семейства Microsoft Windows.

### **5.7.8 Последний незакрытый инцидент**

САИБ автоматически открывает новый инцидент для события или добавляет его к уже открытому инциденту в том случае, если по параметрам правила, нарушенного событием, последнему необходимо присвоить «опасный» или «критический» уровень приоритета инцидентности.

При этом приоритет фиксации отобранного события в журнале инцидентов для правил «Контроль журналов EventLog» (см. п. 5.3.1 настоящего документа) и «Контроль процессов» (см. п. 5.3.6 настоящего документа) и «Контроль целостности ПО» (см. п. 5.3.2 настоящего документа) должен соответствовать «важному» («опасный уровень») и «критическому» («критический уровень»).

Одновременно в САИБ может быть открыт только один инцидент для каждого РС и все вновь возникшие нарушения правил будут автоматически присоединяться к данному инциденту методом накопления до тех пор, пока он не будет закрыт (не будет переведён в соответствующий статус).

Инструмент (Рис. 68) обеспечивает просмотр сведений и обработку последнего (текущего) инцидента, зафиксированного в САИБ и не обладающего статусом закрытого администратором.

Инцидент 'Останов процесса'

Имя:

Ответственный:

Статус:  Приоритет:

Опасный уровень

Нарушения	История			
ДАТА	ОБЪЕКТ	УРОВЕНЬ	СПИСОК СОБЫТИЙ	...
11:23:10 04.09.2015 - 11:29:21 04.09.2015	Рабочая станция	Опасный уровень	- Запуск процесса - Останов процесса	<a href="#">Подробнее</a>

Переместить в инцидент

Сохранить      Закрыть

Рис. 68. Инструмент «Последний незакрытый инцидент».

Для облегчения идентификации инцидента ему может быть присвоено произвольное наименование в поле «Имя».

Поле «Ответственный» позволяет назначить ответственного за исследование и отработку инцидента из числа зарегистрированных пользователей САИБ независимо от группы принадлежности учётной записи. Следует учесть, что члены группы «Операторы» могут лишь просматривать сведения об инцидентах без возможности выполнения действий по ним.

Список «Статус» определяет текущее состояние инцидента:

- «Открыт» (по умолчанию) присваивается САИБ автоматически при регистрации инцидента;
- «В работе» присваивается при назначении ответственного за исследование инцидента;
- «Регламентные работы» присваивается по окончанию исследования причин возникновения инцидента и переводе его в стадию принятия ответных мер (установка данного статуса

позволяет присвоить наименование регламентным работам и дать их описание, а также исключает запись об инциденте из окна «Уведомления» – см. п. 8.1 настоящего документа);

- «*Закрыт*» присваивается по завершению исследованию инцидента;
- «*Закрыт как ложный*» присваивается инциденту в том случае, если инцидент признаётся ложным (например, по причине недостаточной определённости правила контроля события);
- «*Отменён*» присваивается при снятии инцидента с рассмотрения;
- «*Игнорируется*» присваивается при временном игнорировании возникающих инцидентов данного вида (при этом появляется возможность определения периода игнорирования инцидента).

Список «Приоритет» позволяет определить очерёдность действий ответственного для исследования и отработки данного инцидента в ряде других, порученных ему ранее или в будущем:

- «*Низкий*»;
- «*Нормальный*»;
- «*Высокий*»;
- «*Срочный*» (соответствует уровню «Важного события» приоритета инцидентности);
- «*Безотлагательный*» (соответствует уровню «Критического события» приоритета инцидентности).

Следующее поле позволяет указать дополнительные сведения об инциденте в свободной форме.

Список зарегистрированных нарушений относительно определённого правила контроля событий представлен в табличной форме и содержит следующие графы:

- «*Дата*» отражает период фиксации нарушения;

- «*Объект*» содержит наименование контролируемого рабочего места (модуля топологии САИБ), на котором зафиксирован инцидент;
- «*Уровень*» отражает уровень опасности зафиксированного нарушения («Опасный уровень» либо «Критический уровень» в зависимости от приоритета фиксации отобранного события в журнале инцидентов, определённого для нарушенного правила);
- «*Список событий*» включает перечень выполненных условий нарушенных правил контроля событий, вызвавших фиксацию инцидента;
- «...» содержит ссылку «Подробнее» для просмотра сведений о событиях, связанных с инцидентом (аналогичен инструменту «Монитор событий» – см. п. 5.7.3 настоящего документа, но список отображаемых событий ограничивается контекстом инцидента).

Фиксация внесённых изменений в БД осуществляется кнопкой «Сохранить». При этом будет запрошен ввод обязательного комментария к изменениям, журнал которых отображается во вкладке «История».

Кнопка «Переместить в инцидент» позволяет переместить объект данного инцидента (модуль САИБ) в один из ранее открытых или открыть ещё один инцидент.

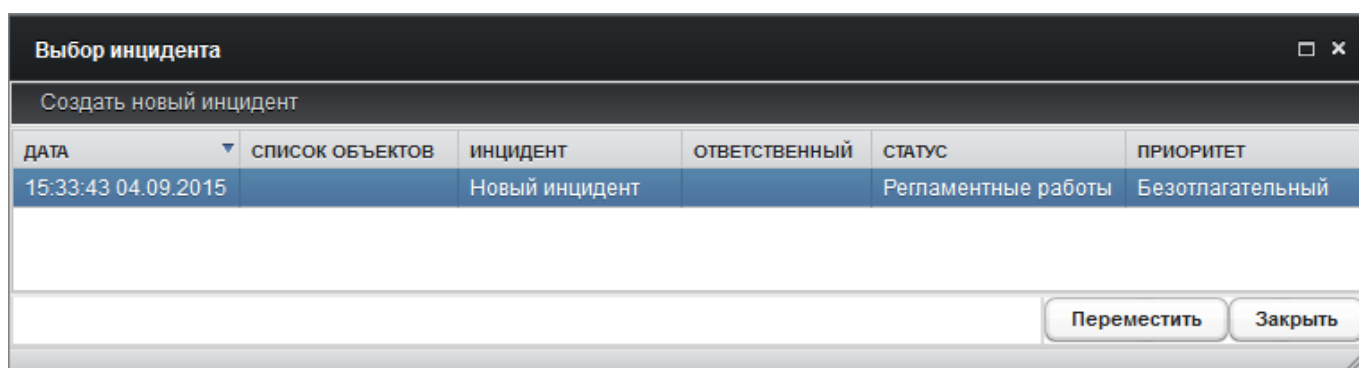


Рис. 69. Дочернее окно «Выбор инцидента».



В дочернем окне выбора инцидента (Рис. 69) указателем мыши или клавишами управления курсором клавиатуры следует выбрать в списке запись о целевом инциденте для переноса объекта.

Восходящая (значок ‘▲’) / нисходящая (значок ‘▼’) сортировка открытых инцидентов САИБ осуществляется щелчком левой кнопки мыши по нужной графе списка.

Если целевой инцидент отсутствует в списке, следует открыть новый инцидент, выбрав раздел меню «Создать новый инцидент» и выбрать созданный инцидент в качестве целевого для переноса объекта.

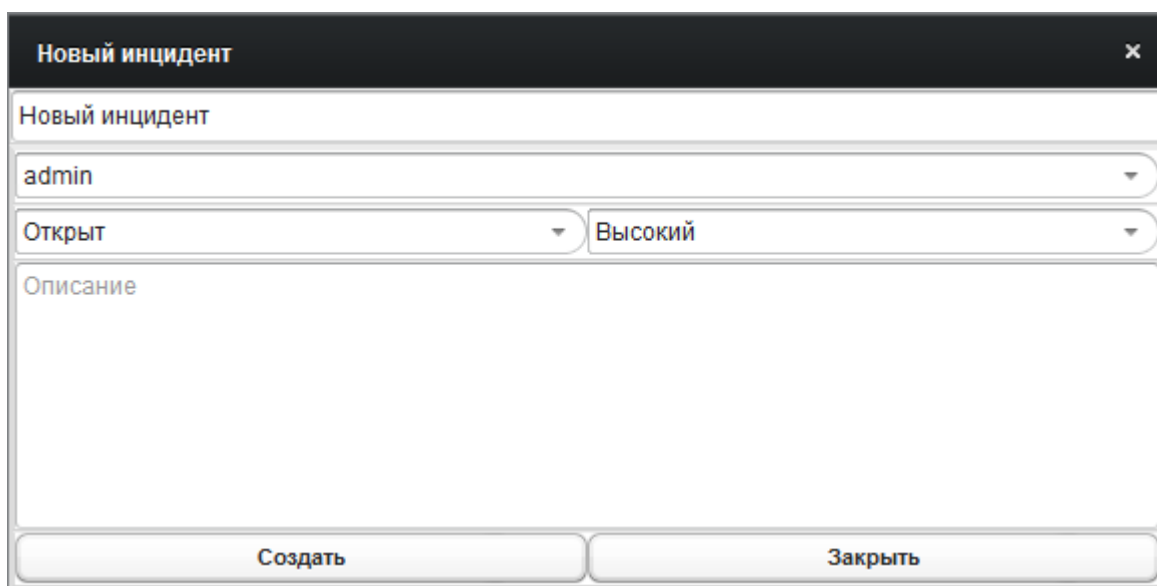


Рис. 70. Дочернее окно «Новый инцидент».

Для создаваемого инцидента (Рис. 70) следует определить наименование в свободной форме (верхнее поле), выбрать ответственного из списка значений, определить статус инцидента в списке («Открыт» или «Регламентные работы»), определить приоритет инцидента в списке («Низкий», «Нормальный», «Высокий» – по умолчанию, «Срочный» или «Безотлагательный») и дать описание инцидента (необязательное). Определив атрибуты инцидента следует нажать кнопку «Создать».

Выбрав целевой инцидент из открытых или возбудив новый инцидент следует нажать кнопку «Переместить» для перемещения в него выбранного объекта.

*Примечание.* При перемещении всех объектов инцидента в целевые исходному инциденту следует присвоить статус «Отменён».

### 5.7.9 Портал администратора

Инструменты «Системный монитор», «Видеотрансляция» и «Монитор событий» можно отобразить в единой области мониторинга «Портал», которая позволяет оценивать текущее состояние нескольких рабочих мест одновременно, оперативно получая их основные параметры и события, возникающие на них. «Портал» ускоряет оповещение администратора безопасности о наступлении критического события.

Представление «Портала» (см. пример на Рис. 71) восстанавливается со всеми настроенными инструментами с началом очередного сеанса (при следующей авторизации в графическом интерфейсе пользователя любой учётной группы).



Рис. 71. Инструмент «Портал».

Для формирования представления «Портала» следует выбрать раздел главного меню *Инструменты* → *Портал*.

Добавление инструмента мониторинга определённого рабочего места начинается с выбора последнего в древе топологии (раздел главного меню *Система* → *Настройки* → *Настройка модулей*). После определения объекта мониторинга следует выбрать раздел меню *Инструменты* → *Панель мониторинга* окна «Настройка модулей» (Рис. 72).

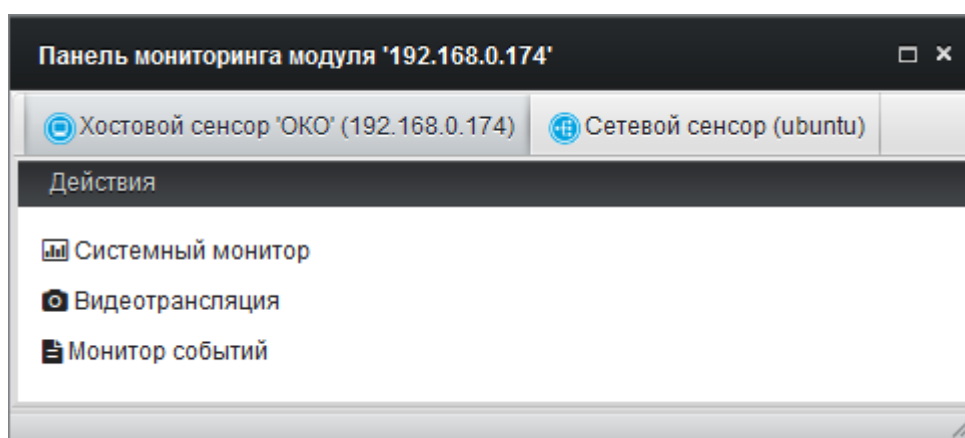


Рис. 72. Панель мониторинга модуля.

Инструмент, который предполагается включить в представление «Портала», следует отбуксировать мышью в окно «Портала». Включённые в представление окна инструментов можно буксировать мышью в оконном пространстве портала, свободно располагая их в нужном порядке.

Также в представление «Портала» буксировкой могут быть включены трансляции сценариев, определённых для выбранного модуля и приведённые во вкладках «Сетевой сенсор» или «АГАТ» (Рис. 73).

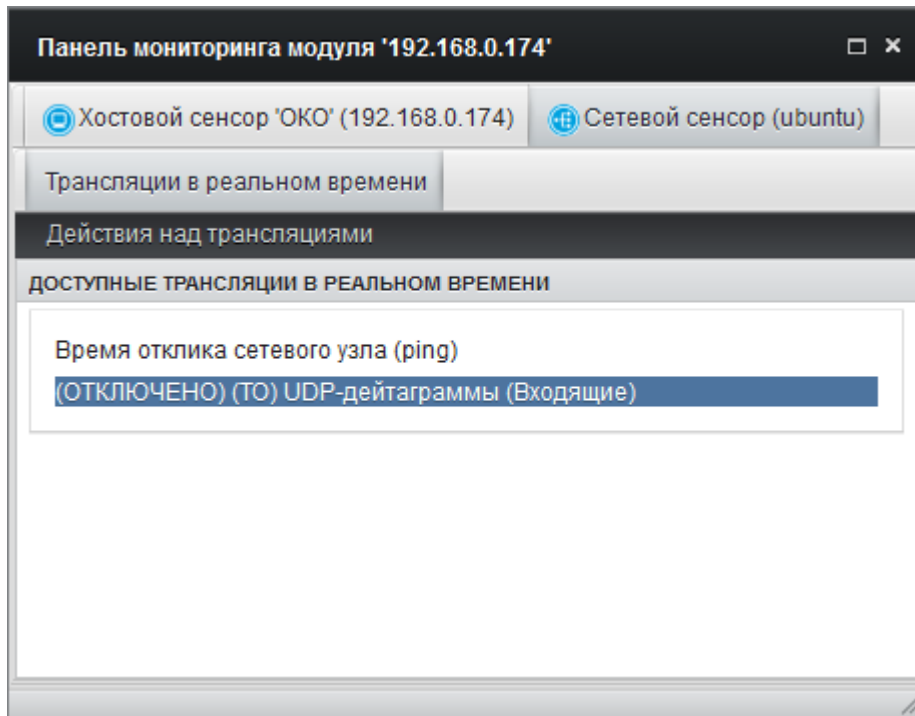


Рис. 73. Трансляции сценариев опроса в инструменте «Панель мониторинга».

Трансляции результатов выполнения сценариев опроса, определённых для модуля, добавляются в представление «Портала» буксировкой нужного сценария из древа топологии.

Нужные трансляции в представление «Портала» можно добавить и буксировкой самого модуля с установленным РС, сетевым сенсором или АГАТ. При этом будет предоставлена возможность выбора определённой трансляции из списка всех имеющихся трансляций САИБ для выбранного средства мониторинга (Рис. 74).

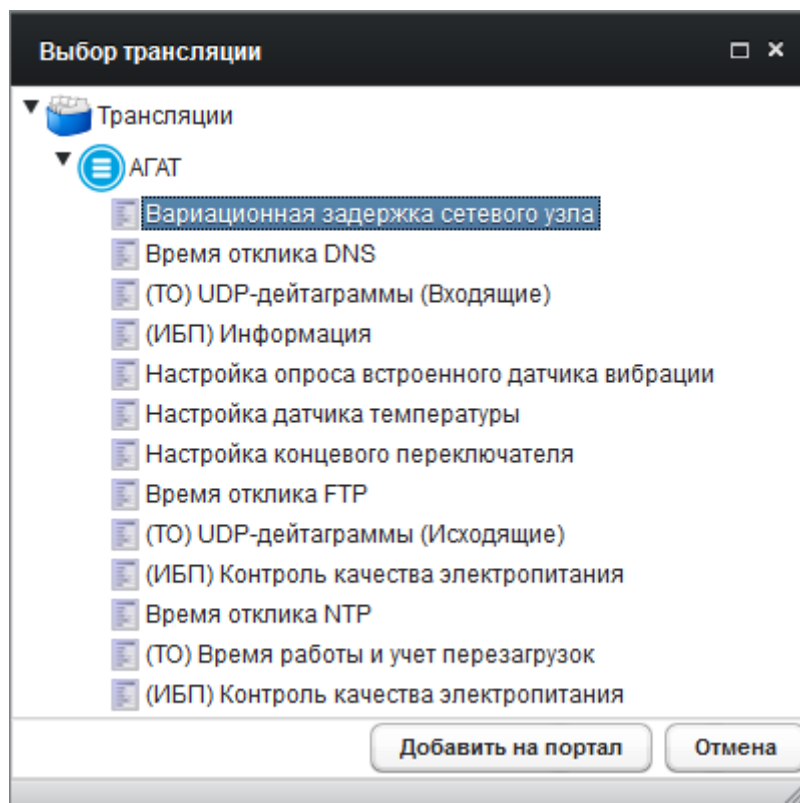


Рис. 74. Выбор трансляции для включения в представление.

*Примечание.* Из-за особенностей программной реализации прокрутка в окнах инструментов «Портала» возможна лишь с помощью кнопок ‘▲’ и ‘▼’ полос прокрутки, а не с помощью ползунков.

Наведение указателя мыши на заголовок инструмента в «Портале» открывает контекстное меню инструмента. Выбор пункта меню «Менеджер задач» вызывает «Менеджер задач» контролируемого рабочего места, соответствующего инструменту (см. п. 5.7.4 настоящего документа). Выбор пункта меню «Закреть» удаляет данный инструмент из представления «Портала».

Раздел меню «Шаблоны» позволяет сохранить сформированное представление для быстрого вызова в будущем. Это выполняется выбором раздела меню *Шаблоны* → *Сохранить портал*. Для загрузки ранее сформированного и сохранённого представления следует выбрать раздел меню *Шаблоны* → *Загрузка и редактирование*. В загруженном представлении

«Портала» можно вновь менять набор и порядок отображения используемых инструментов.

### 5.7.10 Мнемосхема топологии САИБ

Ещё одним инструментом, облегчающим управление и мониторинг компонентов САИБ, является «Мнемосхема», визуально отражающая топологию САИБ с определёнными в ней взаимосвязями (Рис. 75). Его вызов осуществляется из раздела главного меню *Инструменты* → *Мнемосхема*.

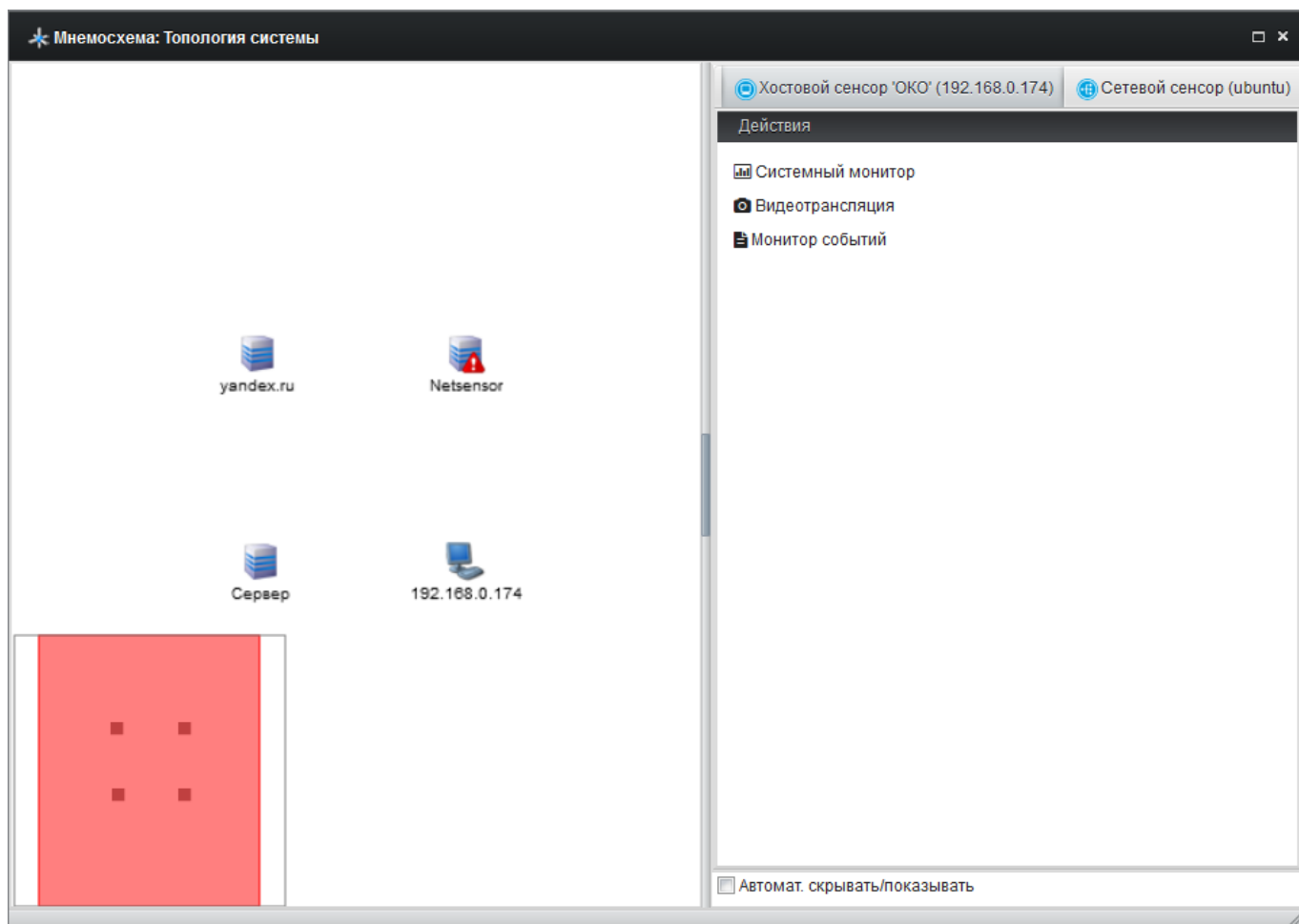


Рис. 75. Инструмент «Мнемосхема».

В окне отображается текущая топология САИБ и навигатор розового цвета (в левом нижнем углу) для удобства перемещения по топологии. Правая часть окна отведена под свойства текущего модуля топологии: для группы отображается состав, для контролируемого рабочего места, сетевого сенсора или АГАТ, – «Панель мониторинга» (см. п. 5.7.9 настоящего документа).

Снятие флага «Автоматически скрывать/показывать» отключает режим автоматического отображения панели свойств в зависимости от того выбран модуль или нет.

Развёртка группы осуществляется щелчком левой кнопки мыши по значку «+», свёртка, – по значку «-». Развёрнутые группы отображаются вместе с вложенными в них модулями в виде таблиц серого цвета. Все типы модулей можно свободно буксировать мышью, как по представлению «Мнемосхемы», так и помещать их внутрь групп. При этом визуальное положение всех модулей до следующего вызова инструмента «Мнемосхема» сохранится неизменным.

Переход на нижележащий уровень иерархической структуры выполняется двойным щелчком левой кнопки мыши по модулю «Группа», возврат к вышележащему уровню, – выбором пункта «Наверх» контекстного меню.

Перемещение по топологии осуществляется буксировкой левой кнопкой мыши по свободному (белому) полю «Мнемосхемы», масштабирование, – прокруткой колеса мыши.

Пункт «Изменить фон» контекстного меню позволяет определить изображение подложки «Мнемосхемы». Выбранное изображение помещается в центр «Мнемосхемы». Для центрирования представления следует выбрать пункт «Отцентровать» контекстного меню.

Пункт «Настройки» контекстного меню открывает окно «Настройка модулей». Если при этом выбран модуль, то указанное окно открывается для выбранного модуля.

Пункт «Хостовой сенсор 'ОКО'» контекстного меню, доступный при выбранном модуле с установленным РС, открывает доступ к инструментам мониторинга контролируемого рабочего места (см. п. 5.7 настоящего документа).

«Панель мониторинга» АГАТ содержит вкладку «Панель подключения датчиков» с отображением вида задней панели устройства АГАТ и

визуализацией текущей конфигурации подключения внешних устройств (датчиков и ТО).

Модуль отображается на «Мнемосхеме» пиктограммой серого цвета в том случае, если на нём не установлен либо деактивирован РС (например, в случае возможного несанкционированного отключения).

Отображение пиктограммы модуля в красном цвете свидетельствует о наличии ошибки функционирования РС (локальная установка не одобрена, установка выполнена некорректно либо не завершена), требующая вмешательства администратора (удаления и повторной установки РС).

При наличии открытых и не отработанных инцидентов (см. п. 5.8.2 настоящего документа) модуль отображается в розовом цвете и помечается пиктограммой с изображением восклицательного знака (!): со статусом «Открыт» – красного цвета, со статусом в «В работе» – жёлтого цвета.



## 5.8. Мониторинг САИБ

Мониторинг функционирования и оценка текущего состояния безопасности САИБ в целом осуществляется инструментами «Журнал событий» и «Инциденты».

### 5.8.1 Журнал событий

В журнале событий фиксируются лишь общесистемные события САИБ, связанные с его функционированием. Сведений о событиях с контролируемых рабочих мест журнал не содержит.

Для работы с журналом событий САИБ следует выбрать раздел главного меню *Инструменты* → *Журнал событий* (Рис. 76).

ИСТОЧНИК	ДАТА	ТИП СОБЫТИЯ	ПОЛЬЗОВАТЕЛЬ	УРОВЕНЬ
Система	28.09.2015 15:38:39	Вход в систему	admin	Информация
Система	28.09.2015 15:05:47	Вход в систему	admin	Информация
Настройка модулей	28.09.2015 13:45:21	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 13:41:22	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 13:03:34	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 13:01:00	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:51:07	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:50:07	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:50:03	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:49:40	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:30:50	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Настройка модулей	28.09.2015 12:30:47	Применение настроек на объекте 'AGAT'	admin	Предупреждение
Одобрение локальных установ	28.09.2015 12:04:12	Установка компонента 'rsm'	admin	Предупреждение
Система	28.09.2015 12:03:54	Вход в систему	admin	Информация
Система	28.09.2015 11:05:26	Вход в систему	admin	Информация
Система	28.09.2015 09:16:23	Выход из системы	admin	Информация
Система	28.09.2015 08:46:03	Вход в систему	admin	Информация

**Подробности:**  
 Объект: AGAT.  
 Компонент: rsm.  
 Описание компонента: install from rsm.  
 Тип компонента: AGAT(506).

Записей на странице: 100 / 1 / 1 >>> Обновить

Рис. 76. Инструмент «Журнал событий».

Список событий представлен в табличной форме и содержит следующие графы:

- «*Источник*» содержит описание происхождения события («*Инциденты*», «*Настройка модулей*», «*Одобрение локальных установок*», «*Система*», «*Удалённая установка*»);
- «*Дата*» содержит дату регистрации события;
- «*Тип события*» содержит описание типа события;
- «*Пользователь*» содержит идентификатор пользователя, породившего событие;
- «*Уровень*» отображает уровень важности события для обеспечения функционирования САИБ в целом.

Полнотекстовый отбор записей осуществляется определением значения поля «*Фильтр*» и нажатием клавиши 'Enter'.

Также можно осуществить мгновенный отбор по источнику происхождения события, выбрав одно из значений списка «*Источники событий*»:

- «*Все источники*» (по умолчанию) – список отразит описания всех событий независимо от источника их происхождения;
- «*Выбор нескольких источников...*» позволяет определить набор источников, события от которых будут включены в список (выбор осуществляется установкой флагов в дочернем диалоговом окне);
- «*Инциденты*» – список отразит лишь описания событий, возбужденных инструментом «*Инциденты*» (см. п. 5.8.2 настоящего документа);
- «*Настройка модулей*» – список отразит лишь описания событий, возникших при настройке модулей (см. п. 3.2.7 настоящего документа);
- «*Одобрение локальных установок*» – список отразит лишь описания событий, возникших при регистрации в САИБ РС, установленных локально (см. п. 3.2.6.3 настоящего документа);

- «Система» – список отразит лишь описания событий общесистемного характера;
- «Удалённая установка» – список отразит лишь описания событий, возникших при удалённой установке РС на контролируемые рабочие места (см. п. 3.2.6.4 настоящего документа).

Отбор записей по времени выполняется выбором значения списка «Временной интервал»:

- «Последний час»;
- «Последние 12 часов»;
- «Последние сутки»;
- «Последняя неделя»;
- «Последний месяц» (по умолчанию);
- «Настраиваемый интервал...» (позволяет определить период отбора начальной и конечной датой с помощью календаря).

Для просмотра дополнительной информации о событии указателем мыши или клавишами управления курсором клавиатуры следует выбрать в списке запись о нужном событии. При наличии дополнительная информация отразится в разделе «Подробности» (текстовый блок можно выделить и скопировать в буфер обмена, например, для передачи в службу технической поддержки производителя).

Восходящая (значок '▲') / нисходящая (значок '▼') сортировка записей журнала осуществляется щелчком левой кнопки мыши по нужной графе списка.

Перемещение по блокам записей журнала осуществляется с помощью страничного навигатора, расположенного под таблицей. Список «Записей на странице» позволяет определить ёмкость одной страницы.

Кнопка «Обновить» актуализирует представление журнала событий на текущий момент времени.

### 5.8.2 Инциденты

Факты нарушения правил контроля событий программной среды рабочих мест с приоритетом инцидентности «важный» и «критический» приводят в САИБ к возбуждению инцидентов, требующих исследования и отработки в соответствии с действующей политикой информационной безопасности эксплуатирующей организации.

Инциденты заносятся в журнал инцидентов САИБ, вызов которого осуществляется выбором раздела главного меню *Инструменты* → *Инциденты*.

Доступ к журналу инцидентов САИБ имеют все зарегистрированные пользователи САИБ независимо от учётной группы, но члены группы «Операторы» обладают лишь возможностью просмотра сведений об инцидентах без возможности управлять ими.

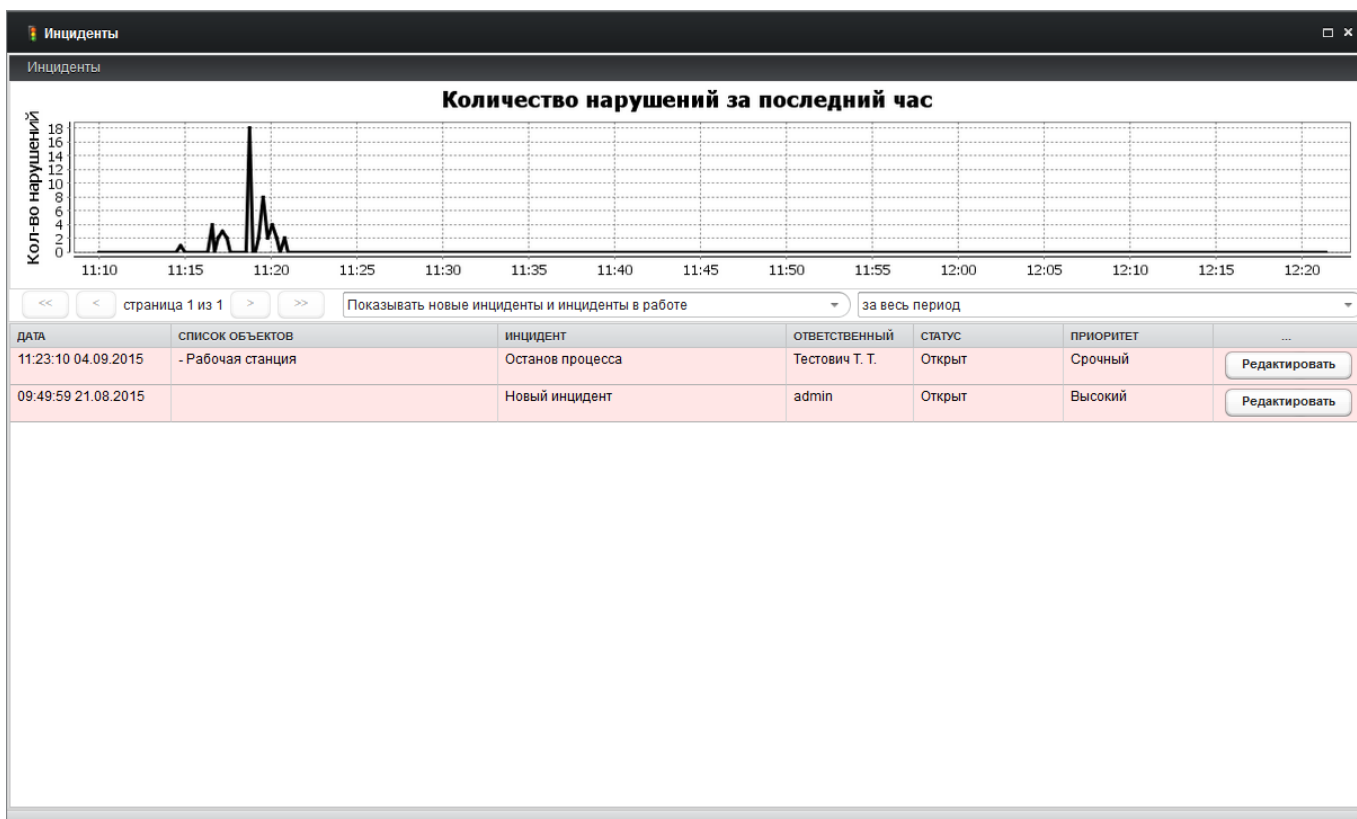


Рис. 77. Инструмент «Инциденты».

Окно журнала инцидентов (Рис. 77) включает динамически обновляемый график «Количество нарушений за последний час», отражающий частоту фиксации нарушений правил в единицу времени.

*Примечание.* Инциденты, открытые в САИБ, также отражаются в качестве уведомлений (см. п. 8.1 настоящего документа) с указанием наименования нарушенного правила.

Список инцидентов САИБ представлен в табличной форме и содержит следующие графы:

- «Дата» отображает дату и время возбуждения инцидента;
- «Список объектов» включает перечень объектов, к которым относится инцидент;
- «Инцидент» отображает наименование инцидента (по умолчанию – наименование первого условия, определённого для первого из нарушенных правил);
- «Ответственный» отображает реквизиты пользователя САИБ, назначенного ответственным за исследование инцидента;
- «Статус» отражает текущее состояние работ по инциденту;
- «Приоритет» отражает уровень значимости инцидента для безопасности АСИ в целом, соответствующий очередности принятия мер по инциденту в ряде других.
- «...» содержит кнопку «Редактировать», вызывающую окно свойств инцидента, аналогичное инструменту «Последний незакрытый инцидент» (см. п. 5.7.8 настоящего документа).

Перемещение по блокам записей журнала осуществляется с помощью страничного навигатора, расположенного над таблицей.

За навигатором имеется список, определяющий режим отображения записей в таблице инцидентов:

- «Показывать все инциденты» – отображаются инциденты со всеми статусами без исключения;

- *«Показывать новые инциденты и инциденты в работе»* (по умолчанию) – отображаются открытые (новые) и не закрытые инциденты;
- *«Показывать только новые инциденты»* – отображаются только открытые (новые) инциденты.

Следующий список определяет временные рамки отображения записей в таблице инцидентов:

- *«за день»*;
- *«за неделю»*;
- *«за месяц»*;
- *«за весь период»* (по умолчанию).

Выбор одного из значений вышеуказанных списков приводит к мгновенной фильтрации таблицы инцидентов.

*Примечание.* Управление отдельным инцидентом подробно описано в п. 5.7.8 настоящего документа.

## 6. Удалённое управление ТО

АГАТ обеспечивает управление ТО, подключенным к АГАТ. Для этого между рабочим местом, с которого предполагается осуществлять удалённое управление, и АГАТ требуется использовать защищённый канал связи по классу защиты информации КС1.

В качестве средств защиты информации применяется сертифицированная ФСБ России реализация OpenVPN – средство криптографической защиты информации АЛДБ.00003-01 ПК «Альфиск-АП» производства ООО «Р-Альфа Лаб», предназначенное для защиты передачи информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Защищённая передача осуществляется посредством организации VPN-туннеля с использованием свободной реализации технологии виртуальной частной сети с открытым исходным кодом (OpenVPN) со встроенной библиотекой защиты конфиденциальной информации «Агава-А» версии 1.1. Библиотека «Агава-А» использует следующие криптографические алгоритмы:

- ГОСТ 28147-89. «Система обработки информации. Защита криптографическая»;
- ГОСТ Р34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ Р34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Построение VPN-туннеля между рабочим местом и АГАТ происходит на основе сертификатов OpenSSL, выдаваемых каждому рабочему месту в качестве идентификаторов подлинности.

Организация VPN-туннеля между удалённым рабочим местом и АГАТ предполагает:

- формирование набора сертификатов OpenSSL для каждого рабочего места и АГАТ;
- настройку и запуск VPN-сервера доступа;
- настройку и запуск VPN-клиента на удалённом рабочем месте.

ПК «Альфиск-АП» может быть развёрнут в следующих ОС [в скобках указано имя файла дистрибутивного комплекта]:

- FreeBSD 8.3 i386 [freebsd8\_i386.tar.gz];
- FreeBSD 8.3 amd64 [freebsd8\_amd64.tar.gz];
- FreeBSD 9.2 i386 [freebsd9\_i386.tar.gz];
- FreeBSD 9.2 amd64 [freebsd9\_amd64.tar.gz];
- Ubuntu Linux 9.04 i686 (linux-kernel version 2.6.28) [linux\_kernel2.6\_amd64.tar.gz];
- Ubuntu Linux 9.04 x86-64 (linux-kernel version 2.6.28) [linux\_kernel2.6\_i386.tar.gz];
- Debian Linux 7 i686 (linux-kernel version 3.2) [linux\_kernel3.2\_amd64.tar.gz];
- Debian Linux 7 x86-64 (linux-kernel version 3.2) [linux\_kernel3.2\_i386.tar.gz];
- Windows 2000/XP/2003/Vista/7/8/8.1 32/64 bit [windows\_all\_version.zip].

*Примечание.* Все нижеприведённые примеры настройки для ОС \*nix реализовывались в ОС FreeBSD 8.3 i386 с использованием оболочки 'bash'.

### **6.1. Распаковка дистрибутива организации VPN-туннеля в ОС \*nix**

Дистрибутив представляет собой tar-архив, который следует распаковать в удобное место (для примера распаковка выполнена в '/opt/agava'). Распакованный дистрибутив включает папки:

- './bin/openssl' – исполняемый модуль OpenSSL для генерации сертификатов;



- ‘./lib’ – папка библиотек OpenVPN и OpenSSL;
- ‘./sbin/openvpn’ – исполняемый модуль OpenVPN для запуска клиента и сервера VPN, соответствующих ГОСТ;
- ‘./share’ – папка официальной документации OpenVPN версии 2.3 на английском языке;
- ‘./ssl/certs’ – пустая папка для размещения сертификатов и ключей, сформированных OpenSSL;
- ‘./ssl/man’ – папка официальной документации OpenSSL версии 1.0.1 на английском языке;
- ‘./ssl/misc’ – коллекция сценариев, облегчающих работу с сертификатами;
- ‘./ssl/openssl.cnf’ – файл конфигурации OpenSSL.

Также в ‘/opt/agava’ необходимо создать папки ‘log’, ‘certs’, ‘conf’.

## 6.2. Формирование сертификатов и ключей OpenSSL в ОС \*nix

Сертификаты формируются сборкой OpenSSL, входящей в состав дистрибутива. Применение сторонней сборки OpenSSL потребует указания использования библиотек, входящих в состав дистрибутива:

```
[user@test.ovpn /opt/agava]$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/agava/lib
```

После этого можно приступать к формированию корневого сертификата<sup>19)</sup>:

```
[user@test.ovpn /opt/agava]$ ./bin/openssl req -new -newkey gost2012 -pkeyopt paramset:A -x509 -days 3650 -nodes -out ssl/certs/ca.crt -keyout ssl/certs/ca.key
```

В результате выполнения данной команды запустится процесс генерации сертификата и в интерактивном режиме последует несколько вопросов об атрибутах объекта, для которого выписывается сертификат. После ввода данных сформируются файлы сертификата (‘./ssl/certs/ca.crt’) и незащищённого паролем ключа (‘./ssl/certs/ca.key’).

---

<sup>19)</sup> За справкой по назначению применяемых ключей командной строки следует обращаться к документации проекта OpenSSL.

Имеется возможность расширить или сузить перечень вопросов и предопределить ответы на них, предварительно изменив параметры файла конфигурации OpenSSL (‘./ssl/openssl.cnf’)<sup>20</sup>.

После формирования корневого сертификата следует создать сертификаты для сервера и клиента. Запрос формирования сертификата для сервера выглядит следующим образом:

```
[user@test.ovpn /opt/agava]$ ./bin/openssl req -nodes -newkey gost2012 -pkeyopt paramset:A -keyout ./ssl/certs/server.key -out ./ssl/certs/server.csr
```

В результате выполнения данной команды запустится процесс генерации сертификата и в интерактивном режиме последует несколько вопросов об атрибутах объекта, для которого выписывается сертификат.

После ввода данных сформируются файлы запроса сертификата (‘./ssl/certs/server.csr’) и незащищённого паролем ключа (‘./ssl/certs/server.key’). Сертификат сервера следует подписать сформированным корневым сертификатом:

```
[user@test.ovpn /opt/agava]$ ./bin/openssl x509 -req -days 365 -in ./ssl/certs/server.csr -CA ./ssl/certs/ca.crt -CAkey ./ssl/certs/ca.key -CAcreateserial -outform PEM -out ./ssl/certs/server.crt
```

Формирование сертификата сервера завершено. Аналогичным методом формируются сертификаты клиентов.

Для дополнительной защиты от DOS-атак формируется секретный ключ TLS-аутентификации:

```
[user@test.vpn /opt/agava]$ ./sbin/openvpn --genkey --secret ./ssl/certs/ta.key
```

Также следует сформировать файл параметра алгоритма Диффи-Хельмана:

```
[user@test.vpn /opt/agava]$ ./bin/openssl dhparam -out ./ssl/certs/1024.dh 1024
```

Требуется сформировать как минимум два набора сертификатов клиентов: один – для АРМ, с которого предполагается вести удалённое управление ТО, второй – для АГАТ.

---

<sup>20</sup>) За справкой по назначению параметров конфигурации следует обращаться к документации проекта OpenSSL.

Набор файлов для VPN-клиента АГАТ следует загрузить в АГАТ в соответствии с эксплуатационной документацией.

### 6.3. Запуск сервера и клиента OpenVPN в ОС \*nix

Запуск сервера OpenVPN, соответствующего требованиям ГОСТ, начинается с размещения сертификатов, например, в папке '/opt/agava/conf', в которую следует поместить корневой сертификат 'ca.crt', серверный сертификат 'server.crt' и ключ 'server.key', а также TLS-ключ 'ta.key' и файл параметра Диффи-Хельмана '1024.dh'.

Затем следует сформировать конфигурационный файл 'server.conf', содержащий, например, следующие параметры<sup>21)</sup>:

```
# Локальный IP-адрес, принимающий вызовы OpenVPN (опционально)
local 192.168.0.64

# Локальный TCP/UDP-порт, принимающий вызовы OpenVPN. При необходимости запустить
# несколько экземпляров OpenVPN на одном СБТ применяются различные номера портов для
# них. Доступ к порту необходимо открыть в межсетевом экране, если таковой
# применяется.
port 9999

# Применяемый протокол транспортного уровня
proto tcp-server

# "dev tun" будет создан маршрутизируемый IP-туннель
# "dev tap" будет создан ETHERNET-туннель
dev tun

# Переход в папку сертификатов
cd /opt/agava/conf

# SSL/TLS корневой сертификат (ca), сертификат (cert) и секретный ключ(key).
# Каждый клиент и сервер должны иметь собственные файлы cert и key.
# Сервер и все клиенты используют идентичный файл ca.
ca ca.crt
cert server.crt
key server.key

# Файл с параметром алгоритма Диффи-Хельмана.
dh 1024.dh

# Конфигурация серверного режима и поддержки подсети VPN для раздачи
# клиентских адресов. Сервер возьмет для себя адрес 10.10.99.1. Каждый клиент
# сможет обращаться к серверу по данному адресу. Закомментируйте данные строки,
# если используете ETHERNET-мост. За подробной информацией по значениям
# параметров обращайтесь к документации OpenVPN.
server 10.10.99.0 255.255.255.0
route 10.10.99.0 255.255.255.252

# Для повышения уровня безопасности SSL/TLS создайте "нМАС-файрвол", помогающий
# блокировать DOS-атаки и UDP-флуд. Сервер и каждый клиент должны иметь копию файла
# ta.key. Значение второго параметра в строке tls-auth должно соответствовать '0' на
# сервере и '1' на клиенте.
```

<sup>21)</sup> За справкой по назначению параметров конфигурации следует обращаться к документации проекта OpenVPN.

```
tls-server
tls-auth ta.key 0
tls-timeout 120
tls-cipher GOST2012-GOST89-GOST89

# Предпишем использовать специфичный OpenSSL-криптодвижок.
engine gost

# Выбор специфичного криптографического шифратора.
cipher gost89

# Предпишем использовать специфичный алгоритм расчёта хеш-суммы для аутентификации
# пакетов.
auth gost-mac

# Директива 'keepalive' предписывает посылать ring-подобные сообщения, по которым
# каждая из сторон узнает о выходе из строя ответной. Сообщение посылать каждые
# 10 секунд. Если в течение 120 секунд ответа не последует, то удалённая сторона
# считается вышедшей из строя.
keepalive 10 120

# Максимальное количество разрешённых одновременно подключенных клиентов.
max-clients 100

# Данная директива разрешает подключаться множеству клиентов с одинаковыми
# сертификатами/ключами или именами. Её применение рекомендуется только с целью
# проверки работоспособности. Для промышленного применения каждый клиент должен
# иметь собственную пару сертификат/ключ.
duplicate-cn

# Вывод в файл краткой информации о статусе текущих подключений. Обрезается и
# переписывается ежеминутно.
status /opt/agava/log/sopenvpn-status.log

# По умолчанию диагностические сообщения поступают с 'syslog' (на ОС Windows при
# условии запуска в качестве службы - в папку '/Program Files/OpenVPN/log'). Можно
# использовать 'log' или 'log-append' для переопределения поведения по умолчанию.
# 'log' будет обрезать файл журнала при запуске OpenVPN, тогда как 'log-append'
# будет дописывать лог в существующий файл. Одновременно используется только одно из
# двух.
log /opt/agava/log/sopenvpn.log

# Установка уровня подробности ведения файла журнала:
# 0 - 'тихий' режим, пишутся только фатальные ошибки;
# 4 - разумное значение для обычного использования;
# 5 и 6 могут помочь выяснить причины проблем подключения;
# 9 - высший уровень подробности;
verb 3
```

Определив конфигурацию, следует запустить сервер:

```
[root@test.ovpn /opt/agava]# ./sbin/openvpn --config ./conf/server.conf
```

Следует отметить, что запуск выполняется с правами суперпользователя и с учётом специфичности OpenVPN, использующего специфичные же библиотеки, размещённые в '/opt/agava/lib'.

После успешного запуска в файле журнала OpenVPN должна появиться запись 'Initialization Sequence Completed', а в выводе команды 'ifconfig' будет присутствовать новый сетевой интерфейс 'tun':

```
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500
options=80000<LINKSTATE>
```

```
inet 10.10.99.1 --> 10.10.99.2 netmask 0xffffffff
Opened by PID 1518
```

Запуск клиента OpenVPN, соответствующего требованиям ГОСТ, начинается с размещения сертификатов, например, в папке '/opt/agava/conf', в которую следует поместить корневой сертификат 'ca.crt', клиентский сертификат 'client.crt' и ключ 'client.key', а также TLS-ключ 'ta.pem' и файл параметра Диффи-Хельмана '1024.pem'.

Затем следует сформировать конфигурационный файл 'client.conf', содержащий, например, следующие параметры (для краткости комментарии включены лишь для директив, отличных от применённых в конфигурационном файле сервера):

```
# Определение режима работы OpenVPN в качестве клиента
client

proto tcp-client
dev tun

cd /opt/agava/conf
ca ca.crt
cert client.crt
key client.key
dh 1024.dh

# Имя/ip-адрес и порт сервера. Можно определить набор директив 'remote' для
# балансировки нагрузки между серверами.
remote 192.168.0.64 9999

# Режим бесконечных попыток определения имени сервера. Очень полезно
# применять на СВТ, не имеющих постоянного подключения к Интернет (например,
# ноутбуки).
# В директиве 'remote' рассматриваемого примера задан IP-адрес, а не доменное
# имя и в данном случае директива несущественна, но приведена как полезная.
resolv-retry infinite

tls-client
tls-auth ta.key 1
tls-timeout 120
tls-cipher GOST2012-GOST89-GOST89

engine gost
cipher gost89
auth gost-mac

keepalive 10 120

# Режим сохранения постоянного состояния при перезапуске.
persist-key
persist-tun
status /opt/agava/log/copenvpn-status.log
log /opt/agava/log/copenvpn.log
verb 4
```

Определив конфигурацию следует запустить клиент:

```
[root@test.ovpn /opt/agava]# ./sbin/openvpn --config ./conf/client.conf
```

После успешного запуска в файле журнала OpenVPN должна появиться запись ‘Initialization Sequence Completed’, в системе появится новый сетевой интерфейс, а к серверу можно обратиться по внутреннему IP-адресу (например, ‘10.10.99.1’):

```
# ping 10.10.99.1
PING 10.10.99.1 (10.10.99.1): 56 data bytes
64 bytes from 10.10.99.1: icmp_seq=0 ttl=64 time=0.762 ms
64 bytes from 10.10.99.1: icmp_seq=1 ttl=64 time=0.894 ms
64 bytes from 10.10.99.1: icmp_seq=2 ttl=64 time=0.962 ms
64 bytes from 10.10.99.1: icmp_seq=3 ttl=64 time=0.798 ms
64 bytes from 10.10.99.1: icmp_seq=4 ttl=64 time=0.831 ms
64 bytes from 10.10.99.1: icmp_seq=5 ttl=64 time=0.734 ms
^C
--- 10.10.99.1 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.734/0.830/0.962/0.078 ms
```

Если на СВТ клиента поступают квитанции на пакеты ‘ping’, отправленные на сервер по внутреннему VPN-адресу, то VPN-канал, соответствующий требованиям ГОСТ, можно считать работоспособным и готовым для подключения к АГАТ с целью терминального управления ТО.

#### **6.4. Распаковка дистрибутива организации VPN-туннеля в ОС Windows**

Дистрибутив представляет собой zip-архив, который следует распаковать в ‘C:\’ (в корневую папку жёсткого диска ‘C:’). В папке ‘C:\openvpn’, полученной в результате распаковки архива, следует создать подпапку ‘log’.

Из распакованной папки ‘C:\openvpn’ необходимо установить дополнительное ПО, запустив исполняемые файлы ‘Microsoft\_Visual\_Studio\_2010\_Redistributable\_Pack\_x32.exe’ и ‘TAP\_Driver\_Windows\_v9.9.2\_Build\_v3.exe’, приняв все параметры, предлагаемые по умолчанию.

Завершив установку ‘TAP\_Driver\_Windows\_v9.9.2\_Build\_v3.exe’ следует перезагрузить ОС даже в том случае, если установщик этого не требует.

## 6.5. Формирование сертификатов и ключей OpenSSL в ОС Windows

Сертификаты формируются сборкой OpenSSL, входящей в состав дистрибутива. Следует запустить интерпретатор командной строки ‘cmd.exe’ и перейти в папку ‘C:\openvpn’:

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\alexis>cd c:\openvpn

c:\openvpn>
```

После этого можно приступать к формированию корневого сертификата<sup>22)</sup>:

```
c:\openvpn>bin\openssl req -new -newkey gost2012 -pkeyopt paramset:A -x509 -days 3650
-nodes -out certs\ca.crt -keyout certs\ca.key
```

В результате выполнения данной команды запустится процесс генерации сертификата и в интерактивном режиме последует несколько вопросов об атрибутах объекта, для которого выписывается сертификат. После ввода данных сформируются файлы сертификата (‘ssl\certs\ca.crt’) и незащищённого паролем ключа (‘ssl\certs\ca.key’).

Имеется возможность расширить или сузить перечень вопросов и предопределить ответы на них, предварительно изменив параметры файла конфигурации OpenSSL (‘ssl\openssl.cnf’)<sup>23)</sup>.

После формирования корневого сертификата следует создать сертификаты для сервера и клиента. Запрос формирования сертификата для сервера выглядит следующим образом:

```
c:\openvpn>bin\openssl req -nodes -newkey gost2012 -pkeyopt paramset:A -keyout
certs\server.key -out certs\server.csr
```

<sup>22)</sup> За справкой по назначению применяемых ключей командной строки следует обращаться к документации проекта OpenSSL.

<sup>23)</sup> За справкой по назначению параметров конфигурации следует обращаться к документации проекта OpenSSL.

В результате выполнения данной команды запустится процесс генерации сертификата и в интерактивном режиме последует несколько вопросов об атрибутах объекта, для которого выписывается сертификат.

После ввода данных сформируются файлы запроса сертификата ('ssl\certs\server.csr') и незащищённого паролем ключа ('ssl\certs\server.key'). Сертификат сервера следует подписать сформированным корневым сертификатом:

```
c:\openvpn>bin\openssl x509 -req -days 365 -in certs\server.csr -CA certs\ca.crt -CAkey certs\ca.key -CAcreateserial -outform PEM -out certs\server.crt
```

Формирование сертификата сервера завершено. Аналогичным методом формируются сертификаты клиентов.

Для дополнительной защиты от DOS-атак формируется секретный ключ TLS-аутентификации:

```
c:\openvpn>bin\openvpn --genkey --secret certs\ta.key
```

Также следует сформировать файл параметра алгоритма Диффи-Хельмана:

```
c:\openvpn>bin\openssl dhparam -out certs\1024.dh 1024
```

Требуется сформировать как минимум два набора сертификатов клиентов: один – для АРМ, с которого предполагается вести удалённое управление ТО, второй – для АГАТ.

Набор файлов для VPN-клиента АГАТ следует загрузить в АГАТ в соответствии с эксплуатационной документацией.

## 6.6. Запуск сервера и клиента OpenVPN в ОС Windows

Запуск сервера OpenVPN, соответствующего требованиям ГОСТ, начинается с размещения сертификатов в папке 'C:\openvpn\ssl\certs', в которую следует поместить корневой сертификат 'ca.crt', серверный сертификат 'server.crt' и ключ 'server.key', а также TLS-ключ 'ta.key' и файл параметра Диффи-Хельмана '1024.dh'.



Затем следует сформировать конфигурационный файл 'server.conf', содержащий, например, следующие параметры<sup>24)</sup>:

```
# Локальный IP-адрес, принимающий вызовы OpenVPN (опционально)
local 192.168.0.64

# Локальный TCP/UDP-порт, принимающий вызовы OpenVPN. При необходимости запустить
# несколько экземпляров OpenVPN на одном СБТ применяются различные номера портов для
# них. Доступ к порту необходимо открыть в межсетевом экране, если таковой
# применяется.
port 9999

# Применяемый протокол транспортного уровня
proto tcp-server

# "dev tun" будет создан маршрутизируемый IP-туннель
# "dev tap" будет создан ETHERNET-туннель
dev tun

# Переход в папку сертификатов
cd C:\openvpn\ssl\certs

# SSL/TLS корневой сертификат (ca), сертификат (cert) и секретный ключ (key).
# Каждый клиент и сервер должны иметь собственные файлы cert и key.
# Сервер и все клиенты используют идентичный файл ca.
ca ca.crt
cert server.crt
key server.key

# Файл с параметром алгоритма Диффи-Хельмана.
dh 1024.dh

# Конфигурация серверного режима и поддержки подсети VPN для раздачи
# клиентских адресов. Сервер возьмет для себя адрес 10.10.99.1. Каждый клиент
# сможет обращаться к серверу по данному адресу. Закомментируйте данные строки,
# если используете ETHERNET-мост. За подробной информацией по значениям
# параметров обращайтесь к документации OpenVPN.
server 10.10.99.0 255.255.255.0
route 10.10.99.0 255.255.255.252

# Для повышения уровня безопасности SSL/TLS создайте "HMAC-файрвол", помогающий
# блокировать DOS-атаки и UDP-флуд. Сервер и каждый клиент должны иметь копию файла
# ta.key. Значение второго параметра в строке tls-auth должно соответствовать '0' на
# сервере и '1' на клиенте.
tls-server
tls-auth ta.key 0
tls-timeout 120
tls-cipher GOST2012-GOST89-GOST89

# Предпишем использовать специфичный OpenSSL-криптодвижок.
engine gost

# Выбор специфичного криптографического шифратора.
cipher gost89

# Предпишем использовать специфичный алгоритм расчёта хеш-суммы для аутентификации
# пакетов.
auth gost-mac

# Директива 'keepalive' предписывает посылать ping-подобные сообщения, по которым
# каждая из сторон узнает о выходе из строя ответной. Сообщение посылать каждые
# 10 секунд. Если в течение 120 секунд ответа не последует, то удалённая сторона
# считается вышедшей из строя.
keepalive 10 120
```

<sup>24)</sup> За справкой по назначению параметров конфигурации следует обращаться к документации проекта OpenVPN.

```
# Максимальное количество разрешённых одновременно подключенных клиентов.
max-clients 100

# Данная директива разрешает подключаться множеству клиентов с одинаковыми
# сертификатами/ключами или именами. Её применение рекомендуется только с целью
# проверки работоспособности. Для промышленного применения каждый клиент должен
# иметь собственную пару сертификат/ключ.
duplicate-cn

# Вывод в файл краткой информации о статусе текущих подключений. Обрезается и
# переписывается ежеминутно.
status c:\openvpn\log\sopenvpn-status.log

# По умолчанию диагностические сообщения поступают с syslog (на ОС Windows при
# условии запуска в качестве службы - в папку '\Program Files\OpenVPN\log'). Можно
# использовать 'log' или 'log-append' для переопределения поведения по умолчанию.
# 'log' будет обрезать файл журнала при запуске OpenVPN, тогда как 'log-append'
# будет дописывать лог в существующий файл. Одновременно используется только одно из
# двух.
log c:\openvpn\log\sopenvpn.log

# Установка уровня подробности ведения файла журнала:
# 0 - 'тихий' режим, пишутся только фатальные ошибки;
# 4 - разумное значение для обычного использования;
# 5 и 6 могут помочь выяснить причины проблем подключения;
# 9 - высший уровень подробности;
verb 3
```

Определив конфигурацию, следует запустить сервер из интерпретатора командной строки 'cmd.exe':

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\alexis>cd c:\openvpn

c:\openvpn>bin\openvpn.exe --config c:\openvpn\server.conf
```

Следует отметить, что запуск выполняется с правами суперпользователя и с учётом специфичности OpenVPN, использующего специфичные же библиотеки.

После успешного запуска в файле журнала OpenVPN должна появиться запись 'Initialization Sequence Completed'.

Запуск клиента OpenVPN, соответствующего требованиям ГОСТ, начинается с размещения сертификатов, например, в папке 'C:\openvpn\ssl\certs', в которую следует поместить корневой сертификат 'ca.crt', клиентский сертификат 'client.crt' и ключ 'client.key', а также TLS-ключ 'ta.pem' и файл параметра Диффи-Хельмана '1024.pem'.

Затем следует сформировать конфигурационный файл 'client.conf', содержащий, например, следующие параметры (для краткости комментарии

включены лишь для директив, отличных от применённых в конфигурационном файле сервера):

```
# Определение режима работы OpenVPN в качестве клиента
client

proto tcp-client
dev tun

cd C:\openvpn\ssl\certs
ca ca.crt
cert client.crt
key client.key
dh 1024.dh

# Имя/ip-адрес и порт сервера. Можно определить набор директив 'remote' для
# балансировки нагрузки между серверами.
remote 192.168.0.64 9999

# Режим бесконечных попыток определения имени сервера. Очень полезно
# применять на СБТ, не имеющих постоянного подключения к Интернет (например,
# ноутбуки).
# В директиве 'remote' рассматриваемого примера задан IP-адрес, а не доменное
# имя и в данном случае директива несущественна, но приведена как полезная.
resolv-retry infinite

tls-client
tls-auth ta.key 1
tls-timeout 120
tls-cipher GOST2012-GOST89-GOST89

engine gost
cipher gost89
auth gost-mac

keepalive 10 120

# Режим сохранения постоянного состояния при перезапуске.
persist-key
persist-tun
status C:\openvpn\log\copenvpn-status.log
log C:\openvpn\log\copenvpn.log
verb 4
```

Определив конфигурацию следует запустить клиент:

```
c:\openvpn>bin\openvpn.exe --config c:\openvpn\client.conf
```

После успешного запуска в файле журнала OpenVPN должна появиться запись 'Initialization Sequence Completed', в системе появится новый сетевой интерфейс, а к серверу можно обратиться по внутреннему IP-адресу (например, '10.10.99.1'):

```
# ping 10.10.99.1
PING 10.10.99.1 (10.10.99.1): 56 data bytes
64 bytes from 10.10.99.1: icmp_seq=0 ttl=64 time=0.762 ms
64 bytes from 10.10.99.1: icmp_seq=1 ttl=64 time=0.894 ms
```

```
64 bytes from 10.10.99.1: icmp_seq=2 ttl=64 time=0.962 ms
64 bytes from 10.10.99.1: icmp_seq=3 ttl=64 time=0.798 ms
64 bytes from 10.10.99.1: icmp_seq=4 ttl=64 time=0.831 ms
64 bytes from 10.10.99.1: icmp_seq=5 ttl=64 time=0.734 ms
^C
--- 10.10.99.1 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.734/0.830/0.962/0.078 ms
```

Если на СВТ клиента поступают квитанции на пакеты 'ping', отправленные на сервер по внутреннему VPN-адресу, то VPN-канал, соответствующий требованиям ГОСТ, можно считать работоспособным и готовым для подключения к ПАС с целью терминального управления ТО.

### 6.7. Настройка АГАТ для управления ТО

Настройка АГАТ для выполнения функций удалённого управления ТО осуществляется применением сценария «Настройка удалённого управления ТО» к АГАТ. Данный сценарий предназначен для формирования защищённого VPN-туннеля между АРМ, с которого предполагается вести удалённое управление ТО, подключенным к АГАТ, и VPN-клиентом, встроенным в АГАТ (Рис. 78).

Для применения сценария следует выбрать раздел главного меню *Система* → *Настройки* → *Настройка модулей* и выбрать в древе топологии нужный объект АГАТ. После этого нужно переключить окно свойств в режим отображения «Правила» (см. Рис. 29).

Затем в разделе свойств «АГАТ» следует выбрать пункт «Настройка удалённого управления ТО» и нажать кнопку «Настроить правило», либо дважды щёлкнуть левой кнопкой мыши по выбранному типу. Применить сценарий к выбранному в текущий момент модулю можно также методом захвата и перетаскивания мышью пункта свойств «Настройка удалённого управления ТО».

Список «Настройки» раздела «Параметры» сценария позволяет сформировать VPN-туннель (выбор значения «Настроить туннель») или расформировать ранее сформированный VPN-туннель (выбор значения «Отключить туннель»). Перезапуск туннеля осуществляется

последовательным выбором значений «Отключить туннель» и «Настроить туннель» с применением настроек.

В разделе «Подробные настройки» следует определить значения сетевых реквизитов VPN-сервера, управляющего формируемым VPN-туннелем:

- «Хост» – IP-адрес или доменное имя;
- «Порт» – номер сетевого порта.

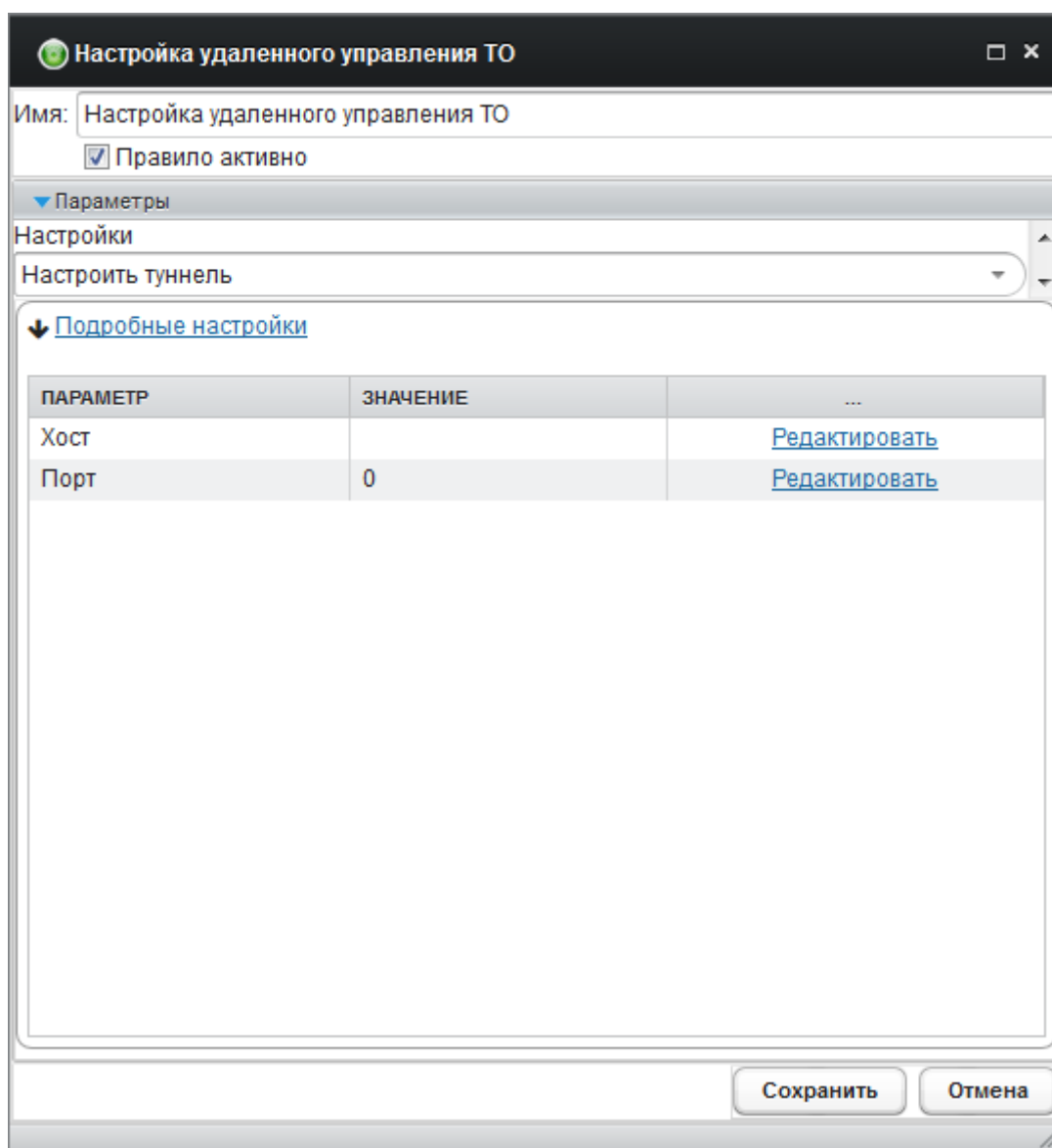


Рис. 78. Окно определения параметров удалённого управления ТО.

После определения настроек следует нажать кнопку «Сохранить», а в окне «Настройка модулей» выбрать раздел меню «Применить настройки» для их фиксации в БД и применения к АГАТ.

### **6.8. Сеанс удалённого управления ТО**

Для осуществления терминального управления ТО по протоколу TELNET или SSH с применением защищённого VPN-подключения сетевые реквизиты развёрнутого VPN-сервера (IP-адрес и порт) необходимо определить в настройках АГАТ через интерфейс системы аудита и сформировать VPN-канал (см. п. 5.6 настоящего документа). После этого можно подключаться к АГАТ с помощью VPN-клиента, развёрнутого на АРМ управления ТО.

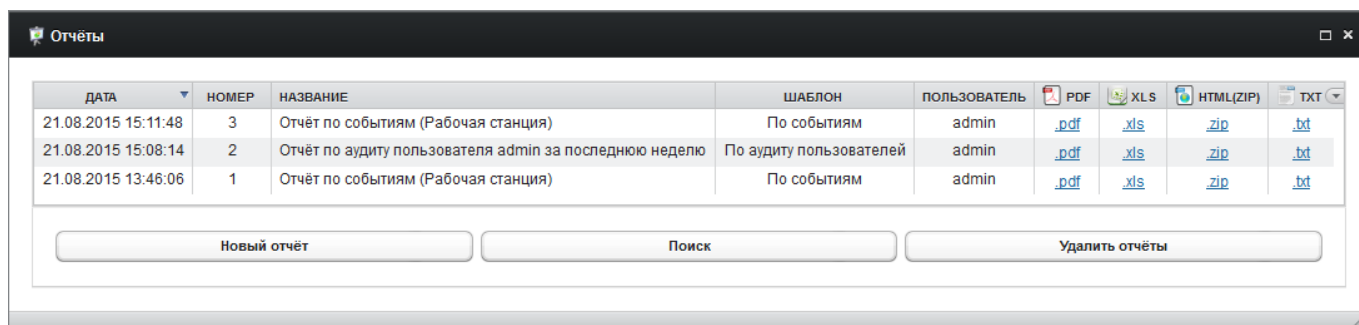
*Примечание.* В случае применения межсетевого экрана в ЛВС необходимо обеспечить транзит сетевых пакетов на порт VPN-сервера.

Динамический IP-адрес встроенного VPN-клиента АГАТ для подключения через VPN-канал можно узнать из файла журнала VPN-сервера или определить статически в соответствии с MAC-адресом АГАТ. За справкой по определению параметров конфигурации следует обращаться к документации проекта OpenVPN.

Для завершения сеанса удалённого управления ТО по протоколам TELNET или SSH следует закрыть терминал либо дать с новой строки команду управления '~.' и нажать клавишу 'Enter'.

## 7. Аналитика событий

Средством отложенной аналитики событий, происходивших на контролируемых рабочих местах и накопленных в БД, являются «Отчеты». Для начала работы с ними следует выбрать раздел меню *Инструменты* → *Отчёты* (Рис. 79).



The screenshot shows a window titled «Отчёты» with a table of reports and three buttons below it. The table has columns for date, number, name, template, user, and download links for PDF, XLS, HTML(ZIP), and TXT formats.

ДАТА	НОМЕР	НАЗВАНИЕ	ШАБЛОН	ПОЛЬЗОВАТЕЛЬ	PDF	XLS	HTML(ZIP)	TXT
21.08.2015 15:11:48	3	Отчёт по событиям (Рабочая станция)	По событиям	admin	<a href="#">.pdf</a>	<a href="#">.xls</a>	<a href="#">.zip</a>	<a href="#">.txt</a>
21.08.2015 15:08:14	2	Отчёт по аудиту пользователя admin за последнюю неделю	По аудиту пользователей	admin	<a href="#">.pdf</a>	<a href="#">.xls</a>	<a href="#">.zip</a>	<a href="#">.txt</a>
21.08.2015 13:46:06	1	Отчёт по событиям (Рабочая станция)	По событиям	admin	<a href="#">.pdf</a>	<a href="#">.xls</a>	<a href="#">.zip</a>	<a href="#">.txt</a>

Buttons: Новый отчёт, Поиск, Удалить отчёты

Рис. 79. Окно «Отчёты».

Окно содержит таблицу, в которую помещаются готовые отчёты, сформированные по заказу администратора. Таблица включает следующие графы:

- «*Дата*» содержит дату окончания формирования отчёта (отражается на титульном листе сформированного отчёта);
- «*Номер*» содержит инвентарный номер отчёта по порядку (отражается на титульном листе сформированного отчёта);
- «*Название*» содержит наименование отчёта, определённое администратором при заказе (отражается на титульном листе сформированного отчёта);
- «*Шаблон*» содержит наименование шаблона, по которому сформирован отчёт;
- «*Пользователь*» содержит идентификатор администратора, заказавшего формирование отчёта (отражается на титульном листе сформированного отчёта);
- «*PDF*» содержит ссылку на загрузку сформированного отчёта в формате Adobe Portable Document Format;

- «*XLS*» содержит ссылку на загрузку сформированного отчёта в формате Microsoft Excel;
- «*HTML(ZIP)*» содержит ссылку на загрузку сформированного отчёта в формате HyperText Markup Language, упакованного в архив формата ZIP;
- «*TXT*» содержит ссылку на загрузку сформированного отчёта в текстовом формате.

Восходящая (значок '▲') / нисходящая (значок '▼') сортировка списка готовых отчётов осуществляется щелчком левой кнопки мыши по нужной графе. Управление отображением отдельных граф осуществляется по щелчку левой кнопки мыши на значке '▼' с правой стороны строки заголовков граф.

Создание нового отчёта начинается нажатием кнопки «Новый отчёт» (рис. 36). В дочернем диалоговом окне следует выбрать тип формируемого отчёта:

- «*По аудиту пользователей*» (\*);
- «*По мониторингу объектов*»;
- «*По подключению датчиков*»;
- «*По инцидентам*».

Выбор последнего пункта списка («Мастер создания отчётов») инициирует процесс пошагового определения параметров формирования отчёта любого типа.

Также «Мастер создания отчётов» позволяет формировать отчёты по шаблонам, заранее созданным администратором. Для этого на странице «Тип отчёта» следует выбрать пункт списка «ПО СОХРАНЁННОМУ ШАБЛОНУ ОТЧЁТА» и нажать кнопку «Далее», выбрав нужный ранее сохранённый шаблон.

В качестве шаблонов могут быть сохранены отчёты, имеющие признак «(\*)». Сохранение отчёта в качестве шаблона выполняется установкой флага



«Сохранить это задание как шаблон отчёта» на шаге определения его параметров в «Мастере создания отчётов».

**Отчёт «По аудиту пользователей»** отражает активность пользователей графического интерфейса администратора. Отчёт формируется с возможностью выбора пользователя САИБ (для быстрого поиска предусмотрен фильтр), временного интервала, уровня приоритетности событий («Информация», «Предупреждение», «Критическое сообщение») и названия отчёта (в разрезе пользователя) для его последующей идентификации в таблице готовых отчётов.

Ссылка «Источники и типы событий» позволяет управлять полнотой отражения данных в отчёте с помощью установки нужных флагов в иерархии. По умолчанию выбраны все источники событий и типы. Иерархия включает следующие источники:

- *«Инциденты»;*
- *«Настройка модулей»;*
- *«Система отчётов»;*
- *«Одобрение локальных установок»;*
- *«Удалённая установка»;*
- *«Система».*

Для параллельного формирования отчёта по нескольким пользователям следует выбрать записи нужных указателем мыши или клавишами управления курсором клавиатуры (с удержанием клавиши 'Ctrl' или 'Shift').

**Отчёт «По мониторингу объектов»** отражает факты нарушения правил, определённых для контролируемых рабочих мест, а также факты отклонения от нормы состояния датчиков АГАТ.

Отчёт формируется с возможностью выбора анализируемого объекта САИБ (РС, сценарий сетевого сенсора или АГАТ, датчик АГАТ) из древа топологии, типов событий, временного интервала, уровня приоритетности событий («Информация», «Предупреждение», «Критическое сообщение») и

названия отчёта для его последующей идентификации в таблице готовых отчётов (после выбора объекта).

**Отчёт «По подключению датчиков»** отражает конфигурацию внешних датчиков, подключенных к АГАТ в графическом интерфейсе администратора САИБ, с указанием типов датчиков и занятых ими групп контактов коммуникационных интерфейсов с отображением на схеме задней панели АГАТ.

*Примечание.* Для отражения фактической (физической) картины подключения датчиков последние должны быть подключены к АГАТ в строгом соответствии с данными отчёта.

Отчёт формируется с возможностью выбора анализируемого АГАТ из древа топологии и названия отчёта для его последующей идентификации в таблице готовых отчётов (после выбора объекта).

**Отчёт «По инцидентам»** формируется по фактам отдельных инцидентов, возбужденных в САИБ, и отражает зафиксированные нарушения и сообщения, соответствующие выбранному инциденту.

Для заказа отчёта выбранного типа по окончании определения его параметров следует нажать кнопку «Сформировать отчёт», после чего новый отчёт добавляется в очередь на формирование. Ход формирования отражается в графе «PDF». О завершении процесса и готовности отчёта к выгрузке сигнализируют ссылки в графах «PDF», «XLS», «HTML(ZIP)» и «TXT». Загрузка отчёта нужного формата осуществляется выбором ссылки соответствующей графы.

Для удаления отдельных отчётов следует выбрать записи ненужных указателем мыши или клавишами управления курсором клавиатуры и нажать кнопку «Удалить отчёты» (последует запрос подтверждения принятого решения). Выбор нескольких записей осуществляется удержанием клавиши 'Ctrl' или 'Shift'.

Кнопка «Поиск» активирует панель мгновенной фильтрации готовых отчётов для быстрого отбора. Отбор отчётов осуществляется по заданным критериям временного интервала, названия отчёта, шаблона и пользователя. В текстовых полях «Название отчёта» и «Пользователь» можно определять подстроки. Активированная панель фильтрации скрывается нажатием кнопки «Скрыть поиск».

## **8. Системные операции**

### **8.1. Настройка уведомлений**

Администратор имеет возможность настройки полноты информирования о системных событиях в окне «Уведомления» графического интерфейса, выбрав раздел главного меню *Система* → *Настройки* → *Настройка уведомлений*. Настройка категорий сообщений выполняется в дочернем окне.

Флаг «Показывать системные оповещения» (по умолчанию установлен) включает отображение всех уведомлений САИБ.

Флаг «Показывать открытые инциденты» (по умолчанию установлен) включает отображение оповещений о возбужденных инцидентах со статусами «Открыт» и «В работе» (см. п. 5.7.8 настоящего документа).

Флаг «Показывать инциденты в работе» (по умолчанию установлен) включает отображение уведомлений по инцидентам, имеющим лишь статус «В работе» (см. п. 5.7.8 настоящего документа).

По окончании настройки уведомлений дочернее окно следует закрыть кнопкой '×' (фиксация в БД внесённых изменений произойдёт при закрытии окна).

При наличии в САИБ действительных уведомлений окно «Уведомления» отображается автоматически при авторизации в графическом интерфейсе пользователя, входящего в любую группу независимо от полномочий.

Уведомление отображается в виде ссылки, выбор которой приводит к вызову окна с параметрами события, о котором уведомляется администратор САИБ (Рис. 80).

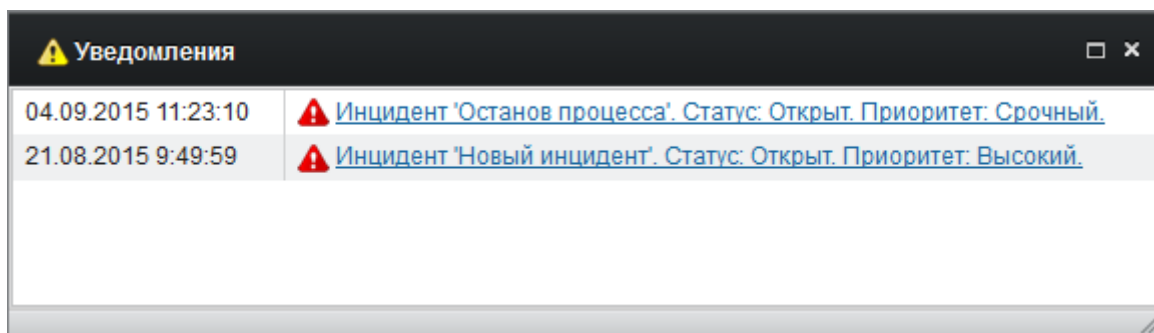


Рис. 80. Окно «Уведомления».

## 8.2. Резервное копирование

В целях обеспечения бесперебойной работы САИБ и сохранности собранных данных о событиях следует проводить регулярное резервное копирование БД. Все операции, связанный с этой задачей, доступны в разделе главного меню *Система* → *Резервное копирование* (Рис. 81).

*Примечание.* Резервное копирование БД также можно выполнять с помощью инструментальных средств, входящих в поставку СУБД, выбранной при установке Сервера.

В диалоговом окне представлен список файлов резервных копий, сохранённых на Сервере к моменту вызова инструмента. Для создания свежей резервной копии следует выбрать раздел меню *Файл* → *Создать файл резервной копии на сервере*. Время создания резервной копии зависит от объёма БД.

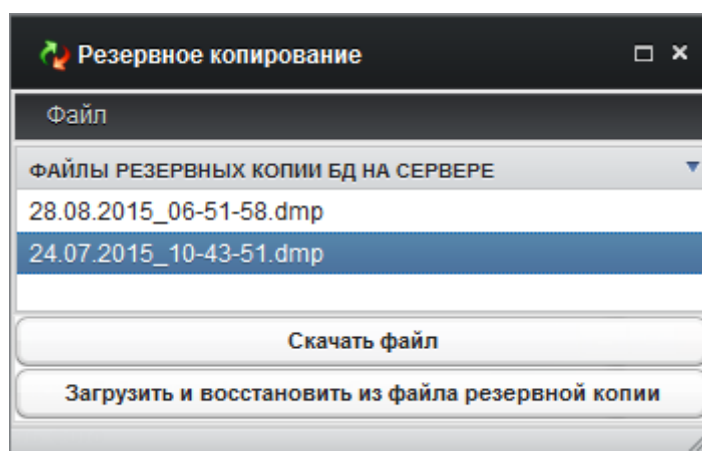


Рис. 81. Окно «Резервное копирование».

Созданный файл резервной копии хранится на Сервере. Однако, для обеспечения его сохранности и доступности в случае отказа СВТ, на котором установлен Сервер, файл резервной копии следует выгрузить и сохранить на внешнем носителе.

Для загрузки файла резервной копии на рабочее место администратора указателем мыши или клавишами управления курсором клавиатуры следует выбрать имя нужной резервной копии и нажать кнопку «Скачать файл» (последует стандартное приглашение на загрузку Web-обозревателя).

После выгрузки резервных копий на рабочее место все или отдельные файлы можно удалить с Сервера. Для удаления одного файла следует выбрать имя ненужной резервной копии указателем мыши или клавишами управления курсором клавиатуры и выбрать раздел меню *Файл* → *Удалить файл резервной копии на сервере*. Для удаления всех резервных копий с Сервера следует выбрать раздел меню *Файл* → *Удалить все резервные копии на сервере* (последует запрос подтверждения принятого решения).

При необходимости восстановления данных из файла резервной копии следует нажать кнопку «Загрузить и восстановить из файла резервной копии» (последует стандартный диалог ОС для выбора файла).

*Примечание. Восстановление данных из резервной копии приводит к полному замещению текущих данных в БД.*

**Список сокращений**

*nix	– операционная система семейства Unix
АГАТ	– аппаратно-программный сенсор серверного оборудования и телекоммуникационных средств, устанавливаемый в телекоммуникационную стойку
АИС	– автоматизированная информационная система
АРМ	– автоматизированное рабочее место
БД	– база данных
ИБП	– источник бесперебойного питания
ОПО	– общее программное обеспечение
КОНСОЛЬ	– консоль управления средством аудита информационной безопасности
ЛВС	– локальная вычислительная сеть
РС	– программный сенсор, устанавливаемый на серверное оборудование и рабочие станции информационной системы
ОС	– операционная система
ПО	– программное обеспечение
БД	– подсистема хранения информации
ПЭВМ	– персональная электронная вычислительная машина
САИБ	– средство аудита информационной безопасности
СВТ	– средство вычислительной техники
СПО	– специальное программное обеспечение
СПС	– специальные программные средства
СУ	– сервер управления программным комплексом
ТО	– телекоммуникационное оборудование

**Термины и определения**

***Контролируемое рабочее место*** – пользовательское или серверное СВТ с установленной РС.

***Нарушение правила (сценария)*** – событие САИБ, обусловленное фактом успешного применения условий определённого правила (сценария) к событию программной среды контролируемого рабочего места (элементу сетевой инфраструктуры).

***Инцидент*** – нарушение правила, которому присвоен важный или критический уровень приоритета инцидентности.



185

ПМБИ.10145-01 90 01

**Для заметок**

