Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. Сервер мониторинга

Руководство администратора

ViPNet®
Virtual Private Network
infotecs®

1991–2014 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00056-08 32 01

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение ... **9**
О документе ... 10
Для кого предназначен документ ... 10
Соглашения документа ... 10
О программе Сервер мониторинга ... 12
Системные требования ... 12
Требования к версиям ПО ViPNet ... 13
Рекомендации по настройке браузера Internet Explorer ... 14
Лицензирование Сервера мониторинга ... 16
Комплект поставки ... 17
Информация о сторонних компонентах ... 18
Новые возможности версии 4.3 ... 19
Обратная связь ... 25

Глава 1. Принципы организации мониторинга ... **26**
Механизм работы Сервера мониторинга ... 27
Средства анализа информации ... 28
Разделение событий по уровням критичности ... 29
Каскадирование Серверов мониторинга ... 30
Управление правилами анализа в каскаде ... 33
Мониторинг кластера горячего резервирования ... 36
Мониторинг узлов по протоколу SNMP ... 37
Взаимодействие с ПАК ViPNet IDS ... 39
Управление Сервером мониторинга ... 40

Глава 2. Установка, обновление и удаление сервера мониторинга ... **41**
Последовательность установки ПО Сервер мониторинга ... 42
Порядок установки обязательного ПО ... 43
Установка ПО Сервер мониторинга ... 47
Проверка правильности установки ПО Сервер мониторинга ... 54
Установка обновлений для стороннего ПО ... 55
Порядок обновления ПО Сервер мониторинга ... 57

Обновление ПО Сервер мониторинга ... 58
Порядок обновления ПО Сервера мониторинга при каскадной организации системы мониторинга ... 62
Обновление пакета настроек ... 64
Удаление ПО Сервер мониторинга ... 66
Подключение к Серверу мониторинга ... 68

Глава 3. Настройка Сервера мониторинга ... 70
Настройка Сервера мониторинга с помощью мастера ... 71
Настройка учетных записей ... 77
Создание и изменение учетной записи ... 78
Удаление учетной записи ... 81
Смена пароля ... 81
Настройка узлов и групп мониторинга ... 83
Создание и изменение группы мониторинга ... 86
Добавление открытых узлов в список связей Сервера мониторинга ... 88
Перемещение новых узлов в группу мониторинга ... 89
Изменение параметров мониторинга узла ... 91
Удаление узла или группы мониторинга ... 93
Удаление открытого узла из списка связей Сервера мониторинга ... 94
Настройка типов узлов мониторинга ... 95
Настройка правил анализа ... 97
Создание и изменение правила анализа ... 98
Задание и изменение параметров правила с помощью конструктора ... 101
Копирование правила анализа ... 104
Удаление правила анализа ... 104
Настройка оповещений ... 106
Способы оповещения ... 107
Создание и изменение шаблонов оповещений ... 109
Настройка визуальных оповещений ... 111
Настройка звуковых оповещений ... 111
Настройка оповещений по электронной почте ... 112
Настройка оповещений по Деловой почте ... 114
Настройка оповещений по SMS ... 115
Настройка оповещений по протоколу Syslog ... 116
Отслеживание событий, связанных с фильтрацией трафика ... 118
Настройка подключения к прокси-серверу ... 119

Настройка карты ... 121
Добавление узлов на карту в соответствии с их координатами ... 125
Настройка каскада ... 127
Добавление Сервера мониторинга в каскад ... 128
Действия администратора дочернего Сервера мониторинга при включении его сервера в каскад ... 130
Удаление Сервера мониторинга из каскада ... 132
Экспорт и импорт настроек Сервера мониторинга ... 133
Особенности импорта настроек ... 135
Тонкая настройка Сервера мониторинга ... 137
Секция [collection] ... 139
Секция [storage] ... 139
Секция [control] ... 140
Секция [sms] ... 143
Секция [gis] ... 144
Секция [export] ... 144
Настройка экспорта необработанных параметров узлов на сетевой ресурс ... 145
Секция [bm] ... 147
Формат расписания ... 147
Ротация данных ... 148
Просмотр журнала событий ... 151

Глава 4. Правила анализа ... 154
Компоненты правил анализа ... 155
Синтаксис правил анализа ... 157
Переменные ... 157
Комментарии ... 157
Типы данных ... 157
Функции ... 158
Операторы ... 158
Объекты и методы для доступа к значениям параметров узлов ... 160
Коллекции ... 162
Объекты и методы для получения вспомогательных параметров ... 163
Объект для доступа к уровням критичности ... 164
Объекты и методы для задания оповещений ... 164
Объекты и методы для записи сообщений в журнал для правил анализа ... 165

Примеры синтаксиса ... 165
Проверка синтаксиса правила анализа ... 168

Глава 5. Резервное копирование и восстановление ... 169
Порядок проведения резервного копирования ... 170
Резервирование и восстановление конфигурационных файлов и отладочных журналов ... 171
Резервирование баз данных ... 172
Определение основных показателей базы данных мониторинга ... 176
Восстановление баз данных ... 179
Восстановление баз данных без переустановки ПО Сервер мониторинга ... 179
Восстановление баз данных после установки ПО Сервер мониторинга ... 188
Проверка корректности восстановления ... 189

Приложение A. Возможные неполадки и способы их устранения ... 190
Не удается установить или запустить PostgreSQL ... 190
Время на Сервере мониторинга не соответствует времени операционной системы ... 192
Неограниченный рост базы данных ... 193
Проблемы при записи событий мониторинга в базу данных ... 194
Не удается запустить службу Apache Tomcat ... 194
Проблемы при подключении к Серверу мониторинга через веб-интерфейс ... 195
Проблемы доступа и аутентификации на АРМ мониторинга ... 196
Не открывается окно информации об узле мониторинга ... 196
Проблемы при использовании прокси-сервера ... 197
Не удается установить каскад ... 197

Приложение B. Создание и изменение шаблонов писем оповещений ... 199

Приложение C. Контролируемые параметры ... 203
Контролируемые параметры узлов мониторинга ... 204
Контролируемые параметры открытых узлов ... 227
Контролируемые параметры ПАК ViPNet IDS ... 242

Приложение D. Шаблон файла импорта открытых узлов ... 247

Приложение E. Показатели производительности системы мониторинга ... 249

Нефункциональные характеристики ПК ViPNet StateWatcher 249
Расчет нагрузки на трафик при использовании ПК ViPNet StateWatcher..... 251

Приложение F. Дополнительные настройки в ОС Windows 253
Настройка службы SNMP на открытом узле 253
Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows..... 257

Приложение G. Встроенные правила анализа 260
Встроенные правила анализа для защищенных узлов 261
Состояние узла 261
Статус программы Монитор 262
Статус программы Деловая почта 262
Статус программы Failover..... 263
Статус программы MFTP 264
Уровень безопасности..... 264
Изменение версии ПО ViPNet..... 267
Прикладные задачи 268
Превышение порога для системных ресурсов..... 269
Тип межсетевого экрана 270
Параметры сетевых интерфейсов 271
Параметры MFTP 275
Журнал ОС 276
Переключение кластера..... 278
Состояние пассивного элемента кластера 279
Встроенные правила анализа для открытых узлов..... 280
Установка приложения 280
Удаление приложения..... 281
Запуск сервисов 281
Остановка сервисов..... 282
Загрузка оперативной памяти 283
Загрузка дисков 284
Скачок атак высокого уровня текущего сенсора IDS 284
Общий скачок атак текущего сенсора..... 285

Приложение H. Глоссарий 287

Приложение I. Указатель 294

Введение

О документе 10

О программе Сервер мониторинга 12

Новые возможности версии 4.3 19

Обратная связь 25

О документе

В данном документе описывается назначение и применение программы Сервер мониторинга, которая входит в программный комплекс мониторинга защищенных сетей ViPNet StateWatcher (далее — ПК ViPNet StateWatcher). В руководстве описаны основные возможности программы Сервер мониторинга, принципы работы с программой, приведено описание пользовательского интерфейса.

Данный документ является частью комплекта документов ПК ViPNet StateWatcher 4.3. В комплект документов ПК ViPNet StateWatcher 4.3 входят следующие документы:

- «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. Общее описание».
- «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. Сервер мониторинга. Руководство администратора» (данный документ).
- «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. АРМ мониторинга. Руководство пользователя».

Для кого предназначен документ

Данный документ предназначен для администраторов, отвечающих за установку и настройку ПО Сервер мониторинга.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.

Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе Сервер мониторинга

Программа Сервер мониторинга является частью ПК ViPNet StateWatcher.

Основной функцией Сервера мониторинга является сбор и анализ информации о текущем состоянии узлов сети ViPNet (см. «Узел мониторинга» на стр. 292) и установленных на них программ ViPNet (Client, Cluster, Coordinator, Coordinator Linux, Coordinator HW), а также оперативное уведомление о событиях, обнаруженных на узлах. Для сбора информации Сервер мониторинга устанавливается на узел сети ViPNet, оснащенный ОС Windows, ПО ViPNet Client и некоторым сторонним ПО, необходимым для корректной работы.

Для управления Сервером мониторинга используется автоматизированное рабочее место (АРМ) мониторинга, представляющее собой узел сети ViPNet с веб-браузером, которому в программе ViPNet Центр управления сетью разрешен доступ к узлу Сервера мониторинга. Описание АРМ мониторинга содержится в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. АРМ мониторинга. Руководство пользователя».

Системные требования

Требования к компьютеру для установки ПО Сервер мониторинга:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 4 Гбайт.

  Использование ресурсов оперативной памяти и процессора ПО Сервер мониторинга зависит от количества контролируемых узлов, активных правил анализа и количества собираемых параметров. При использовании ПО Сервер мониторинга с высокой нагрузкой рекомендуется устанавливать данное ПО на компьютеры с операционной системой Windows Server 2008 R2 и объемом оперативной памяти не менее 8 Гбайт.

  Рекомендуемые характеристики компьютера:

  - При нагрузке до 10000 узлов мониторинга рекомендуется: процессор Intel Core 2 1.8 ГГц или более производительный, объем оперативной памяти от 8 Гбайт, свободное место на жестком диске от 100 Гбайт.

- При нагрузке до 20000 узлов мониторинга рекомендуется: процессор Intel Core 2 Quad 2.8 ГГц или более производительный, объем оперативной памяти от 16 Гбайт, свободное место на жестком диске от 200 Гбайт.

Примечание. Для уменьшения нагрузки на Сервер мониторинга предлагается использовать два и более сервера с распределением контролируемых узлов между ними.

Внимание! Данные о состоянии связей между узлами ViPNet значительно повышают нагрузку на Сервер мониторинга, поэтому рекомендуется либо отключать сбор данных о состоянии связей, либо ограничиваться сбором данных о состоянии связей только между координаторами (см. «Изменение параметров мониторинга узла» на стр. 91), либо увеличить объем оперативной памяти и свободного мести на жестком диске.

- Операционная система — Windows Server 2008 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Server 2012 (64-разрядная), Server 2012 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная).

  Перед установкой программы рекомендуется установить последний пакет обновлений для операционной системы.

- Программное обеспечение — ViPNet Client версии 4.2.2 (34345).
- Установленные последние обновления операционной системы Windows.
- Доступ в Интернет в случае отправки оповещений по SMS.

Требования к версиям ПО ViPNet

На сетевых узлах, задействованных в процессе мониторинга сети с помощью ПК ViPNet StateWatcher, должны быть установлены следующие версии ПО ViPNet:

- На сетевом узле, на котором будет функционировать ПО Сервер мониторинга, должно быть установлено ПО ViPNet Client не ниже версии 4.2.2 (34345).

  Требования к аппаратной конфигурации Сервера мониторинга и установке прочего ПО содержатся в разделе «Системные требования (на стр. 12)» данного документа.

- На сетевом узле, который будет использоваться в качестве АРМ мониторинга, должно быть установлено ПО ViPNet Client не ниже версии 4.2.2 (34345).

Прочие требования к АРМ мониторинга содержатся в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. АРМ мониторинга. Руководство пользователя».

На сетевом узле, используемом в качестве Центра управления сетью (ЦУС) (см. «ViPNet Центр управления сетью (ЦУС)» на стр. 287), должна быть установлена программа ViPNet Центр управления сетью версии 4.4.0.

Рекомендации по настройке браузера Internet Explorer

Для корректного отображения веб-интерфейса веб-браузер Internet Explorer не должен работать в режиме совместимости.

Если вы используете браузер Internet Explorer 9 и операционную систему Windows Server 2008 R2, отключите конфигурацию усиленной безопасности. Для этого выполните соответствующие действия:

1. В меню **Пуск** выберите пункт **Панель управления**.
2. В окне **Все элементы панели управления** щелкните **Программы и компоненты**.
3. В окне **Программы и компоненты** щелкните ссылку **Включение или отключение компонентов Windows**.
4. В окне **Диспетчер сервера** в группе **Сводка сервера** > **Сведения системы безопасности** щелкните ссылку **Настроить конфигурацию усиленной безопасности Internet Explorer**.

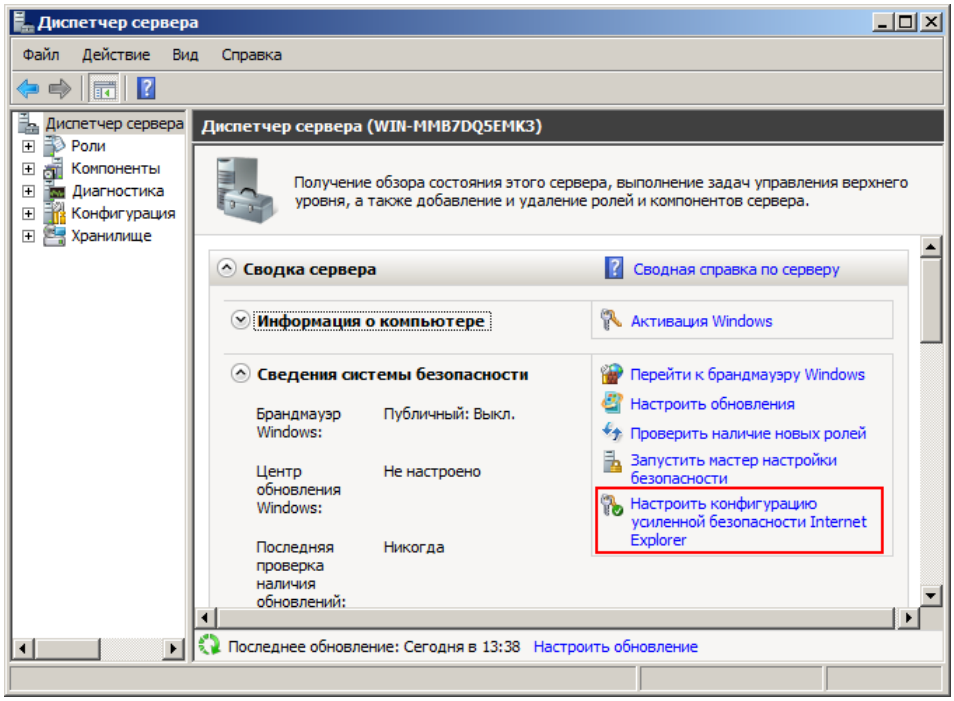

Рисунок 1: Настройка конфигурации усиленной безопасности Internet Explorer

5 В появившемся окне установите переключатели **Администраторы** и **Пользователи** в положение **Отключить** и нажмите кнопку **OK**.

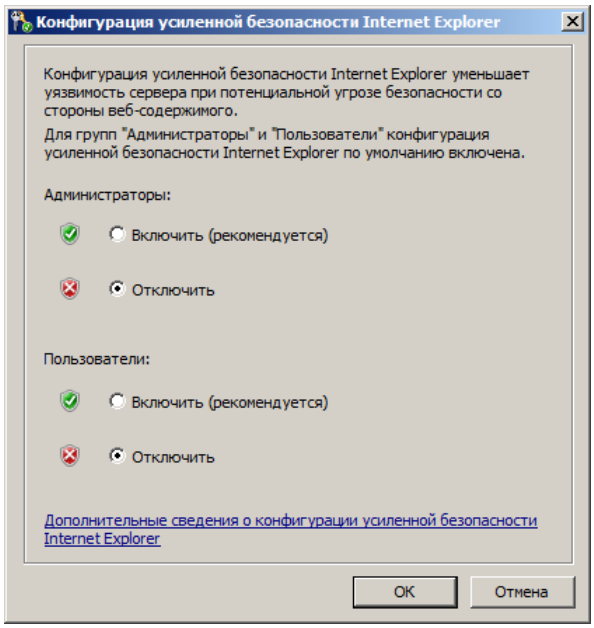

Рисунок 2: Отключение конфигурации усиленной безопасности Internet Explorer

Лицензирование Сервера мониторинга

ViPNet клиент, который будет использоваться в качестве Сервера мониторинга, должен быть зарегистрирован в роли «StateWatcher» в одной из программ:

- ViPNet Центр управления сетью (при использовании системы мониторинга в сети, развернутой на базе ПО ViPNet Administrator). В свойствах роли можно задать максимальное количество узлов, за которыми может наблюдать данный Сервер мониторинга, а также максимальное количество дочерних Серверов мониторинга.
- ViPNet Network Manager (при использовании системы мониторинга в сети, развернутой на базе ПО ViPNet VPN). Максимальное количество узлов мониторинга определяется лицензионным ограничением.

Наличие регистрации в роли «StateWatcher» и текущее количество узлов мониторинга проверяется при старте ПО Сервер мониторинга, а также периодически в процессе его работы. В процессе работы может увеличиваться текущее количество узлов за счет добавления новых узлов (узлов из группы **Узлы для добавления в мониторинг**) в группы мониторинга, а также может быть уменьшено ограничение лицензии по числу узлов. Если регистрация отсутствует или текущее количество узлов мониторинга превышает количество, предусмотренное лицензией, то появляется соответствующее сообщение и Сервер мониторинга останавливает сбор данных с узлов мониторинга и блокирует доступ к полученной информации. Для продолжения корректной работы Сервера мониторинга уменьшите количество узлов с включенным мониторингом (см. «Удаление узла или группы мониторинга» на стр. 93) до количества, разрешенного в лицензии.

Примечание. При проверке текущего количества узлов мониторинга учитываются узлы всех групп, кроме узлов из группы **Узлы для добавления в мониторинг**, независимо от того, включен в данный момент их мониторинг или нет.

Удаление и возобновление регистрации Сервера мониторинга в роли «StateWatcher» влияет на его взаимодействие с другими Серверами мониторинга в рамках каскада. При удалении регистрации прекращается взаимодействие Сервера мониторинга в каскаде. В этом случае Сервер мониторинга становится обычным объектом мониторинга для всех своих дочерних Серверов мониторинга и автоматически добавляется в группу **Узлы для добавления в мониторинг** на дочерних Серверах мониторинга. При возобновлении регистрации Сервер мониторинга появится в списке кандидатов на установление отношений в каскаде у всех Серверов мониторинга, с которыми у него есть связь в рамках сети ViPNet.

Все события, связанные с нарушением условий лицензирования, фиксируются в журнале событий (см. «Просмотр журнала событий» на стр. 151), который хранится в базе данных Сервера мониторинга.

Комплект поставки

В комплект поставки ПК ViPNet StateWatcher входят компоненты, представленные в таблице ниже.

Таблица 3. Комплект поставки ПК ViPNet StateWatcher

	Наименование	Имя файла
ПО для Сервера мониторинга		
	Дистрибутив ПО Сервер мониторинга	`StateWatcherInstaller.jar`
	Пакет настроек	`default_pn.zip`
	Пакет обновления часовых поясов для виртуальной машины Java	`utimezone.zip`
	ПО для 32-разрядной ОС	
	Дистрибутив веб-сервера Apache Tomcat версии 6.0.29	`apache-tomcat-6.0.29.exe`
	Дистрибутив СУБД PostgreSQL версии 9.1.4-1	`postgresql-9.1.4-1-windows.exe`
	Дистрибутив комплекта средств разработки Oracle Java Sun JDK версии 7u21	`jdk-7u21-windows-i586.exe`
	ПО для 64-разрядной ОС	
	Дистрибутив веб-сервера Apache Tomcat версии 6.0.33	`apache-tomcat-6.0.33.exe`
	Дистрибутив СУБД PostgreSQL версии 9.1.4-1	`postgresql-9.1.4-1-windows-x64.exe`
	Дистрибутив комплекта средств разработки Oracle Java Sun JDK версии 7u21	`jdk-7u21-windows-x64.exe`
ПО для АРМ мониторинга		
	Дистрибутив Adobe Flash Player для браузера Mozilla Firefox	`flashplayer_11_plugin_debug_32bit.exe`

	Наименование	Имя файла
	Дистрибутив Adobe Flash Player для браузера Internet Explorer	`flashplayer_11_ax_debug_32bit.exe`
	Дистрибутив Adobe Flash Player для браузера Google Chrome	в комплекте поставки отсутствует, так как входит в состав самого браузера Google Chrome
	Дистрибутив графического редактора шаблонов iReport версии 3.7.6 (можно найти по ссылке http://jasperforge.org/projects/ireport/)	`iReport-3.7.6-windows-installer.exe`
Документация в формате PDF	Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. Общее описание	`vipnet_statewatcher.pdf`
	Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. АРМ мониторинга. Руководство пользователя	`vipnet_statewatcher_userguide.pdf`
	Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 4.3. Сервер мониторинга. Руководство администратора	`vipnet_statewatcher_admguide.pdf`

Информация о сторонних компонентах

В данном разделе содержится информация о сторонних компонентах, которые используются в ПО Сервер мониторинга.

OpenStreetMap

© Участники OpenStreetMap (http://www.openstreetmap.org/) по лицензии Open Data Commons Open Database License (ODbL) | Open Data Commons (http://opendatacommons.org/licenses/odbl/) \ CC-BY-SA (http://creativecommons.org/licenses/by-sa/2.0/).

Компания-производитель ПО ViPNet StateWatcher не несет ответственности за корректность гео-данных, предоставляемых проектом OpenStreetMap.

Новые возможности версии 4.3

В этом разделе представлен краткий обзор изменений и новых возможностей ПК ViPNet StateWatcher версии 4.3 по сравнению с версией 4.2.1. Информация об изменениях в предыдущих версиях системы мониторинга содержится в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. Общее описание» в приложении История версий.

- **Мониторинг узлов с помощью инфопанели**

  Для получения актуальной информации об узлах мониторинга в удобном формате у пользователей появилась возможность настроить специальную информационную панель, на которой будут отображаться только интересующие их параметры выбранных узлов (страница **Инфопанель**). На инфопанели могут отображаться текущие значения параметров узлов мониторинга, различные графики и карта.

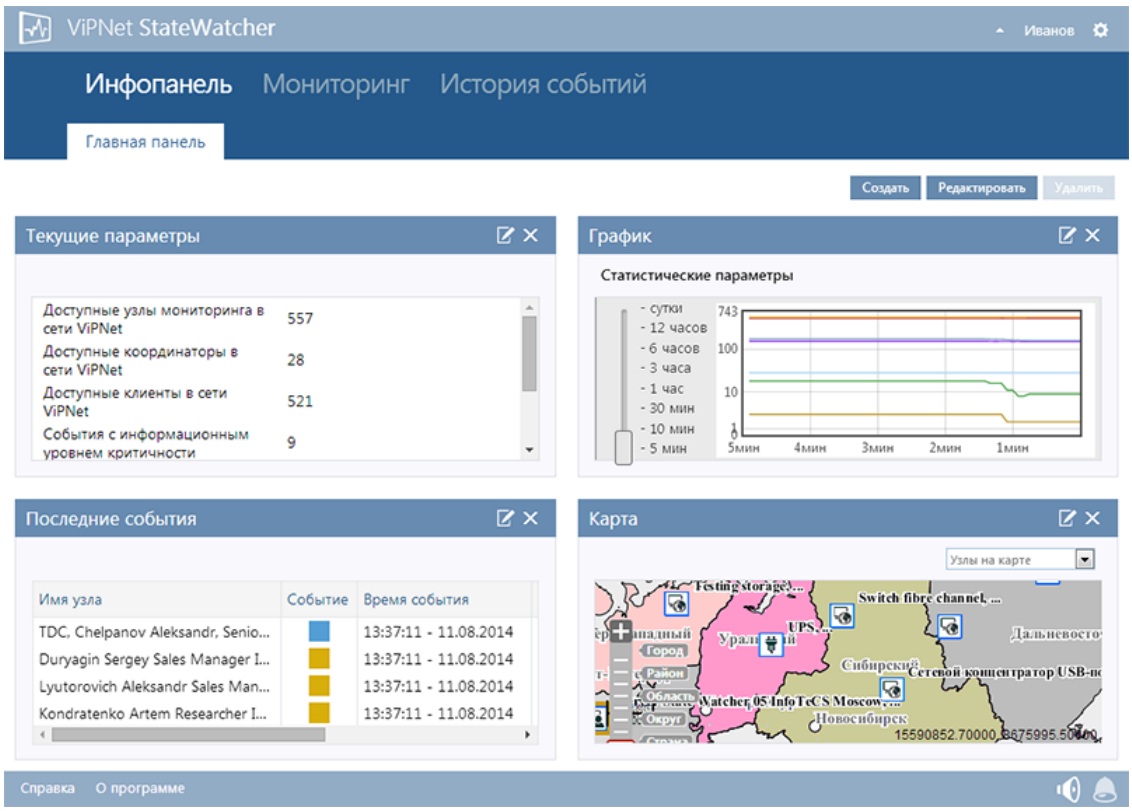

Рисунок 3: Инфопанель

- **Добавление описания узла**

В окне **Информация об узле** появилась новая вкладка **Описание**, которая позволяет пользователям АРМ мониторинга добавлять произвольную информацию об узле. Добавленная информация доступна другим пользователям для просмотра и редактирования.

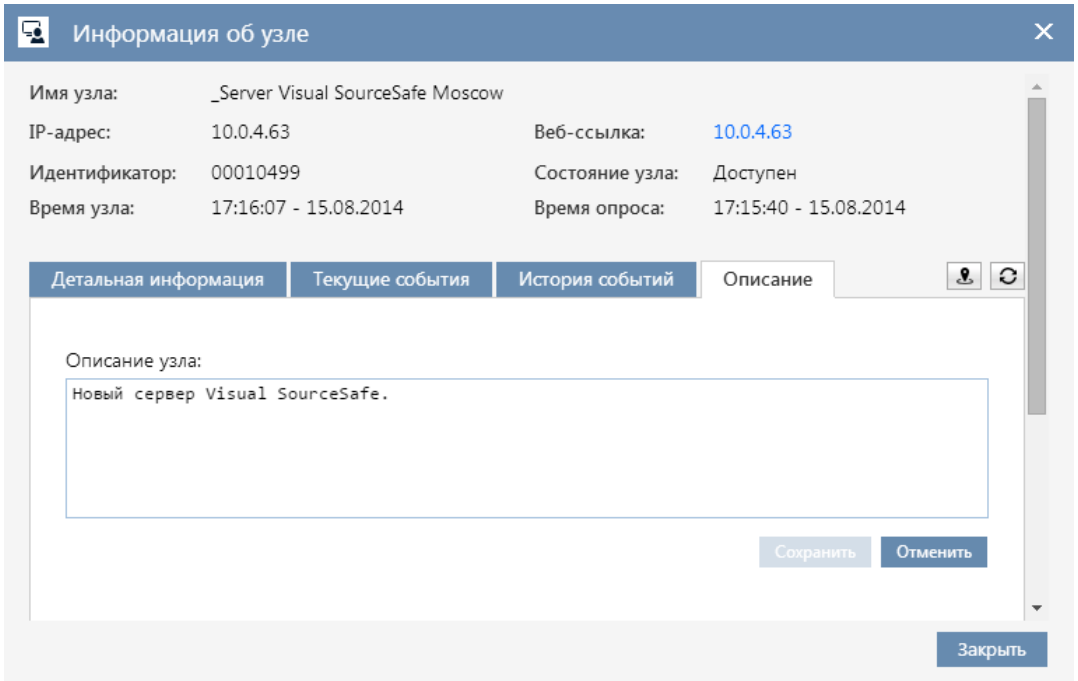

Рисунок 4: Добавление описания узла

- **Мониторинг связи с координаторами**

  Вы можете следить за состоянием связи выбранного узла с координаторами сети ViPNet. Для удобства все координаторы, с которыми установлена связь, объединены в список в окне информации об узле мониторга, что позволяет быстро выяснить, на каком участке сети отсутствует соединение. Также вы можете настроить отображение данной информации на инфопанели.

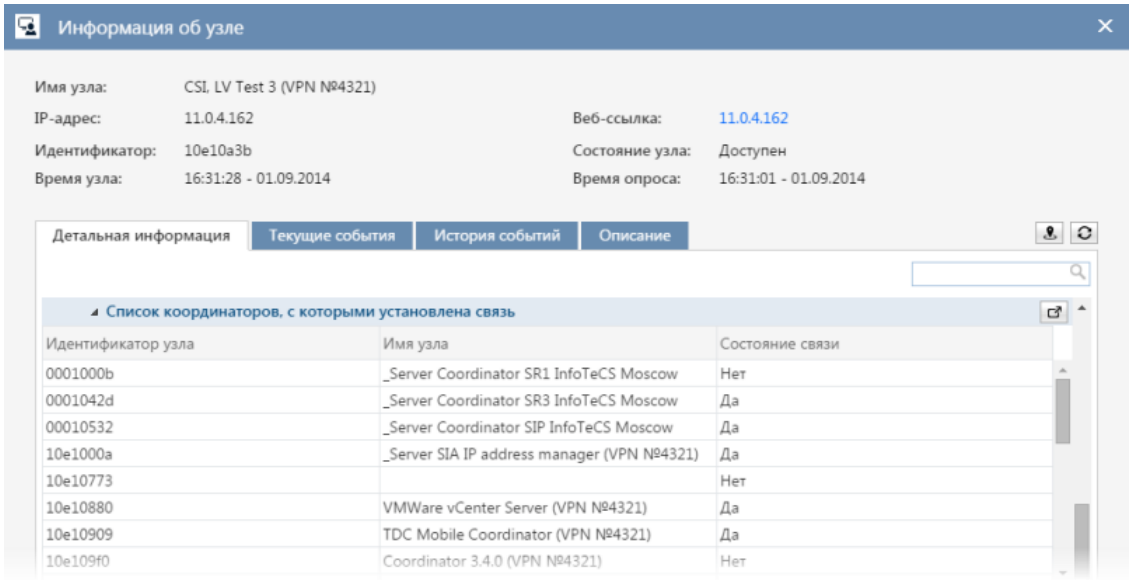

Рисунок 5: Просмотр состояния связи выбранного узла с координаторами сети ViPNet

- **Изменения в интерфейсе АРМ мониторинга**

  Был переработан и улучшен интерфейс АРМ мониторинга. Теперь в АРМ мониторинга используется новый плоский стиль интерфейса, также была улучшена читаемость шрифтов, изменены иконки.

- **Изменен список поддерживаемых операционных систем ПО Сервер мониторинга**

  Из списка поддерживаемых операционных систем ПО Сервер мониторинга удалена ОС Windows Server 2003.

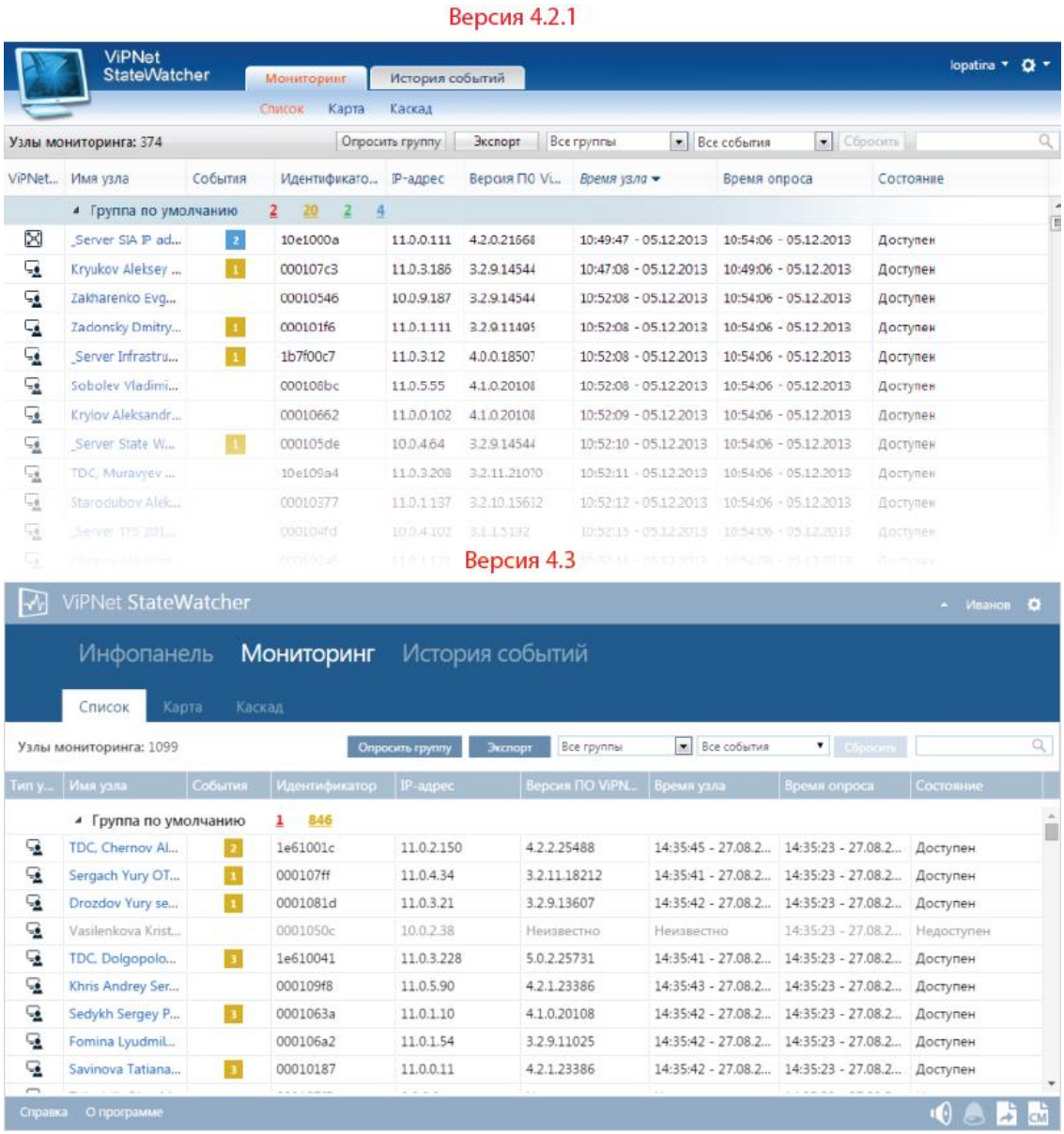

Рисунок 6: Различия в интерфейсе

- **Экспорт и импорт настроек Сервера мониторинга**

  Вы можете экспортировать настройки ПО Сервер мониторинга в файл или импортировать настройки из файла, например, для переноса ПО Сервер мониторинга на новый компьютер или для восстановления настроек из резервной копии.

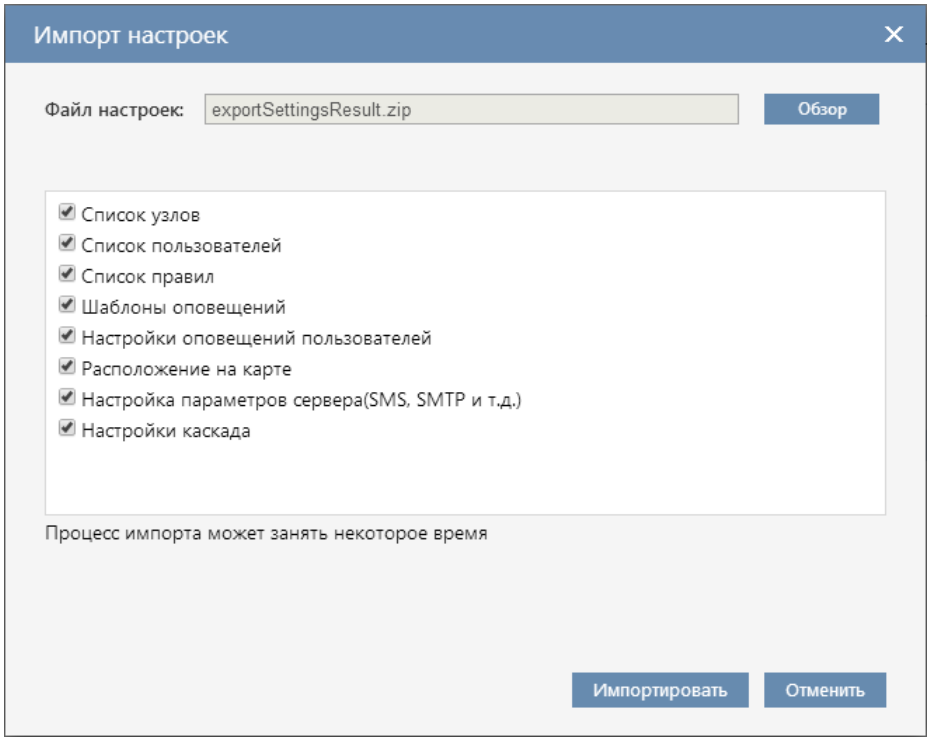

Рисунок 7: Импорт настроек ПО Сервер мониторинга

- **Новый принцип настройки оповещений о событиях мониторинга**

  В новой версии больше не используются фильтры оповещений. Теперь вы можете создавать шаблоны оповещений и включать нужные способы оповещения для отдельных пользователей, правил анализа и узлов мониторинга.

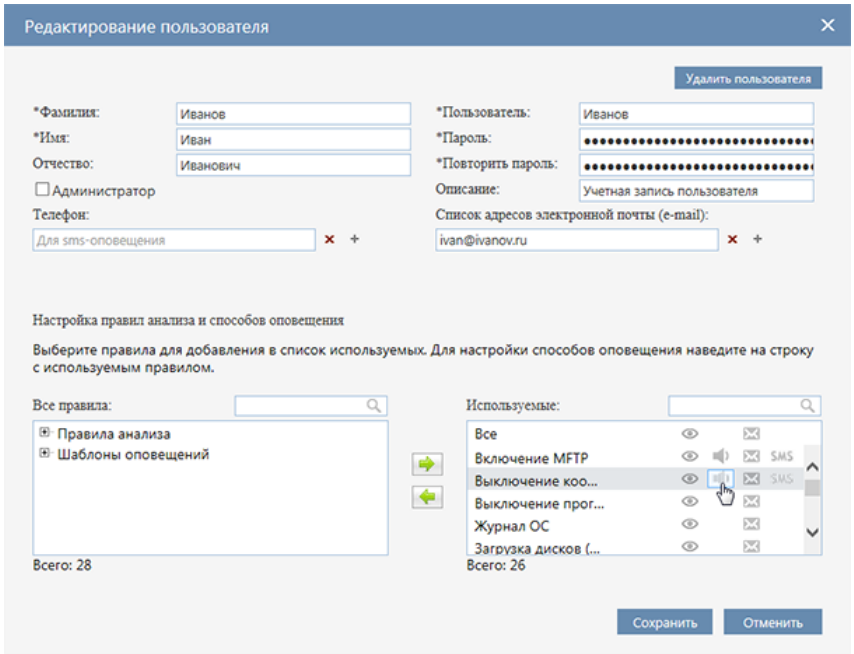

Рисунок 8: Включение способов оповещений для пользователя

- **Оповещения по протоколу Syslog**

  В новой версии ПО Сервер мониторинга появилась возможность настроить оповещения по протоколу Syslog для встроенной учетной записи `Administrator`. Этот способ оповещения позволяет передавать информацию о событиях мониторинга на сервер Syslog.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/products/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

1

Принципы организации мониторинга

Механизм работы Сервера мониторинга 27

Средства анализа информации 28

Разделение событий по уровням критичности 29

Каскадирование Серверов мониторинга 30

Управление правилами анализа в каскаде 33

Мониторинг кластера горячего резервирования 36

Мониторинг узлов по протоколу SNMP 37

Взаимодействие с ПАК ViPNet IDS 39

Управление Сервером мониторинга 40

Механизм работы Сервера мониторинга

Мониторинг состояния узлов сети ViPNet базируется на сборе и анализе значений различных параметров узлов. Для сбора информации Сервер мониторинга устанавливает соединение с ПО ViPNet на узлах мониторинга и периодически с заданным в настройках интервалом времени посылает им запросы. В течение времени, заданного в настройках, Сервер мониторинга ожидает ответы на запросы. Полученные от узлов данные Сервер мониторинга записывает в базу данных. Значения параметров, информация о которых не поступила, считаются неизвестными. Текущие значения параметров для любого узла мониторинга можно посмотреть с помощью веб-интерфейса АРМ мониторинга. После поступления новых данных начинается анализ текущего состояния узлов мониторинга. Анализ проводится на основе правил, заданных на Сервере мониторинга, которые выполняются при каждом поступлении данных мониторинга.

В процессе выполнения правил анализируются изменения в состоянии узлов и по результатам анализа генерируются события. Обнаруженные на узлах события мониторинга Сервер мониторинга сохраняет в базе данных. Записанные в базу данных события мониторинга можно посмотреть с помощью веб-интерфейса АРМ мониторинга, выполнив соответствующий запрос к базе.

Для каждого отслеживаемого события мониторинга в правилах анализа задается оповещение. Оповещения о событиях выводятся на всех АРМ мониторинга, подключенных к Серверу мониторинга, по тем каналам, которые включены в настройках Сервера мониторинга. В случае если Сервер мониторинга является частью каскада, оповещения передаются вверх по каскаду, то есть родительскому Серверу мониторинга. Оповещения передаются родительскому Серверу мониторинга, только если правило было централизованно применено на дочерних Серверах мониторинга.

Средства анализа информации

Анализ информации, полученной Сервером мониторинга от узлов, производится с помощью правил анализа. Каждое правило предназначено для анализа конкретных параметров узлов по определенному алгоритму. Алгоритм задается в компоненте правила, который называется «код правила», и записывается на специальном языке, который содержит все основные элементы и конструкции, используемые в языках программирования (см. «Синтаксис правил анализа» на стр. 157). В коде правила обычно задаются различные критерии проверки значений параметров, и по результатам проверки определяются события мониторинга и оповещения, которые должны выводиться на АРМ мониторинга.

Все правила анализа именованы и хранятся на Сервере мониторинга. В ПК ViPNet StateWatcher имеется набор встроенных правил, которые входят в пакет настроек (на стр. 290), идущий по умолчанию в комплекте поставки ПК ViPNet StateWatcher. Встроенные правила всегда присутствуют на Сервере мониторинга. Эти правила отслеживают наиболее важные события и изменения в состоянии узлов (см. «Встроенные правила анализа» на стр. 260). Набор встроенных правил можно изменить с помощью установки пакета настроек (см. «Обновление пакета настроек» на стр. 64).

Правила анализа, включая встроенные, не обязательно применять ко всем узлам мониторинга. Для управления политикой применения правил предусмотрена привязка узлов к правилам. Для каждого правила задается свой список узлов, на которых оно применяется, так что при анализе информации правило будет выполняться только для тех узлов, которые указаны в этом списке.

События мониторинга, обнаруженные правилами анализа, Сервер мониторинга записывает в базу данных, где они хранятся в течение времени, заданного в настройках Сервера мониторинга. По истечении этого времени устаревшие события мониторинга удаляются из базы. Средствами веб-интерфейса АРМ мониторинга можно просмотреть события мониторинга, а также экспортировать их в файл для дальнейшего просмотра или обработки в других приложениях.

Разделение событий по уровням критичности

Для разделения событий, происходящих на узлах, по степени их важности в ПК ViPNet StateWatcher используется понятие «уровень критичности». Уровень критичности применяется, прежде всего, в правилах анализа для оценки событий и формирования соответствующих оповещений. Поддерживаются следующие уровни критичности (в порядке убывания приоритета):

- высокий уровень — наиболее критичные события;
- средний уровень — события средней степени важности;
- низкий уровень — наименее критичные события;
- информационное сообщение – события, носящие уведомительный характер.

В каждом правиле анализа отслеживаются свои события и принимается решение об уровне критичности, который был задан администратором. При обнаружении события в правиле анализа формируется оповещение, в котором обязательно указывается уровень критичности события. От уровня критичности зависит форма представления оповещений на АРМ мониторинга, эта зависимость задается в настройках оповещений. Настройка оповещений позволяет также управлять включением и отключением оповещений о событиях.

Каскадирование Серверов мониторинга

ПК ViPNet StateWatcher предоставляет возможность сформировать из Серверов мониторинга многоуровневую иерархическую структуру, называемую каскадом. Организация каскада может потребоваться для распределения нагрузки между несколькими Серверами мониторинга или для мониторинга узлов в сегментированной сети при отсутствии связей на уровне ViPNet между узлами из какого-либо сегмента и родительским Сервером мониторинга. Например, в сети имеются сегменты А и Б, узлы сегмента А связаны на уровне ViPNet с родительским Сервером мониторинга, а узлы сегмента Б с ним не связаны. В этом случае родительский Сервер мониторинга может получать информацию об узлах сегмента Б от дочернего Сервера мониторинга, который имеет связи с данными узлами на уровне ViPNet.

Каскад представляет собой древовидную структуру, в которой Серверы мониторинга связаны отношениями «родитель-потомок». Каждый родительский Сервер мониторинга имеет произвольное число дочерних Серверов мониторинга, но каждый дочерний Сервер мониторинга имеет только один родительский Сервер мониторинга (кроме самого верхнего Сервера мониторинга, у самого верхнего Сервера мониторинга родительского сервера не существует).

Отношения в каскаде могут быть установлены только между Серверами мониторинга, имеющими связь в рамках сети ViPNet. Первоначально при наличии такой связи каждый из Серверов мониторинга является объектом мониторинга другого Сервера мониторинга. Однако после установления отношения в каскаде родительский Сервер мониторинга автоматически удаляется из списка узлов мониторинга своего дочернего Сервера мониторинга, при этом дочерний Сервер мониторинга по-прежнему является объектом мониторинга для родительского.

На рисунке ниже приведен пример каскада, организованного на основе существующих связей на уровне ViPNet между различными узлами.

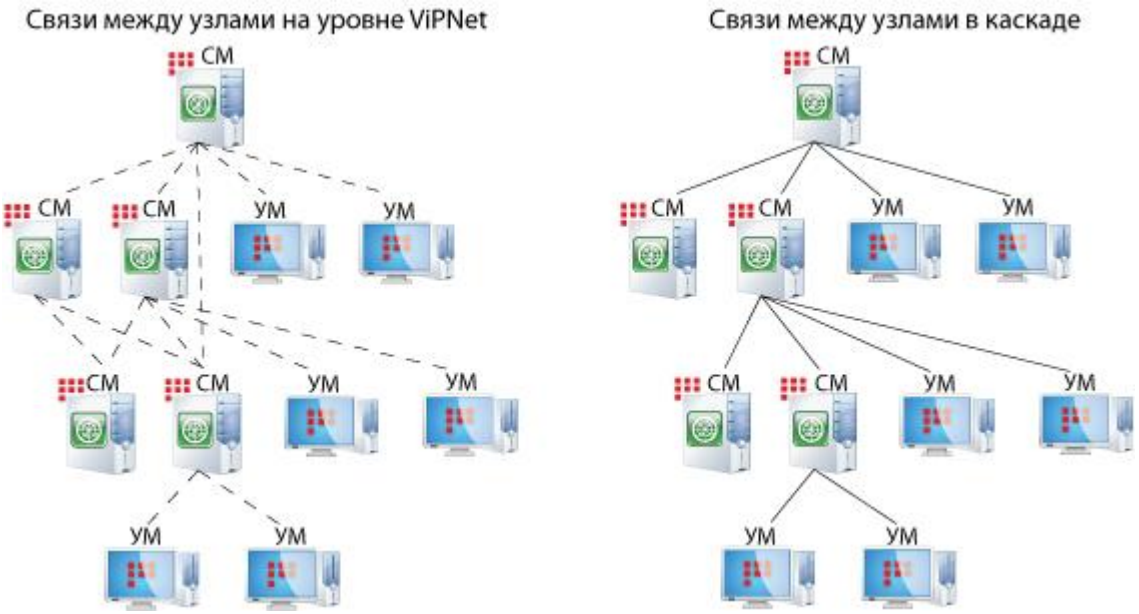

Рисунок 9: Пример каскада

В функции дочерних Серверов мониторинга входит передача своему родительскому Серверу мониторинга:

- Оповещений о событиях, происходящих на их узлах мониторинга.
- Списка каскадируемых узлов и внесенных в него изменений.
- Детальной информации о каскадируемых узлах.

В функции родительского Сервера мониторинга входит передача информации, полученной от дочерних серверов, далее вверх по каскаду, то есть своему родительскому Серверу мониторинга. Так как каждый родительский Сервер мониторинга (кроме самого верхнего) сам является дочерним для какого-либо Сервера мониторинга, он передает ему не только информацию, полученную от дочерних Серверов мониторинга, но также информацию о своих узлах мониторинга и событиях, происходящих на них. Таким образом происходит передача информации снизу вверх по каскаду вплоть до самого верхнего Сервера мониторинга.

На отношения, установленные между Серверами мониторинга в каскаде, не влияют перезагрузка и отключение Серверов мониторинга: после перезагрузки или повторного запуска любого Сервера мониторинга в каскаде он по-прежнему будет присутствовать в иерархии каскада. При отключении Серверов мониторинга только прерывается передача оповещений вверх по каскаду, и на родительских Серверах мониторинга прекращаются текущие оповещения, полученные по каскаду от отключенных Серверов мониторинга.

Отношения между Серверами мониторинга в каскаде зависят от наличия или отсутствия регистрации узлов в прикладной задаче «Сервер мониторинга» (см. «Лицензирование Сервера мониторинга» на стр. 16). При удалении регистрации какого-либо Сервера мониторинга он становится обычным объектом мониторинга для всех своих дочерних Серверов мониторинга и автоматически добавляется в список потенциальных узлов для мониторинга. На родительском Сервере мониторинга при этом прекращается поступление всей информации, полученной от данного дочернего Сервера мониторинга. При возобновлении регистрации узла в прикладной задаче «Сервер мониторинга» он появится в списке кандидатов на установление отношений в каскаде у всех Серверов мониторинга, с которыми у него есть связь в рамках сети ViPNet.

Отношения между Серверами мониторинга в каскаде задаются при настройке каскада (см. «Настройка каскада» на стр. 127).

Управление правилами анализа в каскаде

ПК ViPNet StateWatcher позволяет централизованно управлять правилами анализа в каскаде. Эта функция предоставляет возможность администратору родительского Сервера мониторинга применять созданные на его сервере правила на всех дочерних Серверах мониторинга. При этом администратор родительского Сервера мониторинга может просмотреть были ли применены правила, которые он передал вниз по каскаду.

На каждом родительском Сервере мониторинга может быть создан набор правил анализа, обязательных для применения на дочерних Серверах мониторинга. Данные правила передаются вниз по каскаду всем дочерним Серверам мониторинга и должны применяться ко всем узлам.

Примечание. Правила, переданные вниз по каскаду родительским Сервером мониторинга, невозможно отменить на дочерних серверах.

В результате дочерние Серверы мониторинга будут передавать вверх по каскаду только те оповещения, которые сформированы этими правилами, и не будут передавать оповещения от своих собственных правил анализа.

На схеме ниже представлен пример применения правил анализа в каскаде.

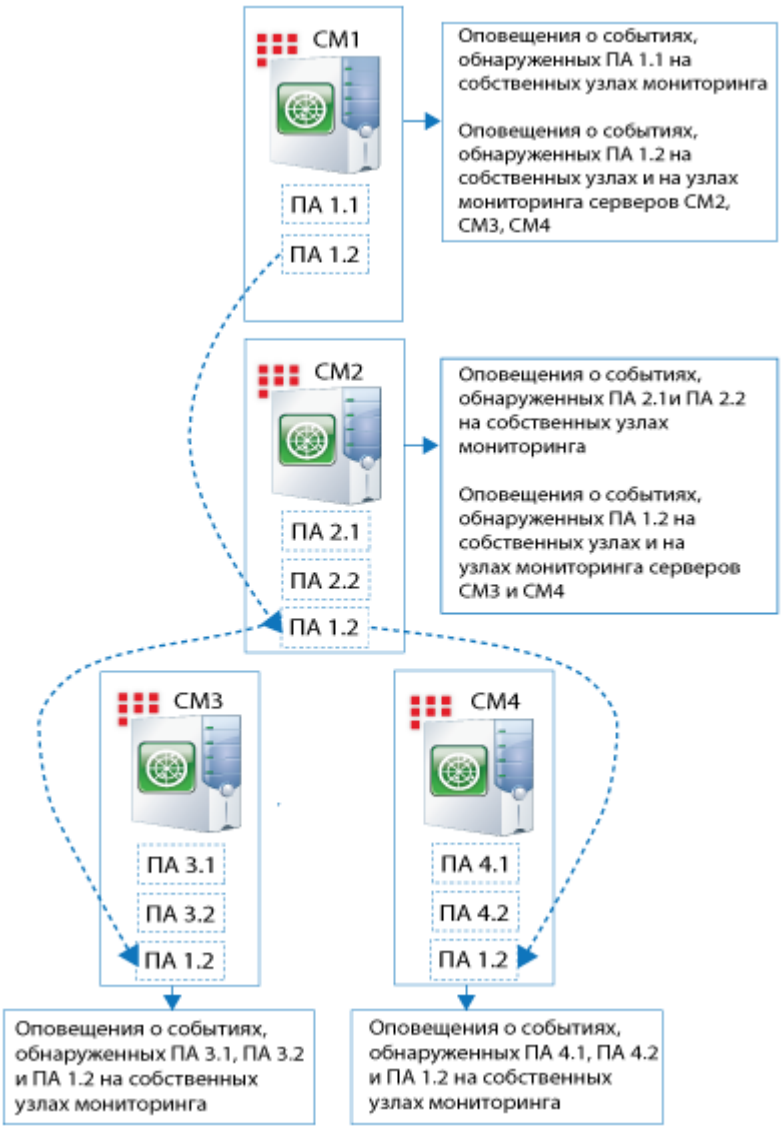

Рисунок 10: Передача правил анализа и оповещений в каскаде

В примере приведен каскад из 4-х Серверов мониторинга СМ1, СМ2, СМ3 и СМ4. На самом верхнем сервере СМ1 заданы правила анализа ПА 1.1 и ПА 1.2, при этом необходимо, чтобы на СМ1 аккумулировались оповещения о срабатывании правила ПА 1.2 на всех узлах сети. На остальных серверах заданы свои правила анализа, которые должны применяться только к их собственным узлам мониторинга. Чтобы обеспечить передачу оповещений с дочерних серверов на сервер СМ1, правило ПА 1.2 распространяется вниз по каскаду: на каждом дочернем сервере автоматически создается копия правила ПА 1.2, которое обязательно для применения на всех без исключения узлах.

При срабатывании правила ПА 1.2 на узлах мониторинга сервера СМ2 оповещения будут передаваться на сервер СМ1 непосредственно, а при срабатывании на узлах мониторинга серверов СМ3 и СМ4 – через сервер СМ2. При этом оповещения, сформированные при срабатывании собственных правил серверов СМ2, СМ3 и СМ4, не будут передаваться на сервер СМ1.

Мониторинг кластера горячего резервирования

Программное обеспечение ViPNet Coordinator Linux и программно-аппаратный комплекс ViPNet Coordinator HW могут работать как в одиночном режиме, так и в режиме кластера горячего резервирования. Режим кластера горячего резервирования предназначен для горячей замены функций одного из серверов в составе кластера другим сервером в случае сбоя первого.

Кластер горячего резервирования серверов состоит из двух взаимосвязанных компьютеров, один из которых (активный элемент) выполняет функции координатора ViPNet, а другой компьютер (пассивный элемент) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet на активном элементе (в первую очередь в случае сбоев в работе сети или сетевого оборудования), пассивный элемент переключается в активный режим, принимая на себя нагрузку и выполняя функции координатора вместо сервера, который зафиксировал сбой.

Сервер мониторинга позволяет осуществлять мониторинг активного и пассивного элементов кластера, что помогает администраторам своевременно выявлять и исправлять проблемы, возникшие на обоих элементах кластера. Также Сервер мониторинга информирует администраторов о переключении между активным и пассивным элементами кластера.

Полный список параметров, получаемых с активного и пассивного элементов кластера, см. в приложении Контролируемые параметры узлов мониторинга (на стр. 204).

Мониторинг узлов по протоколу SNMP

С помощью ПО Сервер мониторинга вы можете осуществлять мониторинг узлов по протоколу SNMP, например, если хотите получать информацию об узлах, не входящих в сеть ViPNet.

Данный протокол использует распределенную архитектуру, состоящую из следующих компонентов:

- SNMP-менеджер — это программный модуль Сервера мониторинга, предназначенный для контроля и управления узлами с использованием протокола SNMP.
- SNMP-агент — программное обеспечение, запускаемое на открытых узлах и предназначенное для передачи параметров данных узлов SNMP-менеджеру.

  В качестве SNMP-агента на открытых узлах может быть использована соответствующая служба Windows — Windows SNMP Service. Запуск и настройка данной службы осуществляются стандартными средствами операционной системы (см. «Настройка службы SNMP на открытом узле» на стр. 253).

С помощью протокола SNMP вы можете осуществлять мониторинг следующих типов узлов:

- Открытые узлы.
- Туннелируемые узлы.
- Защищенные узлы.

Сервер мониторинга передает SNMP-агентам команды с запросом параметров узлов (см. «Контролируемые параметры открытых узлов» на стр. 227) с определенной периодичностью либо по инициативе администратора. SNMP-агенты собирают запрошенные параметры и передают их Серверу мониторинга. При этом собранные параметры каждого узла отображаются на вкладке **Детальная информация** в окне **Информация об узле** АРМ мониторинга. Также при каждом опросе собранные параметры анализируются в соответствии с правилами анализа, заданными на данном Сервере мониторинга.

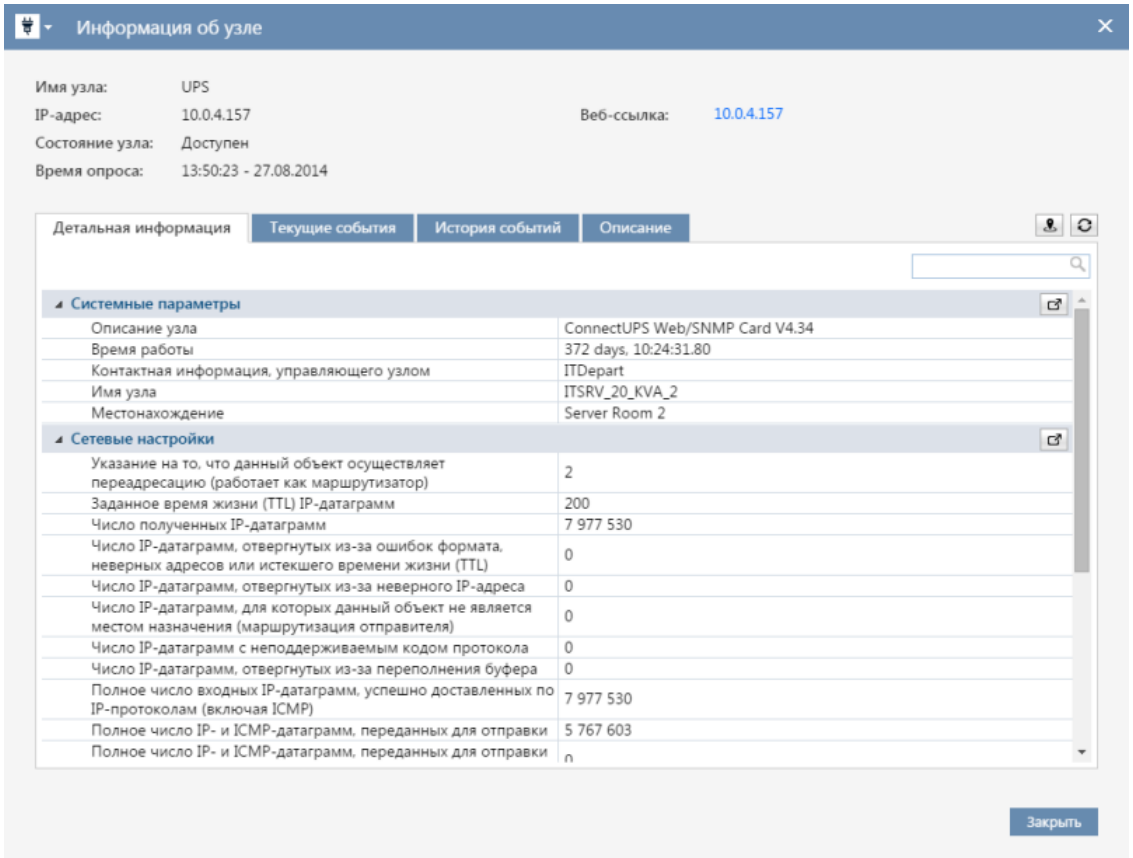

Рисунок 11: Просмотр детальной информации об открытом узле

Взаимодействие с ПАК ViPNet IDS

С помощью ПО Сервер мониторинга вы можете контролировать работу ПАК ViPNet IDS, который предназначен для обнаружения и анализа сетевых атак.

Мониторинг узла, который является ПАК ViPNet IDS, осуществляется по протоколу SNMP (см. «Мониторинг узлов по протоколу SNMP» на стр. 37). На ПАК по умолчанию установлен SNMP-агент, который настроен для взаимодействия с ПО Сервер мониторинга.

С помощью ПО Сервера мониторинга вы можете просмотреть следующую информацию о сетевых атаках, обнаруженных ПАК ViPNet IDS:

- количество обнаруженных сетевых атак с распределением по степени критичности;
- список ста последних атак, обнаруженных ПАК ViPNet IDS;
- список ста наиболее атакуемых узлов;
- список ста самых атакующих узлов.

Полный список параметров, получаемых с ПАК ViPNet IDS, см. в приложении Контролируемые параметры ПАК ViPNet IDS (на стр. 242).

Чтобы осуществлять мониторинг ПАК ViPNet IDS, предварительно добавьте данный узел в список связей Сервера мониторинга (см. «Добавление открытых узлов в список связей Сервера мониторинга» на стр. 88), а затем добавьте его в нужную группу мониторинга (см. «Перемещение новых узлов в группу мониторинга» на стр. 89).

Также вы можете создавать правила анализа событий, происходящих на узле ПАК ViPNet IDS (см. «Настройка правил анализа» на стр. 97).

Управление Сервером мониторинга

Управление Сервером мониторинга осуществляется через службу Apache Tomcat. Набор действий по управлению ограничен – Сервер мониторинга можно запустить или остановить:

- Для запуска Сервера мониторинга щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите команду **Start**. После старта Apache Tomcat автоматически выполняется запуск ПО Сервер мониторинга.
- Для остановки Сервера мониторинга щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите команду **Stop**. При остановке Apache Tomcat автоматически выполняется остановка ПО Сервер мониторинга.

В случае изменения настроек Сервера мониторинга в файле `server.ini` (см. «Тонкая настройка Сервера мониторинга» на стр. 137) необходимо обязательно перезапустить Сервер мониторинга. Для этого остановите Сервер мониторинга, а затем запустите его снова.

Подробнее о работе службы Apache Tomcat см. в соответствующей документации на сайте http://tomcat.apache.org/.

2

Установка, обновление и удаление сервера мониторинга

Последовательность установки ПО Сервер мониторинга 42

Порядок установки обязательного ПО 43

Установка ПО Сервер мониторинга 47

Проверка правильности установки ПО Сервер мониторинга 54

Порядок обновления ПО Сервер мониторинга 57

Обновление ПО Сервер мониторинга 58

Порядок обновления ПО Сервера мониторинга при каскадной организации системы мониторинга 62

Обновление пакета настроек 64

Удаление ПО Сервер мониторинга 66

Подключение к Серверу мониторинга 68

Последовательность установки ПО Сервер мониторинга

Для установки ПО Сервер мониторинга вам потребуются:

- Файлы установки обязательного ПО PostgreSQL, Oracle Java Sun JDK и Apache Tomcat.
- Файл установки ПО Сервер мониторинга `StateWatcherInstaller.jar`.
- Файл пакета настроек (файл по умолчанию — `default_pn.zip`).

Установку ПО Сервер мониторинга и обязательного ПО следует выполнять с использованием учетной записи администратора ОС. Перед установкой отключите контроль учетных записей и примите последние обновления ОС.

Для установки ПО Сервер мониторинга выполните все действия из приведенного ниже списка в предложенном порядке.

Таблица 4. Последовательность установки ПО Сервер мониторинга

	Действие	Примечание
☐	Установите ПО PostgreSQL	Порядок установки обязательного ПО (на стр. 43)
☐	Установите ПО Oracle Java Sun JDK	
☐	Установите ПО Apache Tomcat	
☐	Установите ПО Сервер мониторинга	Установка ПО Сервер мониторинга (на стр. 47)
☐	Проверьте правильность установки ПО Сервер мониторинга	Проверка правильности установки ПО Сервер мониторинга (на стр. 54)
☐	Установите обновления безопасности для обязательного ПО сторонних производителей	Установка обновлений для стороннего ПО (на стр. 55)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Порядок установки обязательного ПО

Перед установкой ПО Сервер мониторинга на компьютере должно быть установлено обязательное программное обеспечение, без которого работа Сервера мониторинга будет невозможна. Установочные файлы обязательного программного обеспечения входят в комплект поставки (на стр. 17). Установка обязательного программного обеспечения и ПО Сервер мониторинга должна осуществляться с использованием учетной записи с именем Administrator, то есть с использованием учетной записи локального администратора операционной системы.

Внимание! Если на компьютере установлена русскоязычная версия ОС Windows, то перед началом установки обязательного ПО необходимо создать пользователя Administrator, назначить ему права администратора и войти в систему с использованием созданной учетной записи.

Категорически не рекомендуется устанавливать версии обязательного ПО, отличные от версий, которые входят в комплект поставки. Также не рекомендуется обновлять данное программное обеспечение после установки ПО Сервер мониторинга.

Выполните установку обязательного программного обеспечения в следующей последовательности:

1. Убедитесь, что контроль учетных записей вашей ОС отключен. Подробнее об отключении контроля учетных записей см. справочное руководство используемой операционной системы.

2. Установите PostgreSQL (версию 9.1.4-1 для 32-разрядной ОС или для 64-разрядной ОС).

   В процессе установки этого ПО используйте настройки, предлагаемые по умолчанию, кроме запуска компонента Stack Builder: в ответ на предложение откажитесь от автоматического запуска этого компонента.

   Запомните номер порта сервера базы данных. По умолчанию — 5432. Если на сервере установлено две версии PostgreSQL (например, при обновлении ПО Сервер мониторинга с версии 3.2 до версии 4.3), то для PostgreSQL 9.1 по умолчанию будет установлен номер порта 5433. При дальнейшей установке и настройке ПО Сервер мониторинга проследите, чтобы везде был задан одинаковый номер порта.

   В процессе установки задайте пароль для пользователя postgres. Пароль может содержать буквы и цифры, набранные в латинской раскладке. Длина пароля должна быть не менее 8 символов. Использовать специальные символы в пароле не разрешается.

Примечание. В процессе установки PostgreSQL 9 могут возникнуть конфликты с компонентами Microsoft Visual Studio. В этом случае информацию о типичных ошибках при установке PostgreSQL и рекомендации по их решению см. на сайте http://wiki.postgresql.org/wiki/Running_%26_Installing_PostgreSQL_On_Native_Windows#Common_installation_errors.

После установки в системе должен появиться пользователь postgres (суперпользователь базы данных PostgreSQL). Необходимо разрешить этому пользователю полный доступ (Full Control) к папке (см. «Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows» на стр. 257), где будет развернута база данных мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47).

3 Установите Oracle Java Sun JDK (версию 7u21 для 32-разрядной ОС или для 64-разрядной ОС).

В процессе установки этого программного обеспечения используйте настройки, предлагаемые по умолчанию.

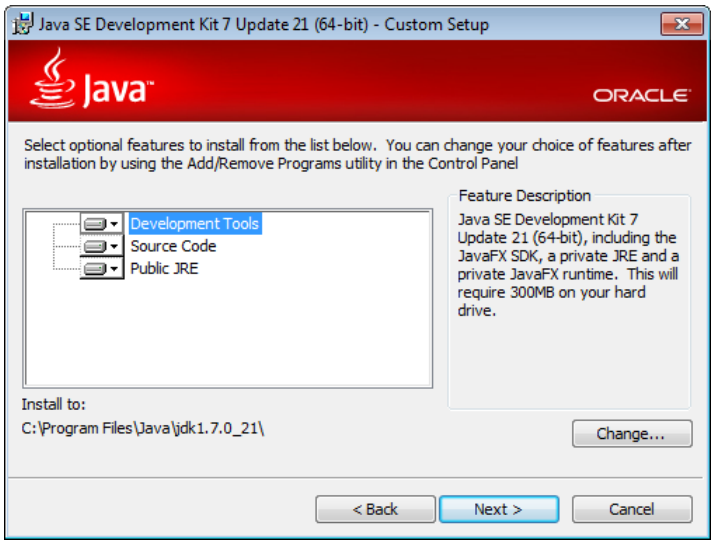

Рисунок 12: Выбор компонентов Java Sun JDK

4 Установите Apache Tomcat (версию 6.0.29 для 32-разрядной ОС или версию 6.0.33 для 64-разрядной ОС).

В процессе установки этого программного обеспечения используйте настройки, предлагаемые по умолчанию. На шаге выбора компонентов для установки (Choose Components) отметьте флажками компоненты Service и Native.

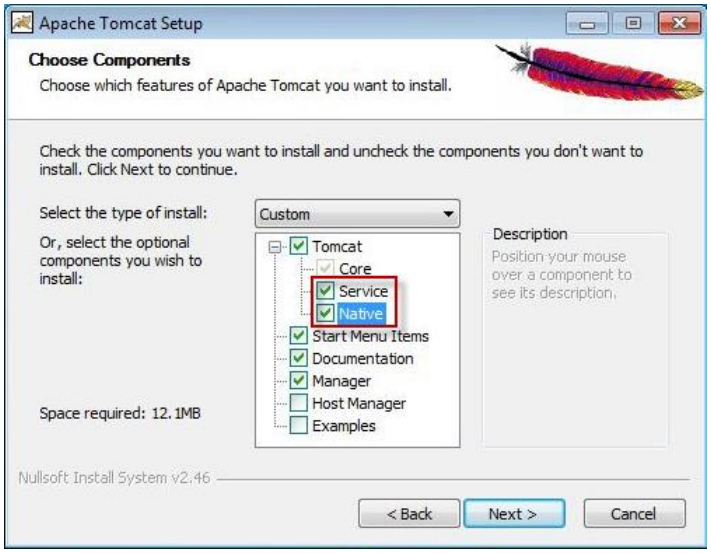

Рисунок 13: Выбор компонентов для установки Apache Tomcat

Для пользователя admin задайте пароль.

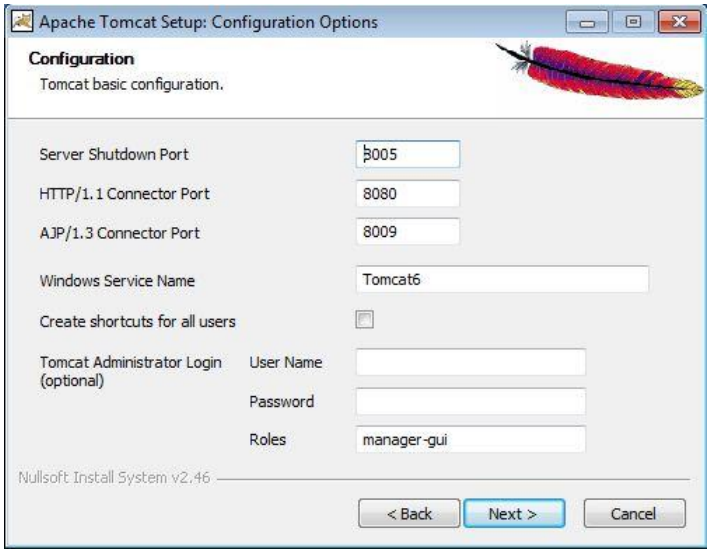

Рисунок 14: Установка пароля администратора

На последнем шаге установки откажитесь от старта службы (снимите флажок Run Apache Tomcat).

Внимание! Служба Apache Tomcat после установки ПО ViPNet StateWatcher будет работать, используя порт 80. До начала установки ПО ViPNet StateWatcher необходимо освободить данный порт.

---

5 Проверьте, что службы PostgreSQL и Apache Tomcat успешно запускаются:

- Для запуска службы Apache Tomcat щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите команду Start.
- Для запуска службы PostgreSQL:
  1. В меню Пуск выберите Панель управления.
  2. На странице Настройка параметров компьютера выберите пункт Администрирование.
  3. В появившемся окне дважды щелкните ярлык Службы .
  4. В окне Службы выберите службу postgrescql-x32-9.1 (или postgrescql-x64-9.1) и на панели инструментов нажмите кнопку Запуск службы .

Внимание! В случае использования системного прокси-сервера при подключении к Интернету необходимо, чтобы запуск службы Apache Tomcat осуществлялся с использованием учетной записи администратора ОС.

Примечание. Для работы с АРМ мониторинга также необходимо установить плагины для веб-браузера (необходимы для воспроизведения оповещений) и iReport, если вы планируете создавать свои шаблоны писем оповещений. Все необходимое программное обеспечение входит в комплект поставки (на стр. 17).

В случае обновления Oracle Java Sun JDK до версии 7u21 выполните следующие действия:

1 Удалите старую версию Oracle Java Sun JDK 6u30.

2 Установите Oracle Java Sun JDK версии 7u21.

3 Остановите сервис Apache Tomcat. Для этого щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите команду Stop.

4 Убедитесь, что в настройках сервиса Apache Tomcat указана правильная версия виртуальной машины Java. Для этого щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите Configure. В открывшемся окне перейдите на вкладку Java и проверьте путь к виртуальной машине Java в поле Java Virtual Machine: C:\Program Files\Java\jdk1.7.0_21\jre\bin\server\jvm.dll.

   Если в поле Java Virtual Machine указан путь к старой версии виртуальной машины Java, то укажите путь к новой версии.

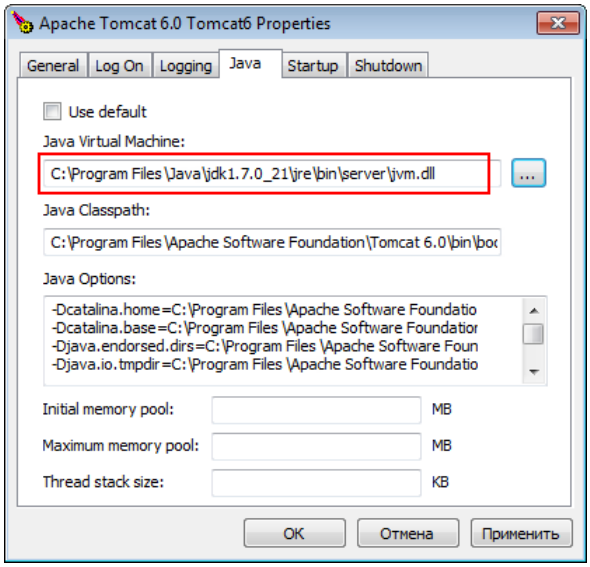

Рисунок 15: Проверка пути к виртуальной машине Java

5 Запустите сервис Apache Tomcat с помощью команды Start.

Установка ПО Сервер мониторинга

Перед установкой ПО Сервер мониторинга:

1 Убедитесь, что контроль учетных записей вашей ОС отключен. Подробнее об отключении контроля учетных записей см. справочное руководство используемой операционной системы.

2 Убедитесь в наличии дистрибутива ПО — файла `StateWatcherInstaller.jar` и пакета настроек (файл пакета настроек, устанавливаемый по умолчанию — `default_pn.zip`).

Внимание! Пути к файлам с дистрибутивом ПО и пакетом настроек не должны содержать символ «восклицательный знак» (!). Например, путь `C:\!Distrib_SW` недопустим.

---

3 Установите программное обеспечение, необходимое для работы Сервера мониторинга (см. «Порядок установки обязательного ПО» на стр. 43).

4 Создайте папку, в которой будут храниться базы данных мониторинга. Установите этой папке права полного доступа (**Full Control**) для суперпользователя базы

данных PostgreSQL (см. «Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows» на стр. 257).

Путь к созданной папке указывается при установке ПО Сервер мониторинга. Эту папку не обязательно создавать заранее, ее можно создать в процессе установки ПО на соответствующем шаге.

Примечание. Не рекомендуется размещать базы данных на одном логическом диске с системой, это приведет к замедлению обработки запросов к базе данных. По возможности создайте папку для базы данных в другом разделе или на другом жестком диске.

Для выполнения первичной установки ПО Сервер мониторинга:

1. Закройте все приложения, которые обращаются к ПО Apache Tomcat и PostgreSQL, иначе установка ПО Сервер мониторинга будет произведена некорректно.

2. Двойным щелчком запустите программу установки `StateWatcherInstaller.jar`. Будет запущен мастер **Установка StateWatcher**, следуйте его указаниям.

   На первой странице мастера нажмите кнопку **Далее**.

3. На странице **Лицензионное соглашение** ознакомьтесь с текстом лицензии, затем выберите пункт **Я согласен с условиями лицензии** и нажмите кнопку **Далее**.

   На странице **Информация** прочтите представленную информацию и нажмите кнопку **Далее**.

4. На странице **Проверка внешнего ПО** будет представлена информация о наличии обязательных программ (см. «Порядок установки обязательного ПО» на стр. 43), их версиях и местоположении.

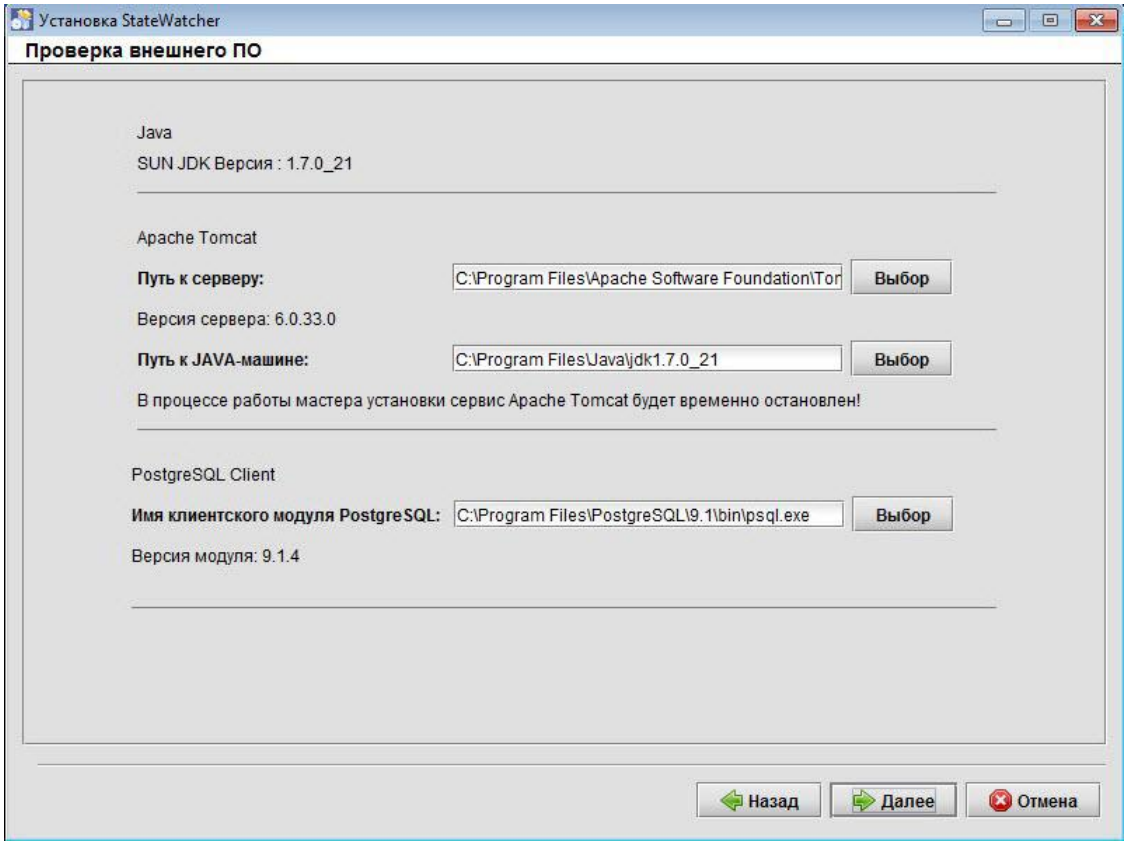

Рисунок 16: Проверка внешних программ

Проверьте представленную информацию, в случае необходимости укажите или измените пути к обязательным программам.

Примечание. Если на компьютере установлены две версии СУБД PostgreSQL (например, 8.4 и 9.1), в поле **Имя клиентского модуля PostgreSQL** укажите путь к версии 9.1, которая требуется для функционирования Сервера мониторинга версии 4.3.

Для продолжения нажмите кнопку **Далее**.

5 На странице **Выбор варианта установки** в случае первичной установки будет предложен единственный вариант. Для продолжения нажмите кнопку **Далее**.

6 На странице **Конфигурирование сервера БД мониторинга для установки** будут представлены настройки сервера базы данных, заданные по умолчанию.

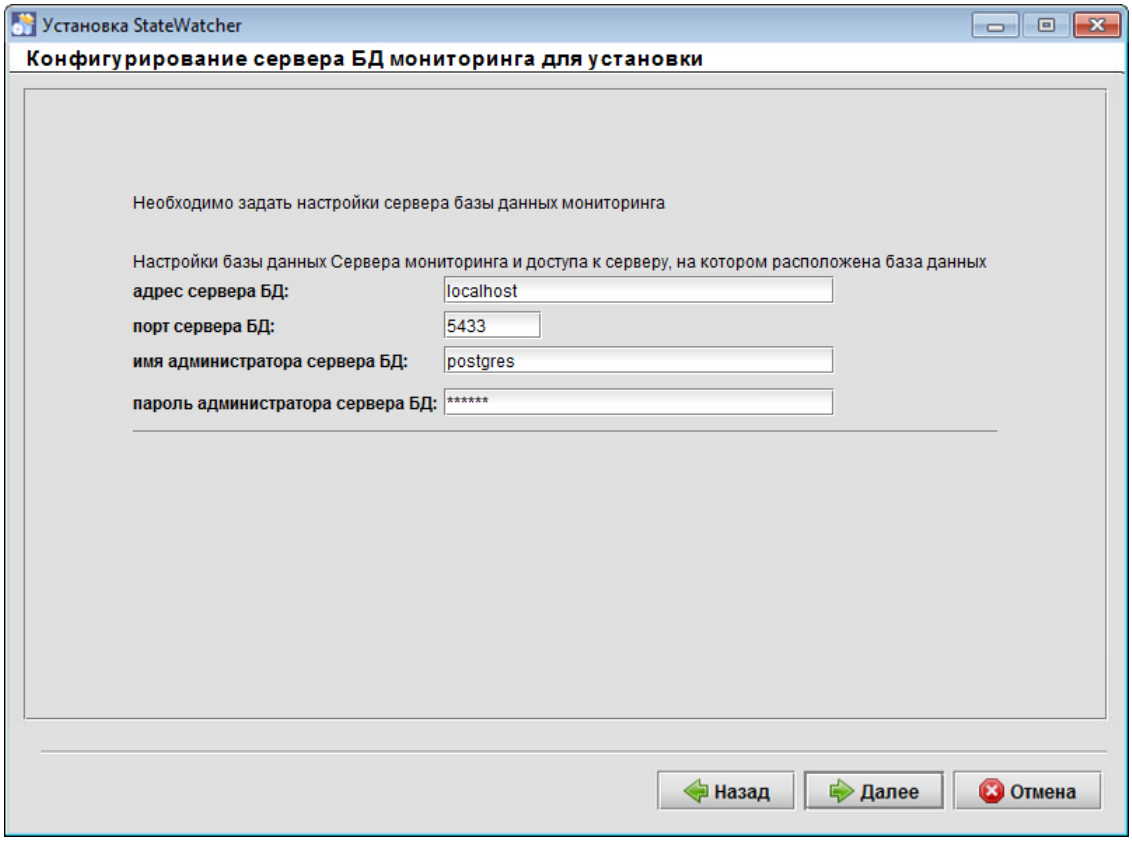

Рисунок 17: Настройка сервера базы данных

Если на сервере установлено две версии PostgreSQL, то по умолчанию в поле **Порт сервера БД** будет установлено значение 5433.

В поле **Пароль администратора сервера БД** введите пароль, заданный при установке PostgreSQL, и нажмите кнопку **Далее**.

7 На второй странице **Конфигурирование сервера БД мониторинга для установки** задайте параметры, с которыми будет создана база данных мониторинга:

- В поле **имя БД** введите имя базы данных (по умолчанию задано имя `sw_olap`).
- В поле **имя администратора БД** введите имя владельца базы данных (по умолчанию задано имя `sw_admin`).
- В поле **пароль владельца БД** задайте пароль доступа к создаваемой базе данных.
- В поле **Каталог хранения данных** укажите путь к папке, предварительно созданной для размещения базы данных. Если эта папка еще не создана, создайте ее. Для этого нажмите кнопу **Выбор** и в появившемся окне нажмите кнопку .

Примечание. Пользователь `postgres` (суперпользователь базы данных) должен иметь полный доступ к этой папке (**Full control**). Если требуемые права не установлены, при нажатии на кнопку **Далее** мастер выдаст сообщение об ошибке.

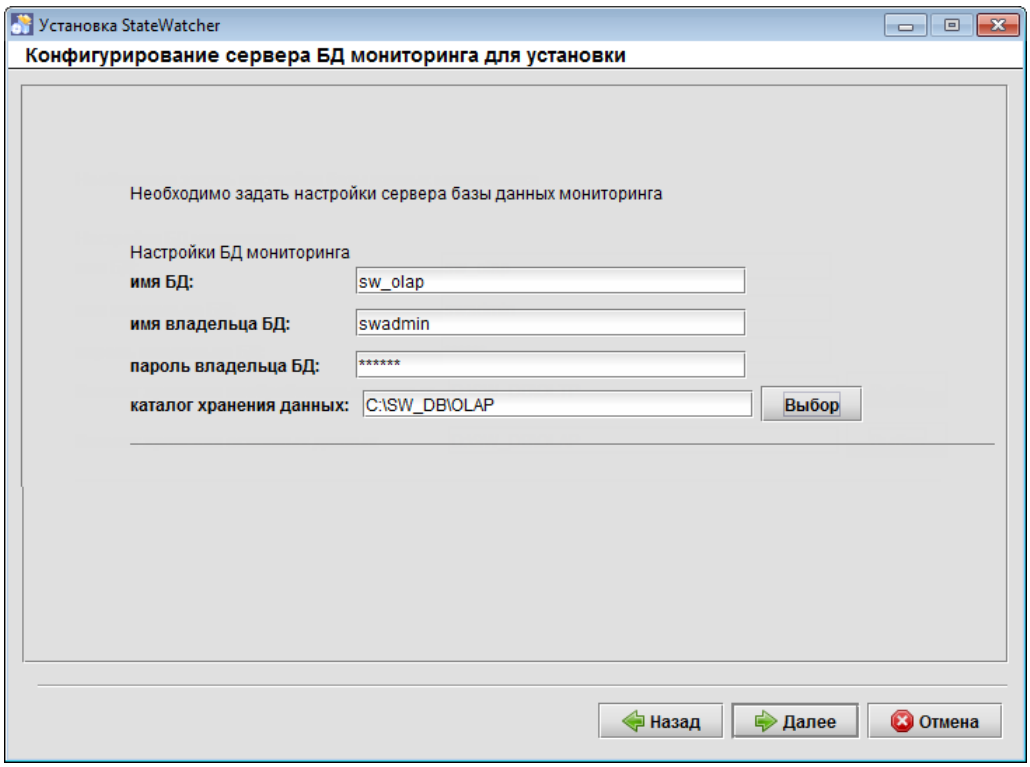

Рисунок 18: Настройка базы данных мониторинга

Нажмите кнопку **Далее**.

8 На странице **Конфигурирование сервера БД ГИС мониторинга** задайте параметры, с которыми будет создана база данных геоинформационной системы (ГИС):

- Значения в полях **адрес сервера БД ГИС**, **порт сервера БД ГИС** и **имя администратора сервера БД ГИС** изменять не рекомендуется, они определяются автоматически.
- В случае необходимости в поле **имя БД ГИС** измените имя базы данных (по умолчанию `sw_gis`).
- В поле **пароль администратора сервера БД ГИС** задайте пароль доступа к создаваемой базе данных.

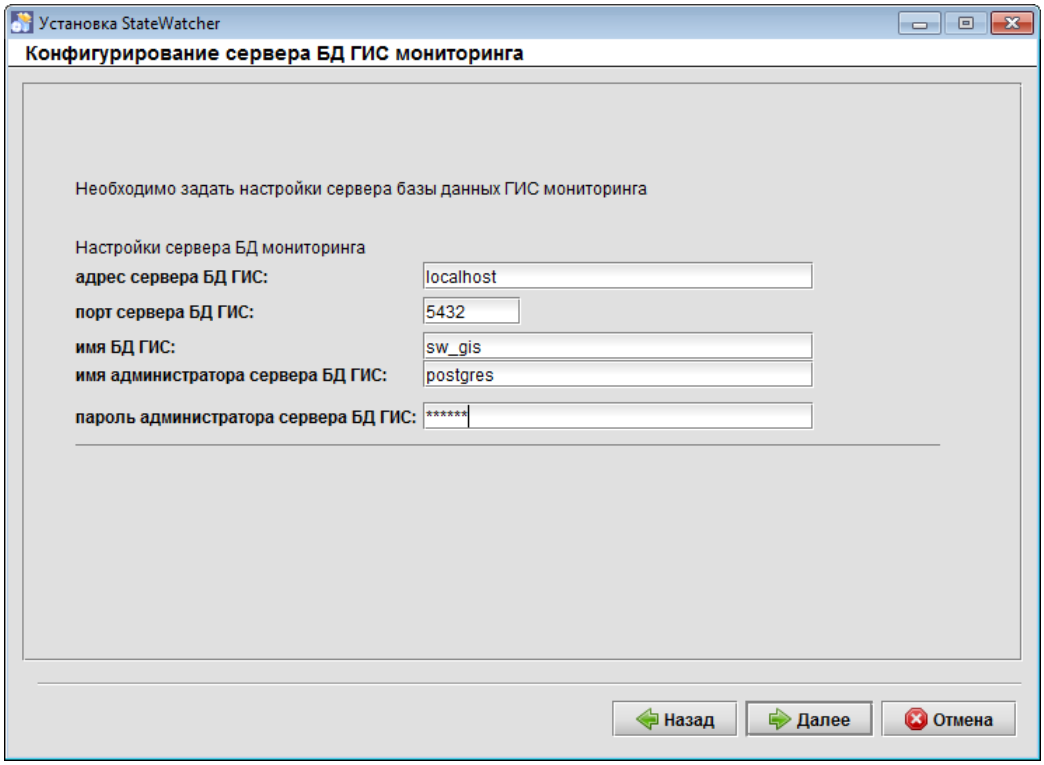

Рисунок 19: Настройка базы данных ГИС

Задав необходимые параметры, нажмите кнопку **Далее**.

Примечание. В базе данных ГИС содержится информация, необходимая для отображения узлов и событий мониторинга на карте.

---

9 На странице **Настройка оповещений для установки** задайте параметры существующего SMTP-сервера, который будет использоваться для отправки оповещений:

- В поле **адрес SMTP-сервера** укажите адрес сервера.
- В поле **порт SMTP-сервера** укажите порт (по умолчанию 25).
- В поле **Электронная почта, с которой будут отправляться оповещения** введите адрес электронной почты, от имени которого будут отправляться оповещения.
- Если на сервере требуется авторизация пользователя, установите флажок **Использовать учетную запись для доступа к SMTP-серверу** и в полях под флажком укажите имя и пароль пользователя SMTP-сервера.

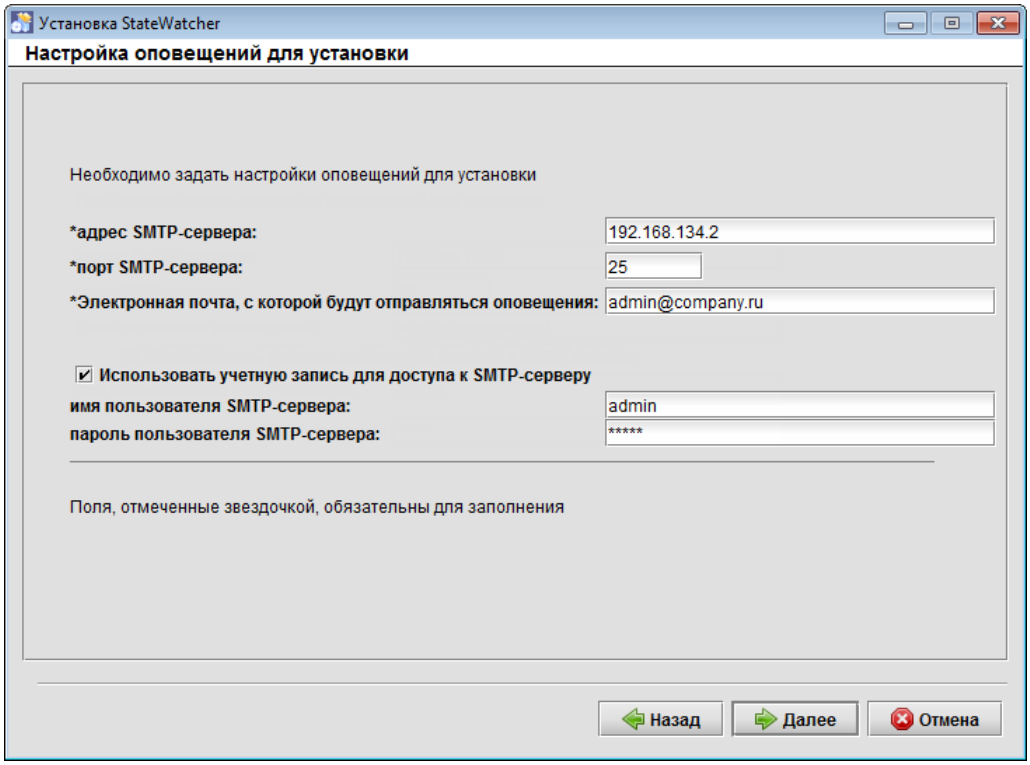

Рисунок 20: Настройка SMTP-сервера

Задав необходимые параметры, нажмите кнопку **Далее**.

10 На странице **Настройка деловой почты** в поле **Путь к директории** укажите папку, в которую Сервер мониторинга будет помещать файлы с оповещениями, предназначенные для обработки правилами автопроцессинга приложения ViPNet Деловая почта.

Для продолжения нажмите кнопку **Далее**.

11 На странице **Требуемый объем дискового пространства** указан доступный объем памяти на диске и объем, требуемый для установки. Если доступного объема памяти недостаточно, освободите дополнительное пространство.

Для продолжения нажмите кнопку **Далее**.

12 На странице **Пакет настроек** укажите путь к файлу с пакетом настроек (см. «Пакет настроек» на стр. 290), который следует установить (пакет настроек, идущий в комплекте поставки по умолчанию `default_pn.zip` или собственный пакет настроек), и нажмите кнопку **Далее**.

Устанавливаемый пакет настроек должен соответствовать определенной версии ПО Сервер мониторинга. Также при установке проверяется корректность устанавливаемого пакета настроек.

Внимание! Если пакет настроек не соответствует версии ПО Сервер мониторинга или является некорректным, мастер установки выдаст соответствующую ошибку, дальнейшие шаги мастера будут недоступны.

Настоятельно рекомендуется использовать пакет настроек, идущий в комплекте поставки по умолчанию, или использовать пакет, разработанный специально для вашей компании.

13 На странице **Подтверждение** проверьте указанные параметры.

Для начала установки нажмите кнопку **Далее**.

14 Начнется процесс установки. На странице **Выполнение** будет отображаться информация о ходе установки.

По окончании установки нажмите кнопку **Далее**.

15 На странице **Завершение выполнения** нажмите кнопку **Завершить**.

Мастер **Установка StateWatcher** закроется, будет запущена служба Apache Tomcat. После запуска Apache Tomcat Сервер мониторинга готов к работе.

Внимание! ПО Сервер мониторинга 4.3 совместимо в каскаде только с версией 4.0 и выше данного ПО. При этом поддерживается организация каскада, если на родительском Сервере мониторинга установлена версия ПО выше или одинаковая с дочерними серверами, и не поддерживается организация каскада, если на родительском сервере установлена версия ПО ниже, чем на дочернем сервере. Если на Серверах мониторинга, которые будут входить в каскад, установлено ПО версии ниже 4.0, то обновите это ПО до версии 4.3 (см. «Обновление ПО Сервер мониторинга» на стр. 58).

Проверка правильности установки ПО Сервер мониторинга

После установки убедитесь правильности в установки ПО Сервер мониторинга и дополнительного ПО. Для этого выполните следующие действия:

1 Подключитесь к Серверу мониторинга с помощью АРМ мониторинга. Для этого:

1.1 В веб-браузере введите адрес `http://<адрес сервера>`.

1.2 В появившемся окне введите имя учетной записи `Administrator` и пароль `Administrator`.

1.3 Нажмите кнопку **Войти**.

2 На странице **Администрирование** > **Узлы** добавьте в мониторинг хотя бы один узел. Для этого:

   2.1 Нажмите кнопку **Добавить узлы в мониторинг**.

   2.2 В окне **Добавление узлов в группу мониторинга** добавьте хотя бы один узел в группу **Группа по умолчанию** и установите флажок **Включить опрос**.

   2.3 Нажмите кнопку **Сохранить**.

3 На странице **Мониторинг** > **Список** произведите опрос какого-либо узла мониторинга. Для этого:

   3.1 Щелкните нужный узел в списке узлов мониторинга.

   3.2 В окне **Информация об узле** нажмите кнопку **Опросить**.

4 Перейдите на страницу **Мониторинг** > **Карта** и в списке карт выберите **Локальная карта**.

Если подключение к Серверу мониторинга, опрос узла и просмотр локальной карты производятся успешно, то установку ПО Сервер мониторинга и дополнительного ПО можно считать корректной.

Установка обновлений для стороннего ПО

Программное обеспечение сторонних производителей, которое необходимо для работы Сервера мониторинга, может содержать уязвимости. Чтобы избежать влияния возможных уязвимостей на работу ПК ViPNet StateWatcher, необходимо своевременно устанавливать обновления безопасности, выпускаемые производителями стороннего ПО.

После установки ПО Сервера мониторинга выполните следующие действия:

1 Проверьте наличие обновлений безопасности или новых версий стороннего программного обеспечения на официальных сайтах производителей:

   - PostgreSQL версии 9.1.x на сайте http://www.enterprisedb.com/products-services-training/pgdownload.
   - Oracle Java SE Development Kit версии 7 на сайте http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html.
   - Apache Tomcat версии 6.0.x на сайте https://tomcat.apache.org/download-60.cgi.

2 При наличии обновлений установите их.

3 В процессе эксплуатации ПК ViPNet StateWatcher регулярно устанавливайте выпускаемые обновления ПО сторонних производителей.

Порядок обновления ПО Сервер мониторинга

Внимание! Если на компьютере установлено ПО Сервер мониторинга версии 2.1, необходимо сначала выполнить обновление до версии 3.2, а затем — до версии 4.3. Об обновлении ПО Сервер мониторинга до версии 3.2 см. в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher 3.2. Сервер мониторинга. Руководство администратора».

Перед обновлением ПО Сервер мониторинга необходимо установить обязательное ПО, входящее в комплект поставки новой версии Сервера мониторинга (если версии обязательного ПО изменились).

Перед обновлением проверьте, какие версии обязательного ПО входят в комплект поставки (на стр. 17) новой версии ПО Сервер мониторинга. Если версии обязательного ПО изменились, то необходимо установить актуальные версии данного ПО.

Для обновления ПО Сервер мониторинга вам потребуются:

- Файлы установки обязательного ПО PostgreSQL, Oracle Java Sun JDK и Apache Tomcat, если версии изменились. Они будут включены в комплект поставки обновления.
- Файл установки ПО Сервер мониторинга `StateWatcherInstaller.jar`.
- Файл пакета настроек (файл по умолчанию — `default_pn.zip`).

Обновление ПО Сервер мониторинга и установка новых версий обязательного ПО следует выполнять с использованием учетной записи администратора ОС.

Для обновления ПО Сервер мониторинга выполните все действия из приведенного ниже списка в предложенном порядке.

Таблица 5. Последовательность обновления ПО Сервер мониторинга

	Действие	Примечание
☐	Установите обязательное ПО, если версия данного ПО изменилась В случае обновления Oracle Java Sun JDK предварительно удалите старую версию данного ПО	Порядок установки обязательного ПО (на стр. 43)
☐	Обновите ПО Сервер мониторинга	Обновление ПО Сервер мониторинга (на стр. 58)
☐	Проверьте правильность установки новой версии ПО Сервер мониторинга	Проверка правильности установки ПО Сервер мониторинга (на стр. 54)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Обновление ПО Сервер мониторинга

Перед обновлением ПО Сервер мониторинга обновите обязательное ПО (см. «Порядок установки обязательного ПО» на стр. 43). Все необходимые дистрибутивы будут включены в комплект поставки (на стр. 17).

Обновить версию ПО Сервер мониторинга можно с помощью файла дистрибутива `StateWatcherInstaller.jar`.

Для обновления ПО Сервер мониторинга выполните следующие действия:

1. Остановите службу Apache Tomcat на Сервере мониторинга (см. «Управление Сервером мониторинга» на стр. 40).
2. Двойным щелчком запустите программу установки `StateWatcherInstaller.jar`. Будет запущен мастер **Установка StateWatcher**, следуйте его указаниям.
3. На странице **Лицензионное соглашение** ознакомьтесь с текстом лицензии, затем выберите пункт **Я согласен с условиями лицензии** и нажмите кнопку **Далее**.
4. На странице **Информация** также нажмите кнопку **Далее**.
5. На странице **Проверка внешнего ПО** будет представлена информация о наличии обязательных программ (см. «Порядок установки обязательного ПО» на стр. 43), их

версиях и местоположении. Проверьте представленную информацию, в случае необходимости укажите или измените путь к СУБД PostgreSQL версии 9.1.

6 Для продолжения нажмите кнопку **Далее**.

7 На странице **Выбор варианта установки** выберите пункт **Обновление версии с 3.2.x до 4.3.x**. Для продолжения нажмите кнопку **Далее**.

8 На странице **Конфигурирование сервера БД мониторинга** будут представлены настройки существующей базы данных мониторинга:

- Значения полей **адрес сервера БД**, **порт сервера БД**, **имя БД** и **имя администратора БД** определяются мастером установки автоматически. В случае необходимости измените значения этих полей.
- В поле **пароль администратора БД** введите пароль доступа к базе данных мониторинга.

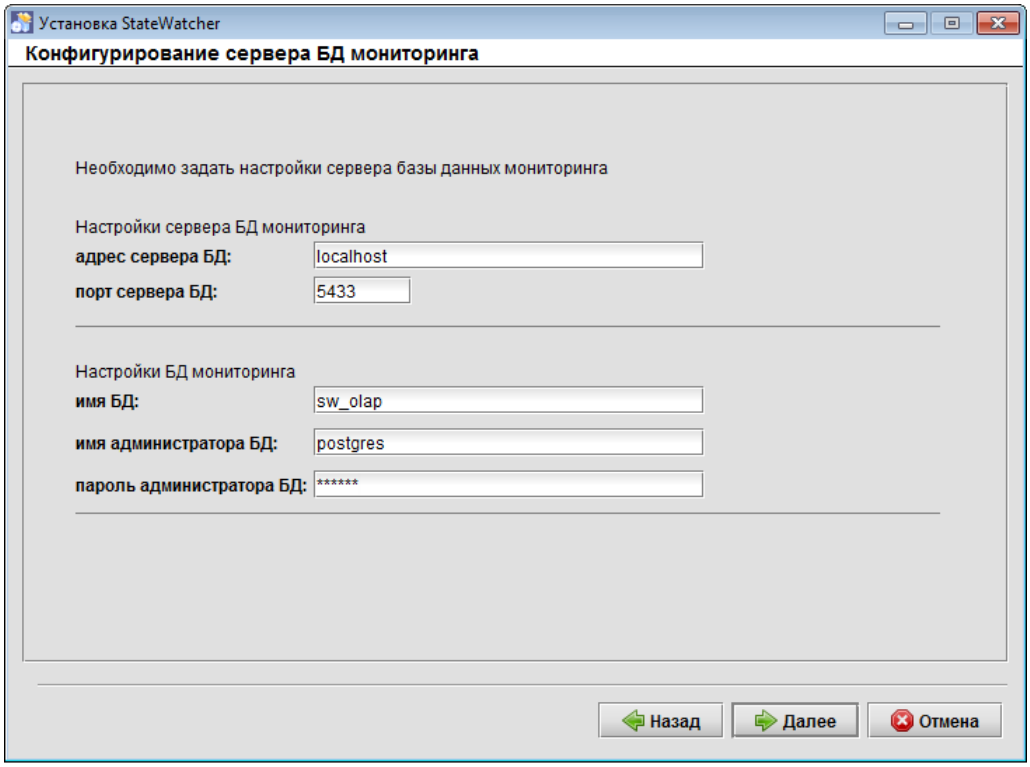

Рисунок 21: Настройка сервера базы данных

Для продолжения нажмите кнопку **Далее**.

Примечание. При обновлении ПО Сервер мониторинга с версии 3.2.x до версии 4.3 на компьютере будут установлены две версии PostgreSQL — 8.4 и 9.1. При этом во время обновления ПО Сервер мониторинга данные, содержащиеся в

таблицах версии 8.4, будут автоматически перенесены в таблицы версии 9.1. По завершении обновления вы сможете удалить PostgreSQL 8.4.

9 На странице **Конфигурирование сервера БД ГИС мониторинга** (см. Рисунок 20 на стр. 52) будут представлены настройки существующей базы данных ГИС.

В поле **пароль администратора сервера БД ГИС** задайте пароль доступа к базе данных ГИС, значения остальных полей оставьте без изменения. Нажмите кнопку **Далее.**

10 На странице **Настройка оповещений для установки** (см. Рисунок 21 на стр. 53) будут представлены существующие настройки оповещений.

Введите, если требуется, данные для авторизации пользователя на SMTP-сервере и нажмите кнопку **Далее.**

11 На странице **Настройка деловой почты** в поле **Путь к директории** укажите папку, в которую Сервер мониторинга будет помещать файлы с оповещениями, предназначенные для обработки правилами автопроцессинга приложения ViPNet Деловая почта.

12 На странице **Требуемый объем дискового пространства** указан доступный объем памяти на диске и объем, требуемый для обновления ПО. Если доступного объема памяти недостаточно, освободите дополнительное пространство. Для продолжения нажмите кнопку **Далее.**

13 На странице **Пакет настроек** укажите путь к файлу с пакетом настроек (см. «Пакет настроек» на стр. 290), который следует установить, и нажмите кнопку **Далее**. Вы можете установить как пакет, идущий в комплекте поставки, так и специально созданный для вашей компании пакет настроек.

Устанавливаемый пакет настроек должен соответствовать определенной версии ПО Сервер мониторинга. Также при установке проверяется корректность устанавливаемого пакета настроек.

Внимание! Если пакет настроек не соответствует версии ПО Сервер мониторинга или является некорректным, мастер установки выдаст соответствующую ошибку, дальнейшие шаги мастера будут недоступны.

14 На странице **Миграция необработанных параметров и событий мониторинга** выберите данные, которые будут перенесены в новую базу данных при обновлении ПО Сервер мониторинга до версии 4.3.

Примечание. Если какие-либо данные не будут переноситься в новую базу данных, то обновление ПО Сервер мониторинга займет значительно меньше времени.

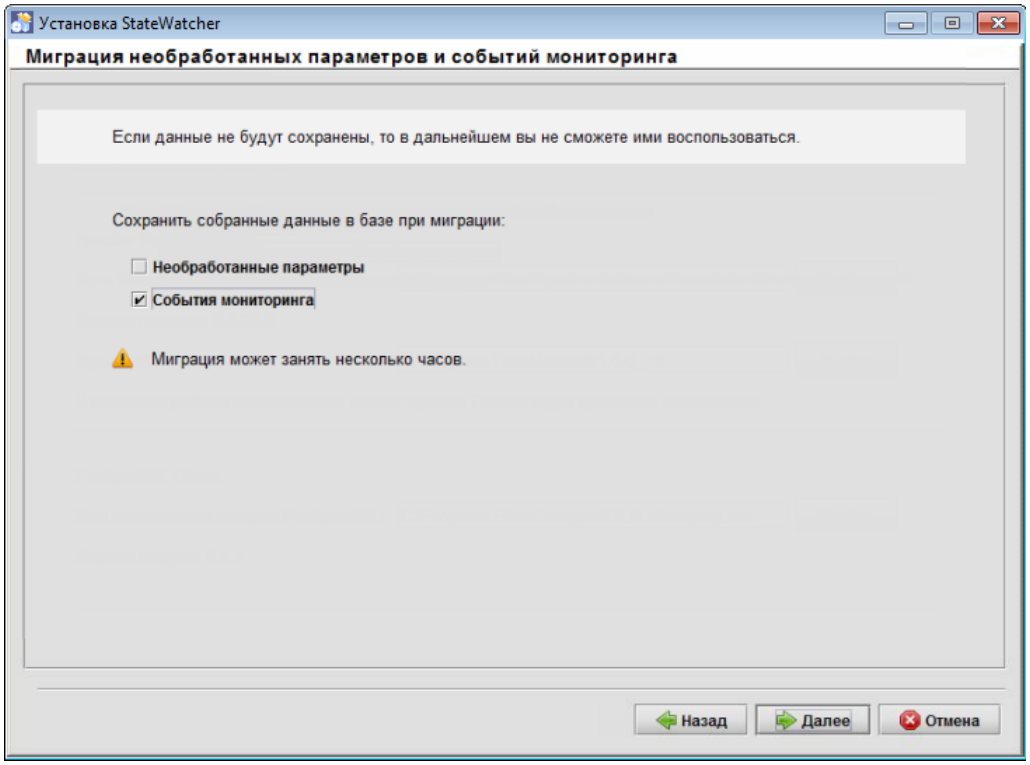

Рисунок 22: Выбор данных для переноса в новую базу данных

15 На странице **Подтверждение** проверьте указанные параметры. Для начала обновления нажмите кнопку **Далее**.

16 Начнется процесс обновления ПО Сервер мониторинга. На странице **Выполнение** будет отображаться информация о ходе обновления. По завершении обновления нажмите кнопку **Далее**.

Примечание. При большом размере базы данных системы мониторинга обновление может занимать несколько часов. Например, обновление с версии 3.2 до версии 4.3 при размере базы основных данных 5 ГБ и базы необработанных данных 15 ГБ занимает около 3 часов.

17 На странице **Завершение выполнения** нажмите кнопку **Завершить**.

Мастер **Установка StateWatcher** закроется, будет запущена служба Apache Tomcat. После запуска Apache Tomcat Сервер мониторинга будет готов к работе.

Внимание! При обновлении ПО Сервер мониторинга необработанные параметры узлов не сохраняются.

Порядок обновления ПО Сервера мониторинга при каскадной организации системы мониторинга

Примечание. В случае каскадной организации системы мониторинга для обновления ПО Сервер мониторинга до версии 4.3 настоятельно рекомендуется удалить старые и установить новые версии этого ПО на всех серверах, входящих в каскад.

Рекомендуется выполнять обновление каскада строго в порядке, представленном в одной из таблиц ниже. В противном случае возможна сборка каскада, в котором версия ПО на родительском Сервере мониторинга ниже, чем на дочерних серверах, однако данная организация каскада не поддерживается.

Обновление ПО Сервер мониторинга до версии 4.3 в случае удаления старых версий ПО происходит в порядке, описанном в таблице ниже (при этом связи в каскаде разрывать не требуется).

Таблица 6. Последовательность обновления ПО Сервер мониторинга в случае удаления старых версий ПО

Действие	Примечание
☐ На всех дочерних Серверах мониторинга удалите старые версии ПО Сервер мониторинга	Удаление ПО Сервер мониторинга (на стр. 66)
☐ На родительском Сервере мониторинга удалите старую версию ПО Сервера мониторинга	
☐ На родительском Сервере мониторинга установите ПО Сервер мониторинга версии 4.3	Установка ПО Сервер мониторинга (на стр. 47)
☐ На всех дочерних Серверах мониторинга по очереди установите ПО Сервер мониторинга 4.3	

	Действие	Примечание
☐	По мере установки ПО добавляйте дочерние серверы в каскад	Добавление Сервера мониторинга в каскад (на стр. 128)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

В случае, если удаление старых версий ПО Сервер мониторинга невозможно (например, если нежелательна потеря данных, содержащихся в старой версии ПО), обновление до версии 4.3 происходит в порядке, описанном в таблице ниже.

Таблица 7. Последовательность обновления ПО Сервер мониторинга без удаления старых версий ПО

	Действие	Примечание
☐	Подключитесь к родительскому Серверу мониторинга с помощью программы АРМ мониторинга и отмените применение правил анализа на дочерних Серверах мониторинга	Применение правила анализа на дочерних Серверах мониторинга
☐	Удалите все дочерние Серверы мониторинга из каскада	Удаление Сервера мониторинга из каскада (на стр. 132)
☐	На родительском Сервере мониторинга обновите ПО Сервер мониторинга до версии 4.3	Обновление ПО Сервер мониторинга (на стр. 58)
☐	На дочерних Серверах мониторинга по очереди обновите ПО Сервер мониторинга до версии 4.3	
☐	По мере установки ПО добавляйте дочерние серверы в каскад	Добавление Сервера мониторинга в каскад (на стр. 128)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Обновление пакета настроек

Начиная с версии 3.2, в ПК ViPNet StateWatcher поддерживается пакет настроек (на стр. 290), позволяющий расширить или сократить доступный пользователю функционал системы мониторинга. Пакет настроек устанавливается на компьютер при первичной установке ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47) или при обновлении ПО Сервер мониторинга (см. «Обновление ПО Сервер мониторинга» на стр. 58).

Также вы можете обновить уже установленный пакет настроек во время работы с ПО Сервер мониторинга версии 3.2 и выше. Ранее установленный пакет настроек можно обновить с помощью мастера установки.

Для обновления пакета настроек выполните следующие действия:

1. Двойным щелчком запустите программу установки `StateWatcherInstaller.jar`. Будет запущен мастер **Установка StateWatcher**, следуйте его указаниям.
2. На странице **Лицензионное соглашение** ознакомьтесь с текстом лицензии, затем выберите пункт **Я согласен с условиями лицензии** и нажмите кнопку **Далее**.

   На странице **Информация** также нажмите кнопку **Далее**.
3. На странице **Проверка внешнего ПО** (см. Рисунок 17 на стр. 49) будет представлена информация о наличии обязательных программ (см. «Порядок установки обязательного ПО» на стр. 43), их версиях и местоположении. Для продолжения нажмите кнопку **Далее**.
4. На странице **Выбор варианта установки** выберите пункт **Установить пакет настроек**. Для продолжения нажмите кнопку **Далее**.
5. На странице **Пакет настроек** укажите путь к файлу с пакетом, который следует установить, и нажмите кнопку **Далее**.

   Устанавливаемый пакет настроек должен соответствовать определенной версии ПО Сервер мониторинга. Также при установке проверяется корректность устанавливаемого пакета настроек.

Внимание! Если пакет настроек не соответствует версии ПО Сервер мониторинга или является некорректным, мастер установки выдаст соответствующую ошибку, дальнейшие шаги мастера будут недоступны.

Настоятельно рекомендуется использовать пакет настроек, идущий в комплекте поставки по умолчанию, или использовать пакет, разработанный специально для вашей компании.

---

6 На странице **Подтверждение** проверьте указанные параметры. Для начала установки пакета настроек нажмите кнопку **Далее.**

7 Начнется процесс установки пакета настроек. На странице **Выполнение** будет отображаться информация о ходе установки.

8 На странице **Завершение выполнения** нажмите кнопку **Завершить**.

Мастер **Установка StateWatcher** закроется, будет запущена служба Apache Tomcat. После запуска Apache Tomcat Сервер мониторинга готов к работе.

В результате обновления пакета настроек будут произведены следующие изменения:

- Изменены имеющиеся географические координаты узлов согласно системе координат, заданной в новом пакете настроек.
- Изменен набор стандартных масштабов и настройки режимов отображения по умолчанию для каждого масштаба.
- Изменен список поддерживаемых типов сетевых узлов.
- Изменен шаблон письма для оповещений по электронной почте.
- Изменен язык интерфейса.

Примечание. Каждое из перечисленных изменений производится только при наличии в новом пакете настроек соответствующих данных.

Удаление ПО Сервер мониторинга

Внимание! После удаления ПО Сервер мониторинга будут удалены база данных мониторинга и база данных ГИС! Перед удалением вы можете сделать резервную копию баз данных (см. «Резервирование баз данных» на стр. 172), если планируете переустанавливать ПО Сервер мониторинга.

Для удаления ПО Сервер мониторинга выполните следующие действия:

1. Двойным щелчком запустите программу установки `StateWatcherInstaller.jar`. Будет запущен мастер **Установка StateWatcher**, следуйте его указаниям.
2. На странице **Лицензионное соглашение** выберите пункт **Я согласен с условиями лицензии** и нажмите кнопку **Далее**.

   На странице **Информация** также нажмите кнопку **Далее**.
3. На странице **Проверка внешнего ПО** (см. Рисунок 17 на стр. 49) будет представлена информация о наличии обязательных программ, их версиях и местоположении. Для продолжения нажмите кнопку **Далее**.
4. На странице **Выбор варианта установки** выберите пункт **Удаление**. Для продолжения нажмите кнопку **Далее**.
5. На странице **Конфигурирование сервера БД мониторинга** (см. Рисунок 22 на стр. 59):
   - Проверьте правильность указанных параметров сервера базы данных мониторинга.
   - В поле **пароль администратора БД** введите пароль доступа к базе данных мониторинга.

   Для продолжения нажмите кнопку **Далее**.
6. На странице **Конфигурирование сервера БД ГИС мониторинга** (см. Рисунок 20 на стр. 52):
   - Проверьте правильность указанных параметров сервера базы данных ГИС.
   - В поле **пароль администратора сервера БД ГИС** введите пароль к базе данных ГИС.

   Для продолжения нажмите кнопку **Далее**.

7 На странице **Подтверждение** мастер выдаст предупреждение об удалении баз данных и ПО Сервер мониторинга. Для продолжения нажмите кнопку **Далее**.

8 Начнется процесс удаления ПО Сервер мониторинга. На странице **Выполнение** будет отображаться информация о ходе удаления. По окончании удаления нажмите кнопку **Далее**.

9 На странице **Завершение выполнения** нажмите кнопку **Завершить**. ПО Сервер мониторинга и базы данных будут удалены.

Подключение к Серверу мониторинга

Подключиться к Серверу мониторинга можно на любом АРМ мониторинга, связанном (в ЦУСе) с данным Сервером мониторинга.

Чтобы начать работу с Сервером мониторинга, на АРМ мониторинга:

1 Подключитесь к Серверу мониторинга одним из следующих способов:

- В веб-браузере введите адрес `http://<адрес_сервера>:<порт>`. Порт можно не указывать, если Сервер мониторинга использует порт по умолчанию (80).
- В программе ViPNet Монитор в окне **Защищенная сеть** выберите Сервер мониторинга и нажмите команду **Web-ссылка** в главном меню **Действия** или в контекстном меню, либо нажмите кнопку (**Веб-ресурс**) на панели инструментов.

Появится окно для аутентификации пользователя.

Рисунок 23: Аутентификация пользователя

2 Введите в поле **Пользователь** имя учетной записи администратора, в поле **Пароль** — пароль администратора и нажмите кнопку **Войти**.

Примечание. Для управления Сервером мониторинга вы можете использовать встроенную учетную запись `Administrator` с паролем `Administrator` или создать другую учетную запись администратора (см. «Создание и изменение

учетной записи» на стр. 78). Администратор также может сменить пароль встроенной учетной записи, задав собственный пароль (см. «Создание и изменение учетной записи» на стр. 78).

После успешной аутентификации администратору будет доступен просмотр информации и все действия по настройке и управлению Сервером мониторинга.

Примечание. Чтобы веб-страницы отображались без вертикальной и горизонтальной полос прокрутки, необходимо установить на АРМ мониторинга разрешение экрана не менее 1024x768.

3

Настройка Сервера мониторинга

Настройка Сервера мониторинга с помощью мастера 71

Настройка учетных записей 77

Настройка узлов и групп мониторинга 83

Настройка типов узлов мониторинга 95

Настройка правил анализа 97

Настройка оповещений 106

Настройка подключения к прокси-серверу 119

Настройка карты 121

Настройка каскада 127

Экспорт и импорт настроек Сервера мониторинга 133

Тонкая настройка Сервера мониторинга 137

Просмотр журнала событий 151

Настройка Сервера мониторинга с помощью мастера

При первом подключении к Серверу мониторинга с использованием встроенной учетной записи `Administrator` будет запущен **Мастер быстрой настройки**. С помощью данного мастера вы можете:

- Настроить способы оповещения для каждого уровня критичности событий.
- Выбрать узлы для мониторинга.
- Добавить в список мониторинга открытые узлы.
- Настроить подключение к SMTP-серверу и SMS-шлюзу.

Чтобы отказаться от настройки с помощью мастера (например, если вы хотите настроить Сервер мониторинга позже), нажмите кнопку **Отмена**. Вы можете запустить мастер быстрой настройки позже, для этого в правом верхнем углу главного окна АРМ мониторинга в меню **Настройки** выберите пункт **Мастер быстрой настройки**. Данная функция доступна только для учетной записи `Administrator`.

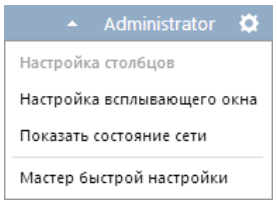

Рисунок 24: Вызов мастера быстрой настройки

Чтобы настроить Сервер мониторинга с помощью мастера, выполните следующие действия:

1. На первой странице мастера в группе **Способ оповещения** выберите желаемые способы оповещения для событий критичного уровня.

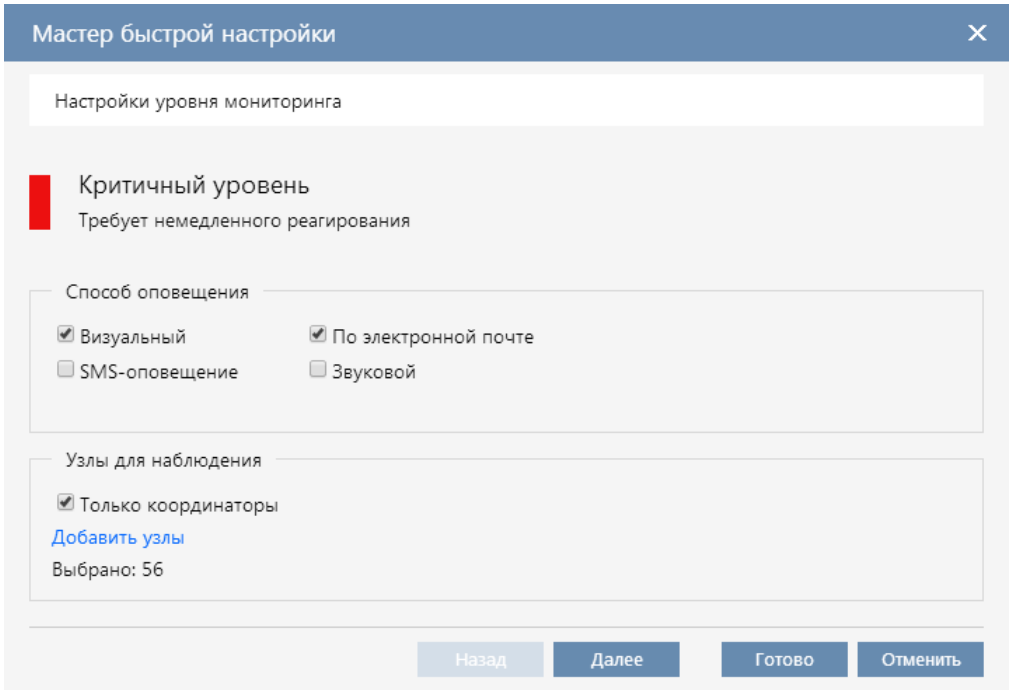

Рисунок 25: Настройка оповещений критичного уровня важности

2 В группе **Узлы для наблюдения** добавьте узлы мониторинга, для которых будут формироваться оповещения. Для этого:

2.1 Щелкните ссылку **Добавить узлы**.

2.2 В окне **Узлы для добавления в мониторинг** установите флажки рядом с нужными узлами мониторинга.

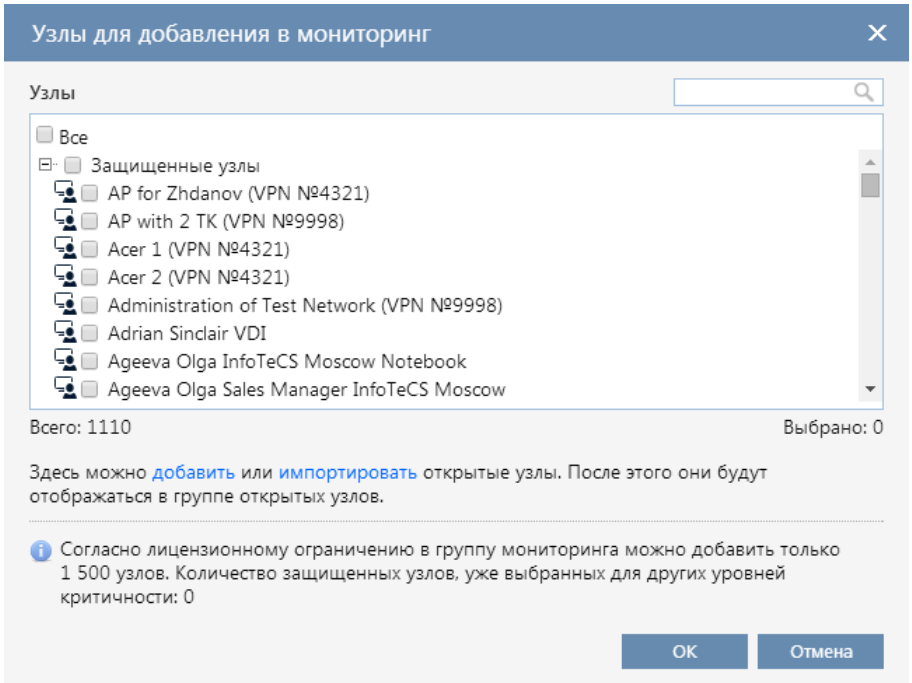

Рисунок 26: Выбор узлов для добавления в мониторинг

2.3 При необходимости добавьте или импортируйте в список связей Сервера мониторинга открытые узлы:

- Для добавления открытого узла нажмите ссылку **Добавить** и укажите название, IP-адрес, сетевой протокол и порт открытого узла.

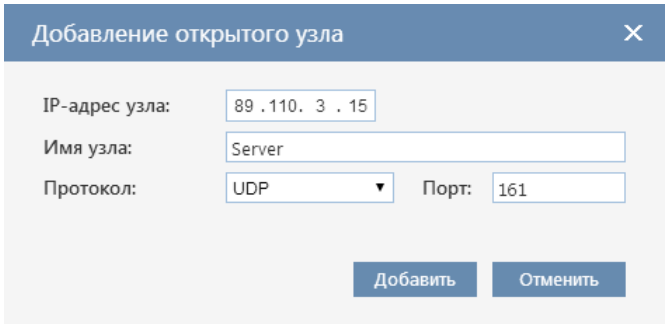

Рисунок 27: Добавление открытого узла

- Для импорта списка открытых узлов нажмите ссылку **Импортировать** и укажите файл со списком открытых узлов.

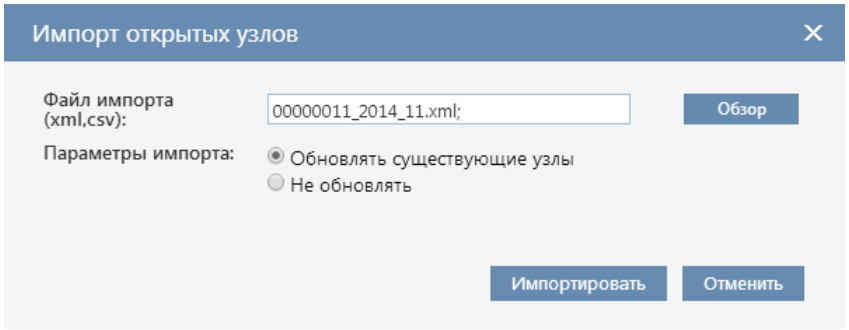

Рисунок 28: Импорт открытых узлов

После добавления в список открытых узлов установите флажки рядом с нужными узлами.

2.4 Нажмите кнопку **OK**.

3 На второй и третьей странице мастера аналогичным образом настройте оповещения для предупреждающего и информационного уровней событий.

4 Если для одного из уровней критичности было выбрано оповещение по электронной почте, на следующей странице мастера настройте параметры подключения к SMTP-серверу, который будет использоваться для отправки оповещений. Укажите адрес и порт SMTP-сервера, а также адрес электронной почты, с которого будут приходить оповещения, и адреса электронной почты администраторов, которые будут получать оповещения. При необходимости задайте имя и пароль пользователя для аутентификации на SMTP-сервере.

Подробнее о настройках SMTP-сервера см. в разделе Настройка оповещений по электронной почте (на стр. 112).

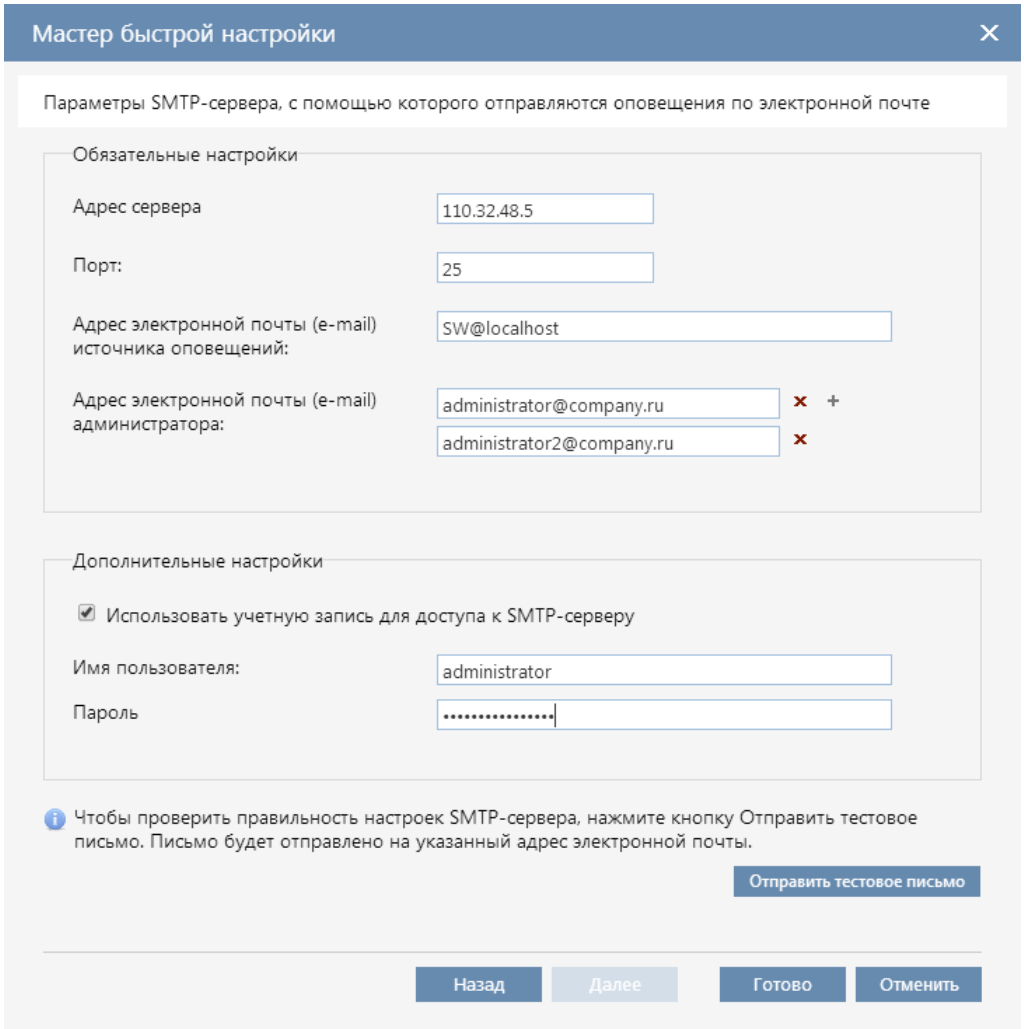

Рисунок 29: Настройка подключения в SMTP-серверу

5 Если для одного из уровней критичности было выбрано оповещение по SMS, на следующей странице мастера настройте параметры подключения к SMS-шлюзу, который будет использоваться для отправки оповещений. Укажите адрес, порт, название учетной записи и пароль для подключения к SMS-шлюзу, а также телефон администратора, который будет получать оповещения по SMS.

Подробнее о настройках SMS-шлюза см. в разделе Настройка оповещений по SMS (на стр. 115).

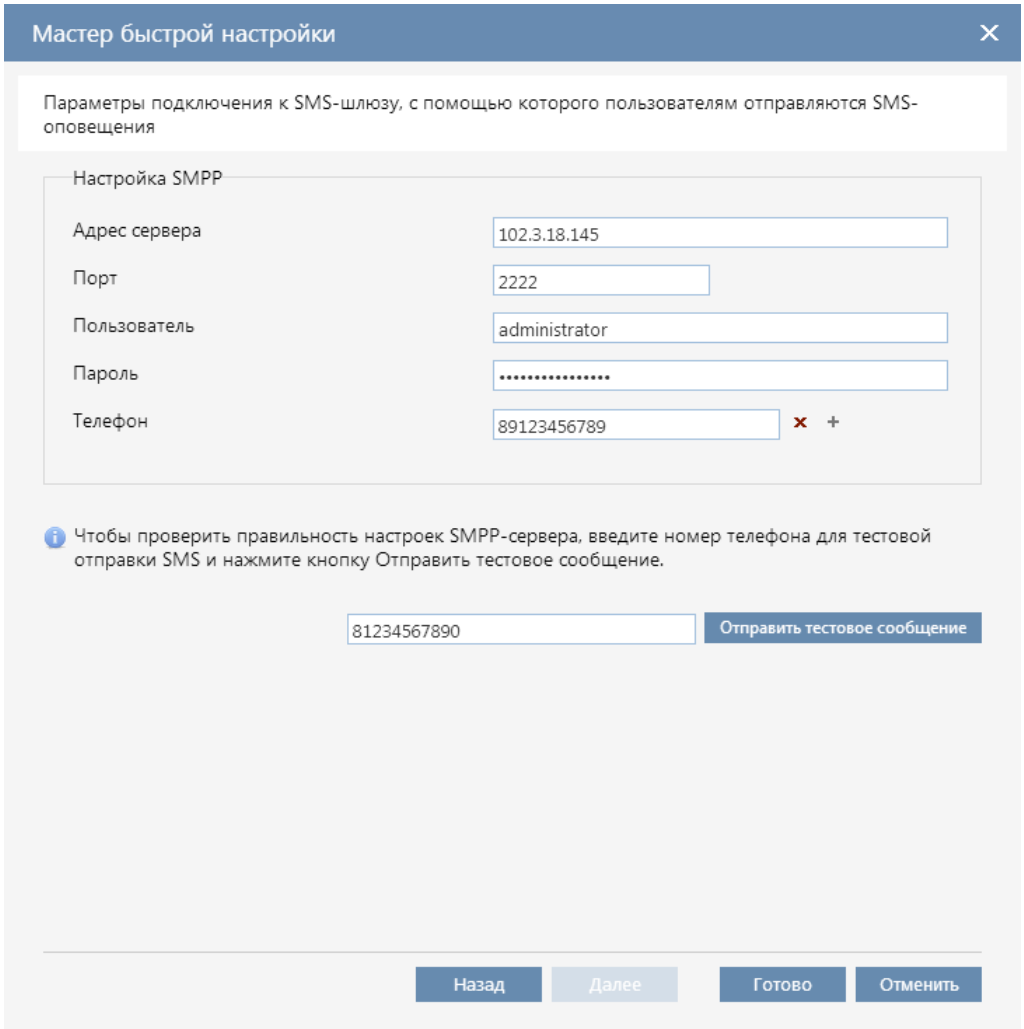

Рисунок 30: Настройка подключения к SMS-шлюзу

6 По завершении настройки нажмите кнопку **Готово**.

Настройка учетных записей

Учетные записи пользователей и администраторов хранятся в базе данных Сервера мониторинга и содержат фамилии, имена, пароли и другие атрибуты. Одна из учетных записей является встроенной, она содержит сведения об администраторе Сервера мониторинга – пользователе `Administrator`. Встроенную учетную запись нельзя удалить.

Учетным записям могут быть назначены различные права:

- Администраторам разрешен просмотр информации об узлах мониторинга и все действия по настройке и управлению Сервером мониторинга.
- Пользователям разрешен только просмотр информации об узлах мониторинга.

Права назначаются при создании или изменении учетных записей (см. «Создание и изменение учетной записи» на стр. 78).

Подключение к Серверу мониторинга (на стр. 68) под одной учетной записью разрешено только одному пользователю. Если пользователь на другом АРМ мониторинга также подключается к Серверу мониторинга под данной учетной записью, то текущая сессия первого пользователя принудительно завершается (с соответствующим предупреждением) и управление переходит к вновь подключившемуся пользователю.

Настройка учетных записей выполняется с помощью АРМ мониторинга под учетной записью администратора. Эта настройка позволяет управлять учетными записями (создавать, изменять (см. «Создание и изменение учетной записи» на стр. 78) и удалять (см. «Удаление учетной записи» на стр. 81)), а также осуществлять поиск нужных записей. Для настройки учетных записей выполните следующие действия:

1. Подключитесь к нужному Серверу мониторинга под учетной записью администратора.
2. На вкладке **Администрирование** перейдите на страницу **Пользователи**. На данной странице отображается список существующих учетных записей. Учетные записи администраторов отмечаются значком .

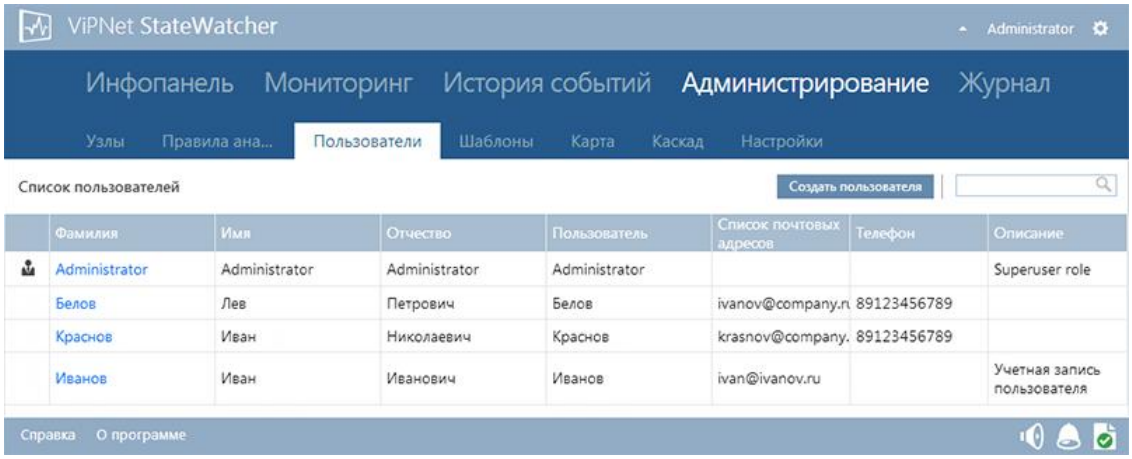

Рисунок 31: Учетные записи администраторов и пользователей

Записи в списке отсортированы по фамилии в алфавитном порядке.

Список учетных записей можно отфильтровать, чтобы в нем отображались только нужные записи. Для этого введите в поле, расположенное над списком, искомую подстроку. При вводе в это поле очередного символа происходит автоматическая фильтрация списка по вхождению заданной подстроки в любой из атрибутов пользователей. Для очистки поля фильтра используйте находящийся справа от него значок ✕.

Создание и изменение учетной записи

Чтобы создать или изменить учетную запись пользователя или администратора:

1 На странице **Пользователи** выполните одно из действий:

- Для создания учетной записи нажмите кнопку **Создать нового пользователя**.
- Для редактирования учетной записи щелкните мышью по имени учетной записи.

Появится окно с выбранной учетной записью. Для новой учетной записи все атрибуты будут пустыми.

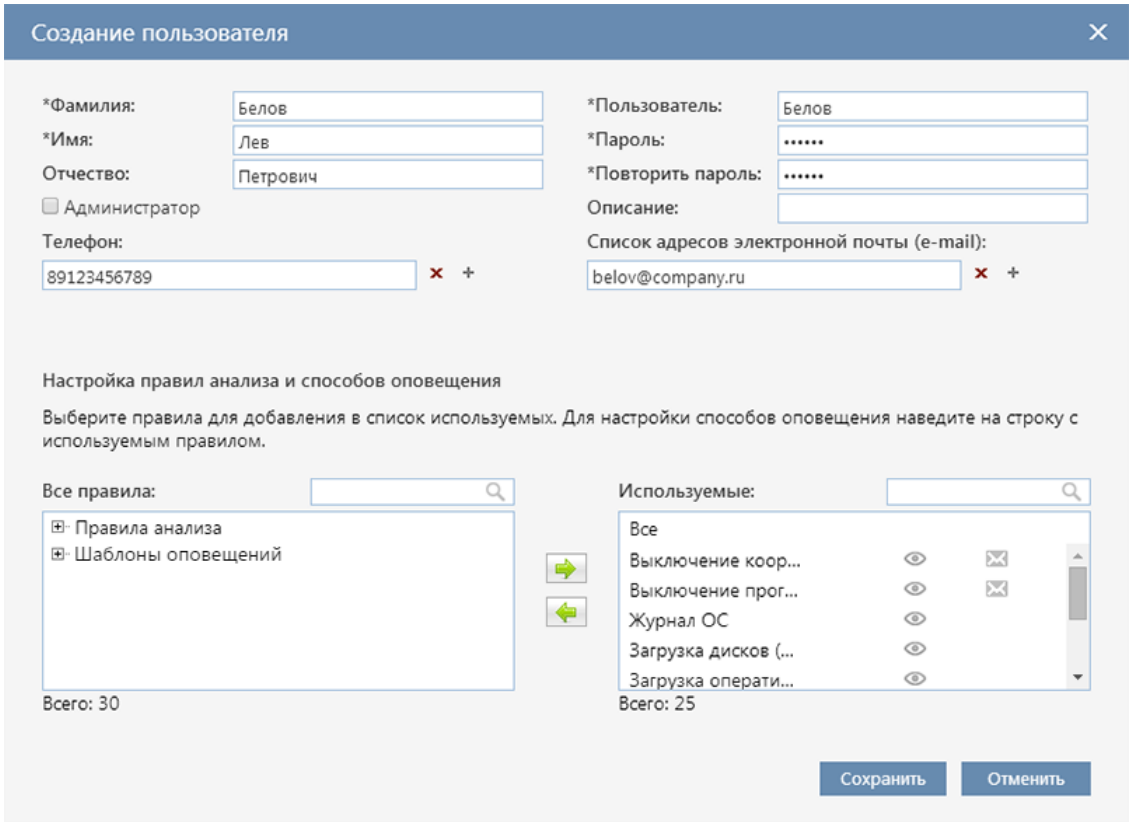

Рисунок 32: Изменение учетной записи

2 Задайте или измените следующие атрибуты учетной записи:

Примечание. Атрибуты, обязательные для заполнения, отмечены звездочкой.

- **Фамилия**, **Имя**, **Отчество**, **Пользователь** и **Пароль** – основные атрибуты учетной записи. В поле **Пользователь** вводится имя создаваемой учетной записи. Пароль необходимо повторить в поле **Повторить пароль**.

  В полях **Фамилия**, **Имя** и **Отчество** можно вводить только буквы (не более 30-ти).

  В поле **Пользователь** можно вводить только буквы латинского алфавита и цифры (не менее 4-х и не более 20-ти).

Внимание! Имя встроенной учетной записи `Administrator` изменить невозможно.

В поле **Пароль** можно вводить только буквы латинского алфавита и цифры. Длина пароля должна быть не менее 6-ти символов.

Телефон — номер телефона пользователя, на который будут отправляться SMS-оповещения (например, 89012345678). В данное поле можно вводить только цифры.

Список адресов электронной почты (e-mail) – список адресов для оповещений по электронной почте (максимум 15 адресов).

Для управления списком адресов используйте кнопки **Добавить** и **Удалить**, расположенные справа от каждого элемента списка.

- Флажок **Администратор** определяет, какие права будут назначены учетной записи. Если данный флажок установлен, то учетной записи будут назначены права администратора, если флажок снят — то права пользователя.

  Если вы удалите роль администратора для своей учетной записи (снимите флажок **Администратор**), появится сообщение с запросом подтвердить удаление роли администратора. В окне сообщения нажмите кнопку **Да**. При этом вашей учетной записи будут назначены права пользователя, и откроется окно аутентификации.

- **Описание** – произвольное описание учетной записи (максимум 100 символов).

- **Настройка правил анализа и способов оповещения** – список правил анализа и способов оповещения для данного пользователя.

  В этом разделе вы можете назначить следующие способы оповещения (на стр. 107) для выбранных правил анализа: визуальный, звуковой, по электронной почте и по SMS. Для встроенной учетной записи `Administrator` также можно выбрать оповещение по Деловой почте и по протоколу Syslog. С помощью кнопок и перенесите в список **Используемые** правила анализа и шаблоны правил анализа для данного пользователя. В списке **Используемые** отметьте способы оповещения для каждого правила или шаблона.

3 Задайте все требуемые атрибуты и нажмите кнопку **Сохранить**.

Чтобы отказаться от создания новой учетной записи или изменения существующей записи, нажмите кнопку **Отменить**.

В результате будет создана или изменена учетная запись администратора или пользователя.

Удаление учетной записи

Чтобы удалить учетную запись:

1. В главном окне на вкладке **Администрирование** перейдите на страницу **Пользователи**.
2. На странице **Пользователи** щелкните название учетной записи, которую необходимо удалить.
3. В окне **Редактирование пользователя** нажмите кнопку **Удалить пользователя**.

   Перед удалением появится запрос на подтверждение удаления.
4. Для удаления учетной записи нажмите кнопку **Сохранить**, для отмены удаления – кнопку **Отменить**.
5. Если вы удаляете собственную учетную запись, появится сообщение с запросом подтвердить удаление. В окне сообщения нажмите кнопку **Да**. При этом ваша учетная запись будет удалена, и откроется окно аутентификации пользователя.

Примечание. Если удаляется учетная запись пользователя, который работает в данный момент с Сервером мониторинга, то при любом его действии после удаления появляется сообщение о том, что данная учетная запись удалена, и сессия принудительно завершается.

Встроенную учетную запись `Administrator` удалить невозможно.

Смена пароля

Пароль пользователя или администратора, заданный в его учетной записи, может сменить администратор Сервера мониторинга при настройке учетных записей. Кроме того, пользователь может сам сменить свой пароль при работе с Сервером мониторинга.

Для этого выполните следующие действия:

1. В верхнем правом углу веб-страницы в меню с названием вашей учетной записи выберите пункт **Редактировать**. Появится окно для смены пароля. В поле **Пользователь** отображается имя учетной записи пользователя.

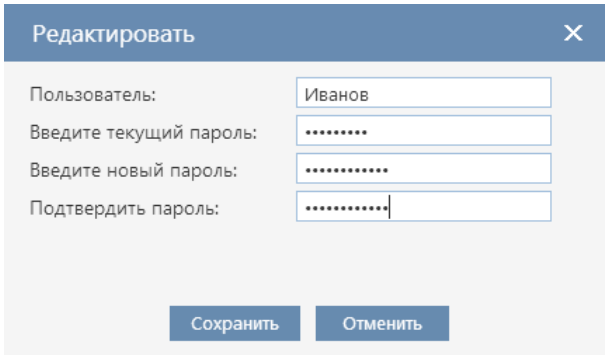

Рисунок 33: Смена пароля пользователя

2 Введите текущий пароль в соответствующее поле, затем введите новый пароль и подтвердите его в поле **Подтвердить пароль**.

3 Нажмите кнопку **Сохранить**, чтобы сменить пароль. Чтобы отказаться от смены пароля, нажмите кнопку **Отменить**.

Настройка узлов и групп мониторинга

Настройка узлов и групп мониторинга выполняется с помощью АРМ мониторинга под учетной записью администратора. Эта настройка позволяет задавать параметры мониторинга отдельных узлов и групп мониторинга, а также управлять группами мониторинга (создавать, удалять и определять состав групп).

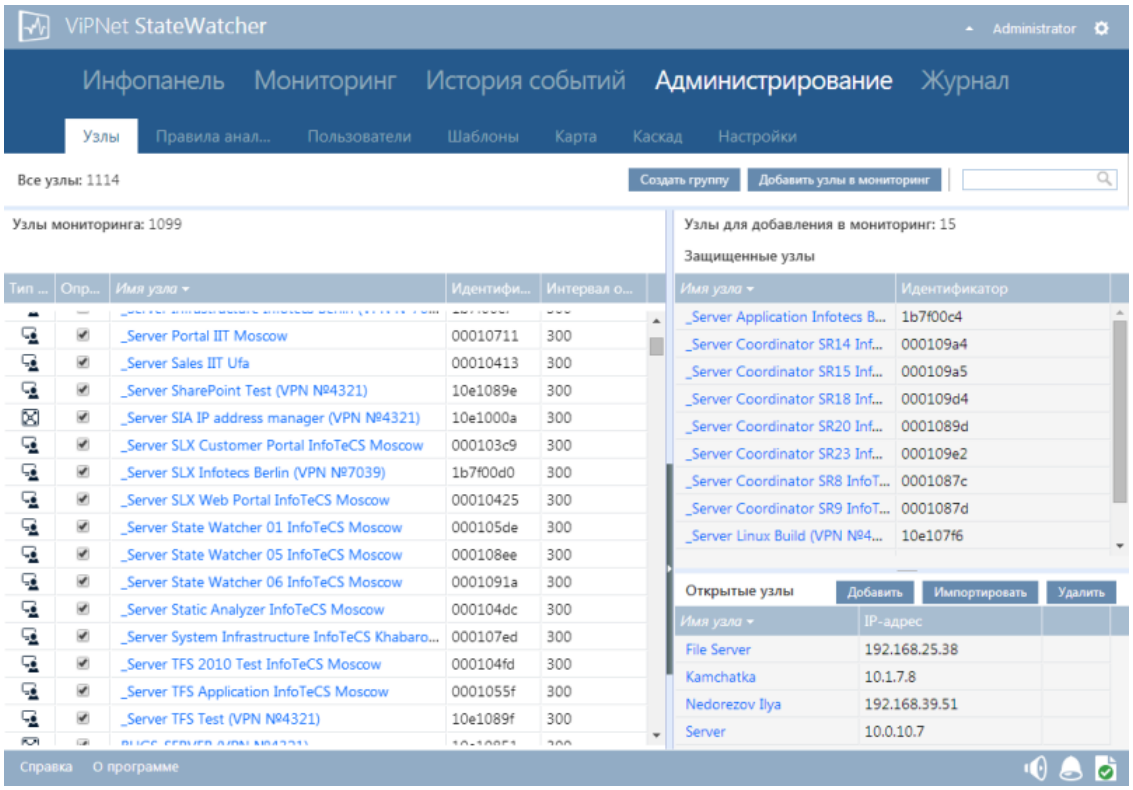

Рисунок 34: Текущие настройки узлов и групп мониторинга

Список **Узлы для добавления в мониторинг** состоит из двух разделов: **Защищенные узлы** и **Открытые узлы**. Состав раздела **Защищенные узлы** определяется связями Сервера мониторинга, заданными в программе Центр управления сетью. В процессе своей работы Сервер мониторинга периодически обращается к программному компоненту ViPNet Монитор, установленному на Сервере мониторинга, для получения актуальной информации о связанных с ним защищенных узлах (см. «Защищенный узел» на стр. 289). В соответствии с полученной от ViPNet Монитор информацией Сервер

мониторинга корректирует текущий список узлов для добавления в мониторинг. Узлы в раздел **Открытые узлы** добавляются вручную администратором Сервера мониторинга.

На Сервере мониторинга также есть **Группа по умолчанию**. Это обязательная (предопределенная) группа, объединяющая узлы мониторинга, не входящие ни в одну из групп.

Примечание. Узлы, расположенные в списке узлов для добавления в мониторинг, не опрашиваются Сервером мониторинга и не учитываются при проверке лицензионных ограничений на максимальное количество узлов мониторинга.

При первом (после установки ПО) запуске Сервера мониторинга на странице **Администрирование > Узлы** все доступные для мониторинга узлы размещаются в списке узлов для добавления в мониторинг и по умолчанию у всех узлов отключен мониторинг. Чтобы настроить мониторинг сети, администратор должен создать группы мониторинга (если это необходимо), перенести узлы из списка узлов для добавления в мониторинг в группу **Группа по умолчанию** или в любую группу, созданную администратором, и задать параметры мониторинга узлов или групп (как минимум, включить мониторинг).

Внимание! Количество узлов с включенным мониторингом (то есть количество одновременно опрашиваемых узлов) не должно превышать 20000.

Перемещение узлов мониторинга из списка узлов для добавления в мониторинг в другие группы можно выполнить следующими способами:

- путем изменения параметров мониторинга отдельного узла (см. «Изменение параметров мониторинга узла» на стр. 91);
- массовым переносом новых узлов в какую-либо группу (см. «Перемещение новых узлов в группу мониторинга» на стр. 89).

Примечание. Опрос узлов, перемещенных из списка узлов для добавления в мониторинг в группы мониторинга, производится не сразу, а с некоторой задержкой, зависящей от интервала опроса. Поэтому в интерфейсе АРМ мониторинга для этих узлов первоначально будет установлено состояние «Неизвестно». Состояние этих узлов изменится, как только Сервер мониторинга произведет их опрос.

Для настройки узлов и групп мониторинга на вкладке **Администрирование** перейдите на страницу **Узлы**. На данной странице отображается список групп мониторинга и входящих в них узлов и их текущие настройки.

Узлы в списке распределены по группам согласно текущим настройкам Сервера мониторинга. Для удобства просмотра любую группу мониторинга можно раскрыть, чтобы увидеть список входящих в нее узлов, или закрыть (свернуть). Для этого используйте значок, расположенный слева от имени группы. Список узлов можно отфильтровать, чтобы в нем отображались только нужные узлы. Для этого введите имя или часть имени в поле поиска, расположенное над списком узлов.

Чтобы изменить параметры мониторинга отдельного узла, щелкните в списке название нужного узла.

Для каждого элемента списка (группы или узла мониторинга) выводится информация, приведенная в таблице ниже.

Таблица 8. Столбцы списков узлов мониторинга и узлов для добавления в мониторинг

Название столбца	Описание
ViPNet тип	Значок типа узла. Определяется Сервером мониторинга автоматически при добавлении узла в мониторинг.
Опрос	Флажок, указывающий на включение или отключение мониторинга всей группы либо отдельного узла. Если мониторинг включен, то флажок установлен, иначе флажок снят. Отсутствует для группы **Узлы для добавления в мониторинг** и узлов, входящих в эту группу. Сервер мониторинга не опрашивает узлы, не имеющие IP-адресов или имеющие нулевые IP-адреса (независимо от того, включен или отключен мониторинг этих узлов). Впоследствии при появлении адресов у тех узлов, мониторинг которых включен, опрос включается автоматически. Для группы вместо флажка может отображаться значок – в том случае, когда у части узлов, входящих в группу, мониторинг включен, но при этом мониторинг всей группы отключен. Этот флажок можно устанавливать и снимать непосредственно в списке. При установке флажка у группы автоматически устанавливаются флажки у всех узлов, входящих в группу.
Имя узла	Имя узла мониторинга.

	Для открытых узлов имя узла может быть изменено при редактировании узла. Для защищенных узлов имя узла неизменно и задается в программе ViPNet Центр управления сетью.
Идентификатор/IP-адрес	Идентификатор узла мониторинга в сети ViPNet или IP-адрес открытого узла.
Интервал опроса узла мониторинга	Периодичность опроса (в секундах) узла мониторинга Сервером мониторинга. Отображается только для узлов мониторинга.

Создание и изменение группы мониторинга

Чтобы создать или изменить группу мониторинга:

1 На странице **Администрирование** > **Узлы** выполните одно из действий:

- Нажмите кнопку **Создать группу**, чтобы создать новую группу узлов мониторинга.
- В списке **Узлы мониторинга** щелкните название группы, чтобы отредактировать параметры этой группы.

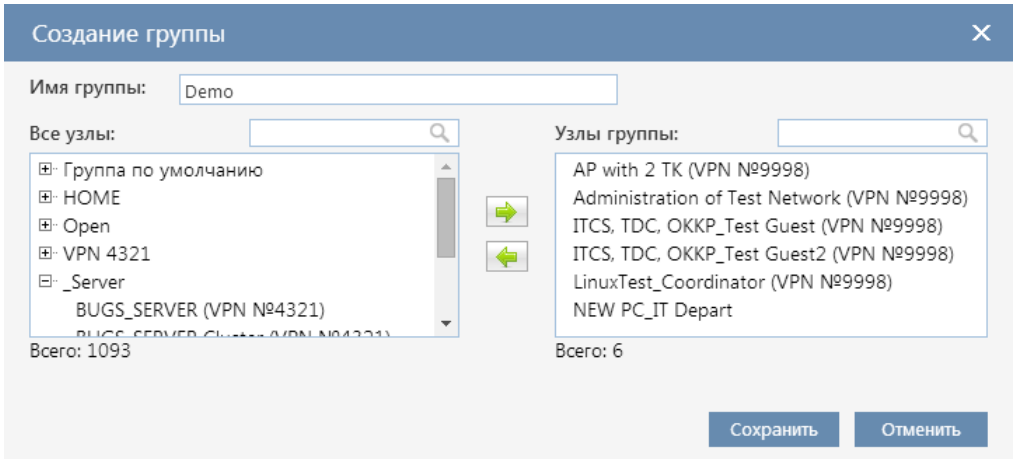

Рисунок 35: Изменение параметров группы

2 Задайте или измените следующие параметры группы мониторинга:

- **Имя группы** – имя группы мониторинга. В имени группы можно использовать только буквы, цифры и символы «-» (дефис) и «_» (подчеркивание).

Внимание! Имена групп мониторинга должны быть уникальными для одного Сервера мониторинга.

- **Узлы группы** – список узлов, входящих в состав группы. Заполните список **Узлы группы** узлами, которые должны быть включены в группу.

Внимание! При включении узла в создаваемую группу он автоматически удаляется из своей текущей группы.

С помощью кнопок и перенесите нужные узлы из списка **Все узлы** в список **Узлы группы**. Первоначально список **Все узлы** содержит все узлы мониторинга с их текущим распределением по группам (кроме узлов списка **Узлы для добавления в мониторинг**).

Примечание. При переносе узлов обратно в список **Все узлы** они будут помещены в группу **Группа по умолчанию**, даже если первоначально узлы находились в другой группе мониторинга.

Узлы, содержащиеся в списках **Все узлы** и **Узлы группы**, можно отфильтровать по имени узла. Для этого введите имя или часть имени в поле поиска, расположенное над соответствующим списком.

Примечание. При создании новой группы мониторинга можно не задавать список узлов группы, а определить его в дальнейшем при редактировании группы.

3 После того, как будут заданы параметры группы мониторинга, нажмите кнопку **Сохранить**. Чтобы отказаться от создания группы или от сделанных изменений, нажмите кнопку **Отменить**.

Добавление открытых узлов в список связей Сервера мониторинга

Для возможности добавления открытых узлов в группу мониторинга предварительно необходимо добавить данные узлы в список связей Сервера мониторинга в раздел **Открытые узлы** группы **Узлы для добавления в мониторинг**. На открытых узлах должен быть настроен и запущен SNMP-агент (служба SNMP) (см. «Настройка службы SNMP на открытом узле» на стр. 253).

Чтобы добавить открытый узел в список связей Сервера мониторинга, выполните следующие действия:

1. В главном окне программы перейдите на страницу **Администрирование** > **Узлы**.
2. В разделе **Открытые узлы** нажмите кнопку **Добавить**.
3. В окне **Добавление открытого узла** укажите следующие параметры:
   - IP-адрес открытого узла.
   - Имя открытого узла.
   - Сетевой протокол, по которому происходит взаимодействие с открытым узлом. По умолчанию UDP, также возможно взаимодействие по протоколу TCP.
   - Порт, с использованием которого происходит подключение к открытому узлу. По умолчанию используется порт 161 — стандартный порт для опроса SNMP-агента.

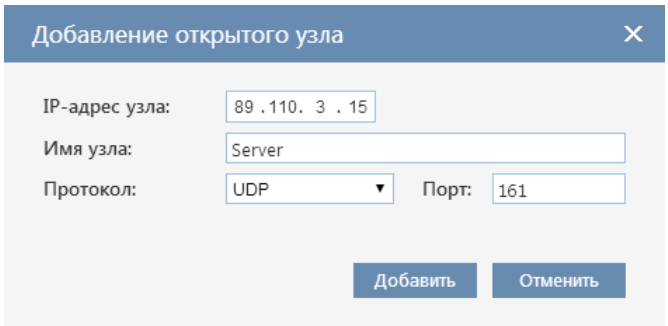

Рисунок 36: Добавление открытого узла

4. Нажмите кнопку **Добавить**. Для отмены добавления узла в список связей нажмите кнопку **Отменить**.

В результате добавленный узел отобразится в списке открытых узлов группы **Узлы для добавления в мониторинг**.

Также при необходимости вы можете импортировать сразу несколько открытых узлов и обновить информацию об уже добавленных узлах с помощью файла импорта открытых узлов `*.xml`, который вы можете сформировать по специальному шаблону (см. «Шаблон файла импорта открытых узлов» на стр. 247).

Чтобы импортировать открытые узлы в список связей Сервера мониторинга, выполните следующие действия:

1. В главном окне программы перейдите на страницу **Администрирование** > **Узлы**.
2. В разделе **Открытые узлы** нажмите кнопку **Импортировать**.
3. В окне **Импорт открытых узлов** воспользуйтесь кнопкой **Обзор**, чтобы выбрать нужный файл импорта открытых узлов в формате XML.

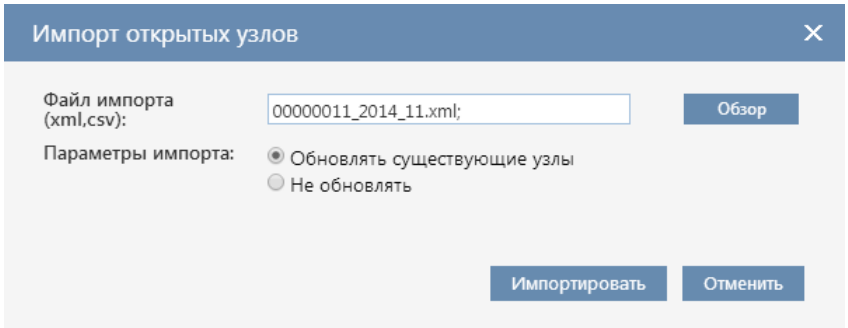

Рисунок 37: Импорт открытых узлов

4. Если необходимо обновить информацию об уже добавленных открытых узлах, установите переключатель **Параметры импорта** в положение **Обновлять существующие узлы**.
5. Нажмите кнопку **Импортировать**. Для отмены импорта открытых узлов нажмите кнопку **Отменить**.

В результате в список связей Сервера мониторинга будут добавлены все открытые узлы, параметры которых указаны в файле импорта.

Перемещение новых узлов в группу мониторинга

Существует возможность группового переноса новых узлов (находящихся в списке **Узлы для добавления в мониторинг**) в какую-либо группу мониторинга.

Для этого:

1. В главном окне на вкладке **Администрирование** перейдите на страницу **Узлы**.

2 На открывшейся странице нажмите кнопку **Добавить узлы в мониторинг**. Откроется окно, содержащее список узлов для добавления в мониторинг.

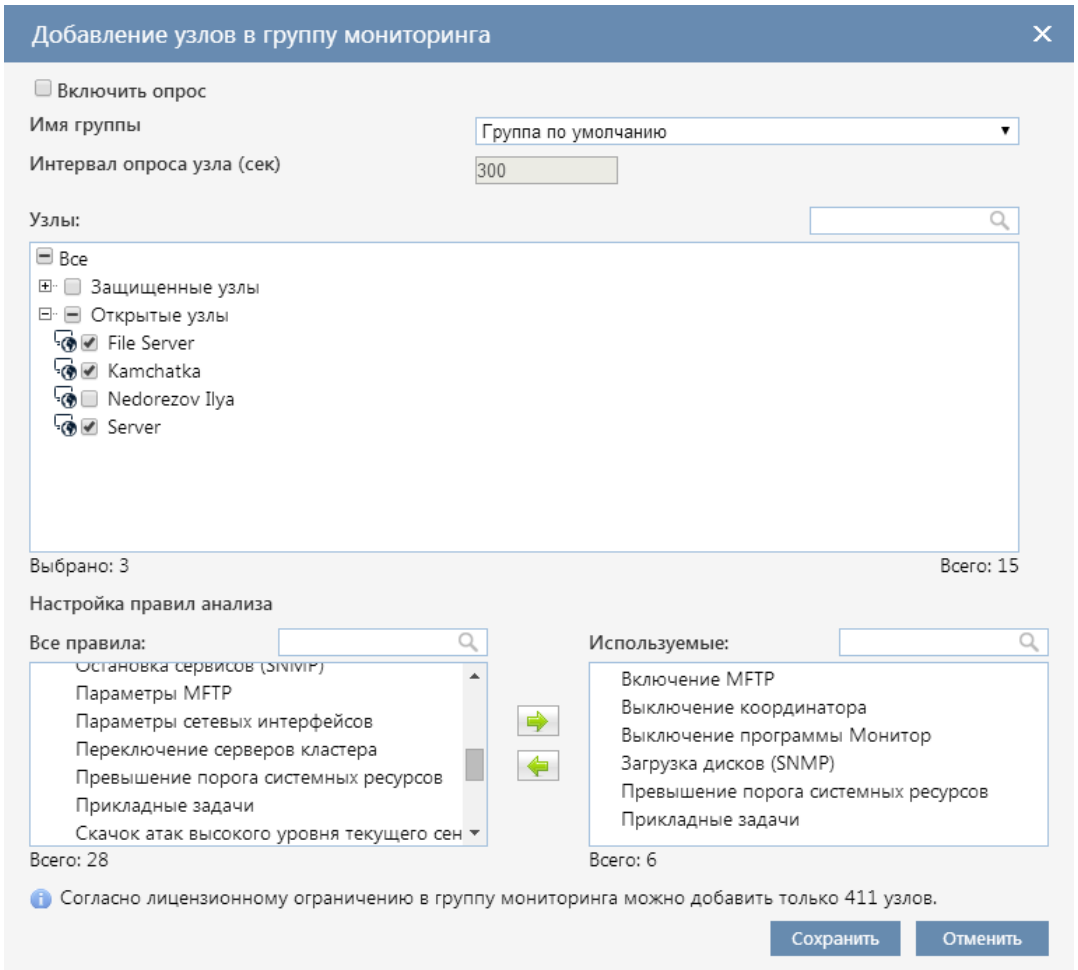

Рисунок 38: Перемещение новых узлов в группу мониторинга

3 Для переноса новых узлов выполните следующее:

3.1 В списке **Имя группы** выберите группу, в которую следует перенести новые узлы.

3.2 В списке **Узлы** отметьте флажками узлы, которые необходимо перенести.

Узлы, содержащиеся в списке **Узлы**, можно отфильтровать по имени узла. Для этого введите имя или часть имени в поле, расположенное над списком. Чтобы выбрать все новые узлы, установите флажок **все**.

3.3 Для выбранной группы можно установить следующие параметры мониторинга:

- **Включить опрос** — флажок для включения или отключения мониторинга узлов группы.

- **Интервал опроса узла (сек)** — периодичность опроса узлов группы Сервером мониторинга (в секундах). Минимальное возможное значение 30 (секунд). Данное поле недоступно для редактирования, если не установлен флажок **Включить опрос**.
- **Все правила** — список всех правил анализа и наборов правил анализа из шаблонов оповещений.
- **Используемые** — список всех правил анализа и наборов правил анализа из шаблонов оповещений, которые будут применены на выбранных узлах мониторинга. С помощью кнопок и перенесите в список **Используемые** правила анализа для данного пользователя. В списке **Используемые** отметьте способы оповещения для каждого правила.

4 Установите требуемые значения параметров мониторинга группы и нажмите кнопку **Сохранить**. Чтобы отказаться от перемещения новых узлов в группу мониторинга, нажмите кнопку **Отменить**.

Примечание. Перемещение большого количества новых узлов мониторинга может занять некоторое время, при этом появится значок и сообщение о перемещении узлов в выбранную группу. В этом случае необходимо дождаться завершения процесса перемещения узлов.

При переносе новых узлов в группу мониторинга проверяется соблюдение лицензионного ограничения на максимальное количество узлов мониторинга для данного Сервера мониторинга. Если суммарное количество узлов по всем группам мониторинга и выбранных для переноса узлов больше, чем задано в лицензии, то появляется соответствующее сообщение и перемещение новых узлов в группу не выполняется. В сообщении будет указано количество узлов, допустимое для переноса без нарушения лицензии.

Изменение параметров мониторинга узла

Чтобы изменить параметры мониторинга отдельного узла:

1 В главном окне на вкладке **Администрирование** перейдите на страницу **Узлы**.

2 На открывшейся странице в списке **Узлы мониторинга** щелкните название нужного узла. Появится окно с текущими параметрами мониторинга выбранного узла.

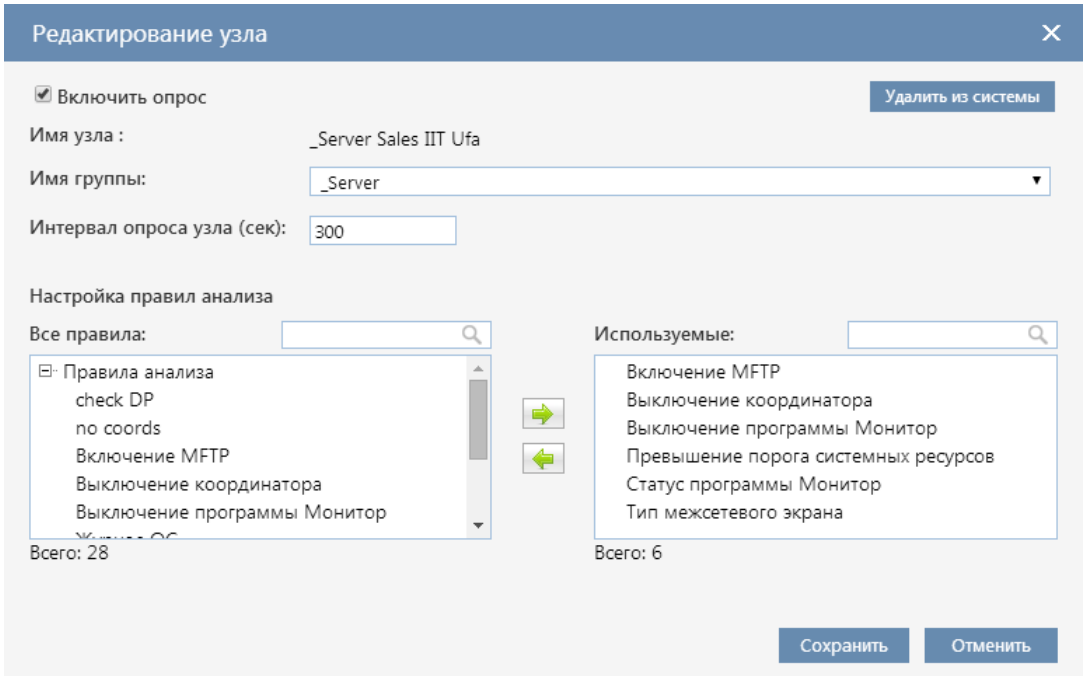

Рисунок 39: Изменение параметров мониторинга узла

3 Задайте параметры мониторинга узла:

- **Включить опрос** – флажок для включения или отключения мониторинга узла. Установите флажок, если Сервер мониторинга должен опрашивать узел, иначе снимите флажок.
- **Имя группы** — имя группы мониторинга, в которую входит узел. Чтобы переместить узел в другую группу, раскройте список с именами групп и выберите нужную группу.
- **Интервал опроса узла (сек)** — периодичность опроса узла Сервером мониторинга (в секундах). Минимальное возможное значение 30 (секунд). Данное поле недоступно для редактирования, если не установлен флажок **Включить опрос**.
- **Все правила** — список всех правил анализа и наборов правил анализа из шаблонов оповещений.
- **Используемые** — список всех правил анализа и наборов правил анализа из шаблонов оповещений, которые будут применены на выбранных узлах мониторинга. С помощью кнопок и перенесите в список **Используемые** правила анализа для данного пользователя. В списке **Используемые** отметьте способы оповещения для каждого правила.
- **Протокол** — сетевой протокол, по которому происходит взаимодействие с открытым узлом.

- **Порт** — порт, с использованием которого происходит подключение к открытому узлу.

Примечание. Параметры **Протокол** и **Порт** указываются только для открытых узлов. Для защищенных узлов данные параметры в окне **Редактирование узла** отсутствуют.

Для открытых узлов имя узла может быть изменено при редактировании узла. Для защищенных узлов имя узла неизменно и задается в программе ViPNet Центр управления сетью.

---

4 Установите требуемые значения параметров мониторинга узла и нажмите кнопку **Сохранить**. Чтобы отказаться от сделанных изменений, нажмите кнопку **Отменить**.

Удаление узла или группы мониторинга

Чтобы удалить узел или группу мониторинга:

1 В главном окне на вкладке **Администрирование** перейдите на страницу **Узлы**.

2 Щелкните название элемента (узла или группы):

- Для удаления узла из группы в окне **Редактирование узла** нажмите кнопку **Удалить из группы**. После удаления узла из группы он будет перемещен в группу **Узлы для добавления в мониторинг**.
- Для удаления группы в окне **Редактирование группы** нажмите кнопку **Удалить группу**. После удаления группы все узлы, входящие в нее будут перемещены в группу **Узлы для добавления в мониторинг**.

3 Для удаления выбранных элементов нажмите кнопку **Сохранить**, для отмены удаления – кнопку **Отменить**.

Примечание. При удалении узла на Сервере мониторинга сохраняются все собранные по этому узлу данные и его история событий.

Удаление открытого узла из списка связей Сервера мониторинга

Вы можете удалить из списка связей Сервера мониторинга открытый узел, который еще не был добавлен в какую-либо из групп мониторинга (например, если какой-то узел был добавлен в список связей ошибочно).

Чтобы удалить открытый узел из списка связей Сервера мониторинга, выполните следующие действия:

1. В главном окне программы перейдите на страницу **Администрирование** > **Узлы**.
2. В разделе **Открытые узлы** выполните одно из действий:
   - В списке узлов щелкните кнопку рядом с открытым узлом, который хотите удалить.
   - На панели инструментов нажмите кнопку **Удалить**. В появившемся окне **Удаление открытых узлов** установите флажки рядом с открытым узлом или несколькими узлами, которые хотите удалить, и нажмите кнопку **Удалить**.

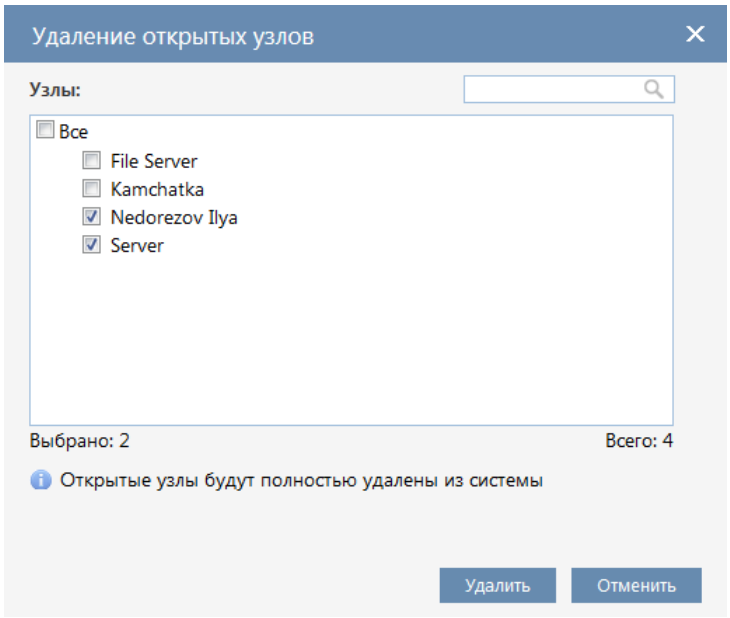

Рисунок 40: Удаление открытых узлов

В результате выбранный открытый узел (или несколько узлов) будет удален из списка связей Сервера мониторинга.

Настройка типов узлов мониторинга

Определение типов узлов мониторинга производится Сервером мониторинга автоматически при добавлении узлов в мониторинг. Типы узлов определяются:

- Для защищенных узлов — на основе списка ролей (см. «Роль» на стр. 291), назначенных узлам.
- Для открытых узлов — на основе параметров, получаемых по протоколу SNMP.

Определение типов узлов мониторинга позволяет администраторам организовать более дифференцированный подход к выявлению событий на узлах, так как правила анализа могут быть привязаны к конкретным типам узлов. Также отображение типов узлов в АРМ мониторинга помогает визуально быстрее определить, на каком узле требуется устранение неполадок, и какие действия при этом вероятнее всего потребуется выполнить.

В системе мониторинга поддерживаются следующие типы узлов:

- Защищенные узлы:
  - «Клиент».
  - «Координатор».
  - «HW 10».
  - «HW 100».
  - «HW 1000».
  - «HW 2000».
  - «Координатор HW».
  - «Терминал».
  - «Мобильный узел».
  - «Экспресс-3».
  - «Инфотабло».
- Открытые узлы:
  - «Открытый узел».
  - «ИБП».

- «Принтер».
- «Маршрутизатор».
- «IDS».

- «Неизвестный узел» (узел, для которого тип не определен).

При необходимости вы можете изменить тип узла, который был определен Сервером мониторинга автоматически. Например, если вы хотите заменить тип узла, определенный автоматически, на тип, более востребованный при мониторинге в текущей сети ViPNet. Изменять типы узлов могут только администраторы Сервера мониторинга.

Для изменения типа узла мониторинга выполните следующие действия:

1. В главном окне АРМ мониторинга в списке узлов щелкните узел, тип которого вы хотите изменить.
2. В окне **Информация об узле** нажмите кнопку в левом верхнем углу.
3. В появившемся меню щелкните строку с нужным типом узла.

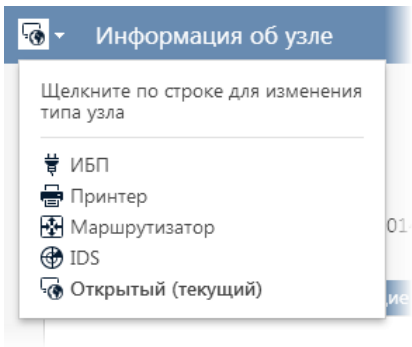

Рисунок 41: Выбор типа узла мониторинга

4. Нажмите кнопку **Закрыть**.

В результате тип узла будет изменен.

Настройка правил анализа

Программа Сервер мониторинга анализирует собранную информацию, чтобы определить текущее состояние узлов мониторинга и выявить возможные неполадки в их работе. Анализ производится на основе правил, заданных в программе. В системе мониторинга предусмотрен ряд встроенных (предустановленных) правил анализа (см. «Встроенные правила анализа» на стр. 260), которые невозможно удалить или изменить, а можно только копировать (например, чтобы создать аналогичное правило с другим уровнем критичности или отличающимся набором параметров) и изменять привязку правила к определенным узлам мониторинга. Также администратор может создавать и настраивать собственные правила анализа.

Настройка правил анализа выполняется под учетной записью администратора. Администратор может выполнять следующие операции, связанные с правилами анализа:

- создавать правила анализа;
- изменять правила анализа;
- копировать правила анализа (см. «Копирование правила анализа» на стр. 104);
- удалять правила анализа (см. «Удаление правила анализа» на стр. 104);
- настраивать оповещения (см. «Настройка оповещений» на стр. 106).

Правила анализа распределены по группам, названия и предназначение которых строго определены. Чтобы просмотреть правила в группе, на вкладке **Администрирование** перейдите на страницу **Правила анализа** и разверните список, щелкнув значок ⊞, расположенный слева от названия группы.

В программе Сервер мониторинга поддерживаются следующие группы правил анализа:

- **Встроенные правила** — группа предустановленных правил (см. «Встроенные правила анализа» на стр. 260). Состав встроенных правил зависит от установленного пакета настроек (см. «Пакет настроек» на стр. 290).
- **Родительские правила —** правила, созданные на родительских серверах и применяемые на всех дочерних Серверах мониторинга в каскаде.

  Применение правил на дочерних серверах в каскаде можно настроить при создании или изменении правила на родительском Сервере мониторинга.

- **Пользовательские правила** — группа правил анализа, созданных администратором.
- **Удаленные правила** — группа правил, удаленных администратором.

  Также в эту группу помещаются:

  - Предыдущие варианты измененных правил. При изменении каких-либо параметров правила создается новый вариант правила, который сохраняется как текущий. При этом вариант правила до изменения сохраняется в группе **Удаленные правила**.
  - Правила, удаленные в результате обновления пакета настроек.
  - Родительские правила анализа данного Сервера мониторинга, в случае, если:
    - администратор родительского сервера отменил применения пользовательских правил анализа на его дочерних Серверах мониторинга (в том числе, на данном Сервере мониторинга);
    - разорвана связь с родительским Сервером мониторинга в каскаде.

Создание и изменение правила анализа

Внимание! Изменять параметры встроенных правил анализа невозможно. Возможно изменить только список узлов, на которых будет применяться встроенное правило.

Удаление всех узлов из списка применения правила равноценно отключению правила.

Чтобы создать или изменить правило анализа:

1. На странице **Администрирование** > **Правила анализа** выполните одно из действий:
   - Нажмите кнопку **Создать новое правило** и выберите тип правила, которое хотите создать:
     - **Простое** для создания простого правила с помощью конструктора (см. «Конструктор правил анализа» на стр. 289).
     - **Сложное** для создания сложного правила с помощью редактора.

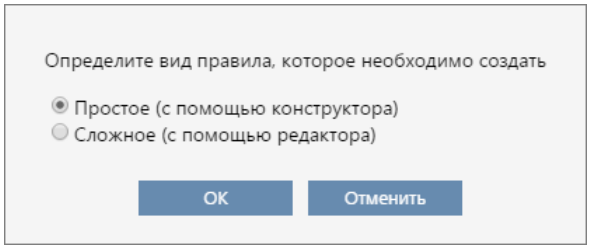

Рисунок 42: Выбор типа создаваемого правила

- На панели навигации выберите правило из группы.

  Для этого разверните группу, щеклнув значок ⊞ рядом с ее названием, и выберите нужное правило. На панели просмотра отобразятся параметры правила.

2 На панели просмотра в поле **Имя правила** задайте или измените название правила анализа.

Внимание! Названия правил анализа должны быть уникальными, но могут совпадать с именами удаленных правил, содержащихся в группе **Удаленные правила**.

---

3 Задайте или измените параметры правила с помощью конструктора или редактора в зависимости от типа правила:

- При работе в редакторе правила введите код алгоритма анализа, написанный на специальном скриптовом языке (см. «Синтаксис правил анализа» на стр. 157).
- При работе с конструктором правил укажите условия правила (см. «Задание и изменение параметров правила с помощью конструктора» на стр. 101).

4 На панели **Настройка оповещений** в списке **Узлы** выберите наблюдаемые напрямую узлы или группы узлов, к которым будет применяться данное правило. Узлы можно отфильтровать по имени. Для этого введите имя или часть имени в поле поиска, расположенное над списком узлов.

Примечание. Изменять список узлов, на которых применяются родительские правила анализа, невозможно.

Родительские правила анализа, примененные на дочерних серверах, всегда применяются на всех узлах дочернего Сервера мониторинга.

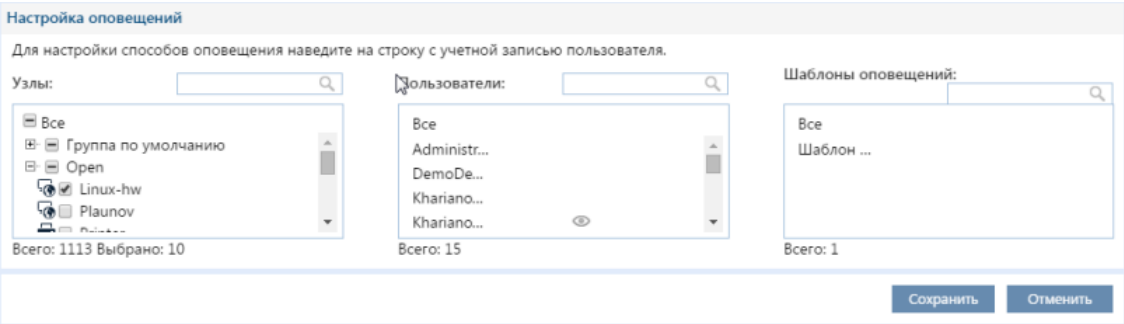

Рисунок 43: Выбор узлов, на которых будет действовать правило анализа, и настройка оповещений

5 На панели **Настройка оповещений** в списке **Пользователи** выберите пользователей, которые будут получать оповещения о событиях, связанных со срабатыванием данного правила. Для этого отметьте способы оповещения для каждого пользователя. Если вы хотите назначить какой-либо способ оповещения для всех пользователей из списка, отметьте нужный способ в строке **Все**.

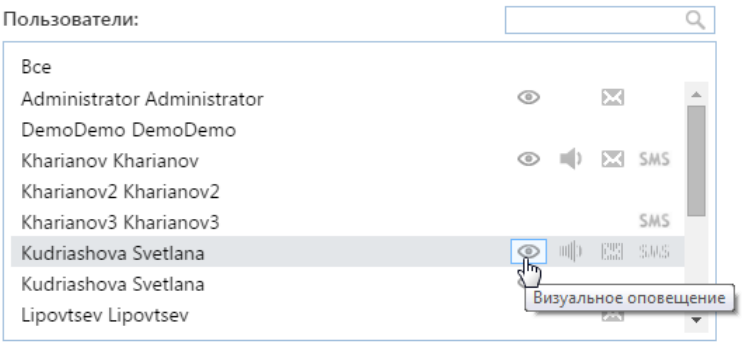

Рисунок 44: Настройка оповещений

6 Чтобы настроить оповещения для правила с помощью шаблонов, в списке **Шаблоны оповещений** отметьте нужные способы оповещения для некоторых шаблонов или в строке **Все**. После сохранения изменений в правиле данное правило и выбранные таким образом способы оповещений будут добавлены в шаблоны.

7 На панели навигации рядом с именем редактируемого правила нажмите кнопку , если хотите, чтобы правило применялось на дочерних Серверах мониторинга.

В результате правило будет передано на все дочерние Серверы мониторинга. На дочерних Серверах мониторинга будет создана точная копия данного правила:

- При применении пользовательского правила на дочерних Серверах мониторинга точная копия правила попадет в группу **Родительские правила**.
- При применении встроенного правила на дочерних Серверах мониторинга точная копия правила попадет в группу **Встроенные правила**.

Примечание. Если какой-либо дочерний Сервер мониторинга недоступен, правило анализа, переданное родительским Сервером мониторинга вниз по каскаду, будет применено только после того как он станет доступным. Доступность серверов вы можете посмотреть на странице **Администрирование** > **Каскад**.

8 Нажмите кнопку **Сохранить**. При сохранении правила будет автоматически произведена проверка синтаксиса созданного правила (см. «Проверка синтаксиса правила анализа» на стр. 168). Если вы не хотите сохранять правило, нажмите кнопку **Отменить**.

Примечание. Применение правила анализа для большого количества узлов мониторинга может занять некоторое время, при этом появится значок и сообщение о сохранении правила анализа. В этом случае необходимо дождаться завершения процесса сохранения правила анализа.

Созданное или измененное правило будет отображаться в группе **Пользовательские правила**.

Задание и изменение параметров правила с помощью конструктора

Чтобы задать или изменить параметры правила с помощью конструктора:

1 На панели просмотра выберите вкладку **Конструктор правила** и в группе **Условие** задайте условия срабатывания правила анализа. Для этого:

1.1 В списке **Параметры** выберите параметр узла, для которого хотите задать условие (например, идентификатор или виртуальный IP-адрес узла).

При необходимости вы можете найти параметры в списке по названию. Для этого щелкните значок рядом со списком **Параметры** и введите название или часть названия параметра. При этом искомый параметр будет выделен в списке, для выбора параметра нажмите клавишу **Enter**.

Примечание. При создании простого правила анализа с помощью конструктора можно использовать только одну коллекцию параметров.

Если был выбран параметр из одной коллекции (например, параметр **Состояние**

интерфейса из коллекции **Сетевые интерфейсы**), то параметры других коллекций (например, коллекции **Диски**) будут недоступны.

1.2 В списке **Тип значения** выберите тип значения параметра узла, для которого будет применяться условие (**Текущее** или **Предыдущее**).

1.3 В списке **Оператор** выберите оператор. При создании правила анализа с помощью конструктора вы можете использовать следующие операторы:

- равно ==;
- не равно **!**=;
- вхождение **входит в**;
- больше >;
- меньше <;
- больше либо равно >=;
- меньше либо равно <=.

Также данные операторы можно использовать для сравнения текущего значения параметра с предыдущим. Для этого в списке **Оператор** выберите нужный оператор с признаком **Текущее** или **Предыдущее** (в зависимости от того, какой тип значения параметра выбран в списке **Тип значения**). При этом в поле **Значение** отобразится значение **Текущее** или **Предыдущее** соответственно.

1.4 В поле **Значение** введите или выберите значение параметра, при котором будет срабатывать условие.

1.5 Чтобы добавить условие, нажмите кнопку ✚. Чтобы удалить условие, нажмите кнопку ✖ напротив нужного условия.

1.6 В списке между двумя условиями выберите логический оператор, которым они будут объединены (**И**, **ИЛИ**).

1.7 Чтобы сгруппировать несколько условий, установите флажки рядом с нужными условиями, нажмите кнопку и при необходимости в списке между условиями измените логический оператор, которым они будут объединены. Чтобы разгруппировать условия нажмите кнопку рядом с ними.

Группирование позволяет установить порядок проверки заданных условий. Несгруппированные условия проверяются в порядке следования в группе **Условие**. При этом объединить все условия можно только одинаковыми логическими операторами.

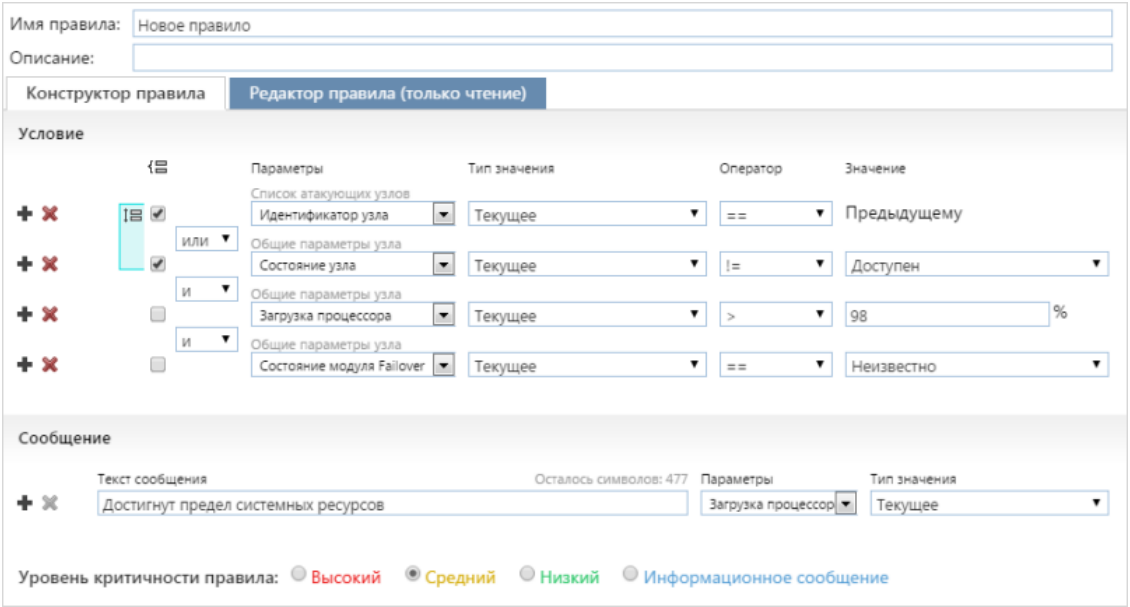

Рисунок 45: Создание правила с помощью конструктора

2 В группе **Сообщение при срабатывании правила** добавьте сообщение, которое будет появляться при срабатывании правила. Для этого:

2.1 В поле **Текст сообщения** введите текст сообщения. Сообщение должно быть кратким и содержательным. Текст сообщения не должен превышать 512 символов.

2.2 В списке **Параметры** выберите параметр узла, который будет добавлен к тексту сообщения.

2.3 В списке **Тип значения** выберите тип значения параметра узла (**Текущее** или **Предыдущее**).

2.4 Чтобы добавить сообщение, нажмите кнопку ✚. Чтобы удалить сообщение, нажмите кнопку ✖ напротив нужного сообщения.

Если будет добавлено несколько сообщений, их текст будет отображаться во всплывающем окне **Информация о событии** в строке **Сообщение** и в окне **Информация о событиях на узлах** в соответствующей ячейке столбца **Сообщение**. Если же не будет добавлено ни одно сообщение, то создаваемое правило невозможно будет сохранить.

3 В разделе **Уровень критичности правила** установите переключатель в положение, соответствующее желаемому уровню критичности события, которое определится при срабатывании правила.

4 В процессе задания условий вы также можете просмотреть код правила. Для этого на панели просмотра выберите вкладку **Редактор правила**. При этом код правила будет доступен только для чтения.

Копирование правила анализа

Чтобы скопировать правило анализа:

1. В главном окне на вкладке **Администрирование** перейдите на страницу **Правила анализа**.
2. На панели навигации в группе правил выберите правило, которое вы хотите скопировать.

   Чтобы выбрать правило из группы, разверните список, щелкнув ⊞, расположенный слева от названия группы.
3. Нажмите кнопку **Создать копию**.
4. Если выбранное правило анализа является простым, в появившемся окне (см. Рисунок 43 на стр. 99) выберите тип правила для создаваемой копии:
   - **Простое** для создания простого правила с помощью конструктора (см. «Задание и изменение параметров правила с помощью конструктора» на стр. 101).
   - **Сложное** для создания сложного правила с помощью редактора.

   После создания копии правила его можно изменить в соответствии с необходимыми требованиями.
5. Нажмите кнопку **Сохранить**.

В результате скопированное правило будет добавлено в группу **Пользовательские правила**. Копия правила отличается от самого правила только именем: к имени правила автоматически добавляется слово «копия», указанное в скобках.

Внимание! При копировании правила сохраняется код правила анализа и настройки применения правила на узлах и дочерних Серверах мониторинга.

Удаление правила анализа

Внимание! Удалить встроенные правила невозможно. Также на дочернем Сервере мониторинга невозможно удалить родительские правила анализа.

Чтобы удалить правило анализа:

1. В главном окне на вкладке **Администрирование** перейдите на страницу **Правила анализа**.
2. На панели навигации в группе правил выберите правило, которое вы хотите удалить.

   Чтобы выбрать правило из группы, разверните список, щелкнув значок ⊞, расположенный слева от названия группы.
3. На панели навигации нажмите кнопку **Удалить**, расположенную над списком с группами.
4. В окне подтверждения нажмите кнопку **OK**.

В результате удаленное правило переместится в группу **Удаленные правила** и прекратит действовать. При необходимости вы можете скопировать удаленное правило (см. «Копирование правила анализа» на стр. 104).

Примечание. При удалении пользовательского правила, созданного на родительском сервере и примененного на дочерних серверах, правило переместится в группу **Удаленные правила**. На дочерних серверах правило удалится из группы **Родительские правила**. Также в журнале появится запись об удалении этого правила.

Настройка оповещений

Функция настройки оповещений позволяет задавать параметры всех видов оповещений для каждого уровня критичности. Заданные параметры действуют для всех правил анализа. Сами оповещения и условия их формирования задаются индивидуально в каждом правиле при его создании или изменении.

После включения оповещений и срабатывания соответствующих правил анализа на АРМ мониторинга будут поступать сообщения о событиях мониторинга. О работе с полученными оповещениями см. документ «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. АРМ мониторинга. Руководство пользователя».

О способах оповещения см. раздел Способы оповещения (на стр. 107).

Вы можете включить или выключить оповещение для того или иного события (правила анализа) при выполнении следующих действий:

1. При настройке Сервера мониторинга в мастере при первом запуске системы (см. «Настройка Сервера мониторинга с помощью мастера» на стр. 71).
2. При создании или изменении шаблонов оповещений (см. «Создание и изменение шаблонов оповещений» на стр. 109).
3. При создании или изменении учетной записи пользователя (см. «Создание и изменение учетной записи» на стр. 78).
4. При добавлении узлов в группу мониторинга (см. «Перемещение новых узлов в группу мониторинга» на стр. 89).
5. При редактировании параметров мониторинга узла (см. «Изменение параметров мониторинга узла» на стр. 91).
6. При добавлении или редактировании правила анализа (см. «Настройка правил анализа» на стр. 97).

Настроить цвет, звуковой сигнал, шаблоны писем и другие параметры оповещений можно на странице **Администрирование** > **Настройки**.

Способы оповещения

Поддерживаемые виды оповещений:

- Визуальные оповещения (см. «Настройка визуальных оповещений» на стр. 111). Эта группа оповещений включает в себя:
  - Оповещения в списке узлов.

    Предназначены для оповещения о количестве событий, обнаруженных на узле, а также об уровне критичности событий. Цвет значка события зависит от цвета, заданного в настройках Сервера мониторинга (например, 1).
  - Всплывающие сообщения на странице **Список.**

    Отображаются в правом нижнем углу страницы при возникновении событий на узлах мониторинга.
  - Оповещения в окне **Информация о событиях** на узлах.

    Выводятся в отдельном окне по мере их обнаружения на узлах.
  - Оповещения на карте.

    Этот вид оповещений предназначен для выделения узлов на карте. Оповещения на карте отображаются в виде мерцающих значков узлов, цвет мерцания соответствует уровню критичности события. Для оповещений на карте используются те же цвета, что и для оповещений в списке узлов.

  Подробнее о визуальных оповещениях см. в документе «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. АРМ мониторинга. Руководство пользователя».

- Звуковые оповещения (см. «Настройка звуковых оповещений» на стр. 111).

  Звуковые оповещения проигрываются на АРМ мониторинга. Для каждого уровня критичности в настройках должен быть задан свой звуковой файл (в формате MP3).

- Оповещения по электронной почте (см. «Настройка оповещений по электронной почте» на стр. 112).

  Оповещения по электронной почте — это почтовые сообщения (письма), которые отправляются пользователям. В теме письма указывается правило анализа, сгенерировавшее оповещение, и узел, на котором сработало правило анализа. Текст письма формируется по шаблону, заданному в настройках или в пакете настроек (см. «Пакет настроек» на стр. 290). Для разных уровней критичности может быть задан один и тот же шаблон.

  Для отправки оповещений используется почтовый сервер (SMTP-сервер). Электронный адрес получателя оповещений задается администратором в настройках учетных записей пользователей.

- Оповещения по Деловой почте (см. «Настройка оповещений по Деловой почте» на стр. 114).

Внимание! Оповещения по Деловой почте предназначены только для встроенной учетной записи Administrator.

Оповещения по Деловой почте представляют собой текстовые файлы, которые могут отправляться пользователям в составе писем с помощью программы ViPNet Деловая почта. Оповещения помещаются либо в текст письма, либо прикрепляются как вложения к письму, это зависит от настроек автопроцессинга программы Деловая почта. Файл содержит текст сообщения, заданного в правиле анализа. Имя файла формируется по шаблону `<имя узла>_<идентификатор узла>_<название правила>_<время срабатывания>.txt`. Если файл с таким именем уже существует, то имя файла формируется по шаблону `<имя узла>_<идентификатор узла>_<название правила>_<время срабатывания>_номер.txt`, где `номер` – очередной номер среди существующих файлов с таким же именем (начиная с 1). Сформированные для отправки файлы помещаются в папку, заданную в настройках Сервера мониторинга, откуда они рассылаются на АРМ мониторинга средствами автоматической обработки писем (автопроцессингом). При поступлении писем на АРМ мониторинга программа Деловая почта оповещает об этом пользователей.

Примечание. При формировании Сервером мониторинга большого количества оповещений возможны перебои в доставке и частичная потеря этих оповещений по Деловой и электронной почте. Это связано с ограниченной производительностью автопроцессинга Деловой почты и некоторых SMTP-серверов. В этом случае рекомендуется ограничить число формируемых оповещений указанных видов, отключив их для некоторых уровней критичности, или использовать SMTP-сервер с более высокой производительностью.

- Оповещения по SMS (см. «Настройка оповещений по SMS» на стр. 115).

  SMS-оповещения представляют собой одно или несколько SMS-сообщений, отправляемых на номера телефонов пользователей. SMS-оповещения формируются на основе сообщения правила анализа.

  В ПО Сервер мониторинга для отправки оповещений по SMS используется SMS-шлюз. Сервер мониторинга взаимодействует с SMS-шлюзом по протоколу SMPP. SMS-шлюз представляет собой сервер, который преобразует сообщения, полученные от Сервера мониторинга, в SMS-сообщения и отправляет их получателям на указанные номера телефонов.

Длина SMS-сообщения составляет 70 символов. Если текст оповещения превышает данное количество символов, то оно разбивается на несколько SMS-сообщений длиной не более 70 символов. Каждое SMS-оповещение состоит из нескольких полей, в которых отображена следующая информация:

- имя Сервера мониторинга (максимум 40 символов);
- имя правила анализа (максимум 40 символов);
- уровень критичности события мониторинга (максимум 10 символов);
- имя узла, на котором сработало правило (максимум 40 символов);
- время срабатывания правила анализа;
- текст сообщения правила анализа (максимум 70 символов).

Каждое поле SMS-оповещения имеет ограничение по длине. Если длина текста какого-либо поля превышает ограничение, то текст может отображаться не полностью в SMS-сообщении.

Для оповещений по SMS существует ограничение количества SMS-сообщений, отправленных за минуту и за сутки. Данные ограничения задаются при тонкой настройке Сервера мониторинга в файле `server.ini`.

- Оповещения по протоколу Syslog (см. «Настройка оповещений по протоколу Syslog» на стр. 116).

Внимание! Оповещения по протоколу Syslog предназначены только для встроенной учетной записи Administrator.

Оповещения по протоколу Syslog представляют собой сообщения о происходящих в системе мониторинга событиях, которые формируются на сервере мониторинга и затем передаются на обработку серверу Syslog по протоколу UDP/TCP. На сервере Syslog описание события мониторинга сохраняется в базу данных с указанием времени события, IP-адреса и идентификатора узла, на котором было зафиксировано событие, полного номера версии ПО ViPNet StateWatcher, информации о правиле анализа, уровня критичности события и некоторой другой информации.

Создание и изменение шаблонов оповещений

Шаблон оповещения содержит в себе список правил анализа и способы оповещения, назначенные каждому из правил. Использование шаблона упрощает процедуру назначения оповещений по умолчанию при настройке учетных записей пользователей, групп мониторинга и правил анализа.

Чтобы создать или изменить шаблон оповещений:

1 На странице **Администрирование** > **Шаблоны** выполните одно из действий:

- Для создания шаблона нажмите кнопку **Создать шаблон**.
- Для редактирования шаблона щелкните мышью по имени шаблона.

2 В открывшемся окне в поле **Название шаблона** укажите имя нового шаблона.

3 С помощью кнопок и перенесите правила анализа и шаблоны оповещений из списка **Правила анализа** в список **Используемые**.

4 В списке **Используемые** отметьте способы оповещения для каждого правила анализа.

Если вы хотите назначить какой-либо способ оповещения для всех выбранных правил, отметьте нужный способ в строке **Все**.

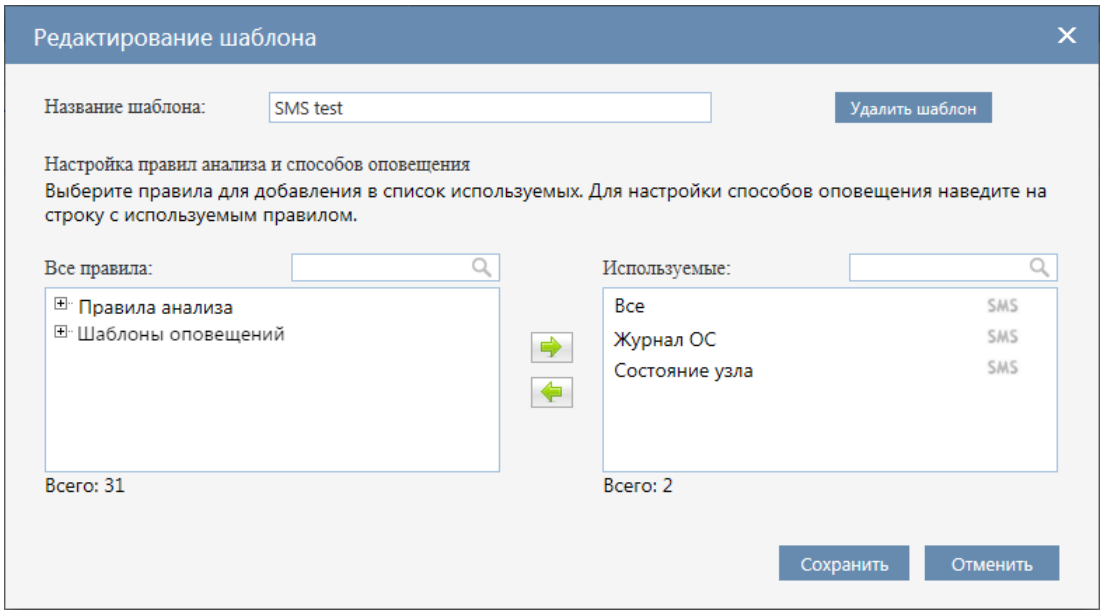

Рисунок 46: Редактирование шаблона оповещения

5 Нажмите кнопку **Сохранить**.

В окне **Редактирование шаблона** вы также можете удалить шаблон. Для этого нажмите кнопку **Удалить шаблон** и подтвердите удаление.

Настройка визуальных оповещений

Чтобы настроить визуальные оповещения, выполните следующие действия:

1. Включите или выключите оповещения для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).
2. При необходимости измените цвет сообщения в списке узлов, на карте и во всплывающих сообщениях (для указанных видов оповещений используется один цвет). Для этого:
   - **2.1** В главном окне на вкладке **Администрирование** > **Настройки** перейдите в раздел **Способы оповещения** > **Визуальный**.
   - **2.2** Нажмите кнопку **Изменить**, расположенную рядом с уровнем критичности события, для которого вы хотите изменить цвет сообщения.
   - **2.3** Выберите нужный цвет и нажмите кнопку **ОК**.
   - **2.4** Чтобы сохранить изменения для всех уровней критичности событий, нажмите кнопку **Сохранить**.

Настройка звуковых оповещений

Чтобы настроить звуковые оповещения, выполните следующие действия:

1. Включите или выключите оповещения для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).
2. При необходимости замените звуковой файл, используемый в качестве звукового оповещения. Для этого:
   - **2.1** В главном окне на вкладке **Администрирование** > **Настройки** перейдите в раздел **Способы оповещения** > **Звуковой**.
   - **2.2** Нажмите кнопку **Заменить**, расположенную рядом с уровнем критичности события, для которого вы хотите изменить звуковой сигнал.
   - **2.3** Выберите нужный звуковой файл и нажмите кнопку **Открыть**.
   - **2.4** Чтобы настроить продолжительность сигнала для всех уровней критичности, в поле **Установить длительность звука** выберите нужное значение.
   - **2.5** Чтобы сохранить изменения, нажмите кнопку **Сохранить**.

Вы можете включить или отключить звук оповещений, нажав кнопку на панели уведомлений.

Настройка оповещений по электронной почте

Чтобы настроить оповещения по электронной почте, выполните следующие действия:

1 Включите оповещение по электронной почте для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).

2 На странице **Администрирование** > **Настройки** > **SMTP** настройте подключение к SMTP-серверу.

Примечание. Первоначальная настройка подключения к SMTP-серверу производится при установке ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47). Далее при работе с данным программным обеспечением вы можете изменить настройки подключения к SMTP-серверу (например, если изменился IP-адрес вашего почтового сервера).

Для этого:

2.1 В группе **Обязательные настройки** задайте параметры подключения к SMTP-серверу:

- **Адрес сервера** — IP-адрес или DNS-имя почтового сервера, с помощью которого будут передаваться оповещения о событиях мониторинга.
- **Порт** — порт подключения к почтовому серверу.
- **Адрес электронной почты (e-mail) источника оповещений** — адрес электронной почты, с которого будут приходить оповещения о событиях мониторинга.

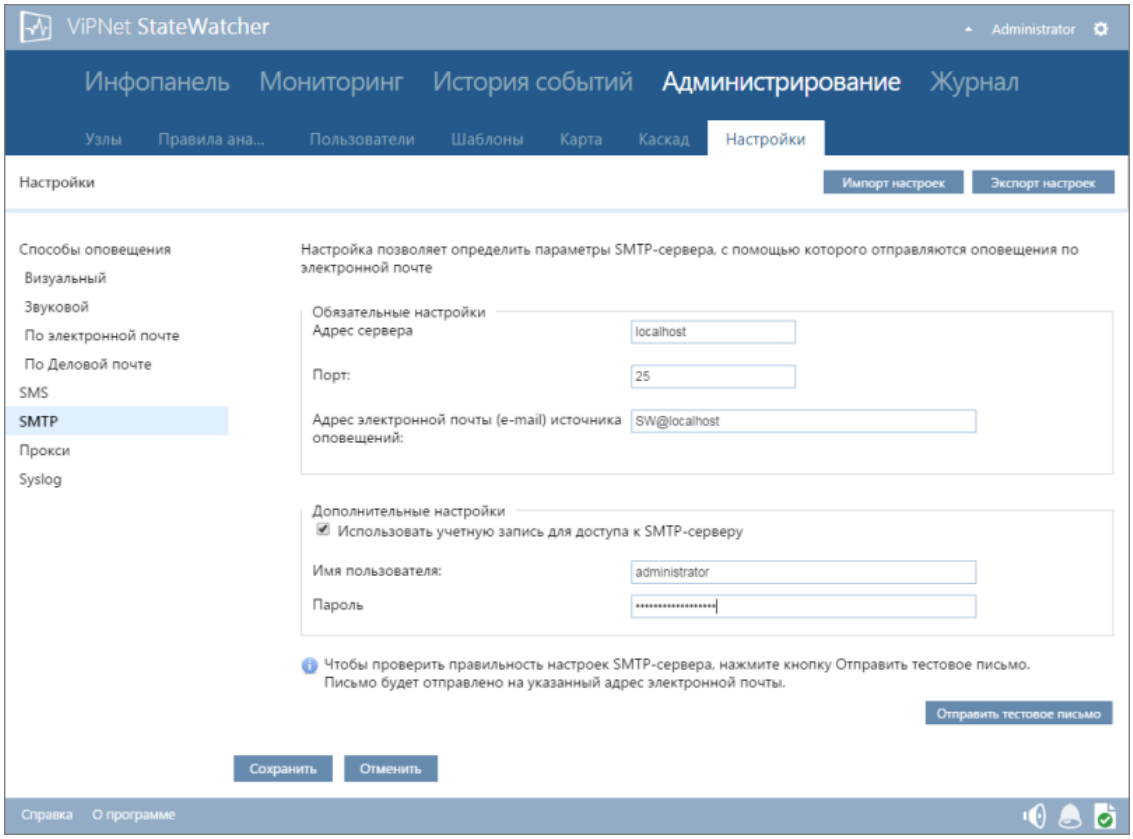

Рисунок 47: Настройка подключения к SMTP-серверу

2.2 Если при подключении к SMTP-серверу требуется аутентификация, в группе **Дополнительные настройки** установите флажок **Использовать учетную запись для доступа к SMTP-серверу** и задайте **Имя пользователя** и **Пароль** для подключения к почтовому серверу.

2.3 Для проверки подключения к SMTP-серверу отправьте тестовое письмо, для этого нажмите кнопку **Отправить тестовое письмо**. При этом тестовое письмо будет отправлено на адрес электронной почты, указанный в поле **Адрес электронной почты (e-mail) источника оповещений**.

2.4 По завершении настройки нажмите кнопку **Сохранить**.

3 Убедитесь, что в учетной записи пользователя указан адрес электронной почты, на который должно приходить оповещение. Для этого на странице **Администрирование** > **Пользователи** щелкните учетную запись пользователя в списке. При необходимости измените список адресов электронной почты и нажмите кнопку **Сохранить**.

4 На странице **Администрирование** > **Настройки** перейдите в раздел **Способы оповещения** > **По электронной почте** и для каждого уровня критичности событий выберите шаблон, который будет использоваться для формирования писем.

Примечание. По умолчанию для всех уровней критичности указан файл с примером шаблона (файл `default.jasper`), который поставляется в пакете настроек вместе с программой Сервер мониторинга. Можно изменить этот шаблон или создать другой шаблон (см. «Создание и изменение шаблонов писем оповещений» на стр. 199).

Чтобы выбрать файл с шаблоном, нажмите кнопку **Заменить**. Чтобы сохранить файл с шаблоном на компьютер, нажмите кнопку **Скачать**. Чтобы сохранить изменения, нажмите кнопку **Сохранить**.

Настройка оповещений по Деловой почте

Внимание! Для возможности отправки и получения оповещений с помощью программы Деловая почта необходимо настроить на Сервере мониторинга автопроцессинг. Подробное описание принципа работы автопроцессинга и его настройки содержится в документе «ViPNet Деловая почта. Руководство пользователя», который входит в комплект поставки ПО ViPNet Client.

Чтобы настроить оповещения по Деловой почте, выполните следующие действия:

1. Включите оповещение по Деловой почте для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).
2. В главном окне на странице **Администрирование** > **Настройки** перейдите в раздел **Способы оповещения** > **По Деловой почте**.
3. Для каждого уровня событий задайте шаблон темы письма, который должен использоваться для формирования темы писем при оповещении по Деловой почте.

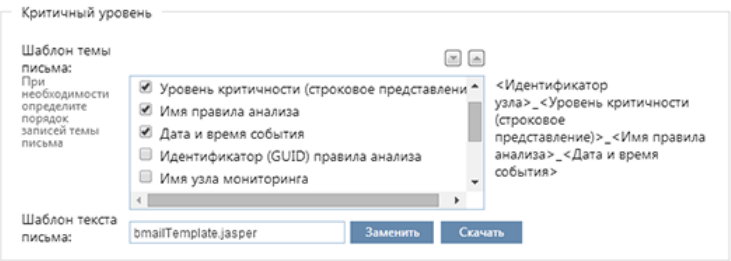

Рисунок 48: Задание шаблонов темы и текста письма

Для этого в списке **Шаблон темы письма** установите флажки напротив параметров, значения которых необходимо включить в тему письма. При необходимости измените порядок следования параметров с помощью кнопок ▼ ▲.

Внимание! Шаблон темы письма не должен быть пустым.

Длина названия итогового письма не должна превышать 160 символов, иначе программа ViPNet Деловая почта будет экстренно завершать свою работу при получении такого письма. Чтобы уменьшить длину названия письма, снимите флажки для некритичных параметров.

---

4 Для каждого уровня событий в поле **Шаблон текста письма** укажите файл с шаблоном текста письма. По умолчанию для всех уровней критичности указан файл с примером шаблона (файл `bmailTemplate.jasper`), который поставляется в пакете настроек вместе с программой Сервер мониторинга. Можно изменить этот шаблон или создать другой шаблон (см. «Создание и изменение шаблонов писем оповещений» на стр. 199). Для изменения этого параметра в группе **Другие** нажмите кнопку **Заменить** рядом с полем **Шаблон текста письма** и выберите нужный файл.

5 Нажмите кнопку **Сохранить**.

Настройка оповещений по SMS

Чтобы настроить оповещения по SMS, выполните следующие действия:

1 Включите оповещение по SMS для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).

2 Настройте подключение к SMS-шлюзу. Для этого:

2.1 В главном окне программы перейдите на страницу **Администрирование** > **Настройки** > **SMS**.

2.2 В группе **Настройка SMPP** укажите параметры подключения к SMS-шлюзу по протоколу SMPP:

- **Адрес сервера** — IP-адрес или DNS-имя SMS-шлюза.
- **Порт** — порт, используемый при подключении к SMS-шлюзу.
- **Пользователь** — имя учетной записи, которая используется при подключении к SMS-шлюзу.
- **Пароль** — пароль к учетной записи.

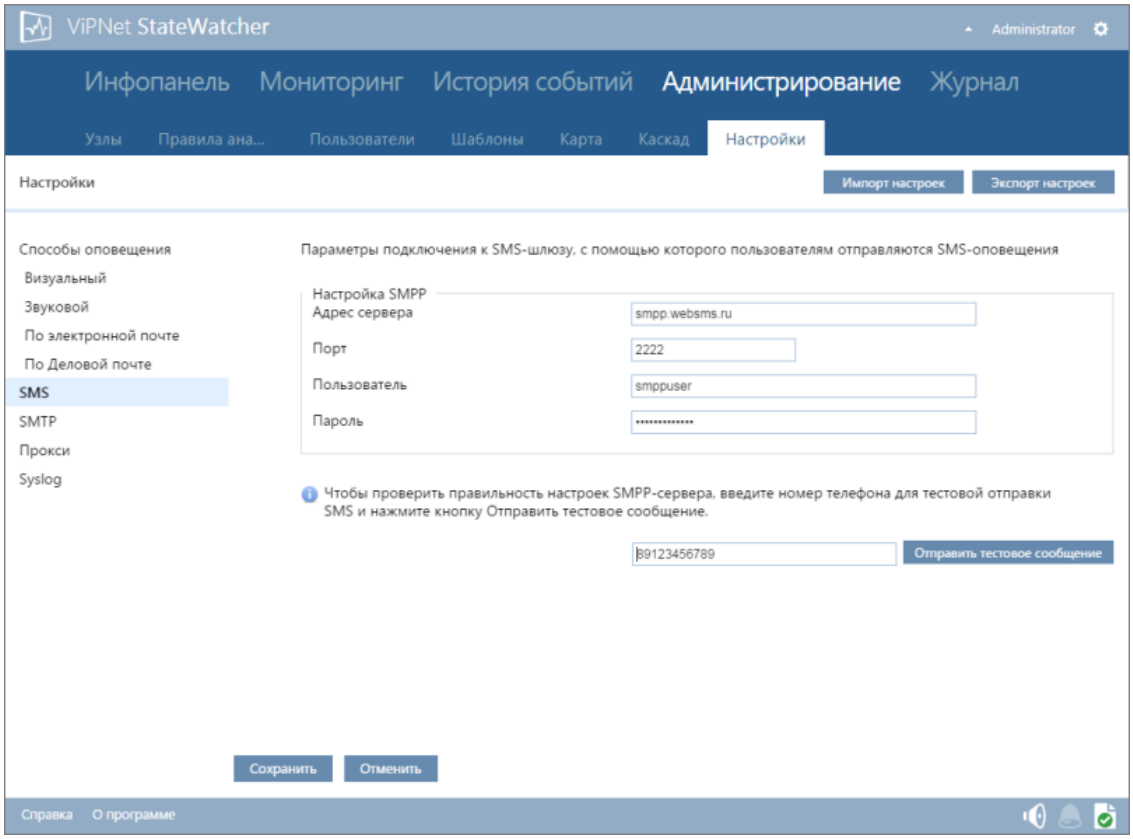

Рисунок 49: Настройка подключения к SMS-шлюзу

2.3 Для проверки подключения к SMS-шлюзу, отправьте тестовое SMS-сообщение. Для этого укажите номер телефона, на который будет отправлено тестовое сообщение, и нажмите кнопку **Отправить тестовое сообщение**.

2.4 По завершении настройки нажмите кнопку **Сохранить**.

3 Укажите ограничения на отправку SMS-оповещений в файле `server.ini` (см. «Секция [sms]» на стр. 143).

4 Убедитесь, что в учетных записях пользователей, которые будут получать оповещения по SMS, указаны номера телефонов. Подробнее см. раздел Создание и изменение учетной записи (на стр. 78).

Настройка оповещений по протоколу Syslog

Чтобы настроить оповещения по протоколу Syslog, выполните следующие действия:

1 Включите оповещение по Syslog для нужных правил анализа одним из возможных способов (см. «Настройка оповещений» на стр. 106).

2 В главном окне на вкладке **Администрирование** > **Настройки** перейдите в раздел **Syslog**.

3 В соответствующих полях задайте протокол (по умолчанию UDP), IP-адрес и порт подключения к серверу Syslog.

4 Нажмите кнопку **Сохранить**.

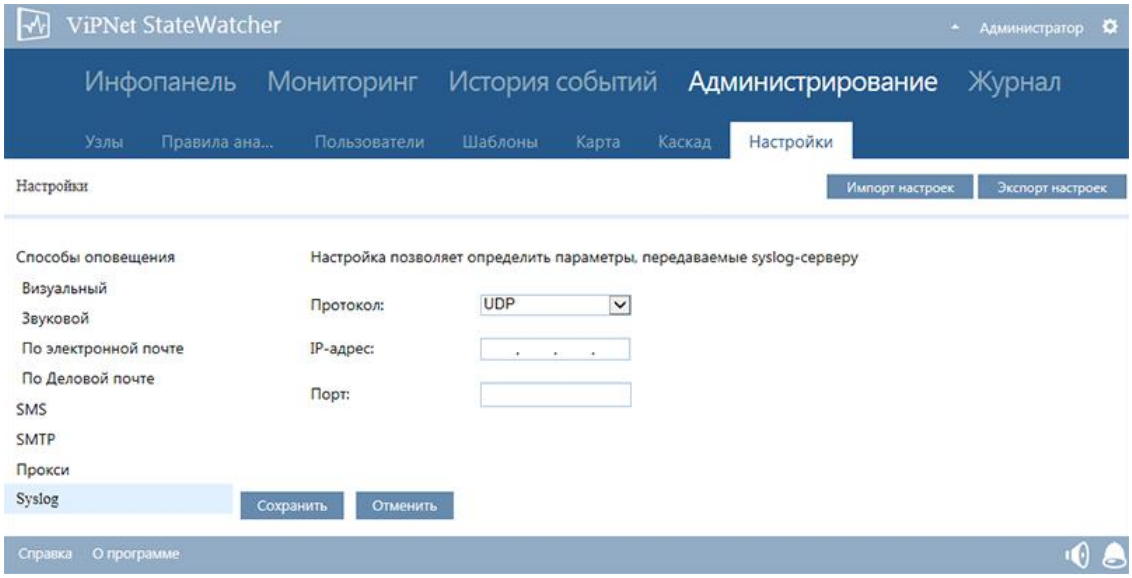

Рисунок 50: Настройка оповещений по протоколу Syslog

Отслеживание событий, связанных с фильтрацией трафика

В программном обеспечении ViPNet Client и ViPNet Coordinator для Windows версии 4.2.2 и выше реализована возможность передачи на Сервер мониторинга информации о следующих событиях:

- Изменение сетевых фильтров пользователем защищенного узла.
- Несанкционированное изменение настроек сетевых фильтров.
- Блокирование IP-пакетов.

Информация об этих событиях будет передаваться на Сервер мониторинга, если администратор сетевого узла выполнит соответствующие настройки.

Если вы хотите получать оповещения об указанных событиях, связанных с фильтрацией трафика на клиентах и координаторах, создайте соответствующее правило анализа (см. «Создание и изменение правила анализа» на стр. 98). Например, вы можете использовать следующий код:

```
foreach (event in Params.EVENTS) {
  if ((event.GFOSYSJ_SOURCE=="ViPNet Client" or event.GFOSYSJ_SOURCE=="ViPNet
  Coordinator") and (event.GFOSYSJ_CATEGORY=="Блокированные IP-пакеты" or
  event.GFOSYSJ_CATEGORY=="Нарушение правил фильтрации" or
  event.GFOSYSJ_CATEGORY=="Изменение правил фильтрации")){
    Notificator.notify(3, "Внимание, " +event.GFOSYSJ_SOURCE+" с узла "+
    event.GFOSYSJ_NODE+" сообщает о следующем событии:
    "+event.GFOSYSJ_CATEGORY+" произошедшем в "+event.GFOSYSJ_TIME+"; Описание
    события: "+event.GFOSYSJ_DESCR+"; ");
  }}
```

Примечание. При задании значений параметра `event.GFOSYSJ_SOURCE` важно соблюдать регистр.

Настройка подключения к прокси-серверу

Для возможности отправки SMS-оповещений и мониторинга узлов на онлайн-карте

и мониторинга узлов на онлайн-карте Серверу мониторинга требуется доступ в Интернет. Доступ в Интернет может быть организован как напрямую, так и через прокси-сервер. Если при подключении к Интернету используется прокси-сервер, то вы можете настроить подключение к этому серверу с помощью АРМ мониторинга.

Внимание! В случае использования прокси-сервера при подключении к Интернету необходимо, чтобы запуск службы Apache Tomcat осуществлялся с использованием учетной записи администратора ОС.

Чтобы настроить подключение к прокси-серверу, выполните следующие действия:

1. В главном окне программы на странице **Администрирование** > **Настройки** перейдите в раздел **Прокси**.
2. Установите переключатель в одно из следующих положений:
   - **Без прокси** — для подключения к Интернету в случае, если прокси-сервер не используется. Данное положение установлено по умолчанию.
   - **Использовать системные настройки прокси** — для подключения к прокси-серверу с использованием системных настроек.
   - **Ручная настройка сервиса прокси** — чтобы задать нужные настройки прокси-сервера с помощью АРМ мониторинга.

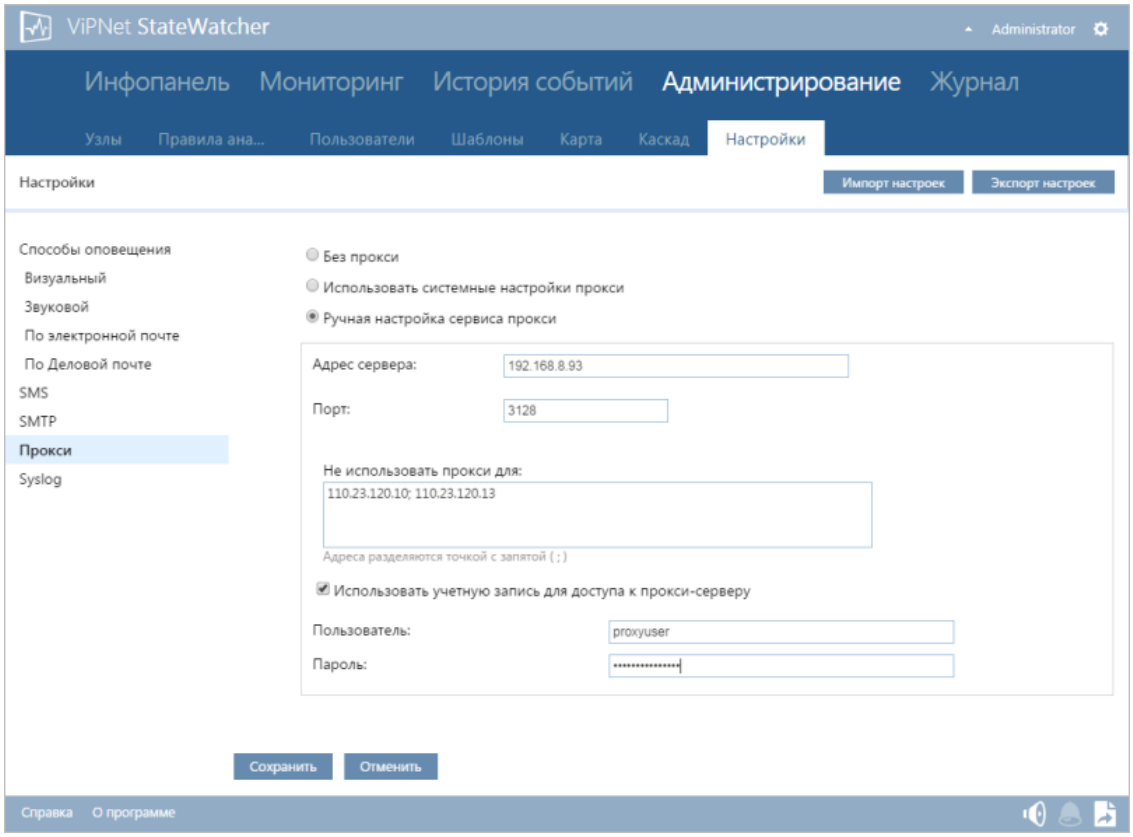

Рисунок 51: Настройка подключения к прокси-серверу

3 Если переключатель был установлен в положение **Ручная настройка сервиса прокси**, укажите параметры подключения к прокси-серверу:

- В поле **Адрес сервера** укажите IP-адрес или DNS-имя прокси-сервера.
- В поле **Порт** укажите порт для подключения к прокси-серверу.
- В поле **Не использовать прокси для** укажите адреса ресурсов, при подключении к которым не используется прокси-сервер. Адреса разделяются с помощью точки с запятой.

4 Если при подключении к прокси-серверу требуется авторизация, установите флажок **Использовать учетную запись для доступа к прокси-серверу** и укажите параметры учетной записи:

- В поле **Пользователь** укажите имя учетной записи, с использованием которой будет производиться подключение к прокси-серверу.
- В поле **Пароль** укажите пароль учетной записи.

5 По завершении настройки нажмите кнопку **Сохранить**.

Настройка карты

Настройка карты выполняется с помощью АРМ мониторинга под учетной записью администратора. Эта настройка позволяет задать расположение узлов мониторинга на географической карте.

Карта, отображаемая в АРМ мониторинга, зависит от установленного пакета настроек. В стандартный пакет настроек входят следующие карты:

- локальная карта России (отображается при первом старте по умолчанию);
- онлайн-карта OpenStreetMap.

Для настройки карты выполните следующие действия:

1. На вкладке **Администрирование** перейдите на страницу **Карта**. На данной странице отображаются текущие настройки расположения узлов мониторинга на карте. Загруженная карта зависит от установленного пакета настроек (см. «Пакет настроек» на стр. 290).
2. При необходимости смените отображаемую карту. Для этого выберите нужную карту в списке карт.

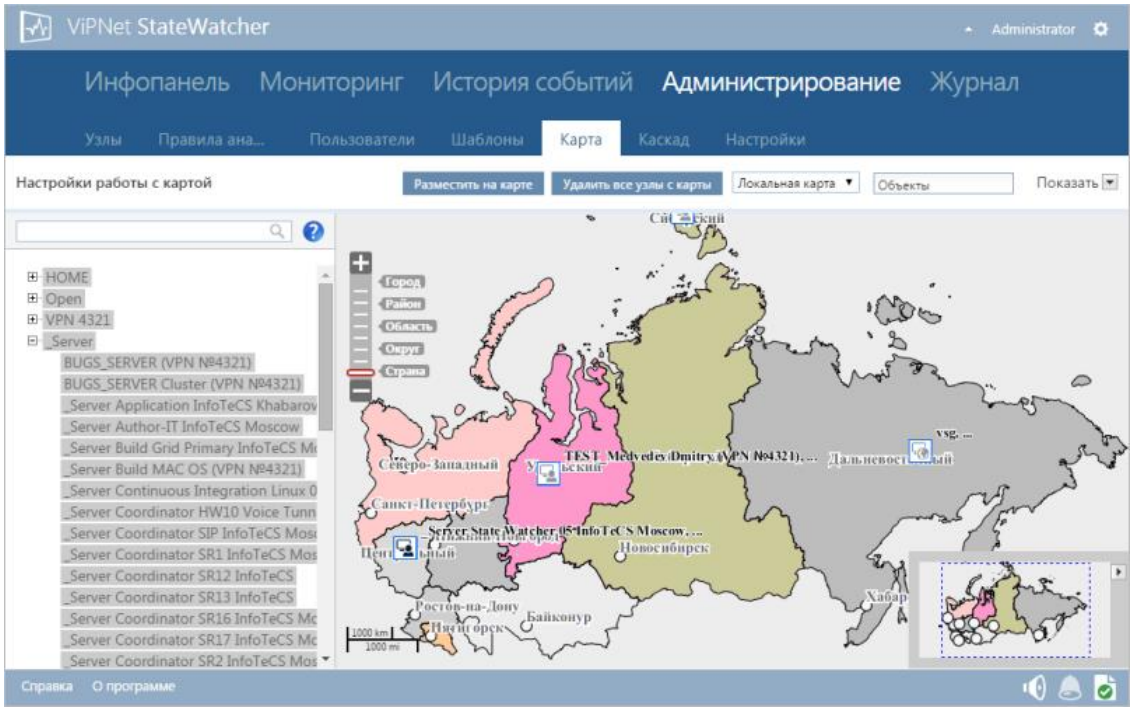

Рисунок 52: Настройка карты

3 При необходимости добавьте или удалите узлы с карты.

- Для добавления узлов на карту:

  - На панели навигации дважды щелкните левой кнопкой мыши по имени узла. В появившемся окне в поле **Населенный пункт** введите первые три буквы названия населенного пункта и в появившемся списке выберите нужный населенный пункт, а затем нажмите кнопку **OK**. Чтобы отказаться от изменений, нажмите кнопку **Отменить**.

Примечание. Добавление узлов на карту данным способом возможно только при использовании локальной карты.

  - На панели навигации выберите узел или группу узлов и перетащите их с помощью мыши в нужное место на карте.

В результате узел или группа узлов будут добавлены на карту.

Также вы можете добавить узлы на карту в соответствии с их реальными координатами, определенными системой геопозиционирования (см. «Добавление узлов на карту в соответствии с их координатами» на стр. 125).

Примечание. Добавление большого количества узлов мониторинга на карту может занять некоторое время, при этом появится значок и сообщение о добавлении узлов. В этом случае необходимо дождаться завершения процесса добавления узлов.

Положение узлов на карте обозначается значками, соответствующими типу узлов:

- — «Клиент» (защищенный узел, на котором установлено ПО ViPNet Client);
- — «Координатор» (защищенный узел, на котором установлено ПО ViPNet Coordinator), «HW 10», «HW 100», «HW 1000», «HW 2000», «Координатор HW»;
- — «Мобильный клиент»;
- — «Терминал»;
- — «Инфотабло»;
- — «Экспресс-3»;
- — «Открытый узел»;
- — «ИБП»;
- — «Принтер»;
- — «Маршрутизатор»;
- — «IDS»;
- — «Неизвестный узел»;
- — группа узлов.

Также узлы, добавленные на карту, будут отображаться в списке узлов на сером фоне.

Примечание. При размещении узла на карте Сервера мониторинга сразу же начнут появляться оповещения о событиях, обнаруженных на добавляемом узле.

- Для удаления узлов с карты щелкните по значку узла. В окне **Информация об узле** нажмите кнопку **Удалить с карты**.

Чтобы удалить все узлы с карты, на панели инструментов нажмите кнопку **Удалить все узлы с карты**.

- Для перемещения узлов на карте наведите курсор на узел, который необходимо переместить, дождитесь появления значка и перетащите узел в выбранное место на карте.
- Для изменения параметров узла щелкните по нему левой кнопкой мыши.

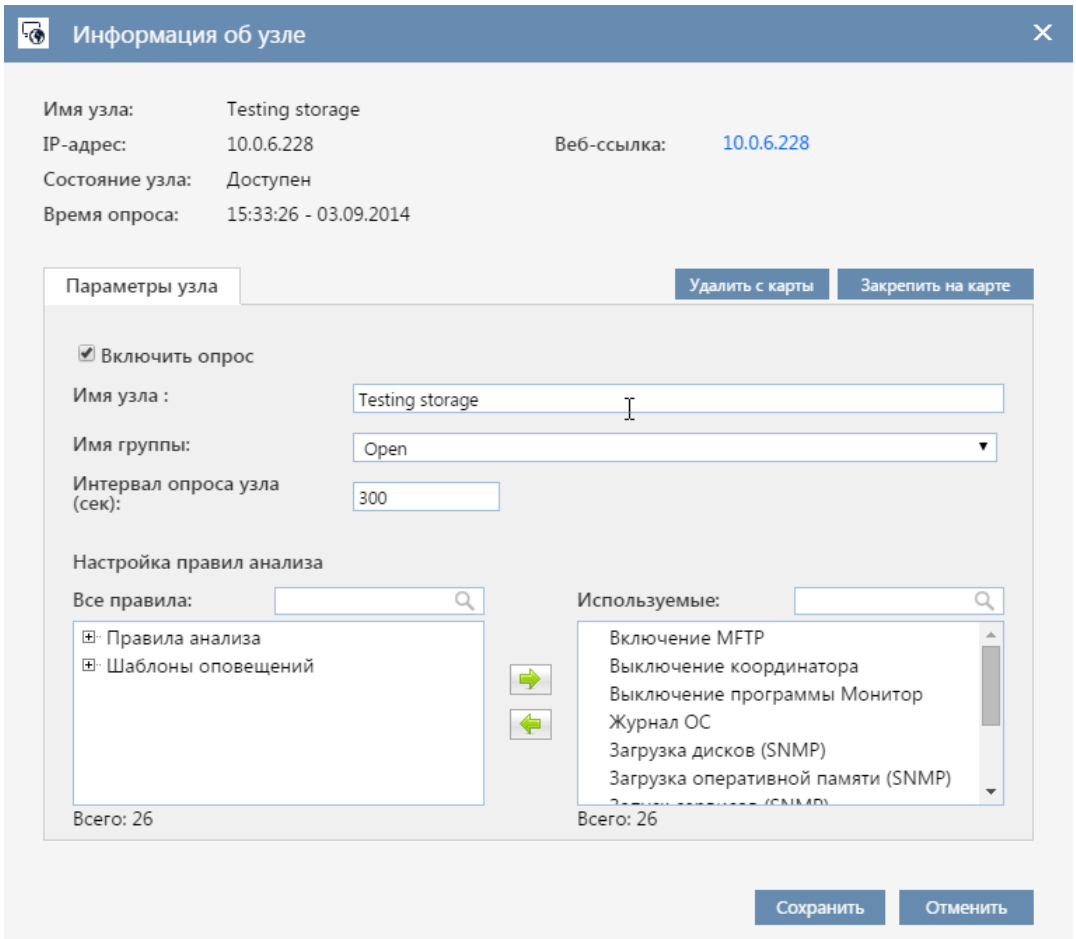

Рисунок 53: Изменение параметров узла

Помимо задания расположения узлов для локальной карты администратор может настроить свои стили отображения. Настройка стилей позволяет задавать степень подробности карты путем включения или отключения отображения различных объектов, а также задавать способ отображения на карте узлов мониторинга. Эти настройки индивидуальны для каждого пользователя, в том числе для администратора, и подробно описаны в документе «Программный комплекс мониторинга защищенных сетей ViPNet

StateWatcher. АРМ мониторинга. Руководство пользователя». В этом документе также описаны возможности, предоставляемые при работе с картой.

Добавление узлов на карту в соответствии с их координатами

В ПО Сервер мониторинга вы можете добавлять узлы на карту в соответствии с их реальными координатами, полученными от системы геопозиционирования.

Система геопозиционирования является модулем ПО Сервер мониторинга и выполняет следующие функции:

- Получение от общедоступных серверов геолокации реальных координат узлов по их IP-адресам.
- Размещение узлов на карте в соответствии с полученными координатами.
- Перемещение узлов на карте в случае изменения их координат.

Текущие координаты узлов мониторинга определяются системой геопозиционирования при каждом опросе узлов. Если координаты каких-либо узлов изменились, то узлы на карте будут автоматически перемещены на новую позицию. Однако администратор Сервера мониторинга может зафиксировать положение необходимых узлов на карте, в этом случае изменение координат узлов не будет влиять на их расположение на карте.

Чтобы добавить узлы на карту в соответствии с их реальными координатами, выполните следующие действия:

1. В главном окне АРМ мониторинга на странице **Мониторинг** > **Список** произведите опрос всех необходимых узлов мониторинга.
2. Откройте страницу **Администрирование** > **Карта**.
3. На панели инструментов нажмите кнопку **Разместить на карте**.

В результате все узлы, для которых были определены текущие координаты, будут размещены на карте.

Чтобы закрепить какой-либо узел на карте, выполните следующие действия:

1. В главном окне АРМ мониторинга перейдите на страницу **Администрирование** > **Карта**.
2. На карте дважды щелкните узел, который хотите закрепить.

3 В окне **Информация об узле** (см. Рисунок 54 на стр. 124) нажмите кнопку **Закрепить на карте**.

В результате узел будет привязан к текущему месту на карте и не будет перемещаться в новое положение при изменении его координат при последующих опросах. Для отмены закрепления узла на карте в окне **Информация об узле** нажмите кнопку **Открепить от карты**.

Настройка каскада

Настройка каскада (см. «Каскад» на стр. 289) позволяет сформировать иерархическую структуру каскада путем установления связей «родитель — потомок» между Серверами мониторинга. Конфигурацию каскада можно модифицировать путем изменения связей между Серверами мониторинга. Настройка каскада выполняется с помощью АРМ мониторинга под учетной записью администратора.

ПО Сервер мониторинга 4.3 совместимо в каскаде только с версией 4.0 и выше данного ПО. При этом поддерживается организация каскада, если на родительском Сервере мониторинга установлена версия ПО выше или одинаковая с дочерними серверами, и не поддерживается организация каскада, если на родительском сервере установлена версия ПО ниже, чем на дочернем сервере. Если на Серверах мониторинга, которые будут входить в каскад, установлено ПО версии ниже 4.0, то обновите это ПО до версии 4.3 (см. «Обновление ПО Сервер мониторинга» на стр. 58).

После настройки каскада необходимо убедиться, что все связи «родитель — потомок» установлены корректно. Для этого просмотрите журнал событий на вкладке **Журнал**, в котором появятся соответствующие записи:

1. При установлении отношения «родитель — потомок» последовательно появятся следующие записи:
   - «Восстановление связи на сетевом уровне с дочерним сервером `<Имя узла>` ViPNet ID `<Идентификатор узла>`».
   - «Установление отношения „родитель — дочерний“ с дочерним сервером `<Имя узла>` ViPNet ID `<Идентификатор узла>`».

   Появление двух последовательных записей связано с механизмом установления связи в каскаде: родительский Сервер мониторинга сначала проверяет связь с дочерним сервером на сетевом уровне, а затем при наличии связи устанавливает отношение «родитель — потомок».
2. При разрыве отношения «родитель — потомок» появится запись «Разрыв отношения „родитель — дочерний“ с дочерним сервером `<Имя узла>` ViPNet ID `<Идентификатор узла>`».
3. При разрыве связи между Серверами мониторинга на сетевом уровне появится запись «Обнаружение разрыва связи на сетевом уровне с дочерним сервером `<Имя узла>` ViPNet ID `<Идентификатор узла>`».

4 При восстановлении связи между Серверами мониторинга на сетевом уровне появится запись «Восстановление связи на сетевом уровне с дочерним сервером `<Имя узла>` ViPNet ID `<Идентификатор узла>`».

Если все связи установлены корректно, то Серверы мониторинга будут успешно функционировать в каскаде. Если же какие-либо связи не были установлены либо были разорваны, установите эти связи заново.

Добавление Сервера мониторинга в каскад

Для добавления Сервера мониторинга в каскад:

1 Подключитесь к Серверу мониторинга, каскад которого вы хотите настроить и который будет родительским по отношению к остальным серверам.

2 В главном окне АРМ мониторинга на вкладке **Администрирование** перейдите на страницу **Каскад**.

На панели навигации отобразится текущая структура каскада. Сервер мониторинга, к которому вы подключились, будет вышестоящим в списке.

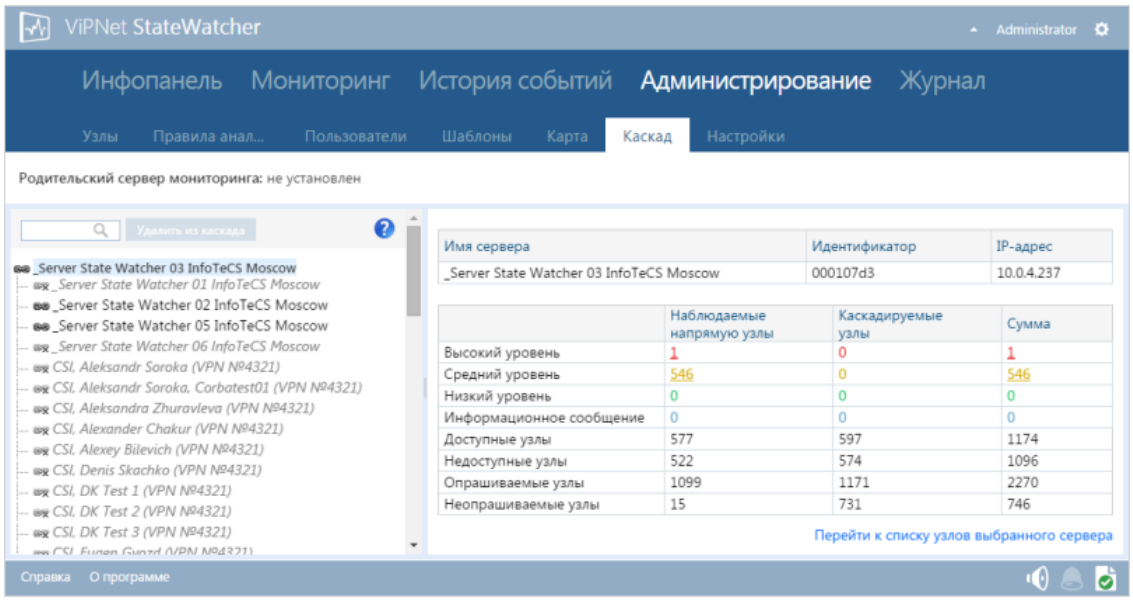

Рисунок 54: Настройка каскада

3 На панели навигации выберите из списка Сервер мониторинга, который вы хотите добавить в каскад (сделать дочерним по отношению к своему серверу) и на панели навигации нажмите кнопку **Добавить в каскад**.

Примечание. В списке отображаются только те Серверы мониторинга, с которыми у данного Сервера мониторинга есть связь, заданная в программе Центр управления сетью (кроме Сервера мониторинга, который уже назначен родительским по отношению к данному Серверу мониторинга).

Таким образом, формирование структуры каскада следует начинать с корневого Сервера мониторинга, постепенно спускаясь вниз по структуре каскада.

Для каждого потенциально дочернего Сервера мониторинга на панели просмотра отображается таблица, содержащая имя сервера, его идентификатор и IP-адрес, а также статус связи в каскаде (**Связь установлена**, **Связь не установлена**, **Ожидается подтверждение установки**). Также слева от названия серверов, с которыми еще не установлена связь в каскаде, отображается значок .

4 Дождитесь подтверждения установки связи с выбранным Сервером мониторинга. Если связь с сервером устанавливается слишком долго, вы можете отменить запрос на установление связи и попробовать установить связь с данным сервером позже. Для этого на панели навигации данного сервера нажмите кнопку **Отменить запрос**.

Для установления или разрыва связи Серверы мониторинга обмениваются специальными сообщениями. Сервер мониторинга, к которому вы подключены, посылает выбранному из списка Серверу мониторинга сообщение о намерении назначить его дочерним, и ожидает подтверждение от администратора данного сервера. На время ожидания ответа от сервера статус связи в каскаде принимает значение **Ожидается подтверждение установки** и на панели навигации, слева от названия сервера, будет показан значок — . После получения ответа статус отношения принимает значение **Связь установлена** или **Связь не установлена**.

Примечание. Связь в каскаде может быть не установлена, если дочерний Сервер мониторинга недоступен (серверы, доступные на сетевом уровне, отображаются черным цветом, недоступные — серым) или его администратор отклонил запрос о добавлении в каскад. В этом случае связь будет установлена после того как дочерний сервер станет доступен или его администратор подтвердит связь. Также связь может быть разорвана, если после установления связи с вашим родительским сервером администратор дочернего сервера принял запрос на добавление в каскад от другого родительского Сервера мониторинга.

Как только администратор дочернего Сервера мониторинга подтвердит добавление этого сервера в каскад, на панели навигации, слева от названия сервера, появится значок . Также на панели просмотра в информационной таблице данного сервера в графе **Связь** статус связи в каскаде с данным сервером примет значение **Связь установлена**.

Внимание! При формировании иерархии каскада необходимо избегать его цикличности, то есть ни один Сервер мониторинга не должен являться одновременно родительским и дочерним для одного и того же Сервера мониторинга. Обратите внимание, что данное условие выполняется для всех элементов каскада.

После установления связи между Серверами мониторинга в АРМ мониторинга происходят следующие изменения:

- На вкладке **Мониторинг** в список узлов добавляется группа **Каскадируемые узлы**, в которой иерархически отображаются все Серверы мониторинга, для которых данный сервер является родительским, и каскадируемые ими узлы.
- На дочернем Сервере мониторинга в группе **Родительские правила** отображаются пользовательские правила, которые были созданы на родительском Сервере мониторинга и для которых при этом был установлен флажок **Применять на дочерних серверах мониторинга**.
- На дочернем Сервере мониторинга встроенные правила, которые были применены для дочерних серверов родительского сервера, отображаются в группе **Встроенные правила** с установленным флажком **Применять на дочерних серверах мониторинга**. Данный флажок невозможно снять. Также данные правила применяются на всех узлах мониторинга данного дочернего сервера.

Действия администратора дочернего Сервера мониторинга при включении его сервера в каскад

При настройке каскада администратор дочернего Сервера мониторинга получает запрос на установку связи в каскаде. Администратор может разрешить установление связи с родительским сервером или отклонить запрос.

Если данный дочерний Сервер мониторинга пытаются добавить в каскад одновременно несколько родительских серверов, то запрос будет содержать список этих серверов. Администратор дочернего сервера может выбрать нужный родительский сервер и разрешить установление связи с ним (при этом остальными родительскими серверами будет отправлен отказ) либо отклонить запрос от всех серверов.

Для разрешения установления связи с родительским Сервером мониторинга выполните следующие действия:

1 Подключитесь к дочернему Серверу мониторинга с использованием учетной записи администратора. Появится окно с запросом на установление связи в каскаде.

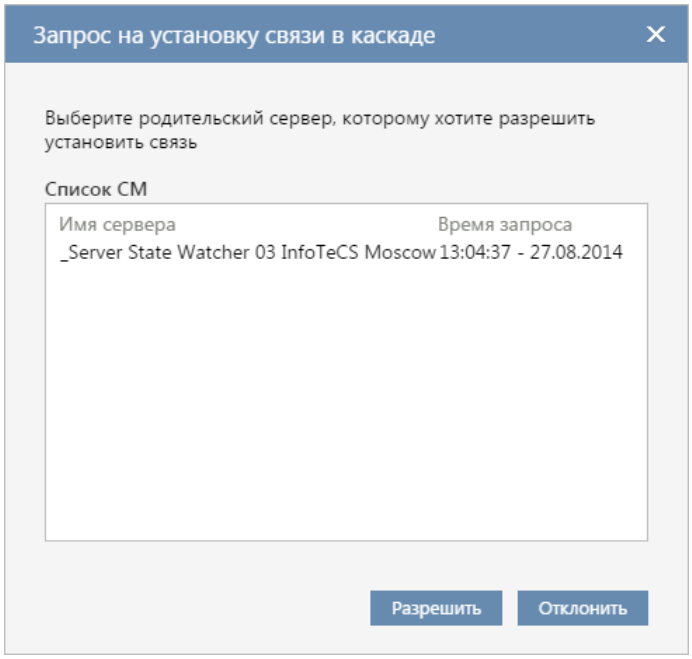

Рисунок 55: Запрос на установку связи в каскаде

2 Если запрос на установление связи был получен одновременно от нескольких родительских Серверов мониторинга, то в окне **Запрос на установку связи в каскаде** выберите из списка нужный сервер, установив переключатель рядом с его именем.

3 Нажмите кнопку **Разрешить**. Для отклонения запроса от всех серверов нажмите кнопку **Отклонить все**.

В результате будет установлена связь с выбранным родительским Сервером мониторинга.

Чтобы отложить установление связи или отклонение запроса, в правом верхнем углу окна **Запрос на установку связи в каскаде** нажмите кнопку . Окно с запросом на установление связи в каскаде будет закрыто, при этом на панели уведомлений появится значок . Для повторного вызова окна **Запрос на установку связи в каскаде** щелкните данный значок.

Удаление Сервера мониторинга из каскада

Для удаления Сервера мониторинга из каскада:

1. Подключитесь к Серверу мониторинга, каскад которого вы хотите настроить.
2. В главном окне АРМ мониторинга на вкладке **Администрирование** перейдите на страницу **Каскад**.

   На панели навигации отобразится текущая структура каскада. Сервер мониторинга, к которому вы подключились, будет вышестоящим в списке.
3. На панели навигации выберите Сервер мониторинга, с которым вы хотите разорвать в каскаде.
4. На панели навигации нажмите кнопку **Удалить из каскада**.
5. В окне **Удаление из каскада** убедитесь, что вы удаляете именно нужный сервер из каскада, и нажмите кнопку **Удалить.** В результате сервер будет удален из каскада.

Примечание. Разорвать связь между Серверами мониторинга в каскаде вы можете только для серверов, напрямую подчиненных вашему Серверу мониторинга.

При удалении сервера из каскада в АРМ мониторинга произойдут следующие изменения:

- На дочернем Сервере мониторинга правила, примененные родительским сервером, будут перемещены из группы **Родительские правила** в группу **Удаленные правила** и перестанут срабатывать.
- На дочернем Сервере мониторинга встроенные правила, примененные родительским сервером, перестанут срабатывать.
- Не будет производиться сбор статистики с узлов сервера, удаленного из каскада.

Экспорт и импорт настроек Сервера мониторинга

В случае необходимости вы можете экспортировать настройки ПО Сервер мониторинга в файл или импортировать настройки из файла.

Функцию экспорта и импорта настроек удобно использовать в следующих случаях:

- Чтобы перенести ПО Сервер мониторинга вместе со всеми настройками на новый компьютер. Для этого:
  - На старом компьютере выполните экспорт настроек ПО Сервер мониторинга.
  - На новом компьютере установите программу ПО Сервер мониторинга.
  - На новом компьютере импортируйте настройки из созданного ранее файла.
- Чтобы создать резервную копию настроек программы ПО Сервер мониторинга на случай отказа оборудования или программного обеспечения. Для этого экспортируйте файл настроек программы на съемный носитель и сохраните его в надежном месте.

Настройки ПО Сервер мониторинга сохраняются в файл `exportSettingsResult.xml` (помещенный в архив `exportSettingsResult.zip`), который содержит списки пользователей, узлов и правил анализа, шаблоны оповещений, информацию о привязке правил анализа к пользователям и способам оповещения, настройки протоколов SMTP, SMPP, SNMP и прокси-сервера, настройки способов оповещения, параметры каскада и расположение узлов на карте.

Внимание! Импорт настроек ПО Сервер мониторинга имеет некоторые особенности. Убедитесь, что выполняемые вами действия соответствуют вашей задаче, ознакомившись с информацией в разделе Особенности импорта настроек (на стр. 135).

Чтобы сохранить настройки ПО Сервер мониторинга в файл, выполните следующие действия:

1. В главном окне программы перейдите на страницу **Администрирование** > **Настройки**.

2 Нажмите кнопку **Экспорт настроек**.

3 Следуйте указаниям менеджера загрузки файлов вашего браузера.

Чтобы импортировать настройки ПО Сервер мониторинга:

1 В главном окне программы перейдите на страницу **Администрирование** > **Настройки** и нажмите кнопку **Импорт настроек**.

2 В окне **Импорт настроек** нажмите кнопку **Обзор** и выберите файл настроек `*.xml` или `*.zip`.

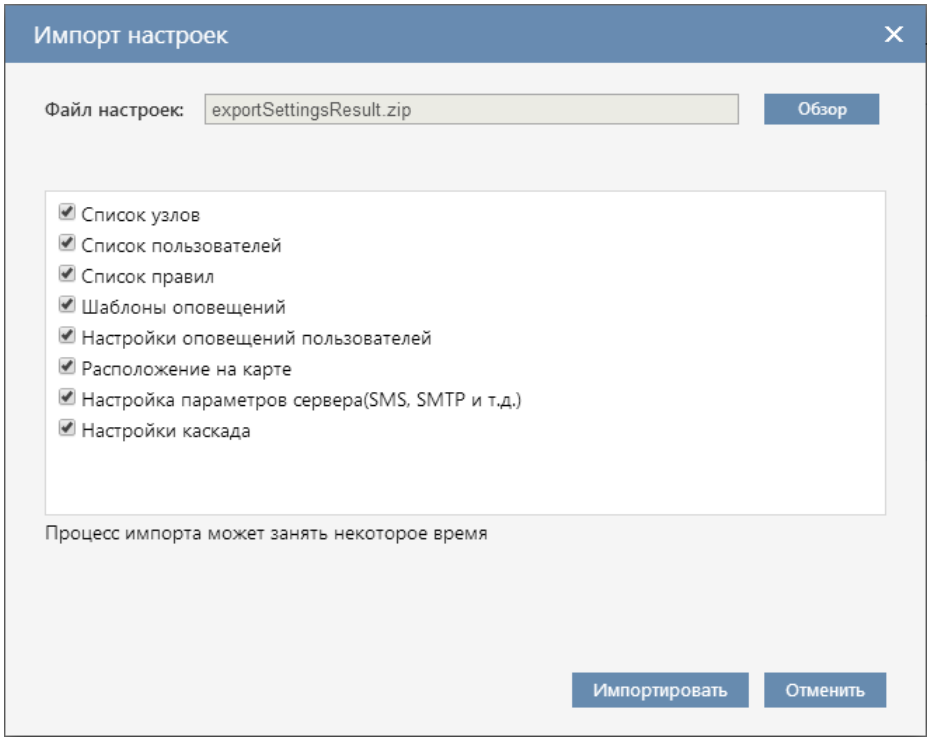

Рисунок 56: Импорт настроек ПО Сервер мониторинга

При необходимости снимите флажки с настроек, которые вы не хотите импортировать.

3 Нажмите кнопку **Импортировать**.

4 Дождитесь сообщения о том, что импорт настроек завершен, и нажмите кнопку **Закрыть**.

Особенности импорта настроек

В данном разделе описаны особенности импорта настроек ПО Сервер мониторинга из файла настроек.

Список пользователей

Учетные записи пользователей, чьи имена не совпадают с именами в файле настроек, будут удалены. Учетные записи пользователей, чьи имена совпадают с именами в файле настроек, и встроенная учетная запись `Administrator` будут обновлены. На основе информации о новых пользователях в файле настроек будут созданы новые учетные записи пользователей.

После импорта будет отображена информация о добавленных, обновленных и удаленных учетных записях с указанием ФИО пользователей.

Список узлов

Список узлов мониторинга будет очищен. В список доступных для мониторинга открытых узлов будут добавлены все открытые узлы из файла настроек и защищенные узлы из справочника ViPNet; уже имеющиеся в списке узлы удалены не будут. Информация об узлах доступных для мониторнга, чьи IP-адреса совпадают IP-адресами узлов из файла настроек, будет обновлена.

После импорта будет отображена информация об удаленных узлах, обновленных открытых узлах и узлах, которые не были добавлены (которых нет в справочнике ViPNet).

Шаблоны оповещения

Все шаблоны будут удалены кроме шаблона по умолчанию. Новые шаблоны будут добавлены из файла настроек. В шаблоне по умолчанию список правил и способы оповещения будут обновлены согласно информации из файла настроек.

После импорта будет показан список удаленных и добавленных шаблонов.

Список правил анализа

Правила анализа, которые не были заданы, будут добавлены. Правила анализа, которые были заданы ранее в ПО Сервер мониторинга, но отсутствуют в файле настроек, будут перенесены в удаленные. Правила анализа будут применены к узлам мониторинга и переданы по каскаду согласно файлу настроек.

После импорта будет выведен список добавленных и удаленных правил анализа.

Настройки протоколов SMTP, SMPP, прокси-сервера, SysLog

Данные настройки будут обновлены согласно файлу настроек. Если настройки протоколов не заданы в файле, то текущие настройки останутся без изменений.

Способы оповещения

Соответствие между правилами анализа, пользователями и способами оповещения будет назначено согласно файлу настроек.

Настройки каскада

Отношения с дочерними серверами, которые не указаны в файле настроек, будут разорваны. Запрос на установление каскадных отношений будет отправлен на серверы (при условии что они указаны в справочнике ViPNet), которые есть в файле настроек, но ранее не были дочерними серверами по отношению к вашему серверу.

После импорта будет показан список имен серверов, с которыми были разорваны отношения и которым был отправлен запрос на установление отношений.

Расположение узлов на карте

С карты будут удалены все узлы; вместо них на карту будут добавлены узлы, указанные в настройках.

Тонкая настройка Сервера мониторинга

Параметры, предназначенные для тонкой настройки Сервера мониторинга, хранятся в файле конфигурации `server.ini`. Этот файл находится в каталоге `\Tomcat_dir\webapps\ROOT\WEB-INF\classes`, где `Tomcat_dir` – каталог установки Apache Tomcat. Значения параметров нельзя изменить с помощью АРМ мониторинга, их настройка осуществляется путем редактирования файла `server.ini` в каком-либо текстовом редакторе. Чтобы новые настройки вступили в силу, после редактирования и сохранения файла `server.ini` необходимо перезапустить Сервер мониторинга (см. «Управление Сервером мониторинга» на стр. 40).

Примечание. Параметры подключения к SMTP-серверу, которые необходимы для отправки оповещений о событиях мониторинга, хранятся в базе данных и настраиваются с помощью АРМ мониторинга.

Файл `server.ini` представляет собой текстовый файл, имеющий стандартную структуру файла конфигурации. Он состоит из фиксированного набора секций, содержащих различные параметры.

Пример файла `server.ini`:

```
[collection]
MaxConnection=200
CollectionThreads=1
ThreadChannels=50
TCPConnectionTimeout=20
TCPReadWriteTimeout=60
UDPTimeout=10
PingTimeout=4

[storage]
OlapDBUser=swadmin
OlapDBPassword=tevaJsGaMpCNJaUVQLEfTw==
DBServer=localhost
DBPort=5432
DBName=sw_olap

[analyze]
AnalyzeThreads=1
AnalyzeThreadTimeout=10
AnalyzeThreadLatency=1
```

```
[control]
SyncInterval=300
OlapDBMaxSize=5000MB
OlapDBMaxTime=365
RawDataMaxSize=15GB
RawDataMaxTime=90
MaintananceDB=0 0 0-23/1 * * ?
MaintananceReindex=0 0 1 * * ?
MainLogLevel=ERROR
AnalyzeLogLevel=ERROR
MainLogPath=logs/statewatcher.log
MainLogMaxSize=10MB
MainLogBackups=7
AnalyzeDebugLogPath=logs/analyze-debug.log
AnalyzeDebugLogMaxSize=5MB
AnalyzeDebugLogBackups=0

SWJournalLogPath=logs/swjournal.log
SWJournalLogMaxSize=5MB
SWJournalLogBackups=1
SWJournalLogLevel=ERROR


[smtp]
SmtpQueueLimit=300

[sms]
SMSperMinute=30
MaxSMSperDay=2000
SMSSendRepeatTime=120000

[gis]
postgis.server=localhost
postgis.port=5432
postgis.dbname=sw_gis
postgis.user=swadmin
postgis.password=tevaJsGaMpCNJaUVQLEfTw==

[export]
RawDataExportDir=log
RawDataExportInterval=0 0 0/1 * * ?
AutomatedExport=OFF

[bm]
BmDir=C:/Users/Admin/AppData/Local/Temp/Деловая почта
BmEncoding=windows-1251
```

Секция [collection]

Данная секция содержит параметры функционирования Сервера мониторинга в процессе сбора информации:

- `MaxConnection` – максимальное количество одновременных соединений. Значение по умолчанию 200.
- `CollectionThreads` – количество потоков, обрабатывающих ввод-вывод на транспортном уровне. Значение по умолчанию 1.
- `ThreadChannels` – максимальное количество соединений, обслуживаемых одним потоком. Значение по умолчанию 50.
- `TCPConnectionTimeout` — время ожидания установки соединения с открытыми узлами по протоколу TCP. Значение по умолчанию 20.
- `TCPReadWriteTimeout` — время ожидания передачи данных от открытых узлов по протоколу TCP. Значение по умолчанию 60.
- `UDPTimeout` — время ожидания ответа от узлов по протоколу UDP. Значение по умолчанию 10.
- `PingTimeout` — время ожидания ответа по время проверки соединения (выполнения команды `ping`). Значение по умолчанию 4.

Внимание! Параметры секции `[collection]` предназначены для оптимизации работы Сервера мониторинга, и изменять их без крайней необходимости не следует.

Секция [storage]

Данная секция содержит параметры доступа к базе данных мониторинга и настройку хранения необработанных данных:

- `OlapDBUser` – имя пользователя базы данных мониторинга. В этот параметр записывается значение соответствующего параметра, заданного во время установки ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47). Значение по умолчанию `swadmin`.
- `OlapDBPassword` – пароль пользователя базы данных мониторинга. В этот параметр записывается в зашифрованном виде значение соответствующего параметра,

заданного во время установки ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47).

- `DBServer` — имя Сервера мониторинга. Значение по умолчанию `localhost`.
- `DBPort` — номер порта, через который работает Сервер мониторинга. Значение по умолчанию `5432`. Если на сервере установлено две версии PostgreSQL (например, при обновлении ПО Сервер мониторинга до версии 4.3), то значение по умолчанию будет `5433`.
- `DBName` — имя базы данных мониторинга. Значение по умолчанию `sw_olap`.

Секция [control]

Данная секция содержит ограничения на хранение информации, расписание запуска ротации данных и настройки протоколирования.

Ограничения на хранение информации позволяют контролировать количество данных, хранимых на Сервере мониторинга. Удаление устаревших данных происходит периодически с использованием механизма ротации. Для каждого вида хранимой информации (необработанных данных и основных данных, полученных после обработки) задаются свои ограничения на объем информации и на время ее хранения. Превышение этих ограничений проверяется при выполнении процедуры ротации, которая запускается по заданному расписанию. Если объем хранимой информации и/или время ее хранения превышают заданные ограничения, из базы удаляются самые старые данные до тех пор, пока не будут выполняться заданные ограничения по объему хранимой информации и времени ее хранения.

Внимание! Ротацию данных рекомендуется проводить раз в час. При более редком запуске ротации возможно существенное замедление выполнения запросов к базам данных (например, при просмотре истории событий мониторинга).

Кроме расписания запуска ротации, в данной секции задается расписание запуска процедуры реиндексации таблиц баз данных. Эту процедуру необходимо выполнять периодически для предотвращения замедления запросов к базам данным. При выполнении процедуры реиндексации блокируется доступ к настройкам Сервера мониторинга и к истории событий мониторинга. Это связано с тем, что в процессе реиндексации идет работа с базами данных, которые при этом становятся недоступны для чтения и записи.

Настройки протоколирования позволяют контролировать количество информации, хранимой в отладочных журналах. В ПК ViPNet StateWatcher поддерживаются два вида журналов – основной отладочный журнал, в котором фиксируются действия пользователей и события мониторинга, и журнал для правил анализа, в котором регистрируются события, связанные с выполнением правил анализа. Для каждого вида журнала задаются свои ограничения на уровень протоколирования, объем журнала и количество сохраняемых файлов журнала. Уровень протоколирования определяет степень детализации записываемых в журнал сообщений, от него зависит объем журнала: чем выше уровень протоколирования, тем больше информации записывается в журнал. При превышении ограничения на объем журнала автоматически выполняется ротация файлов журнала: самые старые файлы журнала удаляются, устаревшие последовательно переименовываются, текущий журнал замещается заново созданным. При этом сохраняется такое количество файлов, которое задано в настройках.

Для основного отладочного журнала используются следующие уровни протоколирования (в порядке убывания приоритета):

- **DEBUG** – для детальной информации о каких-либо процессах или компонентах, наиболее полезной при отладке;
- **INFO** – для сообщений, освещающих работу приложения, как правило, для сообщения о выполнении чего-либо или о состоянии какого-либо компонента;
- **WARN** – для сообщений о потенциально опасных ситуациях, которые могут привести к ошибке, сбою или по какой-либо причине являются нежелательными;
- **ERROR** – для сообщений об ошибках.

В журнале для правил анализа используются 2 уровня протоколирования – **DEBUG** и **ERROR**. Уровень **DEBUG** имеет наивысший приоритет, он предназначен для записи в журнал детальной информации о правилах анализа и используется при отладке. Уровень **ERROR** предназначен для записи сообщений об ошибках.

Секция `[control]` содержит следующие параметры:

- `SyncInterval` – интервал синхронизации (в секундах). Этот параметр задает периодичность обращения Сервера мониторинга к программному компоненту ViPNet Монитор для получения актуальной информации о связанных с ним узлах. Значение по умолчанию `300` (5 минут).
- `OlapDBMaxSize` – максимальный объем базы событий мониторинга (в байтах). Можно задать объем в килобайтах, мегабайтах или гигабайтах, для этого после значения надо указать соответственно KB, MB или GB. Значение по умолчанию `5 GB`.

Примечание. Ограничения на максимальный объем базы считаются отдельно для событий, наблюдаемых напрямую, и событий, происходящих на каскадируемых узлах.

Например, если параметр `OlapDBMaxSize` будет иметь значение 5 ГБ, то максимальный общий объем базы данных событий мониторинга составит 10 ГБ (5 ГБ для событий, наблюдаемых напрямую, и 5 ГБ для событий, происходящих на каскадируемых узлах).

- `OlapDBMaxTime` – максимальное время хранения данных в базе событий мониторинга (в днях). Значение по умолчанию `365` (1 год).
- `MaintananceDB` – расписание запуска процедуры ротации данных в cron-формате (см. «Формат расписания» на стр. 147). Значение по умолчанию `0 0 0/1 * * ?` (запуск каждый час, начиная с 0 часов).
- `RawDataMaxSize` – максимальный объем базы необработанных данных (в байтах). Значение по умолчанию `15GB`.
- `RawDataMaxTime` – максимальное время хранения необработанных данных (в днях). Значение по умолчанию `90` (дней).
- `MaintananceReindex` – расписание запуска процедуры реиндексации таблиц баз данных в cron-формате (см. «Формат расписания» на стр. 147). Значение по умолчанию `0 0 1 * * ?` (запуск каждый день ровно в 1 час ночи).
- `MainLogLevel` – уровень протоколирования основного отладочного журнала. Может принимать значения `ERROR`, `WARN`, `INFO` или `DEBUG`, значение по умолчанию `INFO`.
- `MainLogPath` – путь и имя файла основного отладочного журнала. Значение по умолчанию `logs/statewatcher.log`. Указание пути без имени устройства означает размещение в каталоге установки Apache Tomcat.
- `MainLogMaxSize` – максимальный объем файла основного отладочного журнала. Значение по умолчанию `10MB`.
- `MainLogBackups` – количество резервных копий основного отладочного журнала, сохраняемых после ротации. Значение по умолчанию `7`.
- `AnalyzeLogLevel` – уровень протоколирования отладочного журнала для правил анализа. Может принимать значения `ERROR` или `DEBUG`, значение по умолчанию `ERROR`.

- `AnalyzeDebugLogPath` – путь и имя файла отладочного журнала для правил анализа. Значение по умолчанию `logs/analyze-debug.log`. Указание пути без имени устройства означает размещение в каталоге установки Apache Tomcat.

- `AnalyzeDebugLogMaxSize` – максимальный объем файла отладочного журнала для правил анализа. Значение по умолчанию `5MB`.

- `AnalyzeDebugLogBackups` – количество резервных копий отладочного журнала для правил анализа, сохраняемых после ротации. Значение по умолчанию `0`.

Также в секции содержатся параметры журнала SWJournal. SWJournal — это текстовый файл, который дублирует информацию журнала событий Сервера мониторинга и также содержит дополнительную информацию о внутренних проблемах Сервера мониторинга (подключение и отключение пользователей, отсутствие и восстановление соединения с сервером баз данных и другие). Данная информация необходима разработчикам для анализа в случае возникновения нештатных ситуаций. SWJournal доступен при выключенном Сервере мониторинга и может помочь администратору понять, какие действия производились на Сервере мониторинга.

- `SWJournalLogPath` – путь и имя файла журнала событий, связанных с работой мониторинга. Значение по умолчанию `logs/swjournal.log`. Указание пути без имени устройства означает размещение в каталоге установки Apache Tomcat.

- `SWJournalLogMaxSize` – максимальный объем файла журнала событий. Значение по умолчанию `5MB`.

- `SWJournalLogBackups` – количество резервных копий журнала событий, сохраняемых после ротации. Значение по умолчанию `1`.

- `SWJournalLogLevel` – уровень протоколирования журнала событий. Может принимать значения `ERROR`, `WARN`, `INFO` или `DEBUG`, значение по умолчанию `ERROR`.

Секция [sms]

Данная секция содержит ограничения на отправку оповещений по SMS и включает в себя следующие параметры:

- `SMSperMinute` — максимальная скорость отправки SMS-оповещений, то есть количество SMS-оповещений, которое можно отправить в минуту. В случае достижения данного ограничения отправка SMS-оповещений приостанавливается. Значение по умолчанию равно 30.

- `MaxSMSperDay` — максимальное количество SMS-оповещений, которое можно отправить в сутки. При достижении данного ограничения отправка SMS-оповещений приостанавливается, а в журнале событий появляется запись «Отправлено максимальное количество SMS». Значение по умолчанию 2000. Счетчик отправленных SMS-оповещений обнуляется раз в сутки в 00:00 или при перезагрузке сервера.

- `SMSSendRepeatTime` — интервал времени для повторной отправки SMS-оповещения (например, если отправка оповещения была невозможна из-за отсутствия соединения с SMS-шлюзом). Значение по умолчанию равно 120 секундам.

Секция [gis]

Данная секция содержит параметры доступа к базе данных объектов мониторинга на карте:

- `postgis.server` – расположение базы данных объектов мониторинга на карте. Значение по умолчанию `localhost`.

- `postgis.port` – порт доступа к базе данных. Значение по умолчанию `5432`. Если на сервере установлено две версии PostgreSQL (например, при обновлении ПО Сервер мониторинга до версии 4.3), то значение по умолчанию будет `5433`.

- `postgis.dbname` – имя базы данных. Значение по умолчанию `sw_gis`.

- `postgis.user` – имя пользователя базы данных. Значение по умолчанию `swadmin`.

- `postgis.password` – пароль пользователя базы данных в зашифрованном виде.

Значения всех параметров данной секции задаются во время установки ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47).

Секция [export]

Данная секция содержит параметры настройки автоматического экспорта необработанных параметров узлов (см. «Необработанные параметры» на стр. 289) мониторинга. Настройка позволяет включать и отключать экспорт. Автоматический экспорт выполняется в фоновом режиме по заданному расписанию для всех узлов, если значение параметра `AutomatedExport` равно `on`. Временной интервал для очередного экспорта выбирается от момента выполнения предыдущего экспорта до текущего момента. Результат экспорта записывается в файл с именем `<день>.<месяц>.<год>-<час>-<мин>.xml`. Файлы экспорта помещаются в папку, заданную в настройках.

Примечание. Для каскадируемых узлов экспорт необработанных параметров невозможен.

Секция `[export]` содержит следующие параметры:

- `AutomatedExport` – признак включения или отключения автоматического экспорта. Может принимать значения `on` (экспорт включен) и `off` (экспорт отключен). Значение по умолчанию `off`.

- `RawDataExportDir` – папка для файлов с результатами экспорта. Значение по умолчанию `log`, при значении по умолчанию папка с результатами экспорта располагается `Диск:\Program File\Apache Software Foundation\Tomcat 6.0`. Указание папки без имени устройства означает размещение в каталоге установки Apache Tomcat.

  Примечание. Для того, чтобы автоматический экспорт производился на сетевой ресурс (см. «Настройка экспорта необработанных параметров узлов на сетевой ресурс» на стр. 145), путь к сетевой папке необходимо указывать в следующем виде:

  `RawDataExportDir=\\\\путь к папке\\Shared folder`

  То есть все символы **** должны быть продублированы.

- `RawDataExportInterval` – расписание запуска автоматического экспорта необработанных параметров в cron-формате (см. «Формат расписания» на стр. 147). Значение по умолчанию `0 0 0/1 * * ?` (запуск каждый час, начиная с 0 часов).

Настройка экспорта необработанных параметров узлов на сетевой ресурс

Примечание. Для корректного выполнения экспорта узлы должны быть доступны по сети ViPNet.

Ниже рассматривается пример двух вариантов настройки экспорта необработанных параметров узлов на сетевой ресурс, при условии, когда:

- компьютер, на котором установлена система мониторинга, и компьютер, на котором расположен сетевой ресурс, находятся в домене;

- компьютер, на котором установлена система мониторинга, и компьютер, на котором расположен сетевой ресурс, не находятся в домене.

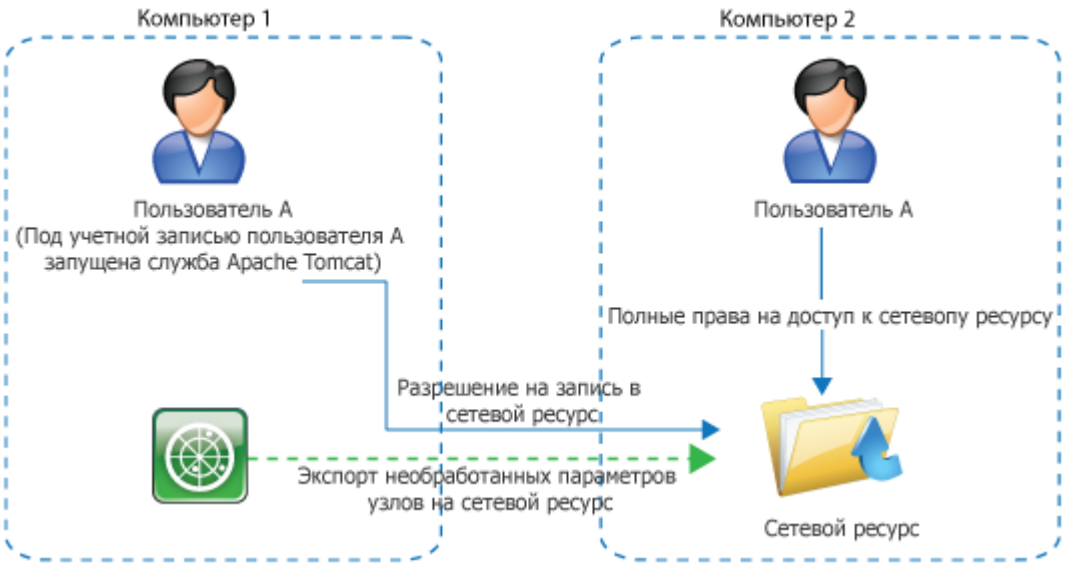

Рисунок 57: Общая схема экспорта необработанных параметров узлов на сетевой ресурс

Если компьютер, на котором установлена система мониторинга, и удаленный компьютер не находятся в домене, то для экспорта необработанных параметров на сетевой ресурс выполните следующие действия :

1. На компьютере 1 создайте учетную запись пользователя А.
2. На компьютере 1 запустите программное обеспечение Apache Tomcat под учетной записью пользователя А.
3. На компьютере 2 создайте учетную запись с параметрами учетной записи пользователя А и таким же паролем.
4. На компьютере 2 предоставьте только что созданной учетной записи пользователя А полный доступ к сетевому ресурсу.
5. На компьютере 2 предоставьте пользователю А компьютера 1 разрешение на запись в сетевой ресурс, расположенный на компьютере 2.
6. На компьютере 1 настройте в ПК ViPNet StateWatcher экспорт необработанных параметров на сетевой ресурс (см. «Секция [export]» на стр. 144), расположенный на компьютере 2.
7. На компьютере 1 в ПК ViPNet StateWatcher выполните экспорт необработанных параметров.

Если указанные компьютеры находятся в одном домене, выполните следующие действия:

1. На компьютере 1 запустите программное обеспечение Apache Tomcat под учетной записью пользователя A.
2. На компьютере 2 предоставьте учетной записи пользователя A полный доступ к сетевому ресурсу компьютера 2.
3. На компьютере 2 предоставьте пользователю A компьютера 1 разрешение на запись в сетевой ресурс, расположенный на компьютере 2.
4. На компьютере 1 настройте в ПК ViPNet StateWatcher экспорт необработанных параметров на сетевой ресурс (см. «Секция [export]» на стр. 144), расположенный на компьютере 2.
5. На компьютере 1 в ПК ViPNet StateWatcher выполните экспорт необработанных параметров.

Секция [bm]

Данная секция содержит путь к каталогу автопроцессинга транспортного модуля MFTP:

- `BmDir` – путь к каталогу, в который помещаются конверты с оповещениями для автоматической отправки с помощью программы Деловая почта. В этот параметр записывается значение, заданное во время установки ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47), но в случае необходимости его можно изменить непосредственно в файле `server.ini`.

Формат расписания

Для задания расписания используется cron-подобный формат. Расписание в этом формате состоит из 7 полей и задается следующей строкой:

```
<секунды> <минуты> <часы> <числа месяца> <месяцы> <дни недели> <годы>
```

Поле `<годы>` можно не указывать.

Месяцы можно задать либо целым числом от 1 до 12, либо коротким английским названием месяца (JAN, FEB и т.д.).

Дни недели можно задать либо целым числом от 0 до 7, где 0 и 7 означает воскресенье, либо коротким английским названием дня недели (SUN, MON и т.д.).

Для задания диапазона чисел используется дефис (-). Например, значение `1-4` означает целые числа 1, 2, 3 и 4.

Для задания списка значений используется запятая (,). Например, значение `3,4,6,8` означает четыре указанных целых числа.

Для задания полей можно использовать следующие специальные символы:

- / – означает шаг значений. Например, значение `5/15` в поле секунд означает каждые 15 секунд, начиная с 5-ой секунды.
- ? – означает отсутствие значения. Используется только для задания одного из полей <числа месяца> и <дни недели> в следующих случаях:
  - если заданы числа месяца, то в поле дней недели нужно указать ?;
  - если заданы дни недели, то в поле чисел месяца нужно указать ?.

  Например, строка `0 0 1 ? 1 SUN` означает запуск в январе по воскресеньям в 1 час 0 минут 0 секунд.
- * – означает все допустимые значения. Можно использовать для задания любых полей. Например, строка `* * * * * ?` означает запуск каждую секунду каждой минуты каждого часа ежедневно.

Примеры расписаний:

`5 0 0 ? * SUN` – запуск по воскресеньям в 0 часов 0 минут 5 секунд.

`0 0/5 * * * ?` – запуск каждые 5 минут.

`0 5 1 1-15 * ?` – запуск в 1 час 5 минут с 1-го по 15-е число каждого месяца.

Ротация данных

Данные, собранные Сервером мониторинга при опросе узлов (необработанные данные), и данные, полученные в результате обработки параметров узлов правилами анализа (события мониторинга), хранятся в базах данных на Сервере мониторинга. С течением времени количество хранимых данных увеличивается, что приводит к уменьшению свободного места на жестком диске. Чтобы ограничить количество хранимых данных, на Сервере мониторинга периодически запускается процедура ротации для удаления устаревших данных.

Условия проведения ротации задаются в настройках Сервера мониторинга. Для каждого вида данных (необработанных данных и событий мониторинга) задаются свои ограничения на объем и время хранения данных, а также периодичность ротации (см. «Секция [control]» на стр. 140). Для автоматического запуска ротации администратору Сервера мониторинга необходимо настроить расписание запуска ротации. Если объем

хранимой информации или время ее хранения превышают заданные ограничения, из базы удаляются самые старые данные до тех пор, пока не будут выполняться заданные ограничения по объему хранимой информации и времени ее хранения.

В процессе ротации не прекращается опрос узлов и обработка параметров узлов правилами анализа. При этом в базу данных записываются только события мониторинга, необработанные параметры узлов не сохраняются. У событий, обнаруженных во время проведения ротации, значения анализируемых параметров отсутствуют.

Ротация данных в аналитической базе выполняется с учетом следующей особенности: для каждого сработавшего правила анализа и каждого узла, для которого сработало правило, в базе должно оставаться хотя бы одно событие. Если по условиям ротации для какого-либо правила и узла должны быть удалены все события, то из базы удаляются все события, кроме самого последнего (по времени срабатывания правила).

Например, пусть в настройках ротации аналитической базы задано, что данные должны храниться за один календарный день и ротация должна запускаться ежедневно в 14 часов. Пусть имеется некое правило анализа, результат которого хранится в параметре A, и к 14 часам 29.01.2010 это правило сработало для некоторого узла 4 раза следующим образом:

```
19:30 28.01.2010    A=1

22:30 28.01.2010    A=2

10:22 29.01.2010    A=1

13:15 29.01.2010    A=3
```

Тогда после выполнения процедуры ротации из базы данных будут удалены 2 записи за предыдущий календарный день и останутся 2 записи за текущий день:

```
10:22 29.01.2010    A=1

13:15 29.01.2010    A=3
```

Если к следующему запуску процедуры ротации (30.01.2010) правило не сработает для данного узла ни разу, то после ротации в базе данных останется последняя запись (с результатом A=3), хотя она является устаревшей. Эта запись будет храниться в базе до тех пор, пока не сработает правило и в очередной раз не запустится процедура ротации. Например, если правило сработает в следующий раз 02.02.2010 в 10:00, то после очередной ротации устаревшая запись за 29.01.2010 будет удалена и в истории правил анализа ее не будет.

Если в файле `server.ini` вы задали размер базы данных (см. «Секция [control]» на стр. 140) существенно меньше, чем текущий, то после проведения ротации данные,

удаленные во время ротации, в системе мониторинга отображаться не будут, при этом размер базы данных реально не уменьшиться. Для реального уменьшения размера базы данных выполните следующие действия:

1. Задайте необходимые ограничения на объем информации, хранимой в базе данных. Для этого в файле `server.ini` в секции `[control]` установите необходимые значения параметров `RawDataMaxSize` и `OlapDBMaxSize`.
2. Дождитесь выполнения процедуры ротации.
3. Остановите ПО Сервер мониторинга.
4. Запустите приложение pgAdmin и на панели навигации выберите имя базы данных, затем на панели инструментов нажмите кнопку (**Выполнить пользовательские SQL запросы**).
5. В открывшемся окне на вкладке **SQL редактор** удалите на панели редактирования имеющийся текст и вставьте следующий SQL-запрос:

   ```
   vacuum full;
   ```

6. Выберите в меню **Запрос** команду **Выполнить** или нажмите на панели инструментов кнопку (**Выполнить запрос**).
7. После выполнения запроса на вкладке **SQL редактор** удалите на панели редактирования имеющийся текст и вставьте следующий SQL-запрос:

   ```
   reindex database sw_olap;
   ```

8. Размер базы данных будет уменьшен до значений, заданных в параметрах `RawDataMaxSize` и `OlapDBMaxSize`.

Запустите Сервер мониторинга.

Просмотр журнала событий

Наиболее важные события, связанные с работой Сервера мониторинга (подключение и отключение пользователей, отсутствие и восстановление соединения с сервером баз данных и другие), фиксируются в журнале, который хранится в базе данных Сервера мониторинга.

Просмотр журнала событий выполняется с помощью АРМ мониторинга под учетной записью администратора.

Для просмотра журнала событий:

1 На главной странице выберите вкладку **Журнал**. Откроется страница, на которой отображаются записи журнала, отсортированные в порядке убывания времени фиксации события.

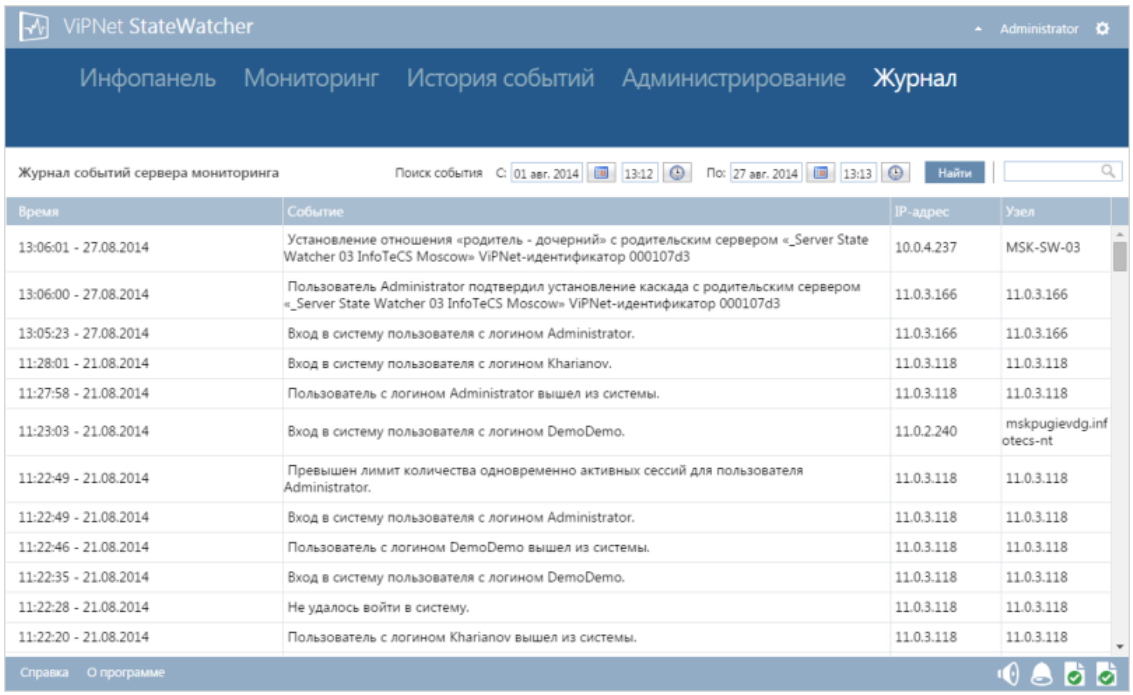

Рисунок 58: Просмотр журнала событий Сервера мониторинга

2 При необходимости отфильтруйте записи в журнале. Записи журнала можно отфильтровать по дате и времени события и/или по заданному слову в описании события.

Для фильтрации задайте начало и конец временного интервала в соответствующих полях и нажмите кнопку **Найти** или в введите искомое слово в поле поиска.

В ПК ViPNet StateWatcher фиксируются следующие события:

- подключение пользователя;
- отключение пользователя;
- прерывание пользовательской сессии;
- разрыв соединения с сервером баз данных (фиксируется только самая первая запись о разрыве соединения);
- восстановление соединения с сервером баз данных;
- разрыв соединения с SMTP-сервером;
- восстановление соединения с SMTP-сервером;
- разрыв соединения с SMS-шлюзом;
- восстановление соединения с SMS-шлюзом;
- достижение максимального количества отправленных SMS-оповещений;
- неудачная попытка отослать оповещение по SMS;
- невозможность экспортировать оповещение для Деловой почты;
- неудачная попытка отослать оповещение о срабатывании правила анализа по электронной почте;
- штатное завершение работы Сервера мониторинга;
- установление отношения «родитель — потомок»;
- отказ в установлении отношения «родитель — потомок»;
- разрыв отношения «родитель — потомок»;
- разрыв связи с дочерним Сервером мониторинга;
- восстановление связи с дочерним Сервером мониторинга;
- восстановление связи с родительским Сервером мониторинга;
- получение сообщения о штатном завершении работы Сервера мониторинга в каскаде;
- получение сообщения от дочернего Сервера мониторинга о смене родителя;
- обнаружение ошибки в синтаксисе правила анализа;
- возникновение ошибки при выполнении правила анализа;
- возникновение ошибок при экспорте необработанных параметров узлов;

- возникновение ошибок при экспорте событий мониторинга;
- применение родительского правила анализа на дочернем Сервере мониторинга;
- отмена применения родительского правила анализа на дочернем Сервере мониторинга;
- изменение лицензии Сервера мониторинга, связанное с уменьшением максимального количества узлов мониторинга;
- получение сообщения об отзыве с Сервера мониторинга прикладной задачи «Сервер мониторинга»;
- получение сообщения о прекращении регистрации в прикладной задаче «Сервер мониторинга» с родительского или дочернего Сервера мониторинга;
- получение сообщения о возврате на Сервер мониторинга прикладной задачи «Сервер мониторинга».

4

Правила анализа

Компоненты правил анализа 155

Синтаксис правил анализа 157

Проверка синтаксиса правила анализа 168

Компоненты правил анализа

Правила анализа (см. «Правило анализа» на стр. 290) состоят из следующих компонентов:

- название правила;
- код правила;
- узлы мониторинга, на которых применяется правило;
- связь правила с пользователями (см. «Создание и изменение учетной записи» на стр. 78) и шаблонами оповещений (см. «Создание и изменение шаблонов оповещений» на стр. 109);
- флаг применения на дочерних Серверах мониторинга.

Все указанные компоненты задаются администратором с помощью веб-интерфейса на странице **Список правил анализа**. Название правила и код правила являются обязательными компонентами.

В коде правила задается алгоритм выполнения правила. В нем анализируются значения параметров узлов, проверяется наличие определенных изменений в состоянии узлов или критических событий и задаются оповещения об изменениях и событиях.

Код правила содержит параметры узлов, которые можно задавать вручную или вставлять из списка параметров.

Чтобы вставить параметр из списка:

1. В главном окне на вкладке **Администрирование** перейдите на странице **Правила анализа**.
2. Создайте правило или откройте на редактирование уже созданное правило.
3. На панели просмотра введите `Params.` в поле **Редактор правила**.

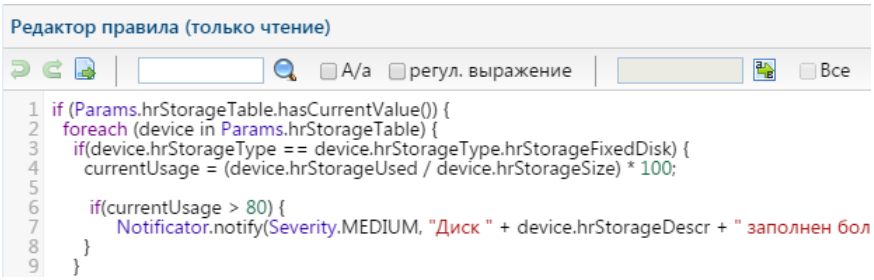

Рисунок 59: Список параметров правил анализа

4 В списке параметров дважды щелкните параметр, который нужно вставить в код правила.

Если вы хотите присвоить какое-либо значение параметру из списка, то после названия параметра установите точку, и в списке параметров выберите нужное значение. Значение для параметров, не входящих в фиксированный список, задаются вручную.

После очередного опроса узла правило выполняется последовательно для каждого из узлов мониторинга, на которых оно применяется. При каждом выполнении правила в нем анализируются параметры только одного узла мониторинга, для которого оно в данный момент выполняется.

При обнаружении события на узле формируется оповещение об этом, и в базу данных Сервера мониторинга записывается идентификатор узла мониторинга, время срабатывания правила анализа, текст оповещения, а также использованные при анализе параметры узла мониторинга. Вся эта информация доступна пользователям при просмотре истории событий мониторинга.

Для написания кода правила используется специальный язык. Допустимые конструкции этого языка и его синтаксис описаны в разделе Синтаксис правил анализа (на стр. 157).

Синтаксис правил анализа

Данный раздел содержит описание языка для составления правил анализа. В этом языке используются все основные элементы и конструкции, присутствующие в языках программирования. В описании не приводятся ключевые понятия, так как предполагается, что администратор знаком с языками shell-сценариев в ОС UNIX или пакетных файлов (`.bat`) в ОС Windows.

Переменные

Имя переменной может начинаться с символов «a»-«z», «A»-Z», «_» или «$». Далее может содержать символы «0»-«9», «a»-«z», «A»-«Z», «_» или «$». Например:

Правильно: `var1, _a99, $1`

Неправильно: `9v, !a99, 1$`

Переменная может содержать точки в имени, однако не может содержать дефисы:

Правильно: `my.dotted.var`

Неправильно: `commons-logging`

Последняя запись воспринимается как разность между переменной `commons` и `logging`.

Комментарии

Комментарий начинается с последовательности «##» и продолжается до конца строки. Например:

```
## Это комментарий
```

Типы данных

Допустимы следующие типы данных:

- целые числа;

- вещественные числа;
- строки, обрамленные либо апострофами (`'строка'`), либо кавычками (`"строка"`);
- булевские значения: `true` и `false`;
- отсутствующее или неизвестное значение: `null`.

Функции

Доступны следующие функции:

1. `empty (var)` – проверка отсутствия значения переменной `var`.

   Функция возвращает `true` в случае:

   - null;
   - пустая строка.

   В остальных случаях функция возвращает `false`.

2. `size (var)` – определение размера переменной `var`.

   Функция возвращает:

   - размер списка;
   - длину строки.

Операторы

Допустимы следующие операторы:

1. Логическое «и». Для обозначения используется `and` либо `&&`:

   ```
   cond1 and cond2
   cond1 && cond2
   ```

2. Логическое «или». Для обозначения используется `or` либо `||`:

   ```
   cond1 or cond2
   cond1 || cond2
   ```

3. Логическое «не». Для обозначения используется `not` либо `!`:

   ```
   not cond1
   !cond1
   ```

4. Двоичное «и». Для обозначения используется `&`:

```
9 & 2
1001 & 0010 = 0
```

5 Двоичное «или». Для обозначения используется `|`:

```
9 | 2
1001 | 0010 = 1011
```

6 Двоичное «исключающее или». Для обозначения используется `^`:

```
9 ^ 2
1001 ^ 0011 = 1010
```

7 Двоичное «не». Для обозначения используется `~`:

```
~9
~1001 = 0110
```

8 Равенство. Для обозначения используется `==` либо `eq`:

```
val1 == val2
val1 eq val2
```

9 Неравенство. Для обозначения используется `!=` либо `ne`:

```
val1 != val2
val1 ne val2
```

10 Меньше. Для обозначения используется `<` либо `lt`:

```
val1 < val2
val1 lt val2
```

11 Меньше либо равно. Для обозначения используется `<=` либо `le`:

```
val1 <= val2
val1 le val2
```

12 Больше. Для обозначения используется `>` либо `gt`:

```
val1 > val2
val1 gt val2
```

13 Больше либо равно. Для обозначения используется `>=` либо `ge`:

```
val1 >= val2
val1 ge val2
```

14 Сложение. Для обозначения используется `+`:

```
val1 + val2
```

15 Вычитание. Для обозначения используется `-`:

```
val1 - val2
```

16 Умножение. Для обозначения используется *:

```
val1 * val2
```

17 Деление. Для обозначения используется /:

```
val1 / val2
```

18 Целочисленное деление. Для обозначения используется `div`:

```
val1 div val2
```

19 Остаток от деления. Для обозначения используется `mod` либо `%`:

```
5 % 2 = 1
5 mod 2 = 1
```

20 Унарный оператор отрицания. Для обозначения используется `-`:

```
-42
```

21 Оператор условия. Для обозначения используется классический `if-else`:

```
if (( x * 2 ) == 5) { y = 1; } else { y = 2; }
```

22 Оператор цикла с перебором объектов. Для обозначения используется `foreach`:

```
foreach (item in list) { x = x + item; }
```

Внимание! После каждого выражения следует обязательно ставить точку с запятой «;».

Например, следующий фрагмент содержит ошибку, т.к. отсутствует точка с запятой:

```
if (Params.GIDNAMES_NAME == 'FIRST NODE') { INT_SCALE_PARAM = 5 }
```

Правильная запись:

```
if (Params.GIDNAMES_NAME == 'FIRST NODE') { INT_SCALE_PARAM = 5; }
```

Объекты и методы для доступа к значениям параметров узлов

Для доступа к значениям параметров узлов мониторинга используется объект `Params`. Для получения значения параметра используется конструкция `Params.Имя_Параметра`, например: `Params.GINFO_PVER`.

Для получения части составного значения (списков, перечислений, разделенных точкой или запятой) используется конструкция `Params.Имя_Параметра.get(Индекс)`, где `Имя_Параметра` – имя параметра, принадлежащего составному типу, `Индекс` — порядковый номер элемента, начиная с 0. Полученная часть составного значения может иметь целый или строковый тип. Типы элементов для конкретных параметров перечислены в Приложении (см. «Контролируемые параметры узлов мониторинга» на стр. 204). Например, параметр `GINFO_PVER` (версия продукта) является составным и содержит разделенные точкой три цифры версии и номер сборки (например, 1.0.0.24). Чтобы получить первую цифру текущего значения версии, нужно использовать конструкцию `Params.GINFO_PVER.get(0)`.

Объект `Params` используется также для доступа к объектам, объединенным в коллекции (см. «Коллекции» на стр. 162).

Для получения различных значений параметров узлов объект `Params` имеет следующие методы:

- `getCurrentValue()` — возвращает текущее значение параметра или коллекции (синоним – `<PARAM_NAME>`).

- `getPrevValue()` — возвращает предыдущее значение параметра или коллекции (полученное при предыдущем опросе). Если правило анализа запрашивает данные, полученные два или более опросов назад (т.е. данные, старше, чем `OldParams`), то система мониторинга выдает сообщение об ошибке. Текст сообщения фиксируется в журнале и в логах Сервера мониторинга.

  Данная ошибка может произойти если в коде правила вы задали `Params.XXX.getPrevValue().getPrevValue()`.

- `getPrevNonNullValue()` — возвращает первое доступное значение параметра или коллекции, полученное на предыдущем опросе или более ранних опросах. Если такового значения нет в базе данных Сервера мониторинга, то система мониторинга выдает сообщение об ошибке. Текст сообщения фиксируется в журнале и в логах Сервера мониторинга.

- `hasCurrentValue()` — проверка наличия текущего значения параметра или коллекции; возвращает `true`, если текущее значение есть, иначе возвращает `false`.

- `hasPrevValue()` — проверка наличия предыдущего значения параметра или коллекции; возвращает `true`, если предыдущее значение есть, иначе возвращает `false`.

- `hasPrevNonNullValue()` — проверка наличия доступного значения параметра или коллекции, полученного на предыдущем опросе или более ранних опросах; возвращает `true`, если такое значение есть, иначе возвращает `false`.

Примечание. Система мониторинга фиксирует ошибки во время срабатывания правил анализа. Ошибки сохраняются в журнале в следующем виде:

Ошибка при выполнении Правила Анализа %s на узле %s: %s,

где %s — значения: имя правила, имя узла, текст сообщения, соответствующие конкретному правилу.

Коллекции

Коллекции служат для объединения однородных объектов, которые используются для доступа к значениям множественных параметров узлов. Например, в общем случае узел имеет несколько сетевых интерфейсов, и все сетевые интерфейсы имеют одинаковые параметры. Коллекция `NETWORK` (см. ниже) объединяет объекты, используемые для доступа к значениям сетевых интерфейсов.

Поддерживаются следующие коллекции:

- `EVENTS` — коллекция объектов для доступа к записям в журналах событий ОС (в интерфейсе АРМ мониторинга — группа параметров **Журнал системных событий**).

  Среди объектов этой коллекции нет одинаковых.

- `NETWORKS` — коллекция объектов для доступа к значениям параметров сетевых интерфейсов (в интерфейсе АРМ мониторинга — группа параметров **Список сетевых интерфейсов и их характеристики**).

  Два объекта этой коллекции равны, если равны их параметры `GIFINFO_IFID`.

- `STORAGE_DEVICES` — коллекция объектов для доступа к значениям параметров устройств на узлах (в интерфейсе АРМ мониторинга — группа параметров **Диски**).

  Два объекта этой коллекции равны, если равны их параметры `GFOFSINFO_NAME`.

- `TUNNELADDRESSES` — коллекция объектов для доступа к значениям туннелируемых диапазонов (в интерфейсе АРМ мониторинга – группа параметров **Туннелируемые диапазоны**).

  Два объекта этой коллекции равны, если одновременно равны их параметры `GSERVLIST_TUNNEL_REAL_START` и `GSERVLIST_TUNNEL_REAL_END`.

Объекты, объединенные в коллекции, доступны через объект `Params`: `Params.имя_коллекции`. Например: `Params.NETWORKS`.

Для перебора объектов коллекции используется оператор цикла `foreach`. Например: `foreach (interface in Params.NETWORKS)`. Значения параметров объектов доступны через переменную, используемую в цикле. Например: `interface.GIFINFO_MODE`.

Объекты и методы для получения вспомогательных параметров

Для операций над коллекциями и получения вспомогательных параметров используется объект `Utils`, который имеет следующие методы:

- `diff(set1, set2)` — разность между коллекциями `set1` и `set2`; возвращает множество объектов из коллекции `set1`, которые не содержатся в коллекции `set2`;
- `equal(set1, set2)` — проверка равенства коллекций `set1` и `set2`; возвращает `true`, если коллекции равны поэлементно, иначе возвращает `false`;
- `intersection(set1, set2)` — пересечение коллекций `set1` и `set2`; возвращает множество объектов, одновременно содержащихся в обеих коллекциях;
- `union(set1, set2)` — объединение (сумма) коллекций `set1` и `set2`; возвращает множество объектов, содержащихся в обеих коллекциях;
- `getTaskName(task)` — получение имени прикладной задачи, в которой зарегистрирован узел мониторинга, по идентификатору задачи, указанному в параметре `task`;
- `getLastRequestDate()` — получение объекта, содержащего дату и время последнего опроса узла Сервером мониторинга (локализованные по часовому поясу Сервера мониторинга). Этот объект, в свою очередь, имеет следующие методы:
  - `getYear()` — возвращает год;
  - `getMonth()` — возвращает месяц: от 1 (январь) до 12 (декабрь);
  - `getDay()` — возвращает номер дня (от 1 до 31);
  - `getDayOfWeek()` — возвращает день недели: от 1 (понедельник) до 7 (воскресенье);
  - `getHours()` — возвращает часы (от 0 до 23);
  - `getMinutes()` — возвращает минуты (от 0 до 59).

  Обращение к этим методам возможно как непосредственно через объект `Utils`, так и через вспомогательную переменную. Например, чтобы получить минуты последнего опроса, можно использовать следующие формы записи:

  ```
  time = Utils.getLastRequestDate().getMinutes();
  ```

или

```
date = Utils.getLastRequestDate();
time = date.getMinutes();
```

Объект для доступа к уровням критичности

Для задания уровня критичности в оповещениях используется объект `Severity`. Этот объект содержит все возможные уровни критичности:

- `HIGH` — высокий уровень;
- `MEDIUM` — средний уровень;
- `LOW` — низкий уровень;
- `INFO` — информационное сообщение.

Уровень критичности указывается в виде `Severity.значение`, например: `Severity.INFO`.

Объекты и методы для задания оповещений

Для задания всех видов оповещений используется объект `Notificator`, имеющий один метод `notify`:

```
notify(Int level, String message)
```

В параметре `level` задается уровень критичности, в параметре `message` указывается текст сообщения.

Уровень критичности можно задать одним из двух способов:

- как одно из допустимых значений объекта `Severity` (от `HIGH` до `INFO`);
- как число от 1 до 4, этим значениям соответствуют следующие уровни критичности:
  - `1` — высокий уровень;
  - `2` — средний уровень;
  - `3` — низкий уровень;
  - `4` — информационное сообщение.

Текст сообщения можно задать непосредственно строкой или через переменную. Например:

```
Notificator.notify(Severity.HIGH, 'Сообщение');
```

или

```
message = "Сообщение";
Notificator.notify(1, message);
```

Объекты и методы для записи сообщений в журнал для правил анализа

Для записи сообщений в отладочный журнал для правил анализа используется объект `Logger`. Журнал для правил анализа хранится в файле, заданном параметром `AnalyzeDebugLogPath` секции `[control]` в файле конфигурации `server.ini` (см. «Тонкая настройка Сервера мониторинга» на стр. 137).

Для протоколирования используются одноименные с уровнем протоколирования методы (записанные в нижнем регистре) со строковым параметром `message`, в котором задается текст сообщения:

- `Logger.debug(String message)`
- `Logger.error(String message)`
- `Logger.info(String message)`
- `Logger.warn(String message)`

Например:

```
Logger.info("Параметр param1 принял значение " + param1);

Logger.error("Правило test_rule_1: значение параметра test_param_1 больше
5!");
```

Примеры синтаксиса

- Пример присвоения значения строковой переменной:

  ```
  STR_SCALE_PARAM = 'ERROR OCCURED';
  ```

- Пример получения текущего состояния программного компонента ViPNet Монитор:

  ```
  Status = Params.MONITOR_STATUS;
  ```

- Пример синтаксиса для получения части составного значения:

```
MajorNumber = Params.GINFO_PVER.get(0);
```

Параметр GINFO_PVER является составным и содержит разделенные точкой три цифры версии и номер сборки ПО ViPNet. Приведенный пример демонстрирует получение из списка первой цифры версии.

- Пример ветвления:

```
if ((Params.GINFO_TYPE == 0) || (Params.GIDNAMES_NAME eq 'Expected
Node'))
{ INT_SCALE_PARAM = 2; }
else if (Params.GINFO_TYPE == 1)
{ INT_SCALE_PARAM = 1; }
else { INT_SCALE_PARAM = 3; }
```

В первом условии проверяются значения параметров GINFO_TYPE (тип сетевого узла) и GIDNAMES_NAME (название сетевого узла). Если тип сетевого узла равен 0 или опрашиваемый узел называется «Expected Node», то целочисленному параметру INT_SCALE_PARAM присваивается значение 2, иначе рассматривается второе условие — равенство параметра GINFO_TYPE единице. Если второе условие выполняется, то параметру INT_SCALE_PARAM присваивается значение 1, иначе присваивается значение 3.

- Пример получения предыдущего или текущего (в зависимости от типа узла) значения времени на узле:

```
if (Params.GINFO_TYPE == 0)
{
     scale_time = Params.GINFO_TIME_LOC.getPrevValue();
}
else
{
     scale_time = Params.GINFO_TIME_LOC;
}
```

- Пример цикла:

```
foreach (interface in Params.NETWORKS)
{
     test_param = test_param + interface.GIFSTAT_RECV_ENC_PASS;
}
```

В цикле выполняется перебор всех интерфейсов, имеющихся на узле. При этом локальная переменная interface на каждой итерации цикла содержит очередной объект из коллекции NETWORKS для доступа к параметрам соответствующего сетевого интерфейса. Параметр GIFSTAT_RECV_ENC_PASS содержит количество зашифрованных пакетов, полученных на данном интерфейсе. В результате переменная test_param будет содержать сумму полученных зашифрованных пакетов по всем интерфейсам.

- Пример правила анализа, которое проверяет связь координатора с другими координаторами:

```
if(Params.Connections.hasCurrentValue() &&
Params.Connections.hasPrevNonNullValue()) {
     foreach(node in Params.Connections) {
            if (!node.NODE_STATUS && node.NODE_STATUS.
PrevNonNullValue() ) {
            Notificator.notify(Severity.INFO, "Узел " +Params.
GIDNAMES_NAME + " потерял связь с узлом " + node.NODE_NAME+ "  ViPNet
ID "+ Params.GIDNAME_ID);
            }
     }
}
```

Проверка синтаксиса правила анализа

Перед сохранением правила анализа заданный в нем код правила проверяется на соответствие следующим требованиям:

- Код правила должен соответствовать синтаксису языка (см. «Синтаксис правил анализа» на стр. 157).
- В коде правила могут использоваться только допустимые объекты (`Params`, `Network`, `StorageDevice`, `Events`, `TunnelAddresses`, а также объекты `Notificator` и `Logger`).
- Оператор `foreach` может применяться только к объектам `Params`, `Network`, `StorageDevices`, `Events`, `TunnelAddresses`.
- В объектах `Notificator` и `Logger` могут использоваться только допустимые методы (`notify` для объекта `Notificator` и `debug`, `error`, `info`, `warn` для объекта `Logger`).
- Функция `get(Индекс)` может применяться только к составным параметрам для получения части значения, соответствующей заданному индексу.

5

Резервное копирование и восстановление

Порядок проведения резервного копирования 170

Резервирование и восстановление конфигурационных файлов и отладочных журналов 171

Резервирование баз данных 172

Восстановление баз данных 179

Проверка корректности восстановления 189

Порядок проведения резервного копирования

Резервирование информации осуществляется с целью возможности восстановления всех данных, хранящихся на Сервере мониторинга, и конфигурационного файла Сервера мониторинга в случае каких-либо сбоев. Резервное копирование необходимо выполнять регулярно, чтобы исключить потерю большого объема информации.

К файлам, подлежащим резервированию, относятся файл конфигурации Сервера мониторинга и файлы, содержащие отладочные журналы. Резервирование файлов и их восстановление осуществляется штатными средствами операционной системы, путем их копирования (см. «Резервирование и восстановление конфигурационных файлов и отладочных журналов» на стр. 171).

Данные, собранные в процессе мониторинга сети, история событий и расположение объектов мониторинга на географической карте хранятся в базах данных. Резервирование баз данных осуществляется с помощью приложения pgAdmin – средства для администрирования баз данных СУБД PostgreSQL. Это приложение входит в состав ПО PostgreSQL версии 9.1.x и находится в папке установки этого ПО. Порядок резервирования баз данных приведен в разделе Резервирование баз данных (на стр. 172).

Для восстановления баз данных из резервных копий используются процедуры, описанные в разделе Восстановление баз данных (на стр. 179) . Восстановление осуществляется с помощью приложения pgAdmin и может быть выполнено с переустановкой ПО Сервер мониторинга или без нее. Процедура восстановления без переустановки ПО более трудоемкая, так как перед собственно восстановлением данных требуется создать базы данных и все объекты, необходимые для их обслуживания. В случае переустановки ПО Сервер мониторинга требуется выполнить только восстановление данных, базы данных в этом случае будут созданы автоматически в процессе установки ПО.

Резервирование и восстановление конфигурационных файлов и отладочных журналов

Конфигурационные файлы и отладочные журналы представляют собой текстовые файлы. Для резервирования файлов достаточно скопировать их в папку, в которой вы хотите хранить резервные копии. Для надежного хранения рекомендуется перенести резервные копии файлов на другие носители информации (флэш-память, сетевой диск и другие).

В целях резервирования следует скопировать следующие файлы:

- Файл `server.ini`, содержащий параметры настройки Сервера мониторинга.

  Этот файл находится в каталоге `\Tomcat_dir\webapps\ROOT\WEB-INF\classes`, где `Tomcat_dir` – каталог установки Apache Tomcat.

- Файл, содержащий основной отладочный журнал.

  Имя этого файла и его расположение заданы параметром `MainLogPath` в файле `server.ini`. По умолчанию этот параметр установлен в значение `logs\statewatcher.log`, то есть файл с отладочным журналом называется `statewatcher.log` и расположен в папке `logs` каталога установки Apache Tomcat.

- Файл, содержащий отладочный журнал для правил анализа.

  Имя этого файла и его расположение заданы параметром `AnalyzeDebugLogPath` в файле `server.ini`. По умолчанию этот параметр установлен в значение `logs\analyze-debug.log`, то есть файл с журналом для правил анализа называется `analyze-debug.log` и расположен в папке `logs` каталога установки Apache Tomcat.

Для восстановления конфигурационных файлов и отладочных журналов необходимо скопировать резервные копии файлов в соответствующие папки.

Резервирование баз данных

Резервирование баз данных осуществляется с помощью приложения pgAdmin http://www.pgadmin.org/. Для создания резервной копии необходимо в приложении pgAdmin подключиться к базе данных PostgreSQL с использованием учетной записи `postgres` и пароля к ней (задается во время установки), затем задать параметры резервирования и сохранить созданную копию в надежном месте. Резервные копии создаются для базы данных мониторинга и для базы данных ГИС.

Чтобы создать резервную копию одной из баз данных:

1 Запустите приложение pgAdmin. Для этого:

1.1 В меню **Пуск** выберите **Все программы > PostgreSQL 9.1 > pgAdmin III**. Откроется главное окно приложения.

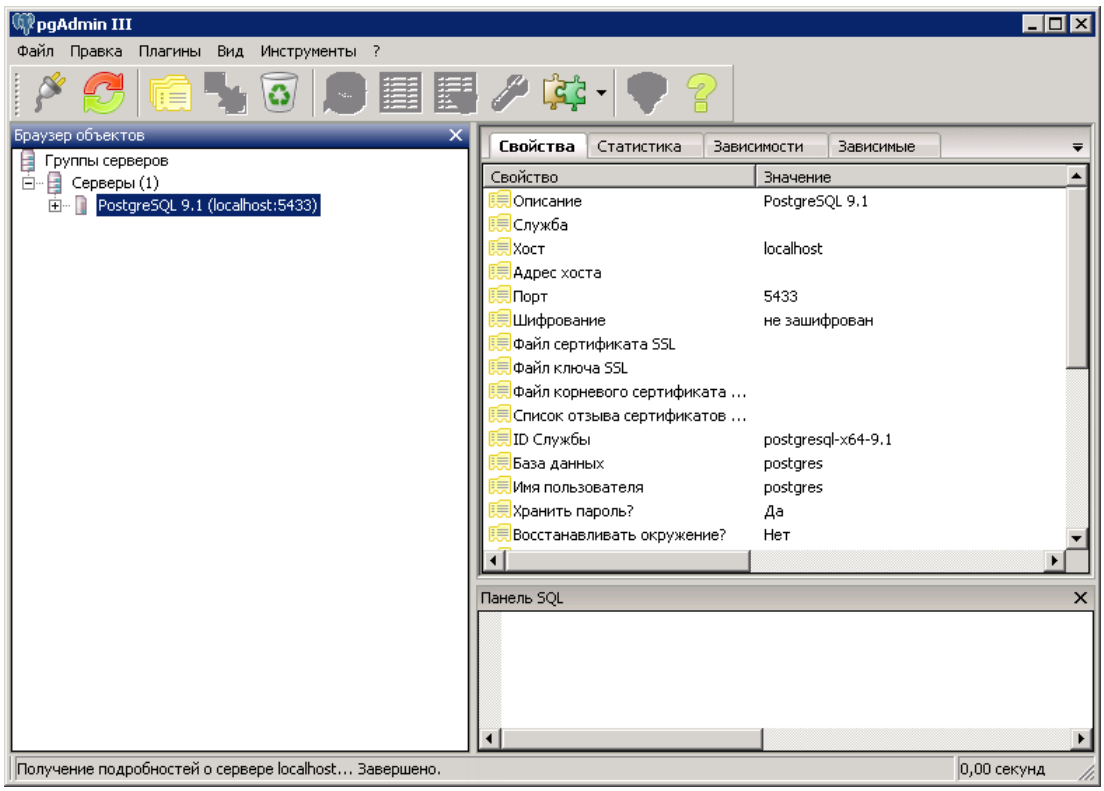

Рисунок 60: Главное окно приложения pgAdmin

В левой части главного окна отображается сервер, на котором расположены базы данных ПК ViPNet StateWatcher. После имени **PostgreSQL 9.1** в скобках указаны параметры доступа к серверу, которые были заданы при установке или

обновлении ПО Сервер мониторинга (по умолчанию `localhost:5432`). Для подсоединения к серверу дважды щелкните его имя, появится окно для ввода пароля пользователя баз данных.

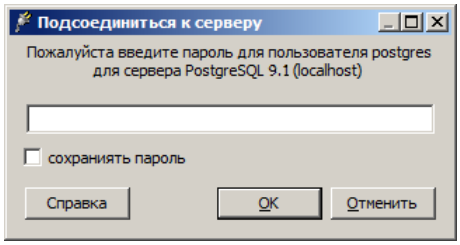

Рисунок 61: Ввод пароля пользователя баз данных

1.1 Введите пароль, который был задан при установке или обновлении ПО Сервер мониторинга. Чтобы при следующих обращениях к серверу подсоединение происходило автоматически, установите флажок **сохранять пароль**.

После успешного подсоединения к серверу в левой части главного окна появится список объектов, находящихся на сервере.

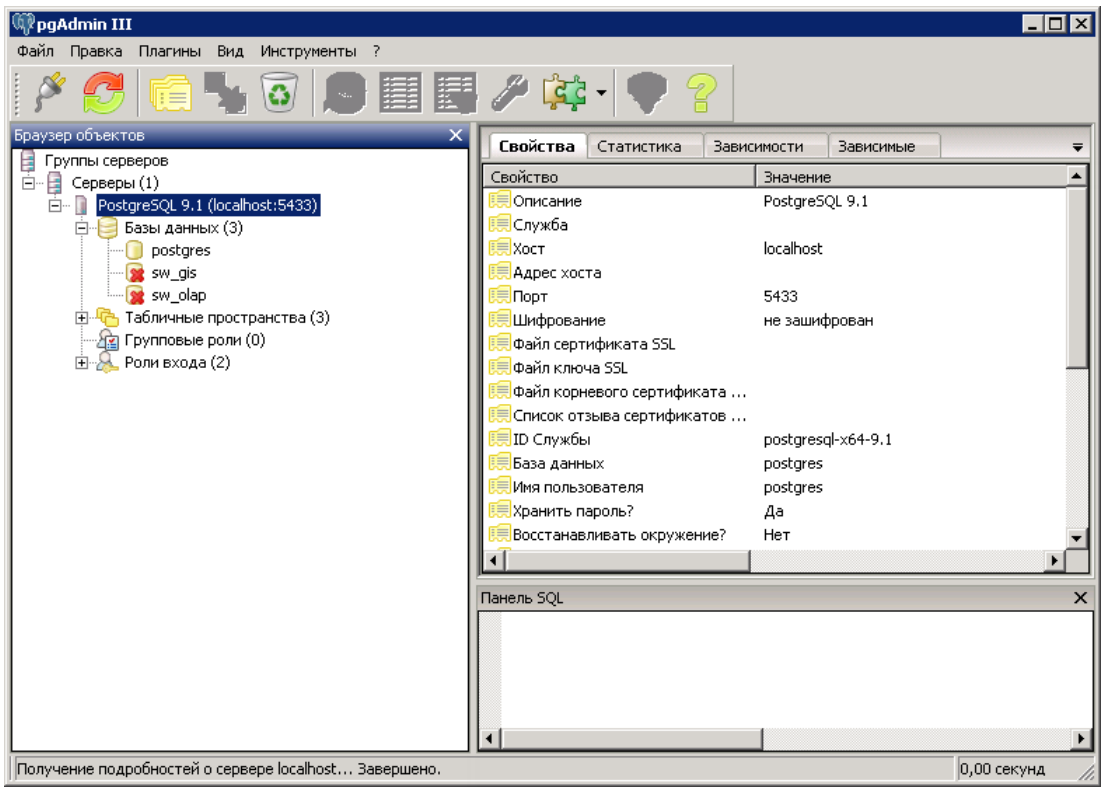

Рисунок 62: Структура объектов на сервере БД

Базы данных содержатся под элементом списка **Базы данных**. По умолчанию базы данных называются `sw_gis` (база данных ГИС) и `sw_olap` (база данных

мониторинга). Если при установке ПО Сервер мониторинга эти базы были названы иначе, в списке отобразятся соответствующие названия.

2 Щелкните в списке имя базы данных и выберите в контекстном меню команду **Резервная копия**.

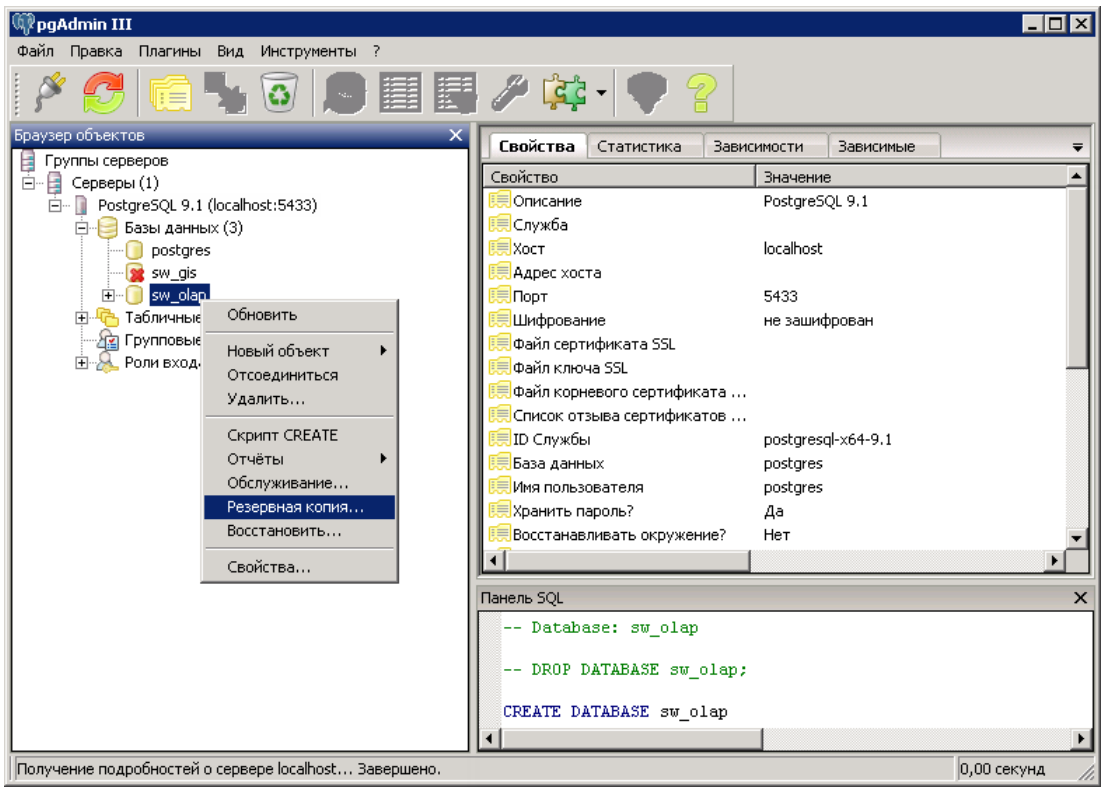

Рисунок 63: Команда для создания резервной копии базы данных

3 В открывшемся окне задайте параметры резервирования:

- В поле **Имя файла** задайте имя файла для резервной копии. Чтобы задать расположение файла, нажмите кнопку справа от поля.
- В списке **Формат** выберите формат `Tar`. Значения остальных параметров оставьте по умолчанию.

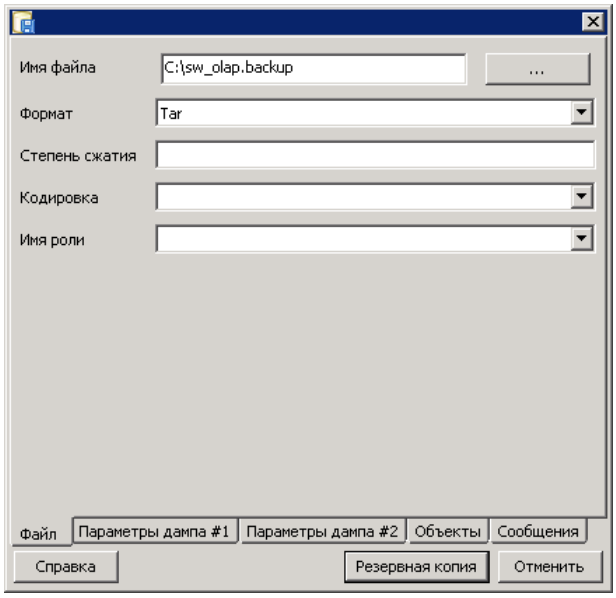

Рисунок 64: Задание параметров резервирования

4 Нажмите кнопку **Резервная копия** для начала резервирования. Если файл резервной копии с таким именем уже существует, появится запрос о его замене. В окне запроса нажмите кнопку **Да**.

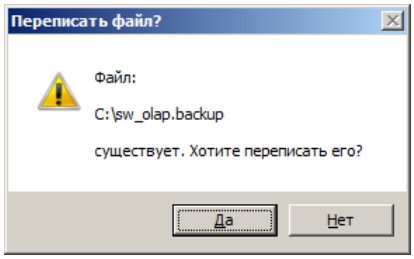

Рисунок 65: Запрос о замене файла

5 В случае успешного завершения создания резервной копии название кнопки **Резервная копия** изменится на **Завершено**. Результат резервирования и сообщения о ходе его выполнения можно посмотреть на вкладке **Сообщения**. При успешном создании резервной копии сообщения должны заканчиваться строкой «Процесс вернул код выхода 0». Чтобы закрыть окно резервирования, нажмите кнопку **Завершено**.

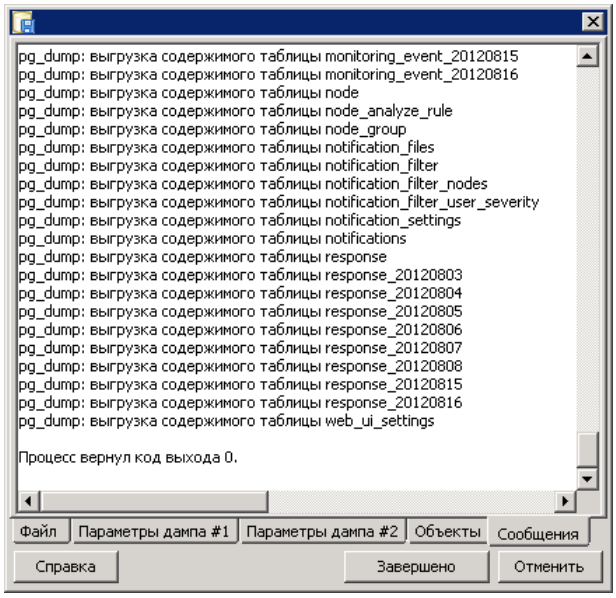

Рисунок 66: Завершение резервирования

В результате будет создана резервная копия базы данных мониторинга.

Внимание! Создайте резервные копии всех баз данных. Для надежности скопируйте резервные копии на другие носители информации (флэш-память, сетевой диск и другие).

Определение основных показателей базы данных мониторинга

Основные показатели базы данных мониторинга используются при проверке корректности восстановления (см. «Проверка корректности восстановления» на стр. 189). К этим показателям относятся общее количество контролируемых сетевых интерфейсов, правил анализа, связей узлов с правилами анализа, а также количество записей в базе данных мониторинга. Определение основных показателей осуществляется с помощью приложения pgAdmin.

Чтобы получить основные показатели базы данных мониторинга:

1 Выберите в списке имя базы данных мониторинга (по умолчанию `sw_olap`), затем на панели инструментов нажмите кнопку (**Выполнить пользовательские SQL запросы**).

2 В открывшемся окне на вкладке **SQL редактор** удалите на панели редактирования имеющийся текст и вставьте следующий SQL-запрос:

```
select 'node = ' || count(n.id) as factor from node n
union
select 'analyze_rules = ' || count(id) from analyze_rule
union
select 'analyze_rules_to_nodes = ' || count(*) from node_analyze_rule
union
select 'value_history = '||count(id) as vhistory from monitoring_event;
```

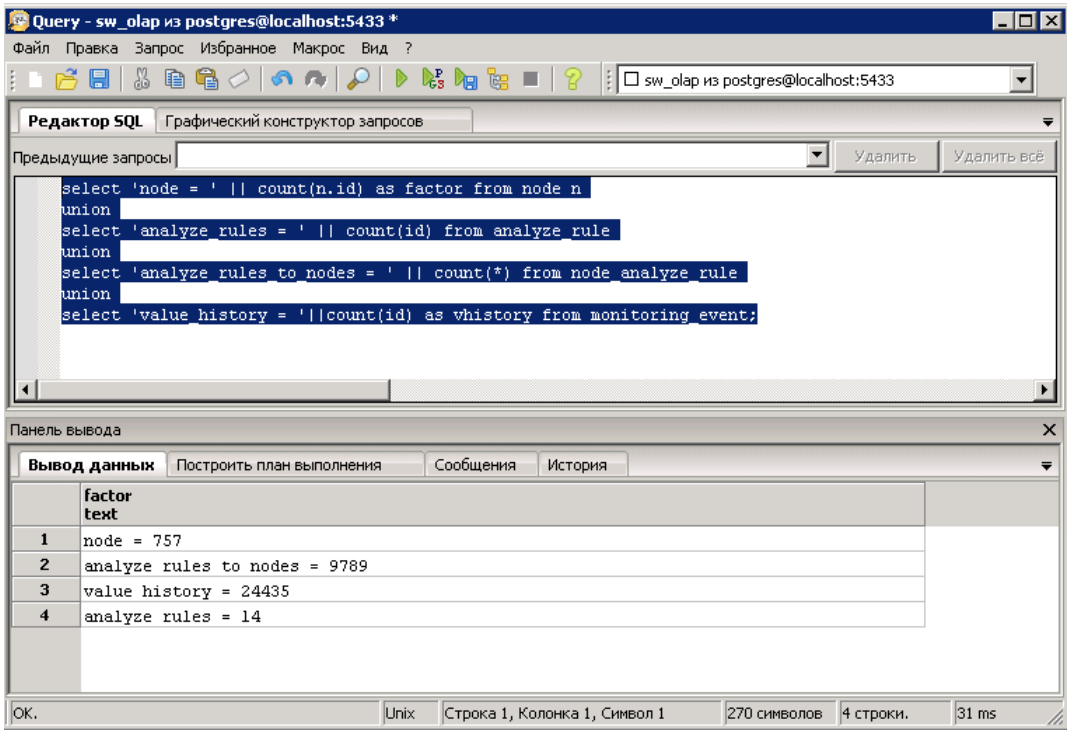

Рисунок 67: SQL-запрос для определения основных показателей базы данных мониторинга

3 Выберите в меню **Запрос** команду **Выполнить** или нажмите на панели инструментов кнопку (**Выполнить запрос**).

4 На панели вывода на вкладке **Вывод данных** появится результат выполнения запроса:

- `node` — количество узлов мониторинга;
- `analyze_rule` — количество правил анализа;
- `analyze_rule_to_node` — количество связей узел-правило;

- `value_history` — количество записей в базе данных мониторинга (то есть общее количество записей с необработанными параметрами и записей с основными данными, полученными после обработки).

5 Перепишите полученные значения и сохраните их для последующего сравнения с аналогичными данными с целью проверки корректности восстановления.

Восстановление баз данных

При возникновении проблем, связанных с работой ПК ViPNet StateWatcher, может потребоваться восстановить данные, собранные в процессе мониторинга и полученные в результате обработки. Восстановление баз данных может быть выполнено одним из способов, выбор которого зависит от характера возникших неполадок:

- Если возникли проблемы, связанные с базами данных, при этом ПО Сервер мониторинга функционирует нормально, необходимо заново создать базы данных ПК ViPNet StateWatcher и восстановить в них данные из резервных копий. Этот способ описан в разделе Восстановление баз данных без переустановки ПО Сервер мониторинга (на стр. 179).

- Если нарушено функционирование Сервера мониторинга, необходимо заново установить ПО, а затем восстановить данные из резервных копий. Установка ПО Сервер мониторинга подробно описана в разделе Первичная установка ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47). Восстановление баз данных для этого случая описано в разделе Восстановление баз данных после установки ПО Сервер мониторинга (на стр. 188).

Восстановление баз данных, как и их резервирование, осуществляется с помощью приложения pgAdmin (см. «Резервирование баз данных» на стр. 172).

Восстановление баз данных без переустановки ПО Сервер мониторинга

Чтобы восстановить базы данных без переустановки ПО Сервер мониторинга, требуется заново создать базы данных и все объекты, необходимые для их обслуживания. К таким объектам относятся:

- пользователь баз данных с произвольным именем и правами на создание других объектов;

- табличное пространство с фиксированным именем `sw_olap_tbls`, необходимое для таблиц базы основных данных (OLAP).

После создания указанных объектов нужно создать две базы данных ПК ViPNet StateWatcher – одну базу для хранения данных мониторинга (база данных мониторинга) и одну базу для хранения координат объектов мониторинга на карте (база данных ГИС).

Для каждой базы можно задать произвольное имя. Затем необходимо для каждой из созданных баз данных провести восстановление из резервной копии.

Создание и восстановление баз данных выполняется в следующей последовательности:

1 В списке объектов щелкните элемент **Роли входа** и выберите в контекстном меню команду **Новая роль**.

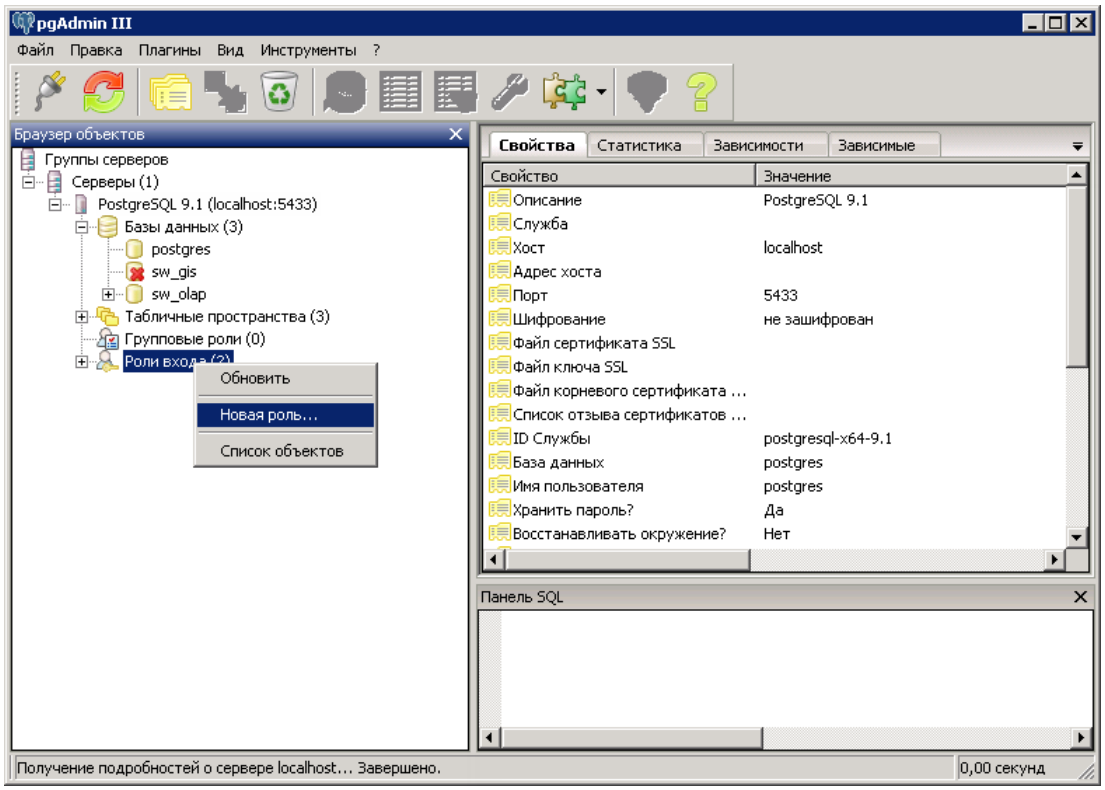

Рисунок 68: Команда для создания нового пользователя

2 В открывшемся окне задайте свойства пользователя:

- На вкладке **Свойства** в поле **Имя роли** задайте имя пользователя (например, `swadmin`).
- На вкладке **Определение** в полях **Пароль** и **Подтверждение** задайте пароль пользователя.
- На вкладке **Привилегии роли** установите флажок **Может создавать объекты базы**.

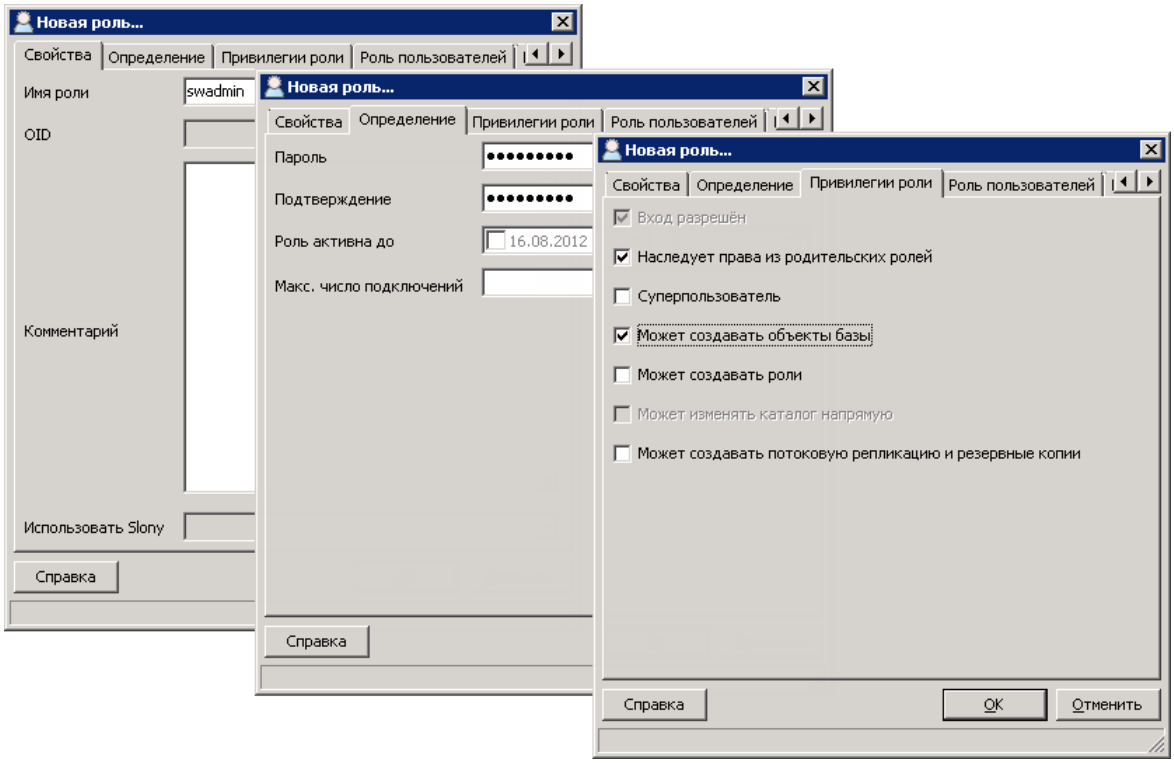

Рисунок 69: Задание свойств пользователя

Значения остальных параметров оставьте по умолчанию.

Нажмите кнопку **OK** для создания нового пользователя. Созданный пользователь появится под элементом списка **Роли входа**.

3 В списке объектов щелкните элемент **Табличные пространства** и выберите в контекстном меню команду **Новый tablespace**.

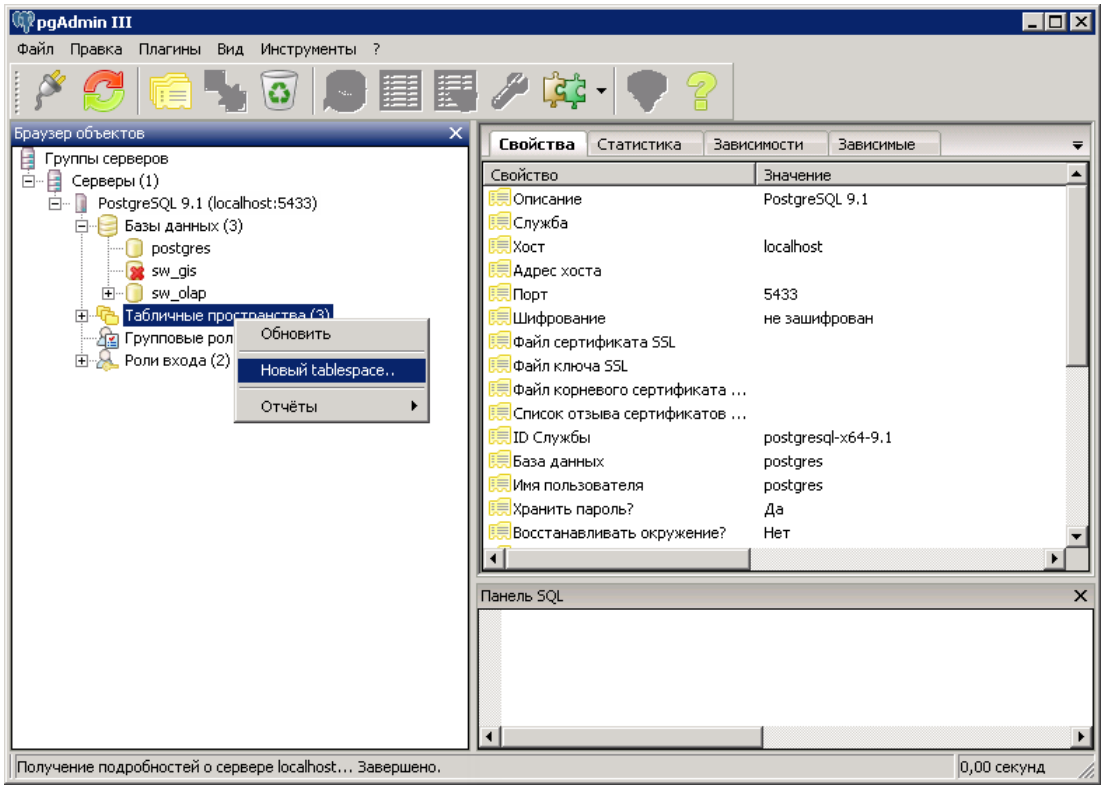

Рисунок 70: Команда для создания нового tablespace (табличного пространства)

4 В открывшемся окне задайте свойства табличного пространства для таблиц базы данных мониторинга:

- На вкладке **Свойства** в поле **Имя** задайте `sw_olap_tbls`, в поле **Владелец** выберите из списка пользователя, созданного на шаге 2.
- На вкладке **Определение** в поле **Местонахождение** задайте расположение табличного пространства (папку).

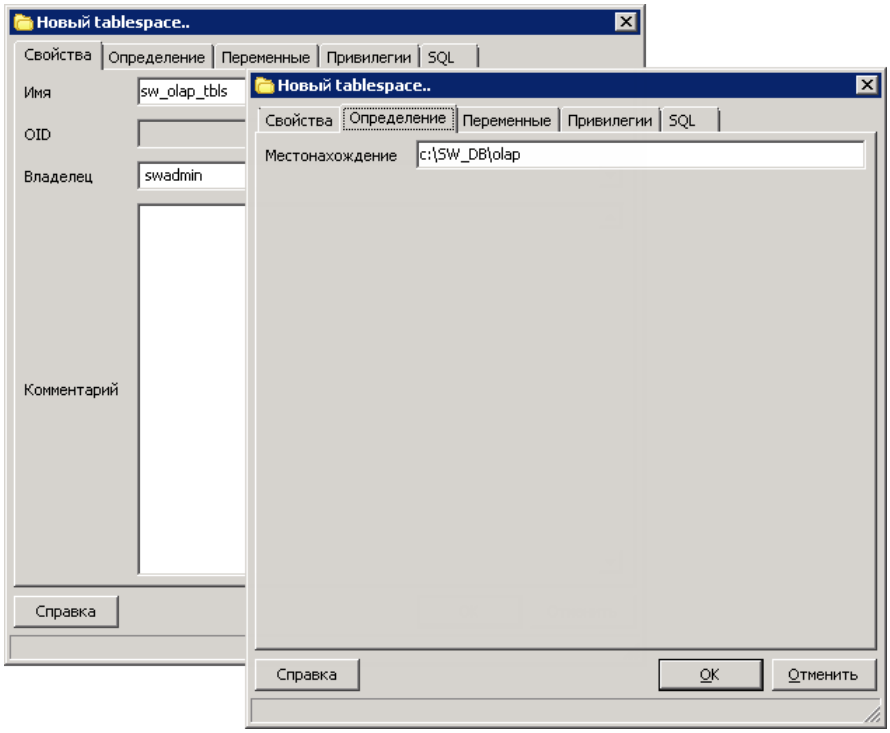

Рисунок 71: Задание свойств tablespace (табличного пространства)

Значения остальных параметров оставьте по умолчанию.

Нажмите кнопку **OK** для создания нового табличного пространства. Табличное пространство `sw_olap_tbls` появится под элементом списка **Табличные пространства**.

5 Проверьте, чтобы у пользователя `postgres` были права полного доступа (**Full Control**) к папке, заданной для табличного пространства `sw_olap_tbls`. Если это не так, разрешите этому пользователю полный доступ (см. «Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows» на стр. 257).

6 В списке объектов щелкните элемент **Базы данных** и выберите в контекстном меню команду **Новая база данных**.

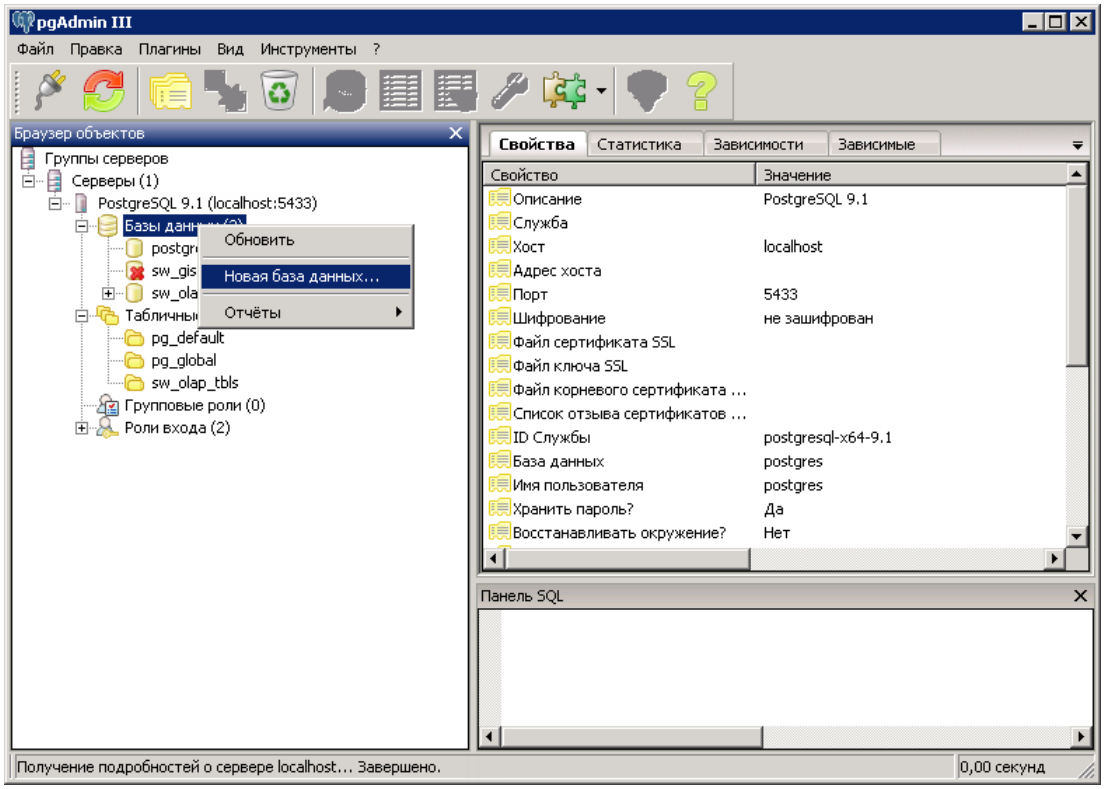

Рисунок 72: Команда для создания новой базы данных

7 В открывшемся окне задайте свойства базы данных мониторинга:

- На вкладке **Свойства**:
  - В поле **Имя** задайте имя базы данных (например, `sw_olap`).
  - В поле **Владелец** выберите из списка пользователя, созданного на шаге 2.
- На вкладке **Определение**:
  - В поле **Кодировка** выберите из списка значение **UTF8**.
  - В поле **Табличное пространство** выберите из списка значение **sw_olap_tbls**.
  - В поле **Сопоставление** выберите из списка значение **Russian_Russia.1251**.
  - В поле **Тип символа** выберите из списка значение **Russian_Russia.1251**.

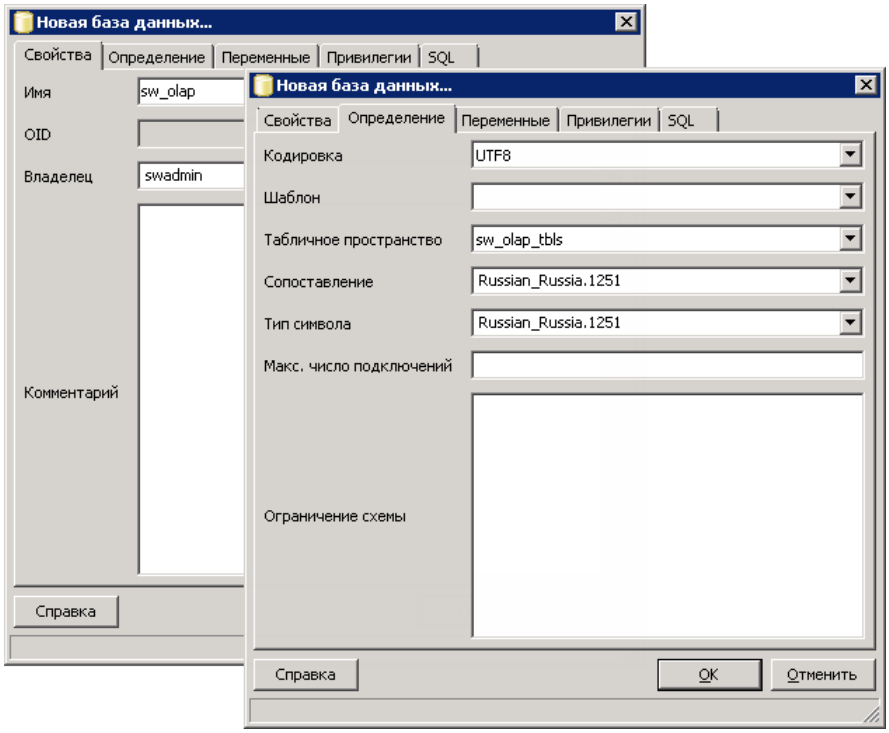

Рисунок 73: Задание свойств базы данных

Значения остальных параметров оставьте по умолчанию.

Нажмите кнопку **OK** для создания новой базы данных. Созданная база данных появится под элементом списка **Базы данных**.

8 Повторите шаги 6-7 для создания базы данных ГИС:

- На вкладке **Свойства**:
  - В поле **Имя** задайте имя базы данных (например, `sw_gis`).
  - В поле **Владелец** выберите из списка пользователя, созданного на шаге 2.
- На вкладке **Определение**:
  - В поле **Кодировка** выберите из списка значение **UTF8**.
  - В поле **Табличное пространство** выберите из списка значение **pg_default**.
  - В поле **Сопоставление** выберите из списка значение **Russian_Russia.1251**.
  - В поле **Тип символа** выберите из списка значение **Russian_Russia.1251**.

9 Щелкните в списке имя базы данных мониторинга, созданной на шаге 7, и выберите в контекстном меню команду **Восстановить**.

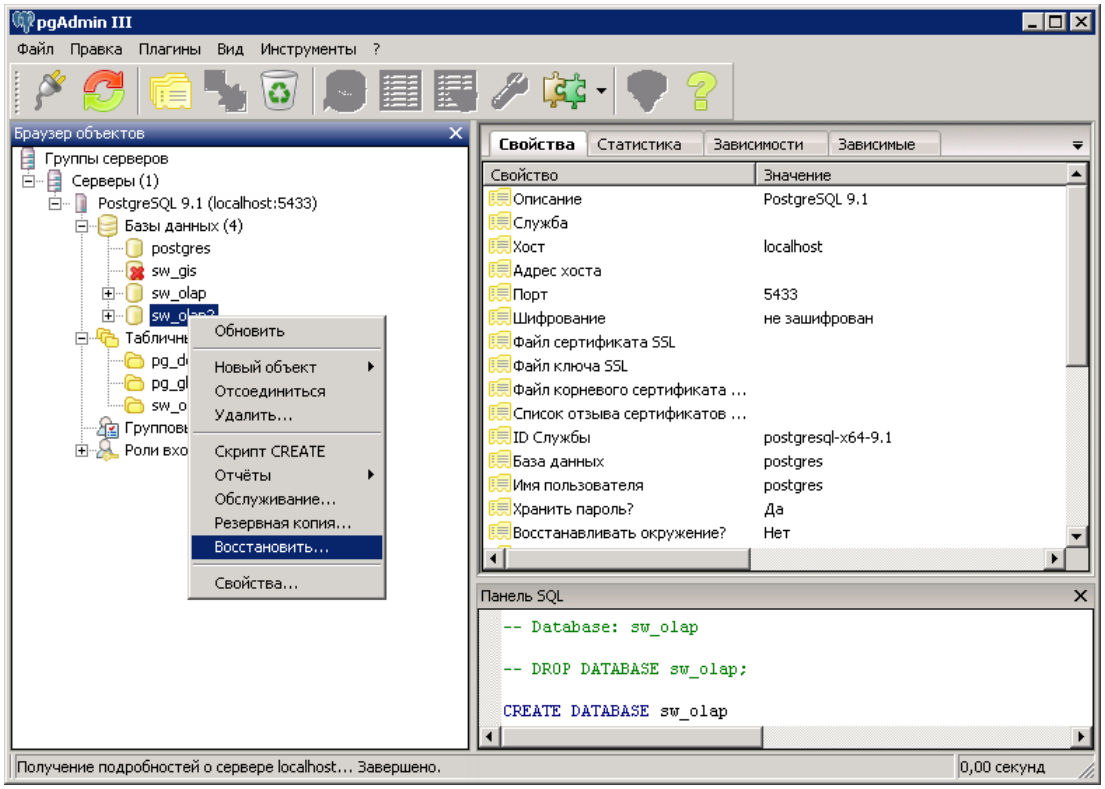

Рисунок 74: Команда для восстановления базы данных

10 В открывшемся окне задайте параметры восстановления:

- В поле **Имя файла** задайте имя файла, содержащего резервную копию базы данных мониторинга. Чтобы найти нужный файл, нажмите кнопку справа от поля.
- Значения остальных параметров оставьте по умолчанию.

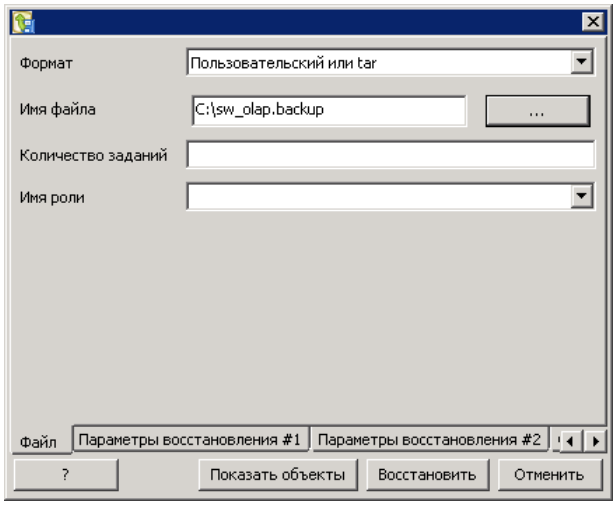

Рисунок 75: Задание параметров восстановления

11 Нажмите кнопку **Восстановить** для начала восстановления базы данных. В случае успешного завершения восстановления название кнопки **Восстановить** изменится на **Завершено**. Результат восстановления и сообщения о ходе его выполнения можно посмотреть на вкладке **Сообщения**. При успешном восстановлении базы данных сообщения должны заканчиваться строкой «Процесс вернул код выхода 0». Чтобы закрыть окно восстановления, нажмите кнопку **Завершено**.

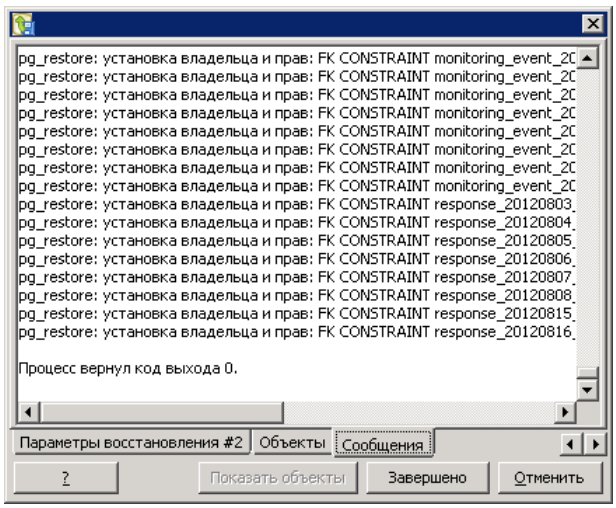

Рисунок 76: Завершение восстановления

12 Повторите шаги 9-11 для восстановления базы данных ГИС, созданной на шаге 8.

В результате базы данных мониторинга и ГИС будут восстановлены.

Восстановление баз данных после установки ПО Сервер мониторинга

В процессе установки ПО Сервер мониторинга в СУБД PostgreSQL создаются все необходимые объекты, в том числе базы данных ПК ViPNet StateWatcher. В этом случае задача по восстановлению баз данных упрощается: с помощью приложения pgAdmin достаточно выполнить только восстановление.

Подробное описание порядка установки ПО Сервер мониторинга содержится в разделе Первичная установка ПО Сервер мониторинга (см. «Установка ПО Сервер мониторинга» на стр. 47). Перед началом установки необходимо создать папку, в которой будут храниться таблицы базы данных мониторинга, и установить этой папке права полного доступа для пользователя `postgres`. Эта папка определяет расположение табличных пространств и будет запрошена в процессе установки. В ходе самой установки создаются следующие объекты и базы данных:

- пользователь баз данных с произвольным именем (по умолчанию предлагается имя `swadmin`);
- база данных мониторинга (по умолчанию предлагается имя `sw_olap`);
- база данных ГИС (по умолчанию предлагается имя `sw_gis`);
- размещение (сервер) баз данных (по умолчанию предлагается `localhost:5432`).

После завершения установки ПО в приложении pgAdmin появится заданный при установке сервер, а в списке его объектов будут присутствовать созданные базы данных (с именами, указанными при установке). Для восстановления баз данных надо выполнить шаги 9-12, описанные в разделе Восстановление баз данных без переустановки ПО Сервер мониторинга (на стр. 179).

Проверка корректности восстановления

Для проверки корректности проведенного восстановления и работоспособности Сервера мониторинга после восстановления можно использовать следующие способы:

1. Визуальный контроль на АРМ мониторинга.

   Проверьте присутствие узлов мониторинга в списке и на карте, наличие параметров узлов (IP-адрес, текущее время, время последнего опроса и другие). Произведите выборочный опрос узлов и убедитесь в изменении параметров в результате опроса (например, в изменении текущего времени на узле).

2. Проверка основных показателей базы данных мониторинга с помощью SQL-запроса.

   С помощью приложения pgAdmin выполните такой же SQL-запрос, как при резервировании баз данных (см. «Определение основных показателей базы данных мониторинга» на стр. 176). Полученные значения должны совпадать с теми, которые были определены при последнем резервировании.

A

Возможные неполадки и способы их устранения

В данном приложении приведены возможные неполадки при работе с ПК ViPNet StateWatcher и способы их устранения.

Не удается установить или запустить PostgreSQL

Описание:

- При установке PostgreSQL появляется сообщение об ошибке, при этом программа устанавливается.
- После установки PostgreSQL не запускается.

Способ устранения:

- Перед установкой PostgreSQL на компьютер рекомендуется принять и установить все важные обновления ОС Windows.
- Удалите программу PostgreSQL средствами ОС, используя панель управления (удаление программы). Удалите папку установки PostgreSQL (по умолчанию располагается в папке `C:\Program Files`). Удалите из системы пользователя `postgres` (если он появился в системе).

  После удаления заново установите PostgreSQL.

Подробную информацию о типичных ошибках при установке PostgreSQL и рекомендации по их решению см. на сайте http://wiki.postgresql.org/wiki/Running_%26_Installing_PostgreSQL_On_Native_Windows#Common_installation_errors. В случае возникновения других ошибок, связанных с установкой или работой PostgreSQL, см. документацию на сайте http://archives.postgresql.org/.

Описание:

- Сервис PostgreSQL не запускается во время установки ПО Сервер мониторинга. При этом программа установки ViPNet StateWatcher не может подключиться к базе данных.

Способ устранения:

1 Перед установкой ПО Сервер мониторинга переназначьте пользователю `postgres` права доступа к папке, в которой хранится база данных Сервера мониторинга (см. «Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows» на стр. 257).

2 Переназначьте пользователю `postgres` право «Вход в качестве службы». Для этого выполните следующие действия:

2.1 В меню **Пуск** выберите **Панель управления**.

2.2 На странице **Настройка параметров компьютера** выберите пункт **Администрирование**.

2.3 В появившемся окне дважды щелкните ярлык **Локальная политика безопасности** .

2.4 В окне **Локальная политика безопасности** на панели навигации выберите раздел **Локальные политики** > **Назначение прав пользователя**.

2.5 На панели просмотра дважды щелкните политику **Вход в качестве службы**.

2.6 В окне **Свойства: Вход в качестве службы** выберите пользователя `postgres` и нажмите кнопку **Удалить**.

2.7 Нажмите кнопку **Добавить пользователя или группу**.

2.8 В появившемся окне в поле **Введите имена выбираемых объектов** введите имя пользователя `postgres` и нажмите кнопку **OK**.

2.9 Нажмите кнопку **OK**.

3 Удалите пользователя `postgres` из групп Users и Administrators. Для этого выполните следующие действия:

3.1 В меню **Пуск** выберите **Панель управления**.

3.2 На странице **Настройка параметров компьютера** выберите пункт **Администрирование**.

3.3 В появившемся окне дважды щелкните ярлык **Управление компьютером** .

3.4 В окне **Управление компьютером** на панели навигации выберите раздел **Служебные программы** > **Локальные пользователи** > **Пользователи**.

3.5 На панели просмотра дважды щелкните пользователя `postgres`.

3.6 В окне **Свойства: postgres** на вкладке **Членство в группах** удалите группы Users и Administrators с помощью кнопки **Удалить**.

3.7 Нажмите кнопку **OK**.

4 Продолжите установку ПО Сервер мониторинга.

Время на Сервере мониторинга не соответствует времени операционной системы

Описание:

Время на Сервере мониторинга не соответствует времени операционной системы.

Данная ошибка отмечена для Серверов мониторинга, в операционной системе которых выбран часовой пояс **(UTC+03:00) Волгоград, Москва, Санкт-Петербург (RTZ 2)**. Проблема связана с тем, что для виртуальной машины Java не обновлены часовые пояса, которые были изменены в связи с отменой перехода на летнее время и обратно, а также с особенностями выбора данного часового пояса.

Способ устранения:

Обновите часовые пояса для виртуальной машины Java. Для этого выполните следующие действия:

5 Войдите в операционную систему под учетной записью администратора.

6 Задайте часовой пояс **(UTC+03:00) Минск**.

7 Скопируйте на жесткий диск файл архива `utimezone.zip`, входящий в комплект поставки (см. «Комплект поставки» на стр. 17).

8 Создайте на диске `C:` папку `TZUPDATE` и извлеките в эту папку файлы из архива `utimezone.zip`.

9 В командной строке Windows в папке `C:\TZUPDATE` выполните последовательно следующие команды:

```
copy.bat
utimezone.bat
upgrade.bat
```

Отчет о выполнении записывается в файл `C:\TZUPDATE\result.log`. Убедитесь, что в файле есть сообщение об успешном обновлении и отсутствуют сообщения об ошибках.

10 Подключитесь к Серверу мониторинга с помощью АРМ мониторинга и на странице **Мониторинг** > **Список** произведите опрос какого-либо узла мониторинга.

11 Убедитесь, что время опроса узла совпадает с текущим временем операционной системы.

Неограниченный рост базы данных

Описание:

Если база данных начинает неограниченно расти, в журнале PostgreSQL (при стандартной настройке журнал располагается по следующему пути `Диск:\Program Files\PostgresSQL\8.4\data\pg_log\`) появляются сообщения следующего вида:

```
2012-01-10 23:52:06 MSK ERROR: could not read block 51 of relation
base/18747802/2619: read only 0 of 8192 bytes
```

Данная ошибка может возникать в результате неисправности диска.

Способ устранения:

Для проверки состояния диска воспользуйтесь программой **Windows chkdsk** или другой программой для проверки состояния диска и проверьте диск на наличие испорченных секторов. При их наличии замените диск и восстановите Сервер мониторинга из резервной копии (см. «Резервное копирование и восстановление» на стр. 169), либо заново установите Сервер мониторинга (см. «Установка, обновление и удаление сервера мониторинга» на стр. 41).

Проблемы при записи событий мониторинга в базу данных

Описание:

- Если во время работы системы мониторинга на жестком диске заканчивается свободное место, останавливается запись событий мониторинга в базу данных. При освобождении свободного места запись событий в базу данных не возобновляется.

Способ устранения:

- Чтобы возобновить запись событий мониторинга в базу данных, перезапустите службы Apache Tomcat и PostgreSQL.

Не удается запустить службу Apache Tomcat

Описание:

- При попытке запустить Apache Tomcat служба не стартует.

Причина и способ устранения:

- Проверьте лог-файл службы. Если в нем присутствуют сообщения, подобные приведенным ниже, то, вероятнее всего, в системе отсутствует библиотека `msvcr71.dll`.

  Добавьте указанный файл в системную папку `C:\Windows\system32`.

Возможные сообщения в лог-файле службы Apache Tomcat:

```
[2010-02-02 14:25:23] [info] Procrun (2.0.4.0) started
[2010-02-02 14:25:23] [info] Running Service...
[2010-02-02 14:25:23] [info] Starting service...
[2010-02-02 14:25:23] [174  javajni.c] [error] Не найден указанный модуль.
[2010-02-02 14:25:23] [994  prunsrv.c] [error] Failed creating java C:\Program
Files\Java\jre6\bin\client\jvm.dll
[2010-02-02 14:25:23] [1269 prunsrv.c] [error] ServiceStart returned 1
[2010-02-02 14:25:24] [info] Run service finished.
[2010-02-02 14:25:24] [info] Procrun finished.
```

Описание:

- После установки Apache Tomcat и перезагрузки операционной системы служба Apache Tomcat не запускается, выдается сообщение об ошибке: «Application System Error Access is denied. Unable to open the service 'Tomcat 6'».

Причина и способ устранения:

- Возникли проблемы с доступом к исполняемому файлу службы Apache Tomcat. Подобные ошибки могут появляться, например, если включен контроль учетных записей пользователей.

  Для решения проблемы выполните следующие действия:

  - Перейдите в папку `C:\Program Files\Apache Software Foundation\Tomcat 6.0\bin`.
  - Щелкните правой кнопкой мыши файл `Tomcat6w.exe` и выберите пункт **Свойства**.
  - В открывшемся окне перейдите на вкладку **Совместимость**.
  - В группе **Уровень прав** установите флажок **Выполнять эту программу от имени администратора**.
  - Нажмите кнопку **OK**.
  - Запустите службу Apache Tomcat.

Проблемы при подключении к Серверу мониторинга через веб-интерфейс

Описание:

- Не удается подключиться к Серверу мониторинга через веб-интерфейс, окно аутентификации пользователя не появляется.

Причина и способ устранения:

- Не запущена служба Apache Tomcat.

  Запустите Apache Tomcat: щелкните правой кнопкой мыши значок Apache Tomcat в области уведомлений и выберите команду **Start**. После старта службы автоматически запускается ПО Сервер мониторинга.

- Отсутствует связь данного узла (АРМ мониторинга) с Сервером мониторинга.

Проверьте наличие связи между данным узлом и Сервером мониторинга путем проверки соединения из программы ViPNet Монитор или с помощью команды `ping`. Если соединение отсутствует, проверьте правильность задания в ЦУСе связей между узлами.

Проблемы доступа и аутентификации на АРМ мониторинга

Описание:

- Во время работы с веб-страницей (при попытке нажать на кнопку или ссылку, запись в списке и тому подобное) появляется сообщение о недоступности Сервера мониторинга.

Причина и способ устранения:

- ПО Сервер мониторинга остановлено.

  Запустите Apache Tomcat на Сервере мониторинга. После старта службы автоматически запускается ПО Сервер мониторинга.

Описание:

- Во время работы с веб-страницей (при попытке нажать на кнопку или ссылку, запись в списке и тому подобное) появляется окно аутентификации пользователя.

Причина и способ устранения:

- На АРМ мониторинга произошло переподключение к Серверу мониторинга из-за перезапуска ПО Сервер мониторинга.

  Введите имя и пароль пользователя для повторного входа.

Не открывается окно информации об узле мониторинга

Описание:

- Вы работаете в Internet Explorer версии 9.0. На странице **Мониторинг** на вкладке **Список** или на странице **Администрирование** на вкладке **Узлы** вы щелкнули ссылку с названием узла мониторинга, но окно с детальной информацией об узле не открылось.

Причина и способ устранения:

- Чтобы решить проблему, рекомендуется обновить Internet Explorer до версии 10.0.
- Если вы не хотите обновлять браузер, внесите следующие изменения в настройки безопасности Internet Explorer 9.0:

  11.1 Откройте Internet Explorer.

  11.2 Нажмите кнопку **Сервис** и выберите пункт **Свойства браузера**.

  11.3 На вкладке **Безопасность** щелкните значок зоны **Интернет**, а затем нажмите кнопку **Другой**.

  11.4 В списке **Параметры безопасности** найдите пункты **Сценарии** и **Активные сценарии**.

  11.5 Щелкните **Включить**, нажмите кнопку **ОК**, а затем снова нажмите кнопку **ОК**.

Проблемы при использовании прокси-сервера

Описание:

- Не отправляются SMS-оповещения и не работает онлайн-карта при использовании прокси-сервера.

Возможные причины и способ устранения:

- Служба Apache Tomcat запущена не с использованием учетной записи администратора ОС.

  Запустите Apache Tomcat с использованием учетной записи администратора ОС.

Не удается установить каскад

Описание:

- Не удается установить каскад. На дочернем Сервере мониторинга не появляется запрос на подтверждение установления связи в каскаде.

Способ устранения:

- В программе ViPNet Монитор на родительском и дочернем Серверах мониторинга создайте фильтры открытой сети:
  - Фильтр, пропускающий входящий трафик по протоколу TCP и порту 80 от одного Сервера мониторинга к другому.
  - Фильтр, пропускающий исходящий трафик по протоколу TCP и портам 1154, 1132, 1210 от одного Сервера мониторинга к другому.

B

Создание и изменение шаблонов писем оповещений

Шаблоны писем оповещений — это файлы с расширением `.jasper`, которые представляют собой скомпилированные шаблоны Jasper-отчетов (JasperReports). Для работы с этими шаблонами используется свободно распространяемый графический редактор отчетов iReport, входящий в комплект поставки. Последнюю версию редактора iReport можно скачать по ссылке http://jasperforge.org/projects/ireport/.

Шаблоны `default.jasper` и `bmailTemplate.jasper`, поставляемый вместе с ПО Сервер мониторинга, можно использовать как образец для создания другого шаблона. Для редактирования шаблона:

1 Запустите программу iReport и по команде **File** > **Open** откройте файл `default.jasper` или `bmailTemplate.jasper`.

   Перед открытием файла на редактирование программа предложит конвертировать файл в формат `Jrxml`.

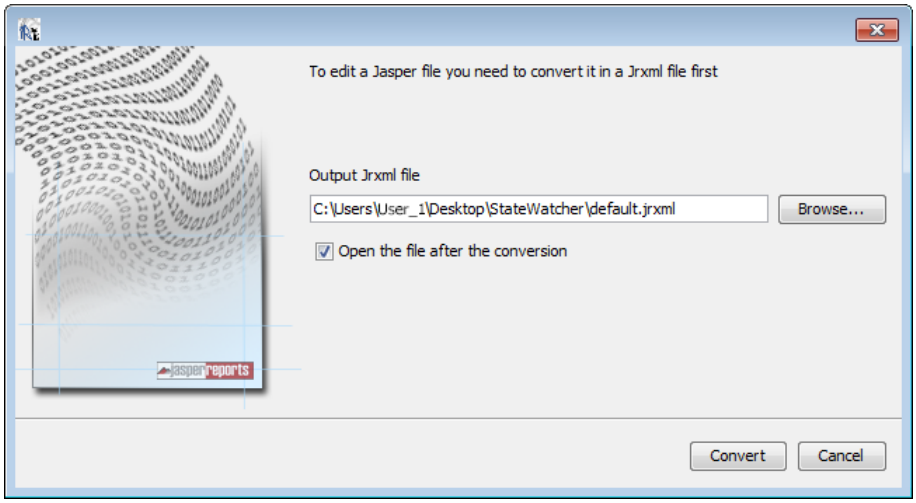

Рисунок 77: Конвертирование шаблона писем

2 Укажите папку, в которую следует поместить конвертированный файл, и установите флажок **Open the file after the conversion**. Нажмите кнопку **Convert**, в результате чего шаблон откроется на редактирование.

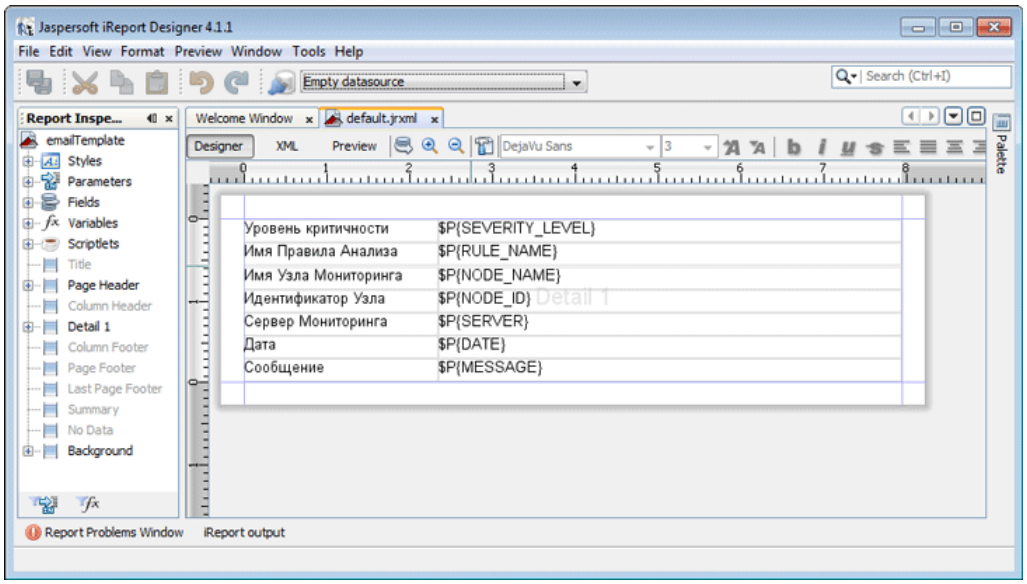

Рисунок 78: Редактирование шаблона писем

В шаблонах `default.jasper` и `bmailTemplate.jasper` задана таблица, в которой содержатся данные о сработавшем правиле анализа, узле мониторинга, Сервере мониторинга и сообщение, сформированное в правиле анализа. Таблица состоит из двух столбцов и семи строк. Первый столбец содержит фиксированный текст (описание параметра), второй столбец содержит имена переменных, которые в процессе формирования сообщения заменяются на значение соответствующего параметра при соответствующем срабатывании правила анализа (список и описание

используемых переменных, соответствующих определенным параметрам представлен в таблице ниже).

Таблица 9. Используемые в шаблонах переменные

Переменная	Описание
SEVERITY_LEVEL	Уровень критичности событий в оповещениях. Может принимать следующие значения: • высокий уровень; • средний уровень; • низкий уровень; • информационное сообщение.
RULE_NAME	Имя правила анализа, указанное при создании правила анализа.
NODE_NAME	Имя узла мониторинга, на котором применяется правило анализа.
NODE_ID	Идентификатор узла мониторинга, на котором применяется правило анализа.
SERVER	Имя Сервера мониторинга, являющегося отправителем оповещений.
DATE	Дата и время последнего опроса узла мониторинга Сервером мониторинга.
MESSAGE	Текст сообщения, заданный в правиле анализа.

При создании отчета (письма с оповещением) вместо параметров подставляются конкретные значения, полученные при срабатывании одного из правил анализа.

3 Результат, который получится при использовании шаблона, можно проверить с помощью предварительного просмотра на вкладке **Preview**.

Перед просмотром программа запросит ввести вручную значение каждого из параметров, присутствующих в шаблоне. Если значение какого-либо параметра не задано, при просмотре в качестве значения будет указано `null`.

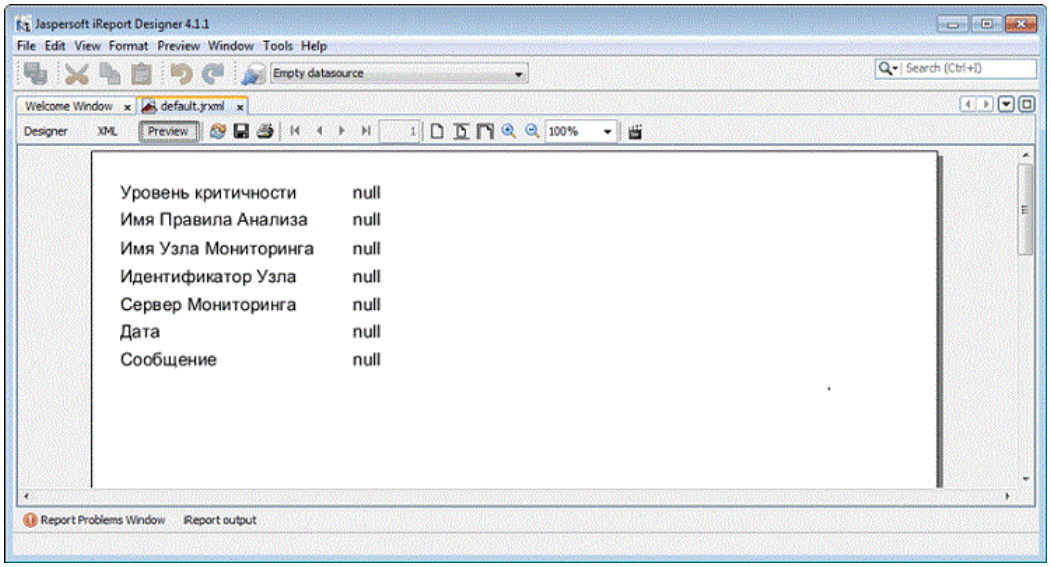

Рисунок 79: Предварительный просмотр письма с оповещением

C

Контролируемые параметры

Контролируемые параметры узлов мониторинга

В данном приложении приведен полный список параметров, контролируемых в текущей версии ПК ViPNet StateWatcher. Параметры объединены в те же логические группы, которые присутствуют в интерфейсе АРМ мониторинга. Описание каждой логической группы параметров приведено в отдельной таблице. Для каждого параметра указывается его название, краткое описание, тип данных, а также возможные значения и комментарий (там, где это необходимо). Название параметра – это то название, которое следует использовать при составлении правила анализа.

Контроль некоторых параметров возможен только начиная с определенных версий ПО, установленных на узлах мониторинга: ПО ViPNet Client/Coordinator – начиная с версии 3.1.3, ПО ViPNet Coordinator Linux – начиная с версии 3.6.1, ПАК ViPNet Coordinator HW – начиная с версии 2.2. Такие параметры отмечены звездочкой (*).

Примечание. Для узлов с установленным ПО ViPNet Client, ViPNet Coordinator версии ниже 3.1 или ПО ViPNet Coordinator Linux версии ниже 3.4 контроль любых параметров невозможен.

Таблица 10. Общие характеристики узла

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GIDNAMES_ID	Идентификатор узла	Целое число		В версиях ПО Сервер мониторинга 1.0 и 1.1 этот параметр

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
				называется COMMON_NODEID
NODE_STATUS	Состояние узла	Целое число	**0** — узел доступен. **1** — узел недоступен.	
GIDNAMES_NAME	Название узла	Строка		В версиях ПО Сервер мониторинга 1.0 и 1.1 этот параметр называется GINFO_NAME
NODE_DESCRIPTION	Описание узла	Строка		Не более 1024 байтов
GFINFO_TYPE	Тип узла в сети ViPNet	Целое число	**0** – ViPNet-клиент; **2** – ViPNet-координатор	
GINFO_TIME_LOC	Текущее время	Дата При обращении к параметру возвращается целое число (дата в формате unixtime)		
POLL_TIME	Время опроса	Дата При опросе сохраняется текущее локальное время сервера в GMT		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
MONITOR_STATUS	Состояние программы ViPNet Монитор	Целое число	**0** — программа работает. **1** — программа не работает. **2** — ошибка декодирования ответа. **3** — состояние программы неизвестно. **4** — программа не установлена.	
GIDNAMES_TASKLIST	Список задач (ролей, в которых зарегистрирован узел)	Составной тип (разделитель – запятая) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		
GFOSTATE_A_TOTAL_MEM*	Общий объем оперативной памяти	Целое число		
GFOSTATE_A_FREE_MEM*	Объем свободной оперативной памяти	Целое число		
MEM_USAGE*	Загрузка памяти	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSTATE_A_TOTAL_CPU*	Загрузка процессора	Целое число		
GFOSTATE_A_BMAIL*	Деловая почта	Целое число		
GIDNAMES_IPLIST	Список IP-адресов узла	Составной тип (разделитель – запятая) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		
GIDNAMES_ISSERVER	Является узел ViPNet-сервером или нет	Целое число	**1** — да. **0** — нет.	
GFOSTATE_A_FAILOVER	Состояние модуля Failover на активном элементе кластера	Целое число	**0** — работает. **1** — не работает. **2** — состояние неизвестно. **3** — модуль не установлен на узле.	
GFOSTATE_A_UPTIME	Продолжительность работы активного элемента кластера (с момента переключения в активный режим или старта	Число в формате ДД/ЧЧ/ММ/СС		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
	в активном режиме)			
GFOINFO_CLUSTER	Признак работы в режиме кластера горячего резервирования	Целое число	**1** — работа в режиме кластера. **0** — работа в обычном режиме.	
GFOSTATE_A_BMAIL	Состояние программы ViPNet Деловая почта на узле	Целое число	**0** — работает. **1** — не работает. **2** — состояние неизвестно. **3** — программа не установлена на узле.	

Таблица 11. Параметры программы ViPNet Монитор

Название параметра	Описание	Тип данных	Возможные значения	Комментарий

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GINFO_PVER	Версия продукта	Составной тип (разделитель – точка) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		В качестве предыдущего значения данного параметра сохраняется только реальное значение, полученное при успешном предшествующем опросе, т.е. неизвестное (отсутствующее) значение не сохраняется.
GINFO_DEMVER	Версия Монитора (Демона)	Составной тип (разделитель – точка) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GINFO_DRVVER	Версия драйвера	Составной тип (разделитель – точка) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		
GINFO_PACKTYPE	Тип пакетов (формат шифрованных пакетов)	Целое число	**0x400** (десятичное значение 1024) – формат 4.0; **0x401** (десятичное значение 1025) – формат 4.1	
GINFO_DUDP_TIMEOUT	Допустимый таймаут отсутствия трафика при работе в режиме с динамической трансляцией адресов	Целое число	**25**	
GINFO_LOGVER	Версия журнала пакетов	Целое число		
GIDSNATSETTINGS_FIREWALLIP	Адрес межсетевого экрана	Целое число		
GIDSNATSETTINGS_PORT	Порт UDP межсетевого экрана	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GIDSNATSETTINGS_FIXFIREWALL	Фиксация межсетевого экрана (признак фиксации межсетевого экрана в режимах использования межсетевого экрана с динамическим или статическим NAT)	Целое число	**1** – настройки работы через межсетевой экран фиксируются; **0** – настройки работы через межсетевой экран не фиксируются	
GIDSNATSETTINGS_PROXYID	Идентификатор прокси-сервера	Целое число		

Таблица 12. Диски

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
HD_USAGE*	Использование всех дисков (в процентах)	Целое число		
GFOFSINFO_NAME*	Название диска	Строка		
GFOFSINFO_DEVICE*	Название устройства	Строка		
GFOFSINFO_TOTAL*	Общий объем диска	Целое число		
GFOFSINFO_FREE*	Свободно (объем свободного места)	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOFSINFO_USAGE*	Использование (использование диска в процентах)	Целое число		GFOFSINFO_USAGE = 100 * GFOFSINFO_FREE / GFOFSINFO_TOTAL

Таблица 13. Туннелируемые диапазоны

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GSERVLIST_TUNNEL_REAL_START*	Начальный адрес	Составной тип (разделитель – точка) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GSERVLIST_TUNNEL_REAL_END*	Конечный адрес	Составной тип (разделитель – точка) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		

Таблица 14. Журнал системных событий

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSYSJ_TIME*	Время события	Дата При обращении к параметру возвращается целое число (дата в формате unixtime)		
GFOSYSJ_TYPE*	Тип события	Целое число		
GFOSYSJ_SOURCE*	Источник	Строка		
GFOSYSJ_CATEGORY*	Категория	Строка		
GFOSYSJ_USER*	Пользователь	Строка		
GFOSYSJ_DESCR*	Описание	Строка		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSYSJ_JOURNAL*	Журнал ОС, которому принадлежит событие	Строка		

Таблица 15. Параметры ГИС

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GEO_CODE_LAT	Широта местонахождения узла	Строка		
GEO_CODE_LON	Долгота местонахождения узла	Строка		

Таблица 16. MFTP

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSTATE_A_MFTP*	Состояние модуля MFTP	Целое число		
GMFTPSTAT_QUEUE_COUNT*	Число конвертов в очереди	Целое число		
GMFTPSTAT_QUEUE_SIZE*	Суммарный размер конвертов в очереди	Целое число		

Таблица 17. Список сетевых интерфейсов и их характеристики

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GIFINFO_NAME	Название интерфейса	Строка		
GIFINFO_IPLIST	Список IP-адресов доступа	Составной тип (разделитель – запятая) При обращении к параметру в целом он имеет строковый тип При обращении к элементам параметра возвращается целое число		
GIFINFO_MODE	Режим обработки открытых IP-пакетов (текущий)	Целое число	Возможные значения – **от 1 до 5**	
GIFINFO_STARTMODE	Режим обработки открытых IP-пакетов при старте	Целое число	Возможные значения – **от 1 до 5**	
GIFINFO_NETMASK	Маска подсети	Строка При обращении к параметру возвращается целое число		
GIFINFO_EXTERNAL	Тип интерфейса	Целое число	**1** – внешний интерфейс; **0** – внутренний интерфейс	

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
GIFINFO_USED	Состояние интерфейса	Целое число	**0** или значение отсутствует – интерфейс недоступен; **1** – интерфейс доступен	

Таблица 18. Статистика по сетевым интерфейсам

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
GIFSTAT_SEND_ENC_PASS	Число успешно посланных зашифрованных пакетов	Целое число		
GIFSTAT_SEND_ENC_PASS_BYTES*	Общий объем успешно посланных зашифрованных пакетов (в мегабайтах)	Целое число		
GIFSTAT_SEND_ENC_DROP	Число блокированных исходящих зашифрованных пакетов	Целое число		
GIFSTAT_SEND_ENC_DROP_BYTES*	Общий объем блокированных исходящих зашифрованных пакетов	Целое число		
GIFSTAT_RECV_ENC_PASS	Число успешно принятых зашифрованных пакетов	Целое число		
GIFSTAT_RECV_ENC_PASS_BYTES*	Общий объем успешно принятых зашифрованных	Целое число		

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
	пакетов			
GIFSTAT_RECV_ENC_DROP	Число блокированных входящих зашифрованных пакетов	Целое число		
GIFSTAT_RECV_ENC_DROP_BYTES*	Общий объем блокированных входящих зашифрованных пакетов	Целое число		
GIFSTAT_SEND_BR_PASS	Число успешно посланных незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_PASS_BYTES*	Общий объем успешно посланных незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_DROP	Число блокированных исходящих незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_DROP_BYTES*	Общий объем блокированных исходящих незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_PASS	Число успешно принятых	Целое число		

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
	незашифрованных широковещательных пакетов			
GIFSTAT_RECV_BR_PASS_BYTES*	Общий объем успешно принятых незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_DROP	Число блокированных входящих незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_DROP_BYTES*	Общий объем блокированных входящих незашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_NOT_ENC_PASS	Число успешно посланных незашифрованных пакетов	Целое число		
GIFSTAT_SEND_NOT_ENC_PASS_BYTES*	Общий объем успешно посланных незашифрованных пакетов	Целое число		
GIFSTAT_SEND_NOT_ENC_DROP	Число блокированных исходящих незашифрованных пакетов	Целое число		
GIFSTAT_SEND_NOT_ENC_DROP_BYTES*	Общий объем блокированных исходящих незашифрованных пакетов	Целое число		

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
GIFSTAT_RECV_NOT_ENC_PASS	Число успешно принятых незашифрованных пакетов	Целое число		
GIFSTAT_RECV_NOT_ENC_PASS_BYTES*	Общий объем успешно принятых незашифрованных пакетов	Целое число		
GIFSTAT_RECV_NOT_ENC_DROP	Число блокированных входящих незашифрованных пакетов	Целое число		
GIFSTAT_RECV_NOT_ENC_DROP_BYTES*	Общий объем блокированных входящих незашифрованных пакетов	Целое число		
GIFSTAT_SEND_BR_ENC_PASS	Число успешно посланных зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_ENC_PASS_BYTES*	Общий объем успешно посланных зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_ENC_DROP	Число блокированных исходящих зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_SEND_BR_ENC_DROP_BYTES*	Общий объем блокированных исходящих зашифрованных	Целое число		

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
	широковещательных пакетов			
GIFSTAT_RECV_BR_ENC_PASS	Число успешно принятых зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_ENC_PASS_BYTES*	Общий объем успешно принятых зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_ENC_DROP	Число блокированных входящих зашифрованных широковещательных пакетов	Целое число		
GIFSTAT_RECV_BR_ENC_DROP_BYTES*	Общий объем блокированных входящих зашифрованных широковещательных пакетов	Целое число		
TRAFFIC_TOTAL_IN*	Суммарный входящий трафик (общее количество байт, пришедших на интерфейс с момента начала работы ViPNet-драйвера)	Целое число		
TRAFFIC_TOTAL_OUT*	Суммарный исходящий трафик (общее количество байт, ушедших в сеть с интерфейса с момента начала работы ViPNet-драйвера)	Целое число		

Название параметра	**Описание**	**Тип данных**	**Возможные значения**	**Комментарий**
TRAFFIC_TOTAL*	Всего (общее количество байт, прошедших через интерфейс с момента начала работы ViPNet-драйвера)	Целое число		TRAFFIC_TOTAL = TRAFFIC_TOTAL_IN + TRAFFIC_TOTAL_OUT
TRAFFIC_LOAD*	Загрузка интерфейса (средняя скорость прохождения трафика через интерфейс за последний период опроса) Измеряется в мегабайтах в секунду (МБ/с)	Целое число		Если хотя бы одно из предыдущих значений TRAFFIC_TOTAL_IN или TRAFFIC_TOTAL_OUT больше, чем текущее, то TRAFFIC_LOAD = TRAFFIC_TOTAL (текущее) / период опроса узла иначе TRAFFIC_LOAD = (TRAFFIC_TOTAL (текущее) - TRAFFIC_TOTAL (предыдущее)) / период опроса узла

Таблица 19. Параметры журнала IP-пакетов

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GDBS_MAXSIZE	Максимальный размер журнала	Целое число		
GDBS_TIMEDIFF	Интервал агрегирования записей	Целое число		
GDBS_REGALL	Регистрировать все IP-пакеты	Целое число	**1** – регистрировать все пакеты; **0** – регистрировать только блокированные пакеты	
GDBS_REGBROADCAST	Регистрировать широковещательные IP-пакеты	Целое число	**1** – регистрировать широковещательные пакеты; **0** – не регистрировать широковещательные пакеты	
GDBS_REGTCPSERVERPORT	Для TCP-соединений регистрировать только порт сервера	Целое число	**1** – регистрировать только порт сервера; **0** – регистрировать порты сервера и клиента	

Таблица 20. Параметры пассивного элемента кластера

Название параметра	Описание	Тип данных	Возможные значения	Комментарий

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSTATE_P_MFTP*	Состояние модуля MFTP на пассивном элементе кластера	Целое число	**0** — работает. **1** — не работает. **2** — состояние неизвестно. **3** — модуль не установлен на узле.	
GFOSTATE_P_IPLIR*	Состояние демона iplir	Целое число	**0** — работает. **1** — не работает. **2** — состояние неизвестно. **3** — модуль не установлен на узле.	
GFOSTATE_P_FAILOVER*	Состояние модуля Failover на пассивном элементе кластера	Целое число	**0** — работает. **1** — не работает. **2** — состояние неизвестно. **3** — модуль не установлен на узле.	
GFOSTATE_P_UPTIME	Продолжительность работы пассивного элемента кластера с момента старта системы резервирования в пассивном режиме	Число в формате ДД/ЧЧ/ММ/СС		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOSTATE_P_TOTAL_CPU*	Загрузка процессора	Целое число		
GFOSTATE_P_TOTAL_MEM*	Загрузка памяти	Целое число		
GFOSTATE_P_FREE_MEM*	Объем свободной оперативной памяти	Целое число		

Таблица 21. События системы горячего резервирования

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOJOURNAL_TIME	Время регистрации события системы горячего резервирования	Дата При обращении к параметру возвращается целое число (дата в формате unixtime)		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GFOJOURNAL_EVENT	Тип зарегистрированного события	Строка	**FO_EVENT_BOOT** — загрузка системы. **FO_EVENT_SWITCH** — переключение в активный режим. **FO_EVENT_START_ACTIVE** — старт работы элемента кластера в активном режиме. **FO_EVENT_START_PASSIVE** — старт работы элемента кластера в пассивном режиме.	

Таблица 22. Параметры связей с координаторами

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GIDSNATSETTINGS_ID	Идентификатор узла	Целое число		
GIDSNATSETTINGS_NAME	Наименование узла	Строка Формируется на основе справочников ViPNet		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
GIDSNATSETTINGS_STATUS	Состояние связи	Целое число	**0** — координатор недоступен. **1** — координатор доступен.	

Контролируемые параметры открытых узлов

В данном приложении приведен полный список параметров открытых узлов, контролируемых в текущей версии ПК ViPNet StateWatcher. Параметры объединены в те же логические группы, которые присутствуют в интерфейсе АРМ мониторинга. Описание каждой логической группы параметров приведено в отдельной таблице. Для каждого параметра указывается его название, краткое описание, тип данных, а также возможные значения и комментарий (там, где это необходимо). Название параметра – это то название, которое следует использовать при составлении правила анализа.

Таблица 23. Системные параметры

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
sysDescr	Описание узла	Строка		
sysUpTime	Время работы	Время (беззнаковое число — количество сотых долей секунд)		
sysContact	Контактная информация лица, управляющего узлом	Строка		
sysName	Имя узла	Строка		Соответствует параметру GIDNAMES_NAME защищенных узлов мониторинга
sysLocation	Местонахождение узла	Строка		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrMemorySize	Размер оперативной памяти	МБ		Соответствует параметру GFOSTATE_A_TOTAL_MEM защищенных узлов мониторинга
hrSystemDate	Текущее время узла	Дата При обращении к параметру возвращается целое число (дата в формате unixtime)		Соответствует параметру GINFO_TIME_LOC защищенных узлов мониторинга

Таблица 24. Сетевые настройки

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
ipForwarding	Маршрутизатор (указание на то, что данный узел осуществляет переадресацию)	Целое число		
IPdefaultTTL	Время жизни IP-датаграмм (TTL)	Целое число		
IPinreceives	Число полученных IP-датаграмм	Целое число		
ipInHdrErrors	Число входных IP-датаграмм с ошибками в заголовке	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
	пакета			
ipInAddrErrors	Число IP-датаграмм, отвергнутых из-за неверного IP-адреса	Целое число		
ipForwDatagrams	Количество IP-датаграмм, которые пытались перенаправить	Целое число		
ipInUnknownProtos	Число IP-датаграмм с неподдерживаемым кодом протокола	Целое число		
ipInDiscards	Число IP-датаграмм, отвергнутых из-за переполнения буфера	Целое число		
ipInDelivers	Полное число входных IP-датаграмм, успешно обработанных на IP-уровне	Целое число		
ipOutRequests	Полное число IP- и ICMP-датаграмм, переданных для отправки	Целое число		
ipOutDiscard	Полное число IP- и ICMP-датаграмм, переданных для отправки и отвергнутых из-за переполнения буфера	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IPoutNoroutes	Число неудач при маршрутизации	Целое число		
ipReasmTimeout	Максимальное число секунд ожидания сборки фрагментов	Целое число		
ipReasmReqds	Число полученных фрагментов	Целое число		
ipReasmOKs	Число полученных и успешно собранных IP-датаграмм	Целое число		
ipReasmFails	Число полученных IP-датаграмм, которые не удалось собрать	Целое число		
IPFragOKs	Число успешно фрагментированных IP-датаграмм	Целое число		
ipFragFails	Число IP-датаграмм, которые нужно фрагментировать, но сделать это нельзя (например, из-за флага)	Целое число		
ipFragCreates	Число фрагментов IP-датаграмм, сформированных данным объектом	Целое число		

Таблица 25. Сетевые интерфейсы

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IfNumber	Число сетевых интерфейсов	Целое число		
IFindex	Список интерфейсов	Целое число	Возможные значения — от **1** до значения параметра IfNumber	
IfDescr	Текстовое описание интерфейса	Строка		
IfType	Тип интерфейса	Целое число	Например: **6** — Ethernet **9** — 802.5 Token Ring **23** — PPP **28** — SLIP	
IfMTU	Максимально допустимый размер передаваемого пакета (MTU)	Целое число		
IfSpeed	Скорость интерфейса в Мбит/с	Целое число		
IfPhysaddress	Физический адрес	Физический адрес	Например, **a0:b3:cc:a0:ac:26**	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IfAdminStatus	Требуемое состояние интерфейса	Целое число	Возможные значения: **1** — интерфейс включен **2** — интерфейс выключен **3** — интерфейс тестируется	
IfOperStatus	Текущее состояние интерфейса	Целое число	Возможные значения: **1** — интерфейс включен **2** — интерфейс выключен **3** — интерфейс тестируется	
IfLactchange	Время текущего состояния интерфейса	Время (беззнаковое число — количество сотых долей секунд)		
IfInOctets	Полное число полученных мегабайтов	Целое число		
IfInUcastpkts	Число unicast-пакетов, доставленных на верхний системный уровень	Целое число		
IfInNUcastpkts	Число multicast- и широковещательных пакетов, доставленных на верхний системный уровень	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IfInDiscads	Число полученных, но отвергнутых пакетов	Целое число		
IfInErrors	Число пакетов, полученных с ошибкой	Целое число		
IfInUnknownProtos	Число пакетов, полученных с ошибочным кодом протокола	Целое число		
IfOutOctets	Число отправленных мегабайтов	Целое число		
IfOutUcastPkts	Число unicast-пакетов, полученных с верхнего системного уровня	Целое число		
IfOutNucastPkts	Число multicast- и широковещательных пакетов, полученных с верхнего системного уровня	Целое число		
IfOutDiscads	Количество отвергнутых пакетов из числа отправленных	Целое число		
IfOutErrors	Число отправленных пакетов, содержащих ошибки	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IfOutQlen	Число пакетов в очереди на отправку	Целое число		

Таблица 26. Таблица адресной информации (ARP)

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
IPAdEntBcastAddr	Значение младшего бита широковещательного адреса	Целое число	Возможные значения — **0** и **1** (обычно **1**)	
IPadentifindex	Идентификатор интерфейса	Целое число		
IPAdEntAddr	IP-адрес интерфейса	IP-адрес		
IPadentnetmask	Маска подсети для данного интерфейса	IP-адрес		
IPAdEntReasmMaxsize	Размер IP-датаграммы (максимальный размер IP-датаграммы, которая может быть собрана)	Целое число	Возможные значения — от **0** до **65535**	

Таблица 27. Хранилища данных

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrStorageAllocationUnits	Размер блока данных в	Целое число		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
	байтах			
hrStorageIndex	Индекс хранилища данных	Целое число		
hrStorageSize	Количество блоков данных	Целое число		
hrStorageDescr	Описание хранилища данных	Строка		
hrStorageUsed	Количество занятых блоков данных	Целое число		
hrStorageAllocationFailuers	Количество запросов к хранилищу данных, которые не могли быть обработаны из-за недостаточного количества места в хранилище	Целое число		
hrStorageType	Тип хранилища данных	Строка (содержит идентификатор типа хранилища данных)		

Таблица 28. Дисковые хранилища данных

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrDiskStorageRemoveble	Извлекаемость дискового хранилища	Булев	Возможные значения — **true** и **false**	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrDiskStorageCapacity	Емкость дискового хранилища	КБ		
hrDiskStorageMedia	Тип дискового хранилища	Целое число	Возможные значения: **8** — диск оперативной памяти (RAM) **7** — оптический перезаписываемый диск (optical RW) **6** — оптический неперезаписываемый диск с записью по типу WORM (optical WORM) **5** — оптический неперезаписываемый диск с записью по типу ROM (optical ROM) **4** — дискета (floppy) **3** — жесткий диск **2** — неизвестный **1** — другой	
hrDiskStorageAccess	Права доступа к устройству	Целое число	Возможные значения:	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
			1 — чтение и запись **2** — только чтение	
hrDeviceIndex	Идентификатор устройства в системе	Целое число		

Таблица 29. Запущенные процессы

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrSWRunIndex	Идентификатор процесса в системе	Целое число		
hrSWRunParameters	Описание параметров, используемых при загрузке процессора	Строка		
hrSWRunStatus	Статус запущенного процесса	Целое число	Возможные значения: **1** — запущен **2** — работоспособен **3** — неработоспособен **4** — ошибочный	
hrSWRunParth	Расположение на диске, откуда был запущен процесс	Строка		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrSWRunType	Тип процесса	Целое число	Возможные значения: **1** — неизвестен **2** — операционная система **3** — драйвер устройства **4** — прикладной процесс	
hrSWRunID	Идентификатор приложения для запущенного процесса	Строка		
hrSWRunName	Описание запущенного процесса	Строка		

Таблица 30. Установленные приложения

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrSWInstalledType	Тип установленного приложения	Целое число	Возможные значения: **1** — неизвестный **2** — операционная система **3** — драйвер устройства **4** — прикладное приложение	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
hrSWInstalledIndex	Индекс установленного приложения	Целое число		
hrSWInstalledName	Описание установленного приложения	Строка		
hrSWInstalledID	Идентификатор приложения	Строка		
hrSWInstalledDate	Дата последнего изменения приложения	Дата При обращении к параметру возвращается целое число (дата в формате unixtime)		

Примечание. В системе мониторинга возможно отображение не всех приложений, установленных на открытом узле, так как SNMP-агент, запущенный на данном узле, может передавать Серверу мониторинга неполный список установленных приложений.

Таблица 31. Сетевые сервисы

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
svSvcNumber	Количество сетевых сервисов	Целое число		
svSvcCanBePaused	Возможность паузы у сервиса	Целое число	Возможные значения: **1** — пауза невозможна	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
			2 — пауза возможна	
svSvcInstalledState	Статус установки сервиса	Целое число	Возможные значения: **1** — не установлен **2** — ожидает установки **3** — ожидает удаления **4** — установлен	
svSvcOperatingState	Текущее состояние сервиса	Целое число	Возможные значения: **1** — активен **2** — ожидает продолжения **3** — ожидает паузы **4** — пауза	
svSvcName	Имя сервиса	Строка		
svSvcCanBeUninstalled	Возможность удаления сервиса	Целое число	Возможные значения: **1** — не может быть удален **2** — может быть удален	

Таблица 32. Параметры принтера

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
prtGeneralPrinterName.1	Имя принтера	Строка		
prtGeneralSerialNumber.1	Серийный номер принтера	Строка		
prtAlertCriticalEvents.1	Количество критических событий	Целое число		
prtAllEvents.1	Количество всех событий	Целое число		

Контролируемые параметры ПАК ViPNet IDS

В данном приложении приведен полный список параметров ПАК ViPNet IDS, контролируемых в текущей версии ПК ViPNet StateWatcher. Параметры объединены в те же логические группы, которые присутствуют в интерфейсе АРМ мониторинга. Описание каждой логической группы параметров приведено в отдельной таблице. Для каждого параметра указывается его название, краткое описание, тип данных, а также возможные значения и комментарий (там, где это необходимо). Название параметра – это то название, которое следует использовать при составлении правила анализа.

Таблица 33. Системные параметры

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
sysDescr	Описание узла	Строка		
sysUpTime	Время работы	Время (беззнаковое число — количество сотых долей секунд)		
sysContact	Контактная информация лица, управляющего узлом	Строка		
sysName	Имя узла	Строка		Соответствует параметру GIDNAMES_NAME защищенных узлов мониторинга
sysLocation	Местонахождение узла	Строка		

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSysSensID	Идентификатор текущего сенсора	Целое число		
infIDSSysReqBegin	Начало промежутка отчета	Дата При обращении к параметру возвращается целое число (дата в формате timeticks)		
infIDSSysReqEnd	Конец промежутка отчета	Дата При обращении к параметру возвращается целое число (дата в формате timeticks)		
infIDSSysAttacksNum	Общее количество атак на текущем сенсоре	Целое число		

Таблица 34. Таблица сенсоров

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSensIndex	Идентификатор сенсора	Целое число		
infIDSSensName	Имя сенсора	Строка		

Таблица 35. Статистика атак

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSensIndex	Идентификатор сенсора	Целое число		
infIDSAgrAttacksSeverity	Уровень важности атак	Целое число	Возможные значения: **1** — высокий уровень важности **2** — средний уровень важности **3** — низкий уровень важности	
infIDSAgrAttacksNum	Количество атак	Целое число		

Таблица 36. Список атак

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSensIndex	Идентификатор сенсора	Целое число		
infIDSAttacksID	Идентификатор атаки	Целое число		
infIDSAttacksName	Имя атаки	Строка		
infIDSAttacksSeverity	Уровень важности атаки	Целое число	Возможные значения: **1** — высокий уровень	

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
			важности **2** — средний уровень важности **3** — низкий уровень важности	
infIDSAttacksNum	Количество атак	Целое число		
infIDSAttacksURL	URL-адрес с описанием атаки	URL-адрес		

Таблица 37. Список атакованных узлов

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSensIndex	Идентификатор сенсора	Целое число		
infIDSAttackedHostIndex	Идентификатор атакованного узла	Целое число		
infIDSAttackedHostIP	IP-адрес атакованного узла	IP-адрес		
infIDSAttackedHostNum	Количество атак на узел	Целое число		

Таблица 38. Список атакующих узлов

Название параметра	Описание	Тип данных	Возможные значения	Комментарий
infIDSSensIndex	Идентификатор сенсора	Целое число		
infIDSAttackerHostIndex	Идентификатор атакующего узла	Целое число		
infIDSAttackerHostIP	IP-адрес атакующего узла	IP-адрес		
infIDSAttackerHostNum	Количество атак с узла	Целое число		

D

Шаблон файла импорта открытых узлов

При необходимости добавить большое количество открытых узлов в список связей Сервера мониторинга вы можете создать файл импорта в формате XML. Файл импорта позволяет добавить в список связей Сервера мониторинга открытые узлы, которые в нем описаны, и должен содержать следующую информацию о каждом узле:

- IP-адрес узла.
- Имя узла. Максимальная длина имени узла — 255 символов. Если данный элемент не заполнен, открытому узлу в качестве имени присваивается его IP-адрес.
- Порт, с использованием которого происходит подключение к открытому узлу. Максимальный номер порта — 65536.
- Сетевой протокол, по которому происходит взаимодействие с открытым узлом. Возможно использование только двух протоколов: TCP и UDP.

Шаблон файла импорта открытых узлов

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="openNodes" type="openNodesType"/>
  <xs:complexType name="openNodesType">
    <xs:sequence>
```

```
      <xs:element name="openNode" type="openNodeType" minOccurs="0"
      maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:float"/>
  </xs:complexType>
  <xs:complexType name="openNodeType">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="ip" type="xs:string" use="required"/>
        <xs:attribute name="name" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:maxLength value="255"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="port" type="xs:integer" use="required"/>
        <xs:attribute name="protocol" type="xs:boolean" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:schema>
```

Пример файла импорта открытых узлов

```
<?xml version="1.0" encoding="UTF-8"?>
<openNodes version="1.0">
  <openNode ip="192.168.1.3" name="Сервер авторизации" port="161"
  protocol="TCP"/>
  <openNode ip="192.168.1.5" name="Сервер DNS" port="161" protocol="UDP"/>
</openNodes>
```

E

Показатели производительности системы мониторинга

Нефункциональные характеристики ПК ViPNet StateWatcher

Таблица 39. Нефункциональные характеристики ПК ViPNet StateWatcher

Нефункциональные характеристики	Значение
Максимальное количество узлов мониторинга (защищенных и открытых), поддерживаемое одиночным Сервером мониторинга	20 000
Время отклика основных страниц пользовательского интерфейса	1-5 секунд
Время выполнения экспорта необработанных параметров узлов	Не более 30-ти секунд
Время выполнения запросов к базе данных Сервера мониторинга при максимальных нагрузках	1-5 секунд

Скорость роста базы данных при расчете на один узел мониторинга	15 Кб/час (при опросе 1 раз в 5 минут)
Пропускная способность каскада	2000 оповещений за 5 минут
Запуск ПК ViPNet StateWatcher с стандартной базой данных при нештатном завершении работы ПО (отключении электричества или завершение работы в связи с ошибкой OutofMemory)	до 10 минут

Примечание. Расчет максимального количества узлов мониторинга, поддерживаемых одиночным Сервером мониторинга, проводился при условии — одно оповещение за опрос одного узла.

Таблица 40. Задержка отклика на страницах пользовательского интерфейса при манипуляциях с 20 000 узлами мониторинга

Выполняемое действие	Время отклика страницы
Сохранение правила анализа при связывании его с большим количеством узлов мониторинга	может достигать 30 секунд
Добавление большого количества узлов из списка узлов для добавления в мониторинг в какую-либо группу узлов	может достигать 30-40 секунд
Установка на опрос большого количества узлов мониторинга	может достигать 5-6 секунд
Удаление большого количества узлов мониторинга из системы	может достигать 20-25 секунд
Перенос большого количества узлов мониторинга из одной группы в другую	может достигать 5-15 секунд

Таблица 41. Скорость роста базы данных необработанных параметров узлов

Количество узлов	1 сутки	1 неделя	1 месяц
50	40 МБ	300 МБ	1,2 ГБ
100	80 МБ	600 МБ	2,5 ГБ
200	160 МБ	1,2 ГБ	5 ГБ
1 000	800 МБ	6 ГБ	25 ГБ
10 000	8 ГБ	60 ГБ	250 ГБ
20 000	16 ГБ	120 ГБ	500 ГБ

Примечание. Расчет скорости роста базы данных проводился при условии — 360 КБ необработанных параметров в сутки с одного узла, при опросе каждого узла раз в 5 минут.

Расчет нагрузки на трафик при использовании ПК ViPNet StateWatcher

В данном приложении приведен приблизительный расчет нагрузки на трафик при использовании ПК ViPNet StateWatcher. Расчет сделан в предположении максимально частого возникновения неполадок на сетевых узлах. Так как в реальности это маловероятно, приведенные оценки определяют предельную нагрузку на трафик.

Размер данных, получаемых Сервером мониторинга при опросе одного узла, равен приблизительно 5 КБ (килобайт). Это максимальная оценка, полученная при условии сбора информации обо всех параметрах, контролируемых ПК ViPNet StateWatcher.

Максимальный размер данных при получении одного оповещения по каскаду также равен приблизительно 5 КБ. Остальные сообщения, которыми Серверы мониторинга обмениваются в рамках каскада, имеют значительно меньший размер.

Для приблизительного расчета нагрузки на трафик (в килобайтах) за некоторый интервал времени можно использовать следующую формулу:

```
5 * <количество узлов> * <временной интервал> / <интервал опроса>
```

Предполагается, что количество узлов – это совокупное количество вместе с каскадируемыми узлами, и за каждый период опроса на каждом каскадируемом узле срабатывает одно из правил анализа.

Например, если количество узлов равно 100, а интервал опроса узлов равен 300 секундам, то за 1 час (3600 секунд) Сервер мониторинга будет получать не более 6000 КБ данных.

Внимание! При расчете по формуле временной интервал и интервал опроса узлов должны быть заданы в одинаковых единицах измерения.

В таблице ниже приведен расчетный размер трафика (в мегабайтах) за день, неделю и месяц для разного количества узлов мониторинга. Расчет произведен для периода опроса, равного 5 минутам (300 секунд).

Количество узлов	1 день	1 неделя	1 месяц
50	72 МБ	504 МБ	2160 МБ
100	144 МБ	1008 МБ	4320 МБ
200	288 МБ	2016 МБ	8640 МБ
1000	1440 МБ	10080 МБ	43200 МБ
10 000	14400 МБ	100800 МБ	432000 МБ
20 000	28800 МБ	201600 МБ	864000 МБ

Для мониторинга 300 узлов с периодом опроса 5 минут рекомендуется скорость канала не менее 40 Кбит/сек.

Для мониторинга 20000 узлов с периодом опроса 5 минут рекомендуется скорость канала 1 Гбит/сек.

F

Дополнительные настройки в ОС Windows

Настройка службы SNMP на открытом узле

Чтобы Сервер мониторинга мог получать информацию об открытом узле, на этом узле должна быть настроена служба SNMP (SNMP-агент) (на стр. 292). Данная служба по запросу Сервера мониторинга собирает и передает информацию о работе открытого узла.

Чтобы настроить службу SNMP, выполните следующие действия:

1. Откройте **Панель управления**.
2. В открывшемся окне щелкните **Программы и компоненты**.
3. На странице **Удаление или изменение программы** на панели навигации щелкните ссылку **Включение или отключение компонентов Windows**.

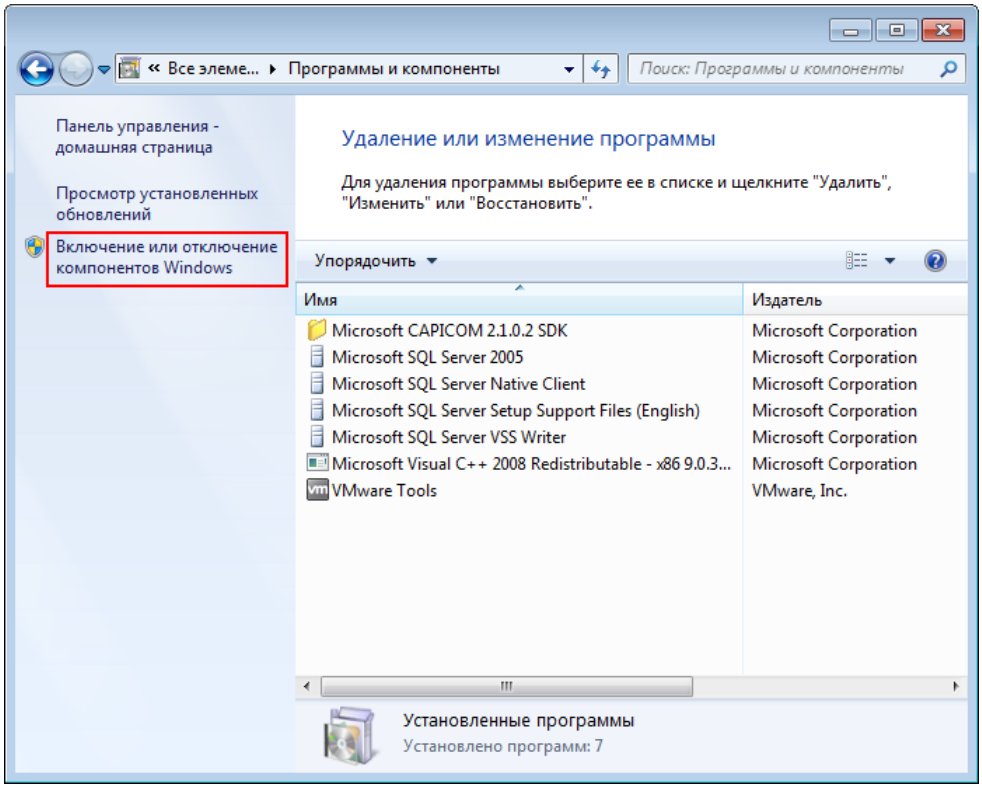

Рисунок 80: Программы и компоненты

4 В открывшемся окне установите флажки **SNMP-протокол** и **WMI поставщик SNMP** и нажмите кнопку **OK**.

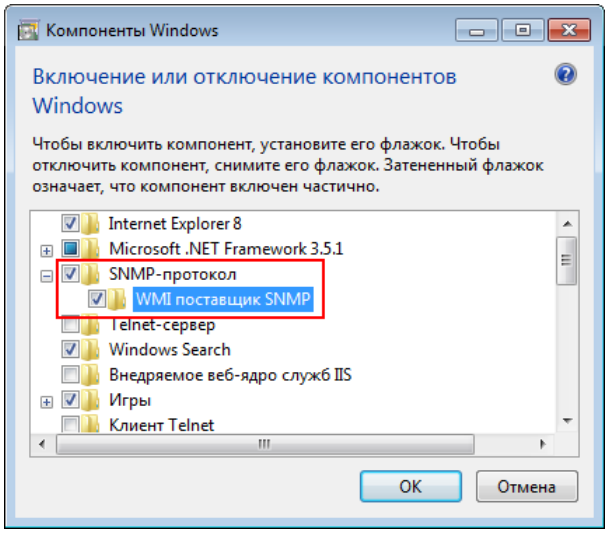

Рисунок 81: Включение службы SNMP

5 Вернитесь в окно **Панель управления**.

6 Щелкните **Администрирование**.

7 В появившемся окне дважды щелкните ярлык **Службы** .

8 В окне **Службы** щелкните службу SNMP правой кнопкой мыши и выберите пункт **Свойства**.

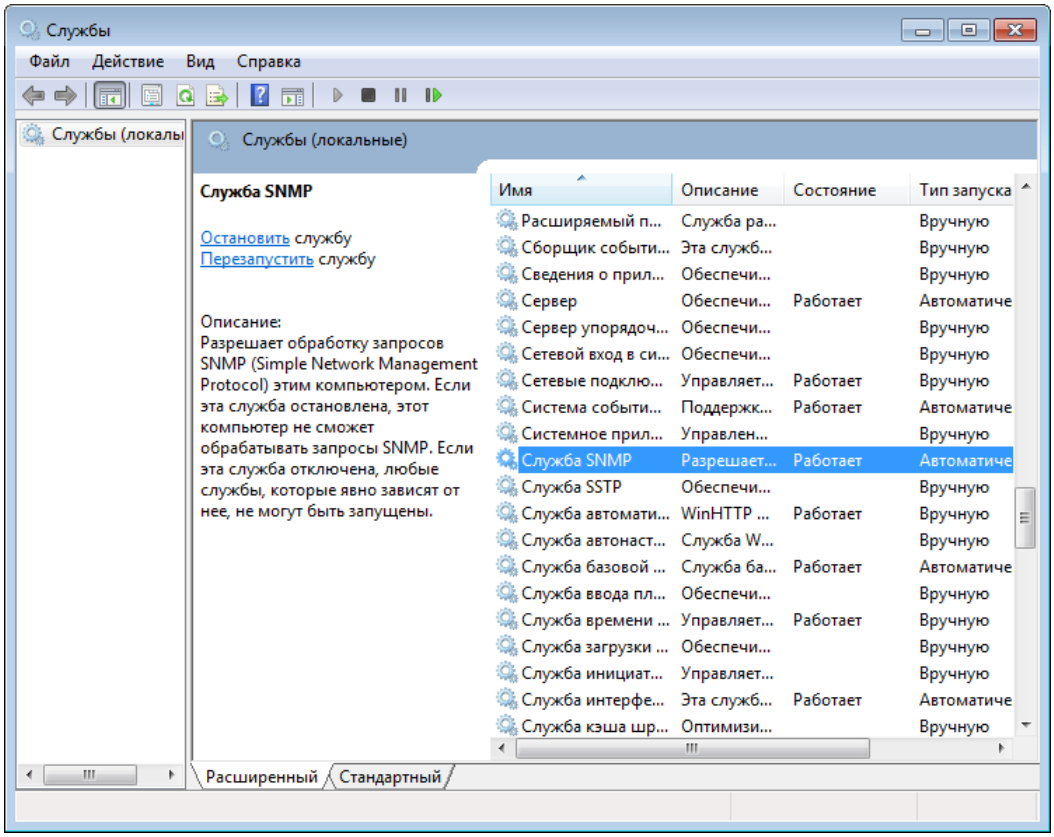

Рисунок 82: Службы Windows

9 В окне **Свойства: Служба SNMP** на вкладке **Агент SNMP** в группе **Службы** установите все флажки.

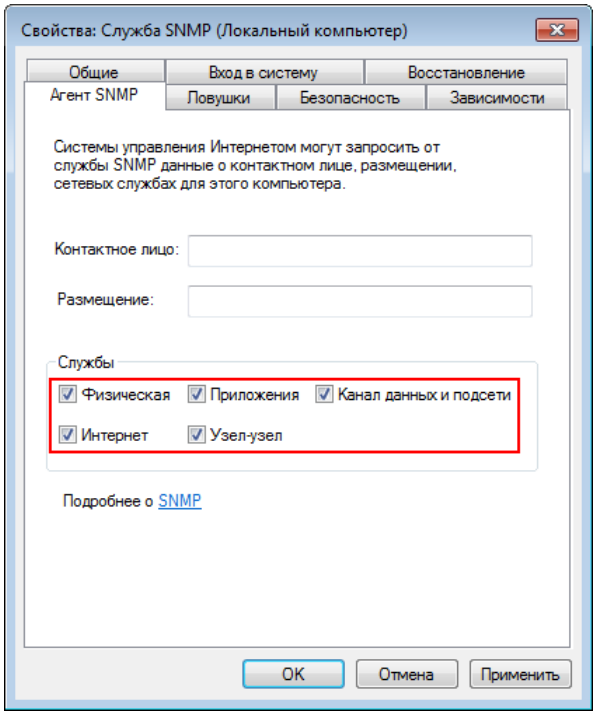

Рисунок 83: Настройка службы SNMP

10 На вкладке **Безопасность** выполните следующие действия:

10.1 Установите флажок **Посылать ловушку проверки подлинности**.

10.2 В группе **Приемлемые имена сообществ** добавьте сообщество `public` с правами доступа не ниже `READ ONLY`.

10.3 Установите переключатель в положение **Принимать пакеты SNMP от любого узла**.

10.4 Нажмите кнопку **OK**.

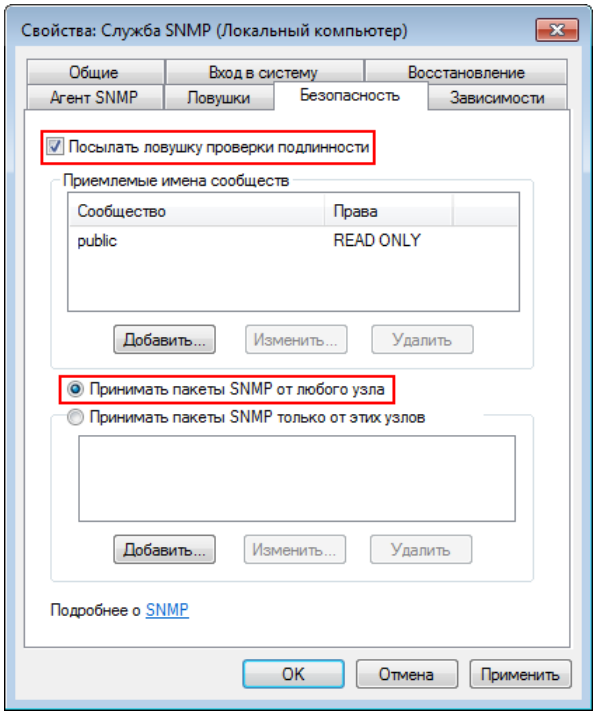

Рисунок 84: Настройка безопасности службы SNMP

11 В окне **Службы** выберите службу SNMP и на панели инструментов нажмите кнопку **Перезапуск службы**.

В результате на открытом узле будет запущена служба SNMP. Теперь вы можете добавить этот узел в систему мониторинга (см. «Добавление открытых узлов в список связей Сервера мониторинга» на стр. 88) и собирать информацию о нем.

Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows

Для разрешения пользователю `postgres` полного доступа (**Full Control**) к папке, в которой будут храниться таблицы базы данных мониторинга, выполните следующие действия:

1 Щелкните правой кнопкой мыши по нужной папке и в контекстном меню выберите пункт **Свойства**.

2 В появившемся окне **Свойства: <Название папки>** выберите вкладку **Безопасность** и нажмите кнопку **Изменить**.

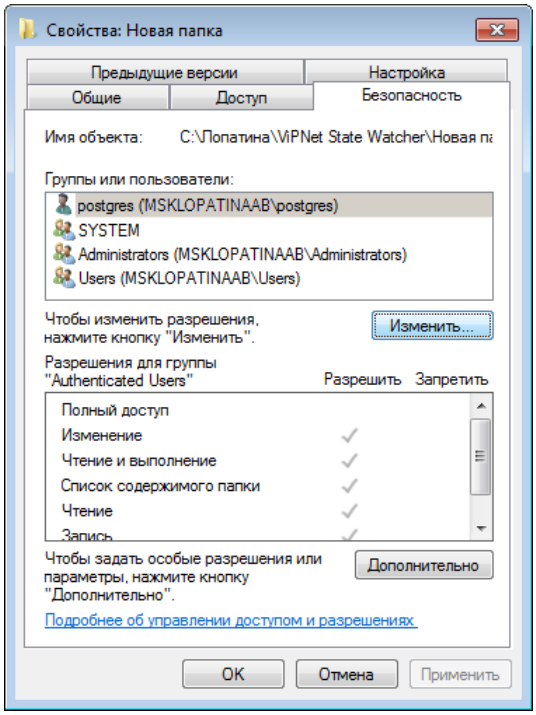

Рисунок 85: Изменение параметров безопасности папки

3 В окне **Разрешения для группы «<Название папки>»** в группе **Группы или пользователи** выберите пользователя `postgres`.

4 В группе **Разрешения для группы «<Имя группы или пользователя>»** в столбце **Разрешить** установите флажок напротив пункта **Полный доступ**.

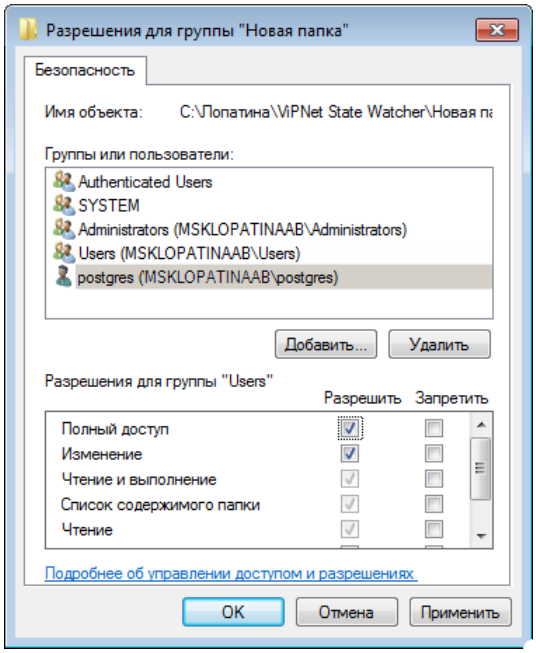

Рисунок 86: Разрешение полного доступа к папке

5 Нажмите кнопку **OK**.

В результате пользователю `postgres` будет разрешен полный доступ к нужной папке.

G

Встроенные правила анализа

В ПК ViPNet StateWatcher имеется ряд встроенных правил анализа, которые по умолчанию применяются ко всем узлам мониторинга. Эти правила предназначены для отслеживания наиболее важных изменений, происходящих на узлах мониторинга, и оповещения об этих изменениях. Набор встроенных правил входит в состав установленного пакета настроек (см. «Пакет настроек» на стр. 290).

Встроенные правила нельзя удалить, но их можно копировать (см. «Копирование правила анализа» на стр. 104) для создания собственных правил анализа на их основе. В этих правилах нельзя изменить название и код правила, можно только изменять списки узлов, на которых применяются данные правила.

Встроенные правила анализа для защищенных узлов

В данном разделе рассматриваются встроенные правила анализа, применяемые при мониторинге защищенных узлов.

Состояние узла

Правило определяет текущее состояние узла мониторинга, на котором установлено ПО ViPNet, и формирует оповещение, соответствующее текущему состоянию узла.

Параметр NODE_STATUS определяет 2 возможных состояния узла:

- Узел доступен — опрашиваемый узел доступен на сетевом уровне для Сервера мониторинга.
- Узел недоступен — опрашиваемый узел недоступен на сетевом уровне для Сервера мониторинга.

Код правила

```
if(Params.NODE_STATUS.hasPrevValue())
{
  if (Params.NODE_STATUS.getPrevValue() != Params.NODE_STATUS.REACHABLE &&
  Params.NODE_STATUS == Params.NODE_STATUS.REACHABLE) {
    Notificator.notify(Severity.INFO, "Узел доступен");
  } else if (Params.NODE_STATUS == Params.NODE_STATUS.UNREACHABLE &&
  Params.NODE_STATUS.getPrevValue() != Params.NODE_STATUS.UNREACHABLE) {
if (Params.GINFO_TYPE.hasPrevValue() &&
Params.GINFO_TYPE.getPrevValue()!=Params.GINFO_TYPE.E_COORDINATOR){
  Notificator.notify(Severity.INFO, "Узел недоступен");
}
  }
}
```

Статус программы Монитор

Правило выполняет проверку изменений состояния программы ViPNet Монитор и формирует оповещения, соответствующие текущему состоянию программы ViPNet Монитор.

Параметр `MONITOR_STATUS` определяет 5 возможных состояний программы ViPNet Монитор:

- Монитор включен — программа запущена.
- Ошибка при декодировании ответа — ошибка при обработке ответа от узла.

Код правила

```
if( Params.MONITOR_STATUS.hasPrevNonNullValue() && Params.NODE_STATUS ==
Params.NODE_STATUS.REACHABLE )
{
  if (Params.MONITOR_STATUS.getPrevNonNullValue() !=
  Params.MONITOR_STATUS.RUNNING && Params.MONITOR_STATUS ==
  Params.MONITOR_STATUS.RUNNING) {
    Notificator.notify(Severity.INFO, "Монитор включен");
  } else if (Params.MONITOR_STATUS == Params.MONITOR_STATUS.UDB_ERROR &&
Params.MONITOR_STATUS.getPrevNonNullValue() !=
Params.MONITOR_STATUS.UDB_ERROR) {
    Notificator.notify(Severity.INFO, "Ошибка при декодировании ответа");
  }
}
```

Статус программы Деловая почта

Правило выполняет проверку изменений состояния программы Деловая почта и формирует оповещения, соответствующие текущему состоянию программы Деловая почта.

Параметр `BMAIL_STATUS` определяет 4 возможных состояния программы Деловая почта:

- Деловая почта включена — программа запущена.
- Деловая почта выключена — программа не запущена.
- Деловая почта отсутствует — программа не установлена.

Код правила

```
if( Params.GINFO_TYPE.hasCurrentValue() && Params.GINFO_TYPE !=
Params.GINFO_TYPE.E_COORDINATOR && Params.BMAIL_STATUS.hasPrevNonNullValue()
&& Params.BMAIL_STATUS.hasCurrentValue() && Params.NODE_STATUS ==
Params.NODE_STATUS.REACHABLE )
{
  if (Params.BMAIL_STATUS.getPrevNonNullValue() != Params.BMAIL_STATUS.RUNNING
  && Params.BMAIL_STATUS == Params.BMAIL_STATUS.RUNNING){
    Notificator.notify(Severity.INFO, "Деловая почта включена");
  } else if (Params.BMAIL_STATUS == Params.BMAIL_STATUS.SHUT_DOWN &&
  Params.BMAIL_STATUS.getPrevNonNullValue() != Params.BMAIL_STATUS.SHUT_DOWN)
  {
    Notificator.notify(Severity.INFO, "Деловая почта выключена");
  } else if (Params.BMAIL_STATUS == Params.BMAIL_STATUS.ABSENT &&
  Params.BMAIL_STATUS.getPrevNonNullValue() != Params.BMAIL_STATUS.ABSENT) {
    Notificator.notify(Severity.INFO, "Деловая почта отсутствует");
  }
}
```

Статус программы Failover

Правило выполняет проверку изменений состояния программы Failover и формирует оповещения, соответствующие текущему состоянию программы Failover.

Параметр `FAILOVER_STATUS` определяет 5 возможных состояний программы Failover:

- Failover включен — программа запущена.
- Failover выключен — программа не запущена.
- Ошибка декодирования ответа узла — ошибка при обработке ответа от узла.
- Failover отсутствует — программа не установлена.

Код правила

```
if( Params.FAILOVER_STATUS.hasPrevNonNullValue() &&
Params.FAILOVER_STATUS.hasCurrentValue() && Params.NODE_STATUS ==
Params.NODE_STATUS.REACHABLE )
{
  if (Params.FAILOVER_STATUS.getPrevNonNullValue() !=
  Params.FAILOVER_STATUS.RUNNING && Params.FAILOVER_STATUS ==
  Params.FAILOVER_STATUS.RUNNING) {
    Notificator.notify(Severity.INFO, "Failover включен");
  } else if (Params.FAILOVER_STATUS == Params.FAILOVER_STATUS.SHUT_DOWN &&
  Params.FAILOVER_STATUS.getPrevNonNullValue() !=
  Params.FAILOVER_STATUS.SHUT_DOWN) {
    Notificator.notify(Severity.INFO, "Failover выключен");
```

```
  }else if (Params.FAILOVER_STATUS == Params.FAILOVER_STATUS.UDB_ERROR &&
  Params.FAILOVER_STATUS.getPrevNonNullValue() !=
  Params.FAILOVER_STATUS.UDB_ERROR) {
    Notificator.notify(Severity.INFO, "Ошибка при декодировании ответа");
  } else if (Params.FAILOVER_STATUS == Params.FAILOVER_STATUS.ABSENT &&
  Params.FAILOVER_STATUS.getPrevNonNullValue() !=
  Params.FAILOVER_STATUS.ABSENT) {
    Notificator.notify(Severity.INFO, "Failover отсутствует");
  }
}
```

Статус программы MFTP

Правило определяет изменения состояния транспортного модуля ViPNet MFTP и формирует оповещения, соответствующие текущему состоянию модуля ViPNet MFTP.

Параметр `MFTP_STATUS` определяет 5 возможных состояний модуля ViPNet MFTP:

- MFTP выключен — модуль MFTP не запущен.
- Ошибка при декодировании ответа — ошибка при декодировании ответа.
- MFTP отсутствует — модуль не установлен.

Код правила

```
if( Params.MFTP_STATUS.hasPrevNonNullValue() &&
Params.MFTP_STATUS.hasCurrentValue() && Params.NODE_STATUS ==
Params.NODE_STATUS.REACHABLE )
{
  if (Params.MFTP_STATUS == Params.MFTP_STATUS.SHUT_DOWN &&
  Params.MFTP_STATUS.getPrevNonNullValue() != Params.MFTP_STATUS.SHUT_DOWN) {
    Notificator.notify(Severity.MEDIUM, "MFTP выключен");
  }else if (Params.MFTP_STATUS == Params.MFTP_STATUS.UDB_ERROR &&
  Params.MFTP_STATUS.getPrevNonNullValue() != Params.MFTP_STATUS.UDB_ERROR) {
    Notificator.notify(Severity.MEDIUM, "Ошибка при декодировании ответа");
  } else if (Params.MFTP_STATUS == Params.MFTP_STATUS.ABSENT &&
  Params.MFTP_STATUS.getPrevNonNullValue() != Params.MFTP_STATUS.ABSENT) {
    Notificator.notify(Severity.MEDIUM, "MFTP отсутствует");
  }
}
```

Уровень безопасности

Правило выполняет проверку интегрального уровня безопасности узла мониторинга. Интегральный уровень безопасности определяется на основании анализа режимов

безопасности всех доступных сетевых интерфейсов узла и оценивается по наименее безопасному сетевому интерфейсу.

Примечание. В программах ViPNet Client и ViPNet Coordinator версии 4.0 и выше не используются режимы безопасности (вместо них создаются сетевые фильтры). Для узлов, на которых используется данное ПО версий 4.x, правило анализа «Уровень безопасности» срабатывать не будет.

В цикле выполняется перебор всех сетевых интерфейсов, имеющихся на узле и имевшихся при предыдущем опросе. При этом локальная переменная `interface` на каждой итерации цикла содержит значение объекта `NETWORKS` для доступа к текущим параметрам очередного сетевого интерфейса. Правило сравнивает текущее значение параметра `GIFINFO_MODE` (режим безопасности сетевого интерфейса) и его предыдущее значение, полученное при помощи метода `getPrevNonNullValue ()`. При изменении значения параметра выполняется проверка уровня безопасности интерфейса.

После опроса всех интерфейсов узла в зависимости от полученного значения переменной `result` производится оповещение с указанием полученного уровня безопасности.

Переменная `result` может принимать следующие значения:

- `1` — Низкий уровень безопасности присваивается сетевому интерфейсу при выполнении всех условий, указанных ниже:
  - Сетевой интерфейс доступен.
  - Сетевой интерфейс находится в режиме 4 или 5, заданном в программе ViPNet Монитор.
- `2` — Средний уровень безопасности присваивается сетевому интерфейсу при выполнении всех условий, указанных ниже:
  - Сетевой интерфейс доступен.
  - Сетевой интерфейс находится в режиме 2 или 3, заданном в программе ViPNet Монитор.
  - Переменная `result` не равна 1.

    Таким образом, если на предыдущих итерациях цикла был определен низкий уровень безопасности (`result=1`), то он не изменяется.
- `3` — Высокий уровень безопасности присваивается сетевому интерфейсу при выполнении всех условий, указанных ниже:
  - Сетевой интерфейс доступен.

- Сетевой интерфейс находится в режиме 1, заданном в программе ViPNet Монитор.
- Переменная `result` не равна 1 или 2.

  Таким образом, если на предыдущих итерациях цикла был определен низкий или средний уровень безопасности (`result=1` или `result=2`), то он не изменяется.

Код правила

```
result = 0; ## Уровень безопасности не изменился

foreach (interface in Params.NETWORKS) {
  if(interface.GIFINFO_MODE.hasCurrentValue() &&
  interface.GIFINFO_MODE.hasPrevNonNullValue()  &&
  interface.GIFINFO_USED.hasCurrentValue()  &&
  interface.GIFINFO_MODE.getPrevNonNullValue() != interface.GIFINFO_MODE){
    if ((interface.GIFINFO_MODE ==
    interface.GIFINFO_MODE.ALLOW_ALL_CONNECTIONS || interface.GIFINFO_MODE ==
    interface.GIFINFO_MODE.ALLOW_ALL_PACKETS) && interface.GIFINFO_USED ==
    interface.GIFINFO_USED.YES) {
      result = 1; ## Низкий уровень безопасности
    } else if ((interface.GIFINFO_MODE ==
    interface.GIFINFO_MODE.ALLOWED_CONNECTIONS_ONLY || interface.GIFINFO_MODE
    == interface.GIFINFO_MODE.ALLOW_ALL_NON_BLOCKED_CONNECTIONS) &&
    interface.GIFINFO_USED == interface.GIFINFO_USED.YES) {
      if( result != 1 ) {
        result = 2; ## Средний уровень безопасности
      }
    } else if (interface.GIFINFO_MODE ==
    interface.GIFINFO_MODE.BLOCK_ALL_PACKETS && interface.GIFINFO_USED ==
    interface.GIFINFO_USED.YES) {
      if( result != 1 && result != 2) {
        result = 3; ## Высокий уровень безопасности
      }
    }
  }
}

if (result == 1) {
  Notificator.notify(Severity.INFO, "Низкий уровень безопасности");
} else if (result == 2) {
  Notificator.notify(Severity.INFO, "Средний уровень безопасности");
} else if (result == 3) {
  Notificator.notify(Severity.INFO, "Высокий уровень безопасности");
}
```

Изменение версии ПО ViPNet

Правило выполняет проверку изменений версии ПО ViPNet, установленного на узле, и в случае изменения производит соответствующее оповещение.

Правило проверяет наличие текущего и предыдущего значений параметра `GINFO_PVER`, который содержит версию ПО ViPNet, установленного на узле мониторинга (включая номер сборки). При наличии текущего и предыдущего значений и при условии их несовпадения последовательно сравниваются четыре составляющие версии программы (начиная с первой). Если одна из составляющих текущей версии:

- больше той же составляющей предыдущей версии, то локальной переменной `result` присваивается значение `"Обновление"` (или значение `"Обновление (Сервис-пак)"` при несовпадении 4-ой составляющей);
- если меньше той же составляющей предыдущей версии, то локальной переменной `result` присваивается значение `"Откат"` (или значение `"Откат (Сервис-пак)"` при несовпадении 4-ой составляющей).

  При совпадении очередных составляющих сравниваются следующие составляющие.

Если все четыре составляющие версий совпадают, то переменной `result` присваивается значение `"Версия не изменилась"`.

Код правила

```
result = "Unknown";
result_ver = 0;

if (Params.GINFO_PVER.hasCurrentValue() &&
Params.GINFO_PVER.hasPrevNonNullValue() && Params.GINFO_PVER !=
Params.GINFO_PVER.getPrevNonNullValue()) {
  if(Params.GINFO_PVER.get(0) >
  Params.GINFO_PVER.getPrevNonNullValue().get(0)) {
    result = "Обновление";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(0) <
  Params.GINFO_PVER.getPrevNonNullValue().get(0)) {
    result = "Откат";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(1) >
  Params.GINFO_PVER.getPrevNonNullValue().get(1)) {
    result = "Обновление";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(1) <
  Params.GINFO_PVER.getPrevNonNullValue().get(1)) {
    result = "Откат";
```

```
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(2) >
  Params.GINFO_PVER.getPrevNonNullValue().get(2)) {
    result = "Обновление";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(2) <
  Params.GINFO_PVER.getPrevNonNullValue().get(2)) {
    result = "Откат";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(3) >
  Params.GINFO_PVER.getPrevNonNullValue().get(3)) {
    result = "Обновление";
    result_ver = Params.GINFO_PVER;
  } else if(Params.GINFO_PVER.get(3) <
  Params.GINFO_PVER.getPrevNonNullValue().get(3)) {
    result = "Откат";
    result_ver = Params.GINFO_PVER;
  } else {
    result = "Версия не изменилась";
  }
}

if(result == "Обновление") {
  event_str = "Обновление версии ПО с " +
  Params.GINFO_PVER.getPrevNonNullValue() + " до версии " + Params.GINFO_PVER;
  Notificator.notify(Severity.INFO, event_str);
} else if(result == "Откат") {
  event_str = "Откат версии ПО с " + Params.GINFO_PVER.getPrevNonNullValue() +
  " на версию " + Params.GINFO_PVER;
  Notificator.notify(Severity.INFO, event_str);
} else if(result != "Unknown") {
  Logger.error("Параметр result=" + result);
}
```

Прикладные задачи

Правило выполняет проверку изменений в списке прикладных задач, в которых зарегистрирован узел, и в случае изменений производит оповещения об изменении.

В правиле проверяется наличие текущего и предыдущего значений параметра `GIDNAMES_TASKLIST`, содержащего список прикладных задач, в которых зарегистрирован узел. При наличии обоих значений и при условии их несовпадения:

- Формируется список добавленных задач (в локальной переменной `grMsg`), то есть определяются задачи, отсутствующие в предыдущем списке, но присутствующие в текущем списке.
- Формируется список удаленных задач (в локальной переменной `revMsg`), то есть определяются задачи, присутствующие в предыдущем списке, но отсутствующие в текущем списке.

Код правила

```
if(Params.GIDNAMES_TASKLIST.hasCurrentValue() &&
Params.GIDNAMES_TASKLIST.hasPrevNonNullValue()){
grantedTasks = Utils.diff(Params.GIDNAMES_TASKLIST,
Params.GIDNAMES_TASKLIST.getPrevNonNullValue());
revokedTasks = Utils.diff(Params.GIDNAMES_TASKLIST.getPrevNonNullValue(),
Params.GIDNAMES_TASKLIST);

grMsg = "Добавлены следующие прикладные задачи: ";
foreach(task in grantedTasks){
  grMsg = grMsg + Utils.getTaskName(task) + ", ";
}

revMsg = "Удалены следующие прикладные задачи: ";
foreach(task in revokedTasks){
  revMsg = revMsg + Utils.getTaskName(task) + ", ";
}

if(grantedTasks.size() > 0){
  Notificator.notify(Severity.INFO, grMsg);
}

if(revokedTasks.size() > 0){
  Notificator.notify(Severity.INFO, revMsg);
}
}
```

Превышение порога для системных ресурсов

Правило выполняет проверку на превышения ограничений при использовании системных ресурсов на узле и формирует сообщение с информацией о текущем использовании системных ресурсов. Если хотя бы один из ресурсов занят более чем на 80% в течение двух последних опросов, правило производит соответствующее оповещение.

В правиле анализируются следующие параметры:

- GFOFSINFO_USAGE — процент использования дискового пространства. Проверяются текущие значения по всем имеющимся дискам.
- MEM_USAGE — процент использования оперативной памяти, проверяются текущее и предыдущее значения.
- GFOSTATE_A_TOTAL_CPU — процент загрузки процессора, проверяются текущее и предыдущее значения.

Код правила

```
disc_usage_result = "";
disc_usage_str = "";

foreach (device in Params.STORAGE_DEVICES) {
if (not Utils.partOf("/dev/ram",device.GFOFSINFO_DEVICE) and not
Utils.partOf("/dev/loop",device.GFOFSINFO_DEVICE)){
  if(device.GFOFSINFO_USAGE.hasCurrentValue() && device.GFOFSINFO_USAGE > 80)
  {
    disc_usage_str = "Диск " + device.GFOFSINFO_NAME + " заполнен более чем на
    80%";
    disc_usage_result = disc_usage_result + disc_usage_str + "; ";
  }
}
}
if (disc_usage_result != "") {
  Notificator.notify(Severity.MEDIUM, disc_usage_result);
}
if (Params.MEM_USAGE.hasCurrentValue() && Params.MEM_USAGE > 80 &&
Params.MEM_USAGE.hasPrevValue() && Params.MEM_USAGE.getPrevValue() > 80) {
  Notificator.notify(Severity.MEDIUM, "Память использована более чем на
  80%");
}
if (Params.GFOSTATE_A_TOTAL_CPU.hasCurrentValue() &&
Params.GFOSTATE_A_TOTAL_CPU > 80 && Params.GFOSTATE_A_TOTAL_CPU.hasPrevValue()
&& Params.GFOSTATE_A_TOTAL_CPU.getPrevValue() > 80) {
  Notificator.notify(Severity.MEDIUM, "Процессор используется более чем на
  80%");
}
```

Тип межсетевого экрана

Правило выполняет проверку изменений в режиме работы узла через межсетевой экран. В случае изменения режима, правило сохраняет новое значение и производит оповещение о текущем режиме.

В правиле проверяется наличие текущего и предыдущего значений параметра GIDSNATSETTINGS_FIREWALLTYPE, содержащего тип межсетевого экрана, за которым установлен узел мониторинга. При наличии текущего и предыдущего значений и при условии их несовпадения правило производит соответствующее оповещение.

Код правила

```
if (Params.GIDSNATSETTINGS_FIREWALLTYPE.hasCurrentValue() &&
Params.GIDSNATSETTINGS_FIREWALLTYPE.hasPrevNonNullValue()  &&
Params.GIDSNATSETTINGS_FIREWALLTYPE.getPrevNonNullValue() !=
Params.GIDSNATSETTINGS_FIREWALLTYPE) {
  if (Params.GIDSNATSETTINGS_FIREWALLTYPE ==
  Params.GIDSNATSETTINGS_FIREWALLTYPE.CLIENT_NO_EXTERNAL_FIREWALL ||
  Params.GIDSNATSETTINGS_FIREWALLTYPE ==
  Params.GIDSNATSETTINGS_FIREWALLTYPE.SERVER_NO_EXERNAL_FIREWALL) {
    Notificator.notify(Severity.INFO, "Установлен тип МСЭ: Внешний межсетевой
    экран не используется");
  } else if (Params.GIDSNATSETTINGS_FIREWALLTYPE ==
  Params.GIDSNATSETTINGS_FIREWALLTYPE.EXTERNAL_VIPNET_PROXY) {
    Notificator.notify(Severity.INFO, "Установлен тип МСЭ: ViPNet-
    координатор");
  } else if (Params.GIDSNATSETTINGS_FIREWALLTYPE ==
  Params.GIDSNATSETTINGS_FIREWALLTYPE.EXTERNAL_DYNAMIC_UDP_PROXY) {
    Notificator.notify(Severity.INFO, "Установлен тип МСЭ: С динамической
    трансляцией адресов");
  } else if (Params.GIDSNATSETTINGS_FIREWALLTYPE ==
  Params.GIDSNATSETTINGS_FIREWALLTYPE.EXTERNAL_STATIC_UDP_PROXY) {
    Notificator.notify(Severity.INFO, "Установлен тип МСЭ: Со статической
    трансляцией адресов");
  }
}
```

Параметры сетевых интерфейсов

Правило проверяет изменения в параметрах сетевых интерфейсов, заданных на узле мониторинга:

- IP-адрес — IP адрес, через который работает сетевой интерфейс.
- Режим безопасности — режим безопасности, заданный в программе ViPNet Монитор, установленной на узле мониторинга.

Примечание. В программах ViPNet Client и ViPNet Coordinator версии 4.0 и выше не используются режимы безопасности (вместо них создаются сетевые фильтры). Для узлов, на которых используется данное ПО версий 4.x, режим безопасности определяться не будет.

- Состояние — состояние сетевого интерфейса (включен или выключен).
- Тип — внешний или внутренний тип сетевого интерфейса.

В случае изменения любого из указанных параметров правило сохраняет новое значение и производит оповещение об изменении.

При помощи методов `hasCurrentValue()` и `hasPrevNonNullValue()` проверяется, существуют ли текущее значение коллекции объектов сетевых адаптеров и как минимум одно значение, полученное при предыдущих опросах. Если оба условия выполнены (оба метода возвращают значение `true`), производится циклический перебор всех сетевых интерфейсов, имеющихся на узле. Для каждого интерфейса сравниваются текущее значение и полученное с помощью метода `getPrevNonNullValue()` предыдущее значение следующих параметров:

- `GIFINFO_IPLIST` — IP-адреса интерфейса.
- `GIFINFO_MODE` — режим безопасности интерфейса.
- `GIFINFO_USED` — признак доступности интерфейса.
- `GIFINFO_EXTERNAL` — признак внешнего интерфейса.

При наличии обоих значений и при условии их неравенства (то есть при изменении значений параметров) производится оповещение о каждом измененном параметре с указанием нового значения.

Код правила

```
if(Params.NETWORKS.hasCurrentValue() &&
Params.NETWORKS.hasPrevNonNullValue()){
mode_result="undefined";
ip_result="undefined";
used_result="undefined";
ext_result="undefined";

foreach (interface in Params.NETWORKS) {

  if (interface.GIFINFO_NAME.hasCurrentValue() &&
  interface.GIFINFO_MODE.hasCurrentValue() &&
  interface.GIFINFO_MODE.hasPrevNonNullValue() &&
  (interface.GIFINFO_MODE.getPrevNonNullValue() != interface.GIFINFO_MODE) &&
  Params.GINFO_TYPE.hasCurrentValue()) {
    if(Params.GINFO_TYPE == Params.GINFO_TYPE.E_HOST  && mode_result ==
    "undefined") {
```

```
      mode_result = "Изменился режим безопасности: Режим=";
      mode_result = mode_result + interface.GIFINFO_MODE;
    } else if(Params.GINFO_TYPE == Params.GINFO_TYPE.E_COORDINATOR) {
      if(mode_result == "undefined") {
        mode_result = "Изменился режим безопасности:";
      }
      mode_result = mode_result + " Имя='";
      mode_result = mode_result + interface.GIFINFO_NAME;
      mode_result = mode_result + "' Режим=";
      mode_result = mode_result + interface.GIFINFO_MODE;
      mode_result = mode_result + ";";
    }
  }

  if (interface.GIFINFO_NAME.hasCurrentValue() &&
  interface.GIFINFO_USED.hasCurrentValue() &&
  interface.GIFINFO_USED.hasPrevNonNullValue() &&
  interface.GIFINFO_USED.getPrevNonNullValue() != interface.GIFINFO_USED) {

    if(used_result == "undefined") {
      used_result = "Изменилось состояние интерфейса(ов):";
    }

    used_result = used_result + " Имя='";
    used_result = used_result + interface.GIFINFO_NAME;
    used_result = used_result + "' - ";
    if(interface.GIFINFO_USED == interface.GIFINFO_USED.YES) {
      used_result = used_result + "Включен;";
    } else {
      used_result = used_result + "Выключен;";
    }
  }
if (Params.GINFO_TYPE.hasCurrentValue() &&
Params.GINFO_TYPE==Params.GINFO_TYPE.E_COORDINATOR)
{
      if (interface.GIFINFO_NAME.hasCurrentValue() &&
      interface.GIFINFO_IPLIST.hasCurrentValue() &&
      interface.GIFINFO_IPLIST.hasPrevNonNullValue() &&
      interface.GIFINFO_IPLIST.getPrevNonNullValue() !=
      interface.GIFINFO_IPLIST) {
        if(ip_result == "undefined") {
          ip_result = "Смена IP-адреса(ов) на интерфейсах:";
        }

          ip_result = ip_result + " Имя='";
```

```
            ip_result = ip_result + interface.GIFINFO_NAME;
            ip_result = ip_result + "' с ";
            ip_result = ip_result +
            interface.GIFINFO_IPLIST.getPrevNonNullValue();
            ip_result = ip_result + " на ";
            ip_result = ip_result + interface.GIFINFO_IPLIST;
            ip_result = ip_result + ";";
            }

            if (interface.GIFINFO_NAME.hasCurrentValue() &&
            interface.GIFINFO_EXTERNAL.hasCurrentValue() &&
            interface.GIFINFO_EXTERNAL.hasPrevNonNullValue() &&
            (interface.GIFINFO_EXTERNAL.getPrevNonNullValue() !=
            interface.GIFINFO_EXTERNAL) &&
            Params.GINFO_TYPE.hasCurrentValue() && (Params.GINFO_TYPE ==
            Params.GINFO_TYPE.E_COORDINATOR)) {
            if(ext_result == "undefined") {
              ext_result = "Изменился признак внешнего интерфейса(ов):";
            }
            ext_result = ext_result + " Имя='";
            ext_result = ext_result + interface.GIFINFO_NAME;
            ext_result = ext_result + "' - ";
            if(interface.GIFINFO_EXTERNAL ==
            interface.GIFINFO_EXTERNAL.EXTERNAL) {
              ext_result = ext_result + "Внешний;";
            } else {
              ext_result = ext_result + "Внутренний;";
            }
            }
}
}

if( mode_result != "undefined") {
  Notificator.notify(Severity.MEDIUM, mode_result);
}

if( ip_result != "undefined") {
  Notificator.notify(Severity.MEDIUM, ip_result);
}

if( used_result != "undefined") {
  Notificator.notify(Severity.MEDIUM, used_result);
}

if( ext_result != "undefined") {
  Notificator.notify(Severity.MEDIUM, ext_result);
}
```

```
}
```

Параметры MFTP

Правило выполняет проверку на превышение допустимого предела на:

- Количество конвертов в очереди MFTP . Максимальное число конвертов в очереди — 500.
- Общий объем конвертов в очереди MFTP. Максимальный объем всех конвертов в очереди — 500 МБ.

В случае превышения допустимого предела любым из указанных параметров правило производит соответствующее оповещение.

В коде правила анализируются значения параметров:

- `GMFTPSTAT_QUEUE_COUNT` — количество конвертов в очереди;
- `GMFTPSTAT_QUEUE_SIZE` — общий объем конвертов в очереди.

Для этих параметров проверяется наличие текущего значения и превышение допустимого предела. При выполнении указанных условий для какого-либо параметра формируется сообщение о превышении, которое записывается в соответствующую переменную.

Примечание. Чтобы изменить условия проверки параметров транспортного модуля MFTP (допустимые пределы), необходимо сделать копию встроенного правила **Параметры MFTP** и в сделанной копии в выражении для анализа присвоить другие значения переменным `max_count` (максимальное количество конвертов в очереди) и `max_size` (максимальный объем конвертов в очереди). Например:

```
max_count = 300;
max_size = 200.
```

Код правила

```
max_count = 1500;
max_size = 1000.0; ## Мегабайт

if (Params.GMFTPSTAT_QUEUE_COUNT.hasCurrentValue() &&
Params.GMFTPSTAT_QUEUE_COUNT > max_count &&
```

```
Params.GMFTPSTAT_QUEUE_COUNT.hasPrevValue() &&
Params.GMFTPSTAT_QUEUE_COUNT.getPrevValue() > max_count) {
  notify_str = "Сейчас в очереди больше допустимых " + max_count + " пакетов";
  Notificator.notify(Severity.INFO, notify_str);
}

if (Params.GMFTPSTAT_QUEUE_SIZE.hasCurrentValue() &&
Params.GMFTPSTAT_QUEUE_SIZE > max_size &&
Params.GMFTPSTAT_QUEUE_SIZE.hasPrevValue() &&
Params.GMFTPSTAT_QUEUE_SIZE.getPrevValue() > max_size) {
  notify_str = "Размер очереди больше максимально допустимого размера в " +
  max_size + " МБ.";
  Notificator.notify(Severity.INFO, notify_str);
}
```

Журнал ОС

Правило проверяет наличие сведений об ошибках и предупреждениях в системном журнале и в журнале приложений операционной системы. При наличии таких сведений правило производит оповещения о найденных событиях.

В коде правила выполняется циклический перебор всех записей, содержащихся в журналах событий ОС. При этом локальная переменная `event` на каждой итерации цикла содержит значение объекта `Events` для доступа к текущим параметрам очередной записи о событии. Для каждой записи с помощью параметра `Events` проверяется наличие значений параметров:

- `GFOSYSJ_TYPE` — тип события;
- `GFOSYSJ_DESCR` — описание события;
- `GFOSYSJ_JOURNAL` — журнал, содержащий запись о событии.

При наличии значений всех указанных параметров проверяется тип события и тип журнала. Если событие является ошибкой (`error_level = 1)` или предупреждением (`warn_level = 2)` и при этом содержится в системном журнале ОС (`System`) или в журнале приложений (`Application`), производится оповещение о событии с уровнем критичности, соответствующим типу события. В случае, если не удалось установить название журнала сообщение об ошибке или предупреждении также записывается в историю событий мониторинга.

Код правила

```
journal_description = "";
journal_name= "";
err_notify = "";
```

```
warn_notify = "";
if (Params.GINFO_TYPE.hasCurrentValue() &&
Params.GINFO_TYPE==Params.GINFO_TYPE.E_COORDINATOR){
foreach (event in Params.EVENTS) {
  if (event.GFOSYSJ_TYPE.hasCurrentValue() &&
  event.GFOSYSJ_DESCR.hasCurrentValue() &&
  event.GFOSYSJ_JOURNAL.hasCurrentValue()) {
    if (event.GFOSYSJ_DESCR == "")
      journal_description = "[описание отсутствует]";
    else
      journal_description = event.GFOSYSJ_DESCR;

    if (event.GFOSYSJ_JOURNAL == "")
      journal_name = "[название отсутствует]";
    else
      journal_name = event.GFOSYSJ_JOURNAL;

    if (event.GFOSYSJ_TYPE == event.GFOSYSJ_TYPE.ERROR) {
      err_notify_str = "Ошибка";
      if(journal_name == "System") {
        err_notify_str = err_notify_str + " в системном журнале: " +
        journal_description + "; ";
      } else if(journal_name == "Application") {
        err_notify_str = err_notify_str + " в журнале приложений: " +
        journal_description + "; ";
      } else {
        err_notify_str = err_notify_str + " в журнале " + journal_name + ": "
        + journal_description + "; ";
        Logger.error("От неизвестного журнала: " + journal_name + " поступила
        ошибка: " + journal_description);
      }

      err_notify = err_notify + err_notify_str;
    }

    if (event.GFOSYSJ_TYPE == event.GFOSYSJ_TYPE.WARNING) {
      warn_notify_str = "Предупреждение";
      if(journal_name == "System") {
        warn_notify_str = warn_notify_str + " в системном журнале: " +
        journal_description + "; ";
      } else if(journal_name == "Application") {
        warn_notify_str = warn_notify_str + " в журнале приложений: " +
        journal_description + "; ";
      } else {
        warn_notify_str = warn_notify_str + " в журнале " + journal_name + ":
        " + journal_description + "; ";
```

```
        Logger.error("От неизвестного журнала: " + journal_name + " поступило
        предупреждение: " + journal_description);
      }

      warn_notify = warn_notify + warn_notify_str;
    }
  }
}

if(err_notify != "")
  Notificator.notify(Severity.INFO, err_notify);

if(warn_notify != "")
  Notificator.notify(Severity.INFO, warn_notify);
}
```

Переключение кластера

Данное правило информирует пользователей о том, что произошло переключение между активным и пассивным элементами кластера, а также фиксирует время переключения кластера.

Правило анализирует следующие параметры событий кластера:

- `GFOJOURNAL_TIME` — время регистрации события.
- `GFOJOURNAL_EVENT` — тип зарегистрированного события. Правило следит за типом события `FO_EVENT_SWITCH` — переключение элемента кластера в активный режим.

Код правила

```
foreach (param in Params.JOURNAL_EVENTS){
  if(param.GFOJOURNAL_TIME.hasCurrentValue() and
  param.GFOJOURNAL_EVENT.hasCurrentValue()){
    if(param.GFOJOURNAL_EVENT.getCurrentValue() ==
    param.GFOJOURNAL_EVENT.FO_EVENT_SWITCH){
      Notificator.notify(Severity.MEDIUM, "Переключение серверов кластера
      произошло в  " + param.GFOJOURNAL_TIME.getCurrentValueFormatted());
      }
  }
}
```

Состояние пассивного элемента кластера

Правило позволяет отслеживать состояние пассивного элемента кластера (доступен или недоступен), в случае недоступности пассивного элемента правило выдает сообщение об этом. Если пассивный элемент кластера будет недоступен, то при сбое активного элемента будет невозможно переключение кластера.

Код правила

```
if(Params.NODE_P_STATUS.hasPrevValue()){
  if (Params.NODE_P_STATUS == Params.NODE_P_STATUS.UNREACHABLE &&
  Params.NODE_P_STATUS.getPrevValue() != Params.NODE_P_STATUS.UNREACHABLE) {
    Notificator.notify(Severity.MEDIUM, "Пассивный элемент кластера
    недоступен");
  }
}
```

Встроенные правила анализа для открытых узлов

В данном разделе рассматриваются встроенные правила анализа, применяемые при мониторинге открытых узлов.

Установка приложения

Правило информирует об установке новых приложений на открытом узле.

Данное правило производит анализ списка установленных приложений (любых приложений, в том числе ViPNet), полученного при предыдущем опросе узла. Если в список были добавлены приложения, правило анализа формирует событие, в сообщении которого указывается список новых установленных приложений.

Примечание. В системе мониторинга возможно отображение не всех приложений, установленных на открытом узле, так как SNMP-агент, запущенный на данном узле, может передавать Серверу мониторинга неполный список установленных приложений.

Код правила

```
if (Params.hrSWInstalledTable.hasCurrentValue() &&
Params.hrSWInstalledTable.hasPrevNonNullValue() &&
Params.NODE_STATUS.getPrevValue()==Params.NODE_STATUS.REACHABLE) {
  installed = Utils.diff(Params.hrSWInstalledTable,
  Params.hrSWInstalledTable.getPrevNonNullValue());
  if (installed.size() > 0) {
    msg = "В системе установлены следующие приложения: ";
    first = true;
    foreach(application in installed){
      if (!first){
        msg = msg + ", ";
      } else {
        first = false;
      }
        msg = msg + application.hrSWInstalledName;
    }
```

```
    Notificator.notify(Severity.INFO, msg);
  }
}
```

Удаление приложения

Правило информирует об удалении приложений на открытом узле.

Данное правило производит анализ списка установленных приложений (любых приложений, в том числе ViPNet), полученного при предыдущем опросе узла. Если из списка были удалены какие-либо приложения, правило анализа формирует событие, в сообщении которого указывается список удаленных приложений.

Код правила

```
if (Params.hrSWInstalledTable.hasCurrentValue() &&
Params.hrSWInstalledTable.hasPrevNonNullValue() &&
Params.NODE_STATUS.getPrevValue()==Params.NODE_STATUS.REACHABLE) {
  uninstalled = Utils.diff(Params.hrSWInstalledTable.getPrevNonNullValue(),
  Params.hrSWInstalledTable);
  if (uninstalled.size() > 0) {
    msg = "Из системы удалены следующие приложения: ";
    first = true;
    foreach(application in uninstalled){
      if (!first){
        msg = msg + ", ";
      } else {
        first = false;
      }
      msg = msg + application.hrSWInstalledName;
    }
    Notificator.notify(Severity.MEDIUM, msg);
  }
}
```

Запуск сервисов

Правило информирует о запустившихся на открытом узле сетевых сервисах.

Данное правило производит анализ списка запущенных сервисов, полученного при предыдущем опросе узла. Если в список добавились новые сервисы, правило анализа формирует событие, в сообщении которого указывается список новых запущенных сервисов.

Код правила

```
if(Params.svSvcTable.hasCurrentValue() &&
Params.svSvcTable.hasPrevNonNullValue()){
  newOrChanged = Utils.diff(Params.svSvcTable,
  Params.svSvcTable.getPrevNonNullValue());
  if (newOrChanged.size() > 0) {
    msg = "Запустились следующие сервисы: ";
    first = true;
    foreach(service in newOrChanged) {
      if(service.svSvcOperatingState == service.svSvcOperatingState.active) {
        if (first){
          first = false;
        } else {
          msg = msg + ", ";
        }
        msg = msg + service.svSvcName;
      }
    }
    if (!first) {
      Notificator.notify(Severity.INFO, msg);
    }
  }
}
```

Остановка сервисов

Правило информирует об остановившихся на открытом узле сетевых сервисах.

Данное правило производит анализ списка запущенных сервисов, полученного при предыдущем опросе узла. Если из списка были удалены какие-либо сервисы, правило анализа формирует событие, в сообщении которого указывается список остановившихся сервисов.

Код правила

```
if(Params.svSvcTable.hasCurrentValue() &&
Params.svSvcTable.hasPrevNonNullValue()){
  stoppedOrChanged = Utils.diff(Params.svSvcTable.getPrevNonNullValue(),
  Params.svSvcTable);
  if (stoppedOrChanged.size() > 0) {
    msg = "Остановились следующие сервисы: ";
    first = true;
    foreach(service in stoppedOrChanged) {
      if (first){
        first = false;
      } else {
```

```
        msg = msg + ", ";
      }
      msg = msg + service.svSvcName;
    }
    if (!first) {
      Notificator.notify(Severity.INFO, msg);
    }
  }
}
```

Загрузка оперативной памяти

Правило информирует о загруженности оперативной памяти открытого узла. Если загруженность оперативной памяти превышает 90%, правилом формируется событие мониторинга с соответствующим сообщением.

Данное правило анализирует следующие параметры открытого узла:

- `hrStorageType` — тип хранилища данных. Правило анализирует тип хранилища `hrStorageRam` (оперативная память).
- `hrStorageSize` — общее количество блоков данных в хранилище.
- `hrStorageUsed` — количество занятых блоков данных.

Код правила

```
if (Params.hrStorageTable.hasCurrentValue() &&
Params.hrStorageTable.hasPrevNonNullValue()) {
  foreach (device in Params.hrStorageTable) {
    if(device.hrStorageType == device.hrStorageType.hrStorageRam) {
      currentUsage = (device.hrStorageUsed / device.hrStorageSize) * 100;

      if(currentUsage > 90) {
        Notificator.notify(Severity.MEDIUM, "Оперативная память занята более
        чем на 90%");
      }
    }
  }
}
```

Загрузка дисков

Правило информирует о загруженности жесткого диска открытого узла. Если загруженность жесткого диска превышает 80%, правилом формируется событие мониторинга с соответствующим сообщением.

Данное правило анализирует следующие параметры открытого узла:

- `hrStorageType` — тип хранилища данных. Правило анализирует тип хранилища `hrStorageFixedDisk` (жесткий диск).
- `hrStorageSize` — общее количество блоков данных в хранилище.
- `hrStorageUsed` — количество занятых блоков данных.

Код правила

```
if (Params.hrStorageTable.hasCurrentValue() &&
Params.hrStorageTable.hasPrevNonNullValue()) {
  foreach (device in Params.hrStorageTable) {
    if(device.hrStorageType == device.hrStorageType.hrStorageFixedDisk) {
      currentUsage = (device.hrStorageUsed / device.hrStorageSize) * 100;

      if(currentUsage > 80) {
        Notificator.notify(Severity.MEDIUM, "Диск " + device.hrStorageDescr +
        " заполнен более чем на 80%");
      }
    }
  }
}
```

Скачок атак высокого уровня текущего сенсора IDS

Правило вычисляет среднее количество атак высокого уровня на текущем сенсоре ViPNet IDS за промежуток времени. В случае превышения заданного значения константы (`AvgAttConst`) правило выдает сообщение с высоким уровнем критичности события.

Код правила

```
AvgAttConst=0.03;
if(Params.infIDSSysReqEnd.hasCurrentValue() and
Params.infIDSSysReqEnd.hasPrevNonNullValue() and
Params.infIDSSysSensID.hasCurrentValue()) {
  TimeDiff = Params.infIDSSysReqEnd.getCurrentValue() -
  Params.infIDSSysReqEnd.getPrevNonNullValue();
```

```
  if(TimeDiff>0){
    foreach (param in Params.infIDSAgrAttacksTable) {
      if(param.infIDSSensIndex.hasCurrentValue() and
      param.infIDSAgrAttacksSeverity.hasCurrentValue() and
      param.infIDSAgrAttacksNum.hasCurrentValue() and
      param.infIDSSensIndex.hasPrevNonNullValue() and
      param.infIDSAgrAttacksSeverity.hasPrevNonNullValue() and
      param.infIDSAgrAttacksNum.hasPrevNonNullValue()) {
        AttackDiff= param.infIDSAgrAttacksNum.getCurrentValue()-
        param.infIDSAgrAttacksNum.getPrevNonNullValue();
        AvgAtt=(AttackDiff*1.0)/(TimeDiff*1.0);
        if(param.infIDSSensIndex.getCurrentValue() ==
        Params.infIDSSysSensID.getCurrentValue() and
        param.infIDSAgrAttacksSeverity.getCurrentValue() ==
        param.infIDSAgrAttacksSeverity.high and AvgAtt>AvgAttConst){
          Notificator.notify(Severity.HIGH, "Внимание, большое количество атак
          на текущем сенсоре IDS");
        }
      }
    }
  }
}
```

Общий скачок атак текущего сенсора

Правило информирует о превышении заданного значения (`AvgAttConst`) среднего количества атак на текущем сенсоре ViPNet IDS за определенный интервал времени.

Код правила

```
AvgAttConst=0.2;
if(Params.infIDSSysReqEnd.hasCurrentValue() and
Params.infIDSSysReqEnd.hasPrevNonNullValue() and
Params.infIDSSysSensID.hasCurrentValue() and
Params.infIDSSysAttacksNum.hasCurrentValue() and
Params.infIDSSysAttacksNum.hasPrevNonNullValue()) {
  TimeDiff = Params.infIDSSysReqEnd.getCurrentValue() -
  Params.infIDSSysReqEnd.getPrevNonNullValue();
  if(TimeDiff>0) {
    AttackDiff= Params.infIDSSysAttacksNum.getCurrentValue()-
    Params.infIDSSysAttacksNum.getPrevNonNullValue();
    AvgAtt=(AttackDiff*1.0)/(TimeDiff*1.0);
```

```
    if(AvgAtt>AvgAttConst) {
      Notificator.notify(Severity.HIGH, "Внимание, произошел скачок общего
      количества атак на текущем сенсоре IDS");
    }
  }
}
```

Глоссарий

S

SWJournal

Текстовый файл, в котором содержится информация из журнала событий Сервера мониторинга, а также о проблемах, возникших при работе Сервера мониторинга. Данный файл может быть использован для анализа работы Сервера мониторинга и действий пользователей, производимых с сервером, в случае нештатных ситуаций, когда подключение к серверу с помощью АРМ мониторинга невозможно.

V

ViPNet Центр управления сетью (ЦУС)

В сети, которая администрируется при помощи ПО ViPNet Administrator, ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;

- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

В сети, которая администрируется при помощи ПО ViPNet Network Manager, Центр управления сетью — это рабочее место администратора сети ViPNet. В ЦУСе создается структура сети ViPNet, формируются и отправляются на сетевые узлы обновления наборов ключей и программного обеспечения ViPNet.

А

АРМ мониторинга

Узел сети ViPNet (ViPNet-клиент), с которого осуществляется подключение через веб-браузер к Серверу мониторинга для его настройки, получения доступа к данным мониторинга и получения оповещений. Один и тот же АРМ мониторинга может использоваться для подключения к нескольким Серверам мониторинга.

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Б

База необработанных данных

База данных, в которой временно хранятся параметры узлов мониторинга до их обработки правилами анализа. База необработанных данных организована как оперативная база OLTP (англ. Online Transaction Processing — оперативная обработка транзакций).

Г

Группа мониторинга

Именованное множество узлов мониторинга из числа узлов, наблюдаемых Сервером мониторинга. Группы используются для логического объединения узлов мониторинга по какому-либо признаку, например, по принадлежности к подразделению или региону. На

каждом Сервере мониторинга задаются свои группы мониторинга, при этом существуют служебные группы, обязательные для всех Серверов мониторинга.

З

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

К

Каскад

Многоуровневая иерархическая структура Серверов мониторинга, связанных отношениями «родитель-потомок». Каждый дочерний Сервер мониторинга в каскаде передает результаты мониторинга своих узлов (объектов мониторинга) родительскому Серверу мониторинга. Каскад может применяться для снижения нагрузки на отдельные Серверы мониторинга, а также для организации мониторинга сегментированной сети при отсутствии связей на уровне ViPNet между узлами из разных сегментов.

Каскадируемый узел мониторинга

Узел, который является объектом мониторинга не данного Сервера мониторинга, а одного из дочерних Серверов мониторинга по всему каскаду. Данный Сервер мониторинга только получает оповещения о событиях на каскадируемом узле от своих дочерних Серверов мониторинга.

Конструктор правил анализа

Средство для создания простых правил анализа, не требующее знания специального языка и стандартных выражений, которые используются при создании сложных правил анализа с помощью редактора. Конструктор позволяет задать совокупность условий, благодаря которым можно легко обнаружить интересующие события, возникающие на узлах мониторинга.

Н

Необработанные параметры

Параметры узлов мониторинга, собранные и сохраненные Сервером мониторинга до их обработки правилами анализа.

О

Оповещения

Информационные сообщения, которые формируются в правилах анализа при обнаружении каких-либо событий. Существуют следующие типы оповещений:

- в списке узлов;
- всплывающие сообщения;
- на карте;
- звуковые;
- по электронной почте;
- по Деловой почте;
- по SMS.

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

П

Пакет настроек

Пакет настроек, позволяющий настроить систему мониторинга с учетом особенностей ее использования. Пакет настроек может содержать файлы локализации, карты, дополнительные встроенные правила анализа, шаблоны писем и типы узлов, отличные от используемых по умолчанию. Пакет настроек устанавливается на компьютер при первичной установке ПО Сервер мониторинга или при обновлении ПО Сервер мониторинга. Установленный пакет настроек можно обновить с помощью файла дистрибутива `StateWatcherInstaller.jar`.

ПК ViPNet StateWatcher

Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, который предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

Правило анализа

Правило, согласно которому производится анализ различных параметров узлов мониторинга и формируются события мониторинга. Существует ряд правил, идущих в составе пакета настроек, эти правила по умолчанию присутствуют на всех Серверах мониторинга, на которых установлен пакет настроек, идущий по умолчанию. При этом на каждом Сервере мониторинга могут быть заданы свои дополнительные правила анализа.

Р

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

С

Сервер мониторинга

Узел сети ViPNet (ViPNet-клиент), на котором установлено специальное программное обеспечение для осуществления мониторинга сети. Сервер мониторинга выполняет все основные функции по мониторингу сети: сбор, анализ и хранение информации о состоянии сетевых узлов, оповещение о сбоях в работе узлов и критических событиях на них. В ПК ViPNet StateWatcher может быть несколько Серверов мониторинга.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Система геопозиционирования

Модуль программного обеспечения Сервер мониторинга, который осуществляет получение от общедоступных серверов геолокации реальных координат узлов по их IP-

адресам. Также с помощью системы геопозиционирования можно разместить узлы на карте в соответствии с полученными координатами, при этом в случае изменения координат узлы будут автоматически перемещены системой геопозиционирования в новое положение на карте.

Служба SNMP (SNMP-агент)

Программное обеспечение, запускаемое на открытых узлах и предназначенное для передачи параметров данных узлов SNMP-менеджеру. В качестве SNMP-агента на открытых узлах может быть использована соответствующая служба Windows — Windows SNMP Service.

Событие мониторинга

Любое изменение состояния узла из числа отслеживаемых правилами анализа, которое было обнаружено на узле мониторинга. Каждому событию мониторинга присваивается атрибут — уровень критичности, который отражает степень важности события. Каждое событие мониторинга сопровождается оповещением, заданным для этого события в соответствующем правиле анализа.

Т

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

У

Узел мониторинга

Узел сети ViPNet (ViPNet-клиент или ViPNet-координатор), являющийся объектом мониторинга. За каждым Сервером мониторинга закрепляется свое множество узлов мониторинга, при этом один и тот же сетевой узел может быть объектом мониторинга нескольких Серверов мониторинга.

Ш

Шаблоны писем оповещений

Файлы с расширением `.jasper`, которые представляют собой скомпилированные шаблоны Jasper-отчета (JasperReports). Для работы с этими шаблонами используется свободно распространяемый графический редактор отчетов iReport, входящий в комплект поставки. Последнюю версию редактора iReport можно скачать по ссылке http://jasperforge.org/projects/ireport/.

Указатель

S
SWJournal - 288

V
ViPNet Центр управления сетью (ЦУС) - 14, 288

А
АРМ мониторинга - 289
Аутентификация - 289

Б
База необработанных данных - 289

В
Введение - 9
Взаимодействие с ПАК ViPNet IDS - 40
Возможные неполадки и способы их устранения - 191
Восстановление баз данных - 171, 180
Восстановление баз данных без переустановки ПО Сервер мониторинга - 180, 189
Восстановление баз данных после установки ПО Сервер мониторинга - 180, 189
Время на Сервере мониторинга не соответствует времени операционной системы - 193
Встроенные правила анализа - 29, 98, 261
Встроенные правила анализа для защищенных узлов - 262
Встроенные правила анализа для открытых узлов - 281

Г
Группа мониторинга - 289

Д
Действия администратора дочернего Сервера мониторинга при включении его сервера в каскад - 131
Для кого предназначен документ - 10
Добавление открытых узлов в список связей Сервера мониторинга - 40, 89, 258
Добавление Сервера мониторинга в каскад - 64, 129
Добавление узлов на карту в соответствии с их координатами - 123, 126
Дополнительные настройки в ОС Windows - 254

Ж
Журнал ОС - 277

З
Загрузка дисков - 285
Загрузка оперативной памяти - 284
Задание и изменение параметров правила с помощью конструктора - 100, 102, 105
Запуск сервисов - 282
Защищенный узел - 84, 290

И
Изменение версии ПО ViPNet - 268
Изменение параметров мониторинга узла - 85, 92, 107
Информация о стороннем коде - 19

К
Каскад - 128, 290
Каскадирование Серверов мониторинга - 31
Каскадируемый узел мониторинга - 290
Коллекции - 162, 163
Комментарии - 158
Комплект поставки - 17, 44, 47, 58, 59, 193
Компоненты правил анализа - 156
Конструктор правил анализа - 99, 290
Контролируемые параметры - 204
Контролируемые параметры открытых узлов - 38, 228
Контролируемые параметры ПАК ViPNet IDS - 40, 243
Контролируемые параметры узлов мониторинга - 37, 162, 205
Копирование правила анализа - 98, 105, 106, 261

Л
Лицензирование Сервера мониторинга - 16, 33

М
Механизм работы Сервера мониторинга - 28
Мониторинг кластера горячего резервирования - 37
Мониторинг узлов по протоколу SNMP - 38, 40

Н
Назначение пользователю postgres прав доступа к папкам в ОС Microsoft Windows - 45, 49, 184, 192, 258
Настройка визуальных оповещений - 108, 112
Настройка звуковых оповещений - 108, 112
Настройка карты - 122
Настройка каскада - 33, 128
Настройка оповещений - 98, 107, 112, 113, 115, 116, 117
Настройка оповещений по SMS - 76, 109, 116
Настройка оповещений по Деловой почте - 109, 115
Настройка оповещений по протоколу Syslog - 110, 117
Настройка оповещений по электронной почте - 75, 108, 113
Настройка подключения к прокси-серверу - 120
Настройка правил анализа - 40, 98, 107
Настройка Сервера мониторинга - 71
Настройка Сервера мониторинга с помощью мастера - 72, 107
Настройка службы SNMP на открытом узле - 38, 89, 254
Настройка типов узлов мониторинга - 96
Настройка узлов и групп мониторинга - 84
Настройка учетных записей - 78
Настройка экспорта необработанных параметров узлов на сетевой ресурс - 146
Не открывается окно информации об узле мониторинга - 197
Не удается запустить службу Apache Tomcat - 195
Не удается установить или запустить PostgreSQL - 191
Не удается установить каскад - 198
Необработанные параметры - 145, 290
Неограниченный рост базы данных - 194
Нефункциональные характеристики ПК ViPNet StateWatcher - 250
Новые возможности версии 4.3 - 20

О
О документе - 10
О программе Сервер мониторинга - 12
Обновление пакета настроек - 29, 65
Обновление ПО Сервер мониторинга - 55, 59, 64, 65, 128
Обратная связь - 26
Общий скачок атак текущего сенсора - 286
Объект для доступа к уровням критичности - 165

Объекты и методы для доступа к значениям параметров узлов - 161
Объекты и методы для задания оповещений - 165
Объекты и методы для записи сообщений в журнал для правил анализа - 166
Объекты и методы для получения вспомогательных параметров - 164
Операторы - 159
Оповещения - 291
Определение основных показателей базы данных мониторинга - 177, 190
Особенности импорта настроек - 134, 136
Остановка сервисов - 283
Открытый узел - 291
Отслеживание событий, связанных с фильтрацией трафика - 119

П

Пакет настроек - 29, 54, 61, 65, 98, 108, 122, 261, 291
Параметры MFTP - 276
Параметры сетевых интерфейсов - 272
Переключение кластера - 279
Переменные - 158
Перемещение новых узлов в группу мониторинга - 40, 85, 90, 107
ПК ViPNet StateWatcher - 291
Подключение к Серверу мониторинга - 69, 78
Показатели производительности системы мониторинга - 250
Порядок обновления ПО Сервер мониторинга - 58
Порядок обновления ПО Сервера мониторинга при каскадной организации системы мониторинга - 63
Порядок проведения резервного копирования - 171
Порядок установки обязательного ПО - 43, 44, 48, 49, 59, 65
Последовательность установки ПО Сервер мониторинга - 43
Правила анализа - 155
Правило анализа - 156, 292
Превышение порога для системных ресурсов - 270
Прикладные задачи - 269
Примеры синтаксиса - 166
Принципы организации мониторинга - 27
Проблемы доступа и аутентификации на АРМ мониторинга - 197
Проблемы при записи событий мониторинга в базу данных - 195
Проблемы при использовании прокси-сервера - 198
Проблемы при подключении к Серверу мониторинга через веб-интерфейс - 196
Проверка корректности восстановления - 177, 190
Проверка правильности установки ПО Сервер мониторинга - 43, 55, 59
Проверка синтаксиса правила анализа - 102, 169
Просмотр журнала событий - 17, 152

Р

Разделение событий по уровням критичности - 30
Расчет нагрузки на трафик при использовании ПК ViPNet StateWatcher - 252
Резервирование баз данных - 67, 171, 173, 180
Резервирование и восстановление конфигурационных файлов и отладочных журналов - 171, 172
Резервное копирование и восстановление - 170, 194
Рекомендации по настройке браузера Internet Explorer - 14
Роль - 96, 292
Ротация данных - 149

С

Секция [bm] - 148
Секция [collection] - 140
Секция [control] - 141, 149, 150
Секция [export] - 145, 147, 148
Секция [gis] - 145
Секция [sms] - 117, 144
Секция [storage] - 140
Сервер мониторинга - 292
Сеть ViPNet - 292

Синтаксис правил анализа - 29, 100, 157, 158, 169
Система геопозиционирования - 292
Системные требования - 12, 13
Скачок атак высокого уровня текущего сенсора IDS - 285
Служба SNMP (SNMP-агент) - 254, 293
Смена пароля - 82
Событие мониторинга - 293
Соглашения документа - 10
Создание и изменение группы мониторинга - 87
Создание и изменение правила анализа - 99, 119
Создание и изменение учетной записи - 69, 78, 79, 107, 117, 156
Создание и изменение шаблонов оповещений - 107, 110, 156
Создание и изменение шаблонов писем оповещений - 115, 116, 200
Состояние пассивного элемента кластера - 280
Состояние узла - 262
Способы оповещения - 81, 107, 108
Средства анализа информации - 29
Статус программы Failover - 264
Статус программы MFTP - 265
Статус программы Деловая почта - 263
Статус программы Монитор - 263

Т

Тип межсетевого экрана - 271
Типы данных - 158
Тонкая настройка Сервера мониторинга - 13, 41, 138, 166
Требования к версиям ПО ViPNet - 13
Туннелируемый узел - 293

У

Удаление открытого узла из списка связей Сервера мониторинга - 95
Удаление ПО Сервер мониторинга - 63, 67
Удаление правила анализа - 98, 105
Удаление приложения - 282
Удаление Сервера мониторинга из каскада - 64, 133
Удаление узла или группы мониторинга - 17, 94
Удаление учетной записи - 78, 82
Узел мониторинга - 12, 293
Управление правилами анализа в каскаде - 34
Управление Сервером мониторинга - 41, 59, 138
Уровень безопасности - 265
Установка обновлений для стороннего ПО - 56
Установка ПО Сервер мониторинга - 43, 45, 48, 63, 65, 113, 140, 141, 145, 148, 180, 189
Установка приложения - 281
Установка, обновление и удаление сервера мониторинга - 42, 194

Ф

Формат расписания - 143, 146, 148
Функции - 159

Ш

Шаблон файла импорта открытых узлов - 90, 248
Шаблоны писем оповещений - 294

Э

Экспорт и импорт настроек Сервера мониторинга - 134