

INFOWATCH

# InfoWatch Traffic Monitor 6.1

Руководство по установке

**InfoWatch Traffic Monitor 6.1**

# Руководство по установке

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

Дата редакции: 2016-10-24

# СОДЕРЖАНИЕ


**1 ВВЕДЕНИЕ ..... 4**

1.1 Аудитория ..... 4
1.2 Комплект документов ..... 4
1.3 Техническая поддержка пользователей ..... 4

**2 ПОДГОТОВКА К УСТАНОВКЕ ..... 6**

2.1 Схемы развертывания Системы и выбор типа установки ..... 6
2.2 Аппаратные и программные требования ..... 8

**3 УСТАНОВКА СИСТЕМЫ ..... 16**

3.1 Общие сведения по этапам установки серверных компонентов ..... 17
*3.1.1 Стартовое окно ..... 18*
*3.1.2 Выбор базы данных ..... 19*
*3.1.3 Выбор режима установки ..... 20*
*3.1.4 Выбор часового пояса ..... 21*
*3.1.5 Установка пароля суперпользователя Системы ..... 22*
*3.1.6 Выбор способа разбиения дискового пространства ..... 22*
*3.1.7 Настройка сети ..... 25*
*3.1.8 Настройка синхронизации времени (NTP-server) ..... 28*
*3.1.9 Настройка локализации ..... 29*
*3.1.10 Настройка автоматического удаления событий из БД ..... 31*
*3.1.11 Завершение установки ..... 33*
3.2 Установка TM Enterprise и TM Standard в режиме "Все-в-одном" (All-in-one) ..... 34
3.3 Распределенная установка TM Enterprise ..... 37
*3.3.1 Установка Базы данных (TM DB server) ..... 37*
*3.3.2 Установка Сервера Traffic Monitor (TME Node server) ..... 39*
3.4 Установка подсистемы Краулер ..... 40
3.5 Предустановленные серверные параметры ..... 46

**4 ОБНОВЛЕНИЕ СИСТЕМЫ ..... 49**

4.1 Обновление пакетов RHEL и IWTM ..... 50
4.2 Обновление схемы БД Oracle ..... 51
4.3 Обновление схемы БД PostgreSQL ..... 52

**5 УДАЛЕНИЕ СИСТЕМЫ ..... 54**

5.1 Удаление схемы базы данных ..... 55
5.2 Crawler ..... 56

**6 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ ..... 57**

**7 ПРИЛОЖЕНИЕ В. ЛИЦЕНЗИИ НА СТОРОННЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ..... 59**

# 1 ВВЕДЕНИЕ

В настоящем руководстве вы можете найти сведения по установке, обновлению и удалению системы InfoWatch Traffic Monitor (IW TM).

## 1.1 Аудитория

Документ предназначен для специалистов службы технической поддержки компании InfoWatch, а также для инженеров компаний-партнеров компании InfoWatch.

## 1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

- «*InfoWatch Traffic Monitor. Руководство пользователя*».

Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).

- «*InfoWatch Traffic Monitor. Руководство администратора*».

Содержит информацию по администрированию Системы (база данных, серверная часть).

- *«InfoWatch Traffic Monitor. Руководство по установке»*

Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.

## 1.3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы Службы технической поддержки – с 7-00 до 21-00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/support.html.
Перед обращением в службу технической поддержки мы рекомендуем вам посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

# 2 ПОДГОТОВКА К УСТАНОВКЕ

В этой главе Вы можете найти информацию о:

- схемах развертывания Системы и возможных типах установки;
- программных и аппаратных требованиях.

## 2.1 Схемы развертывания Системы и выбор типа установки

Система InfoWatch Traffic Monitor может поставляться в нескольких вариантах. При этом имеет значение режим установки системы, используемая база данных (Oracle / PostgreSQL) и редакция системы (Standard / Enterprise).

Можно выделить следующие типичные варианты решений:

- **InfoWatch Traffic Monitor Standard** – решение для компаний размером до 300 сотрудников. Имеет ряд ограничений по сравнению с Enterprise-версией (подробнее см. таблицу ниже и http://www.infowatch.ru/products/traffic_monitor_standard/difference). Разворачивается на едином сервере.
- **InfoWatch Traffic Monitor Enterprise** – полное масштабируемое решение с гибким конфигурированием компонентов. В максимально развернутой конфигурации может выглядеть следующим образом:
    - **Сервер Traffic Monitor**. Обеспечивает работу перехватчиков (IW_SNIFFER, IW_ICAP и IW_SMTPD), подсистемы анализа и подсистемы применения политик. В ряде случаев рекомендуется использовать несколько серверов Traffic Monitor: это позволяет обеспечивать более эффективную работу нагруженных процессов. При этом необходимо учитывать, что некоторые процессы должны быть запущены только на одном сервере (подробнее см. статью "Проверка автозапуска процессов" в Руководстве администратора).
    - **База данных**. Сервер СУБД Oracle или PostgreSQL.

      **Примечание:**

      На сервере Traffic Monitor и Базе данных не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать компьютер в качестве файл-сервера.

    - **Device Monitor**. Модуль перехвата, реализованный в виде серверной части с управлением через Консоль и Агентов, распространяемых на компьютеры и мобильные устройства компании.
    - **Краулер**. Модуль перехвата, реализованный в виде служб сервера и сканера.
    - **Коннекторы**. Набор модулей перехвата для интеграции со сторонними системами.

- **Консоль управления**. Веб-интерфейс управления Системой. Реализован в виде набора процессов, которые должны быть запущены только на одном сервере Traffic Monitor (подробнее см. статью "Проверка автозапуска процессов" в Руководстве администратора).

В следующей таблице описывается функциональная разница между редакциями системы, с учетом используемой базы данных.

| Функция | TM Enterprise | | TM Standard |
|---|---|---|---|
| | TM Enterprise Oracle | TM Enterprise PostgreSQL | TM Standard PostgreSQL |
| Срок хранения перехваченных данных | Ограничивается только размером хранилища | | Ограничивается только размером хранилища |
| Контроль рабочих станций | Контроль использования съемных устройств и коммуникационных портов; контроль печати | | Опционально (Возможность подключения модуля контроля рабочих станций InfoWatch Device Monitor зависит от объема данных и требуемых сроков хранения) |
| Масштабируемость | Решение может быть адаптировано для обслуживания большого количества сотрудников (десятки тысяч) при росте компании. Может использоваться в территориально распределенных филиалах, соединенных любыми каналами связи | | Рассчитано на компании с числом сотрудников до 300 человек |
| Блокирование передачи трафика при выявлении нарушения | Да | | Опционально (внедрение проводится силами сертифицированных инженеров) |
| Схема интеграции | Несколько вариантов на выбор: интеграция «в разрыв», поддержка ICAP, перехват в режиме копии трафика (SPAN, port mirroring и др.) | | Работа в режиме копии трафика (интеграция «в разрыв» - опционально) |

Существуют следующие типы установки:

- *Все-в-одном Standard* – все компоненты Системы (с СУБД PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.
- *Все-в-одном Enterprise* – все компоненты Системы (с СУБД Oracle Enterprise или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.
- *Сервер Traffic Monitor* + *База данных* – сервер Traffic Monitor и СУБД Oracle Enterprise или PostgreSQL устанавливаются на разные машины. Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одной машине.

**Важно**

После установки администратор настраивает Систему в зависимости от целей внедрения

(см. документ "Infowatch Traffic Monitor. Руководство администратора", статья "Настройка Системы после установки").

## 2.2 Аппаратные и программные требования

Требования к аппаратной конфигурации сервера для InfoWatch Traffic Monitor определяются на основании варианта установки, предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание Системы. Поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

Варианты схем развертывания Системы описаны в статье "Схемы развертывания Системы и выбор типа установки". Согласно статье, может выполняться установка следующих элементов:

- **Сервер для установки "Все-в-одном"** – используется для редакции TM Enterprise – установка Enterprise-решения в режиме "Все-в-одном" не рекомендуется, но возможна. *См. требования для отдельностоящего сервера TM Enterprise.*
- **Сервер Traffic Monitor** – отдельностоящий сервер или кластер серверов TM Enterprise. *Требования см. ниже.*
- **Сервер базы данных** – сервер СУБД Oracle или PostgreSQL. На этом компьютере не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать его в качестве файл-сервера. *Требования см. ниже.*
- **Сервер Краулер и сканер Краулер** – службы, работающие на Windows-системах. *Требования см. ниже.*
- **Коннекторы** – требования к этим компонентам описаны в документации, поставляемой вместе с программным обеспечением коннекторов.
- **Сервер Device Monitor с Агентами Device Monitor** – модуль, работающий на Windows-системах. *Требования см. ниже*.
- **Консоль управления** – автоматически устанавливается вместе с сервером Traffic Monitor и не предъявляет дополнительных программно-аппаратных требований к серверу. Для доступа к Консоли достаточно использовать браузер Google Chrome версии не ниже 40.

Для сервера Traffic Monitor аппаратно-программные требования варьируются в очень большом диапазоне. Так, минимальная конфигурация подразумевает следующие ограничения:

- для всех перехватчиков отключено использование OCR;
- сервер не принимает данные от Device Monitor и Краулера.

Также на количество и назначение серверов Traffic Monitor может влиять существенная разница в нагрузке на те или иные каналы перехвата: например, для эффективной обработки трафика и с Device Monitor, и с Краулера, может потребоваться использовать отдельный сервер для процесса **iw_expressd**.

Примерные минимальные программно-аппаратные требования приведены в следующей таблице. Подробный расчет конфигурации настоятельно рекомендуется проводить с участием специалистов InfoWatch или компании-партнера, у которой вы приобретаете продукт.

| **Элемент Системы** | **Дисковая подсистема** | **Процессор** | **Оперативная память** | **Программные требования** | **Дополнительные требования** |
|---|---|---|---|---|---|
| Сервер TM Standard | RAID-массив с fault tolerance: 300 GB | 2CPU 6xC, 2,6 GHz | 24 GB | Не предъявляются: программа-инсталлятор (kickstart) форматирует жесткий диск и устанавливает необходимое ПО. | На сервере Traffic Monitor могут использоваться перехватчики, которые предъявляют дополнительные требования:<br>• **iw_sniffer** может получать копию трафика от управляемого коммутатора с поддержкой функции SPAN/Port Mirroring (рекомендованная модель - Cisco Catalyst 2960 Series) с |
| Сервер TM Enterprise, менее 10 GB трафика в день | RAID-массив с fault tolerance: 600 GB | 2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 - частота 2,6 Hz) | 24 GB | | |
| Сервер TM Enterprise, от 10 до 50 GB трафика в день | RAID-массив с fault tolerance | 2SRVx2CPU 10xC | 32-48 GB на каждый из серверов | | |

| Элемент Системы | Дисковая подсистема | Процессор | Оперативная память | Программные требования | Дополнительные требования |
|---|---|---|---|---|---|
| Сервер TM Enterprise, более 50 GB трафика в день | RAID-массив с fault tolerance | Рассчитывается по запросу | От 32GB на каждый из серверов | | портом, настроенным на режим TRx (BOTH - получение и передача в одном подключении).<br>• **iw_icap** работает с ICAP-клиентом, встроенным в любой прокси-сервер, соответствующий стандарту RFC 3507 (например, SQUID версии не ниже 3.4.x, Cisco IronPort S10 и Blue Coat SG Series). Перед тем, как использовать конкретную модель устройства рекомендуется уточнить совместимость с модулем IW ICAP в службе технической поддержки компании InfoWatch. На прокси-сервере должна присутствовать лицензия на ICAP; включение поддержки ICAP выполняется согласно сопроводительной документации к выбранному прокси-серверу.<br>Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. |
| Сервер БД Oracle или PostgreSQL | RAID-массив с fault tolerance: 500 GB | 2CPU от 6xC, 2,6 GHz | От 16GB и более в зависимости от объема данных, интенсивности вставки и обработки | | Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; без OCR, без Device Monitor |

| Элемент Системы | Дисковая подсистема | Процессор | Оперативная память | Программные требования | Дополнительные требования |
|---|---|---|---|---|---|
| Сервер Crawler и сканер Crawler | 30 GB свободного пространства - для сервера и для сканера: необходимо для временного хранения файлов, скопированных с проверяемых ресурсов и для установки | от 2-х ядер | От 2 GB | ОС:<br>• Microsoft Windows Vista 7/8 SP2<br>• Microsoft Windows Server 2008 R2 SP1 или SP2/2012<br>• Microsoft Windows 7 SP1<br>Платформа:<br>• Microsoft .Net Framework 4.5 | • На сервере ТМ должен быть включен автозапуск процесса **iw_expressd**<br>• И сервер, и сканер Crawler должны быть установлены на компьютеры, находящиеся в одном домене: в том, к которому принадлежат компьютеры, которые предполагается сканировать.<br>• Рекомендуется выбирать расположение компьютера, на котором будет работать сканер Crawler, так, чтобы он находился в сегменте сети, максимально близком к тем сегментам, которые будут подлежать сканированию. Удаленность может существенно увеличить нагрузку на сеть.<br>• Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты порты 1337 (подключение Traffic Monitor к серверу Crawler) и 6556 (подключение сканера Crawler к серверу Crawler). |

| Элемент Системы | Дисковая подсистема | Процессор | Оперативная память | Программные требования | Дополнительные требования |
|---|---|---|---|---|---|
| Сервер Device Monitor | Не менее 200 MB свободного пространства для установки | от 2-х ядер | От 2 GB | ОС (поддерживаются платформы x86 и x64):<br>• Microsoft Windows Server 2003;<br>• Microsoft Windows Server 2008;<br>• Microsoft Windows Server 2008 R2;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2012 R2.<br>Платформа:<br>• Microsoft .Net Framework 4.0<br>Клиент СУБД:<br>• Oracle Database 11. В случае установки Device Monitor на серверную ОС разрядностью x64, необходимо использовать приложение Oracle Client разрядностью также x64.<br>• Microsoft SQL Server 2005, 2008, 2012, 2014 (Express, Developer, Workgroup, Standard, Enterprise).<br>• PostgreSQL версий 8 и 9. | • На сервере ТМ должен быть включен автозапуск процессов **iw_expressd** и **iw_xapi**<br>• Наличие локального DNS для перевода доменных имён в адреса |

| **Элемент Системы** | **Дисковая подсистема** | **Процессор** | **Оперативная память** | **Программные требования** | **Дополнительные требования** |
|---|---|---|---|---|---|
| Агент Device Monitor для рабочих станций | Не менее 320 GB свободного пространства для временного хранения файлов, предназначенных для передачи на анализ | от 2-х ядер | От 2 GB | ОС:<br>• Microsoft Windows XP Professional Service Pack 3 со всеми обновлениями;<br>• Microsoft Windows Vista Service Pack 2;<br>• Microsoft Windows 7 Service Pack 1;<br>• Microsoft Windows 8 и 8.1;<br>• Microsoft Windows 10;<br>• Microsoft Windows Server 2003;<br>• Microsoft Windows Server 2008;<br>• Microsoft Windows Server 2008 R2;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2012 R2.<br>Платформа:<br>• Microsoft .Net Framework 4.5 | Наличие локального DNS для перевода доменных имён в адреса |

| Элемент Системы | Дисковая подсистема | Процессор | Оперативная память | Программные требования | Дополнительные требования |
|---|---|---|---|---|---|
| Агент Device Monitor для мобильных устройств | Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен. | Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен. | Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен. | Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен. | Поддерживаются следующие конфигурации устройств на платформе Android:<br>• ASUS Nexus 7 2013 LTE (K009), версия Android 4.3.0 (версия прошивки JLS36C)<br>• ASUS Nexus 7 2013 LTE (K009), версия Android 4.4.2 (версия прошивки KOT49H)<br>• ASUS Nexus 7 2013 LTE (K009), версия Android 4.4.3 (версия прошивки KTU84L)<br>• ASUS Nexus 7 2013 LTE (K009), версия Android 4.4.4 (версия прошивки KTU84P)<br>• Samsung Galaxy S3 (I9300), версия Android 4.3.0 (версии прошивки JSS15J.I9300XXUGNK1, JSS15J.I9300XXUGND2)<br>• Samsung Galaxy S4 (I9500), версия Android 4.3.0 (версия прошивки JSS15J.I9500XXUEMK8)<br>• Samsung Galaxy S4 (I9505), версия Android 4.3.0 (версии прошивки JSS15J.I9505XXUEMK9, JSS15J.I9505XXUEML4)<br>• Samsung Galaxy S4 (I9505), версия Android 4.4.2 (версии прошивки KOT49H.I9505XXUGNG8, KOT49H.I9505XXUFNC9)<br>• Samsung Galaxy S5 (SM-G900F), версия Android 4.4.2 (версии прошивки KOT49H.G900FXXU1A |

| Элемент Системы | Дисковая подсистема | Процессор | Оперативная память | Программные требования | Дополнительные требования |
|---|---|---|---|---|---|
| Консоль управления Device Monitor | Не менее 35 MB | Как у используемой ОС | Как у используемой ОС | ОС:<br>• Microsoft Windows Server 2003;<br>• Microsoft Windows Server 2008;<br>• Microsoft Windows Server 2008 R2;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2012 R2;<br>• Microsoft Windows XP Professional Service Pack 3;<br>• Microsoft Windows Vista Service Pack 2;<br>• Microsoft Windows 7 Service Pack 1<br>• Microsoft Windows 8 и 8.1;<br>• Microsoft Windows 10. | |

Допустима установка Системы в виртуальную среду: например, VMware, MS Hyper-V или других систем виртуализации.

# 3 УСТАНОВКА СИСТЕМЫ

**Примечание:**

После установки Системы будет автоматически загружена пробная лицензия на технологии Traffic Monitor (более подробную информацию о лицензировании см. в документе «InfoWatch Traffic Monitor. Руководство администратора»).

В данном разделе приведены инструкции для каждого из типов установки Системы.

О выборе типа установки см. "Схемы развертывания Системы и выбор типа установки".

Реализация схем развертывания в имеющейся инфраструктуре описана в документе «InfoWatch Traffic Monitor. Руководство администратора».

**Важно!**

До начала установки убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям (см. "Аппаратные и программные требования").

Установка серверных компонентов системы InfoWatch Traffic Monitor выполняется с помощью программы-инсталлятора (**kickstart**).

В зависимости от целевого назначения сервера, будет различаться набор устанавливаемых компонентов:

| **Назначение сервера** | **Ключ kickstart** | **Компоненты, устанавливаемые инсталлятором** |
|---|---|---|
| Все компоненты InfoWatch Traffic Monitor (Enterprise или Standard) устанавливаются на один компьютер | **TME All-in-one** | • Установка ОС Linux<br>• Настройка сетевого интерфейса<br>• Установка и настройка СУБД Oracle (только для **TME All-in-one**) или PostgreSQL<br>• Установка схемы базы данных IW Traffic Monitor<br>• Установка RPM пакетов сервера IWTM<br>• Установка подсистемы мониторинга<br>• Установка консоли управления |

| Назначение сервера | Ключ kickstart | Компоненты, устанавливаемые инсталлятором |
|---|---|---|
| Установка сервера СУБД со схемой БД Traffic Monitor на отдельный компьютер | **TME DB server** | • Установка ОС Linux<br>• Настройка сетевого интерфейса<br>• Установка и настройка СУБД Oracle Enterprise или PostgreSQL<br>• Установка схемы базы данных IW Traffic Monitor |
| Установка сервера Traffic Monitor на отдельный компьютер | **TME Node server** | • Установка ОС Linux<br>• Настройка сетевого интерфейса<br>• Установка RPM пакетов сервера IWTM<br>• Установка подсистемы мониторинга<br>• Установка консоли управления |

Вы можете найти информацию по интересующему Вас типу установки в статьях:

- Общие сведения по этапам установки серверных компонентов
- Установка TM Enterprise и TM Standard в режиме "Все-в-одном"
- Распределенная установка TM Enterprise
- Установка подсистемы Crawler (опционально)

Сведения о предустановленных учетных записях приведены в статье "Предустановленные серверные параметры".

После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес:

- сервера Traffic Monitor – если выполнена установка «Все-в-одном»;
- основного сервера Traffic Monitor – если компоненты Системы установлены на разные компьютеры.

О выделении основного сервера при распределенной установке см. документ «*InfoWatch Traffic Monitor. Руководство администратора*», статья "*Дополнительные настройки при установке с ключами TME DB Server и TME Node Server*".

# 3.1 Общие сведения по этапам установки серверных компонентов

В этом разделе содержится подробное описание шагов инсталлятора kickstart, являющихся общими для всех типов установки серверных компонентов Системы:

- Стартовое окно

- Выбор базы данных
- Выбор режима установки
- Выбор часового пояса
- Установка пароля суперпользователя Системы
- Выбор способа разбиения дискового пространства
- Настройка сети
- Настройка синхронизации времени (NTP-server)
- Настройка локализации
- Настройка автоматического удаления событий из БД
- Завершение установки

### 3.1.1 Стартовое окно




Первый экран мастера установки (**kickstart**) позволяет выбрать одно из следующих действий:

- **TM Enterprise** – начнется установка InfoWatch Traffic Monitor Enterprise.
- **TM Standard** – начнется установка InfoWatch Traffic Monitor Standard.

**Важно!**

Для редакции **TM Standard** доступна установка только в режиме **TMS All-in-one: TM+DB server - PostgreSQL**. Шаги "Выбор базы данных" и "Выбор режима установки" в этом случае будут пропущены.

О выборе редакции установки см. "Схемы развертывания Системы и выбор типа установки".

- **Boot from local drive** – выполняется загрузка с локального диска компьютера.
- **Rescue installed system** – выполняется аварийное восстановление системы InfoWatch Traffic Monitor. Ввиду сложности данная опция используется только инженерами компании InfoWatch.
- **Memory test** – выполняется тест оборудования компьютера (может занять некоторое время). Используется как вспомогательная функция при необходимости.

**Примечание**

Для просмотра дополнительных опций загрузки нажмите **F1**. Ввиду сложности дальнейших работ вызов дополнительных опций используются только инженерами компании InfoWatch.

## 3.1.2 Выбор базы данных




Для редакции **Enterprise** инсталлятор предложит выбрать СУБД, которая должна быть установлена:

- **DB - Oracle Enterprise**;
- **DB - PostgreSQL**.

## 3.1.3 Выбор режима установки

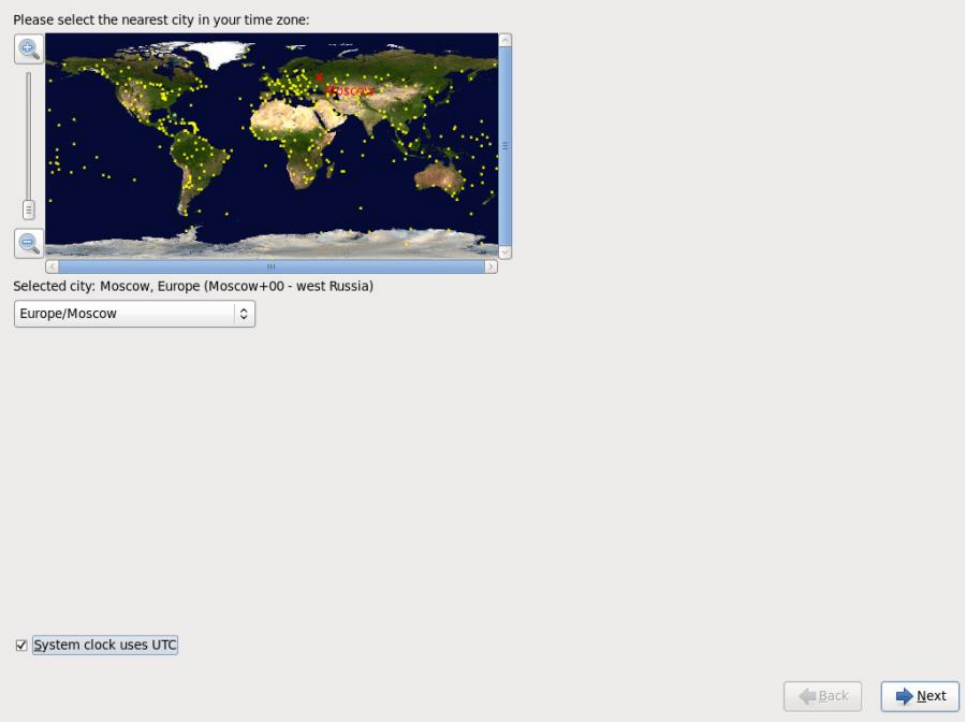



После выбора СУБД потребуется выбрать режим установки. Набор режимов зависит от выбора, сделанного, на предыдущих шагах установки. Могут быть предложены следующие режимы:

- **TME All-in-one: TM+DB server - PostgreSQL** –
  **TME All-in-one: TM+DB server - Oracle** –
  **TMS All-in-one: TM+DB server - PostgreSQL** – все компоненты Системы (с СУБД Oracle или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor. Подробнее см. "Установка TM Enterprise и TM Standard в режиме "Все-в-одном" ".
- **TME DB server (PostgreSQL** или **Oracle**) – установка базы данных вместе с выбранной СУБД на отдельный компьютер. Подробнее об этой установке см. "Установка Базы данных (TM DB server)".
- **TME Node server (PostgreSQL** или **Oracle**) – установка сервера Traffic Monitor на отдельный компьютер. Подробнее об этой установке см. "Установка Сервера Traffic Monitor (TME Node server)".

Подробнее о выборе режима установки см. "Схемы развертывания Системы и выбор типа установки".

### 3.1.4 Выбор часового пояса



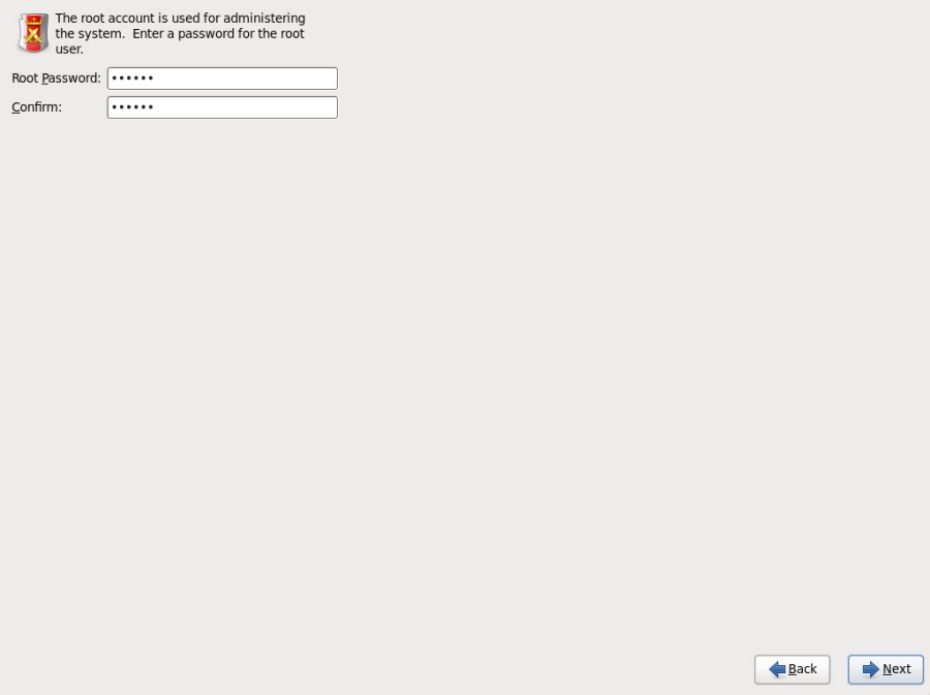

Затем инсталлятор предложит указать часовой пояс сервера.

Нужный город можно выбрать:

- в раскрывающемся списке. Города отсортированы по принадлежности к той или иной части света: например, Москва входит в группу Европа;
- на карте. Для навигации по карте используйте полосы прокрутки и инструменты изменения масштаба).

Поле **System clock uses UTC** показывает, будет ли системное время установлено по Гринвичу (UTC).

### 3.1.5 Установка пароля суперпользователя Системы




Пользователь *root* – это суперпользователь в Системе. Для пользователя *root* требуется указать пароль.

> **Примечание**
>
> Рекомендации по составлению паролей приведены в разделе Приложение А.

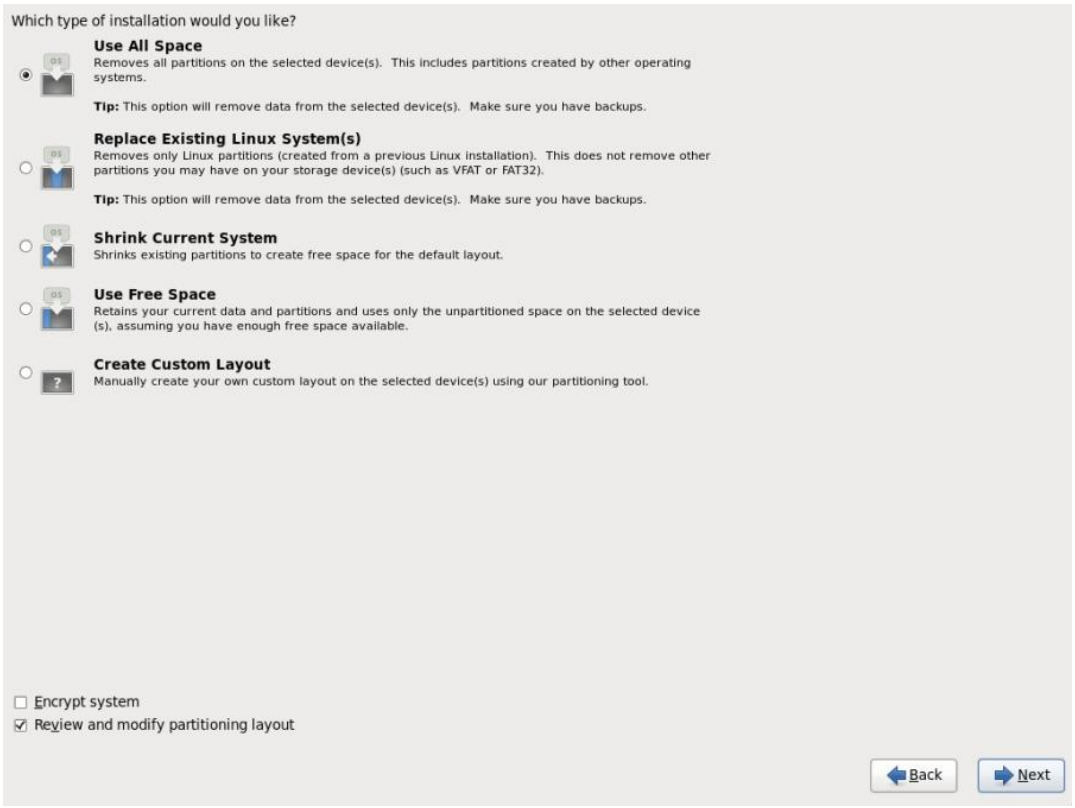
Если введенный пароль не соответствует правилам безопасности, на экране отобразится предупреждающее окно **Weak Password**. Используйте кнопки:

- **Use anyway** – если вы хотите использовать введенный пароль без учета рекомендаций;
- **Cancel** – если вы хотите изменить введенный пароль.

### 3.1.6 Выбор способа разбиения дискового пространства

> **Важно**
>
> По завершении установки Системы компоненты будут установлены в следующие директории:

- InfoWatch Traffic Monitor – в каталог `/opt/iw`;
- БД – в каталоги `/u01` и `/u02` (в версиях ТМ `6.1.100` и ниже БД PostgreSQL устанавливается только в каталог `/u01`).

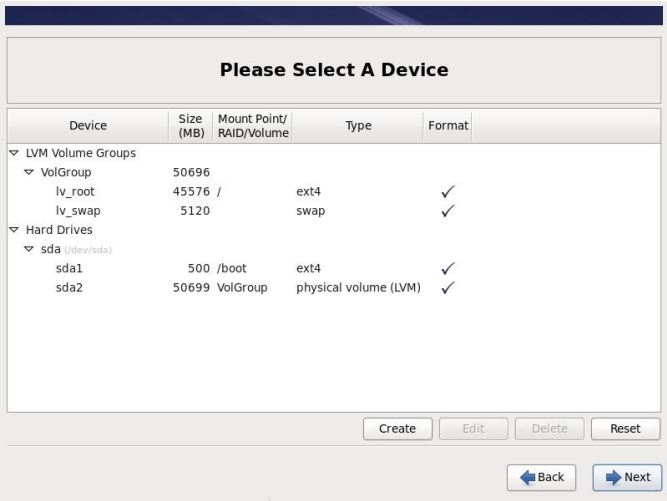



Далее необходимо будет указать инсталлятору, как разбить дисковое пространство. Поскольку дисковое место на сервере InfoWatch Traffic Monitor используется только для самой Системы, на данном шаге нужно выбрать **Use All Space**.

**Важно!**

Удалятся все разделы устройства (устройств), включая разделы, созданные другими операционными системами. *Позаботьтесь о резервном копировании нужных вам данных!*

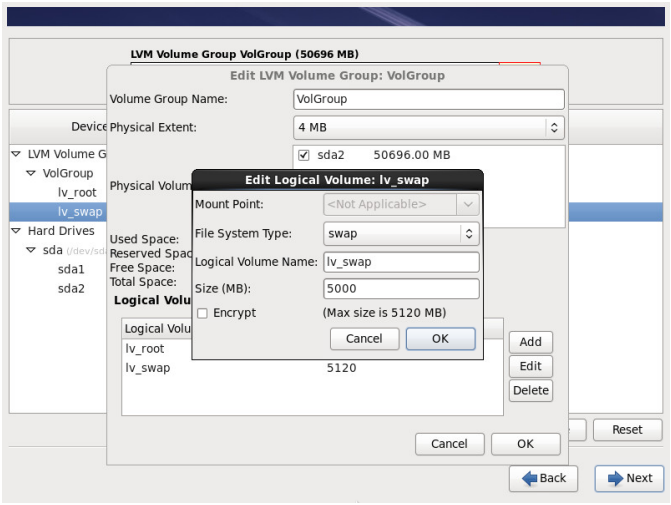
Чтобы настроить разбивку дисков или просто удостовериться в том, что указанные по умолчанию настройки корректны, нужно установить флажок в поле **Review and modify partitioning layout** и нажать **Next**.




Для большинства случаев достаточно разбиения по умолчанию. Если необходимо внести изменения, используйте стандартные средства работы с дисками, доступные в инсталляторе.

Например, требуется поменять размер раздела *lv_swap* на значение *5000*:

1. В окне **Please Select A Device** выберите раздел **lv_swap** и нажмите **Edit**.
2. В поле **Size (MB)** укажите **5000**. Нажмите **OK**.




3. В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
4. В поле **Size (MB)** укажите все оставшееся свободное пространство (отображается под полем - **Max size is**...) . Нажмите **OK**.
5. Нажмите **Next** в окне **Please Select A Device** .

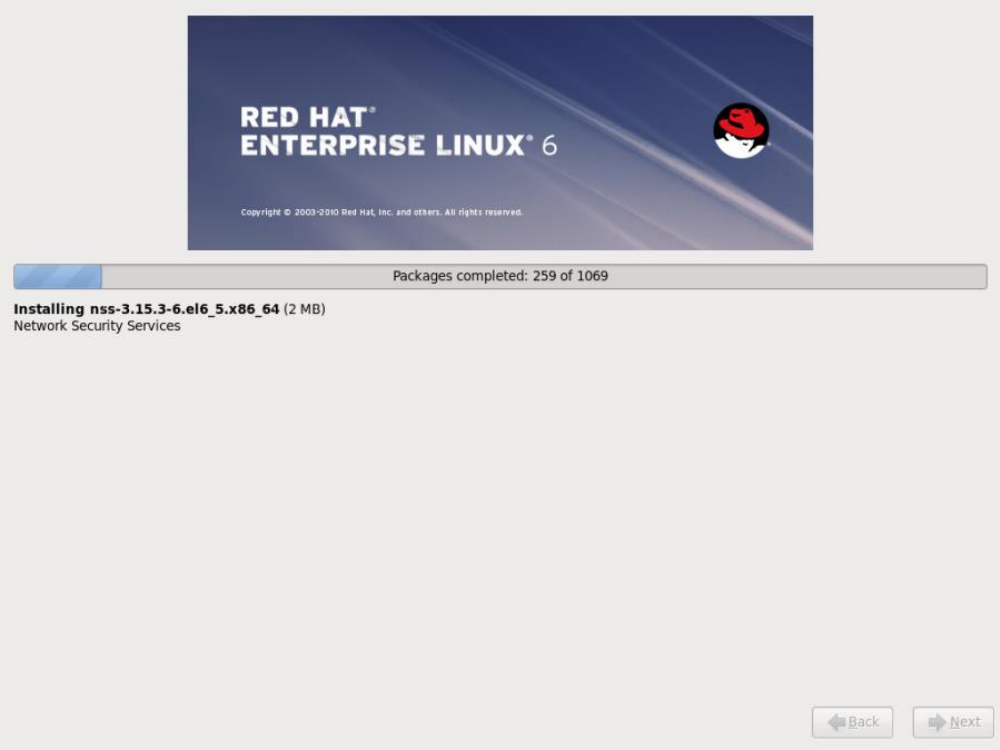
После завершения разбивки и нажатия кнопки **Next** начнется процесс разбиения диска, а затем – установки операционной системы.

**Примечание:**

На экран может быть выведено окно **Format Warnings**, свидетельствующее о том, что требуется отформатировать разделы жесткого диска, которые будут использоваться для

установки. Для продолжения установки нажмите **Format**.

Прогресс отображается на экране:

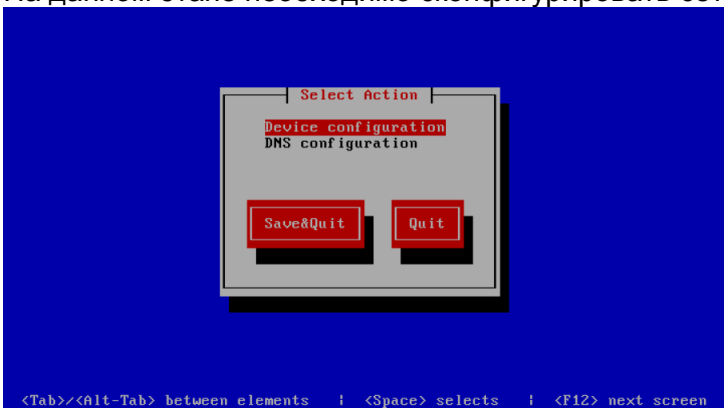



Процесс может занять некоторое время.

По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры (см. "Настройка сети").

## 3.1.7 Настройка сети

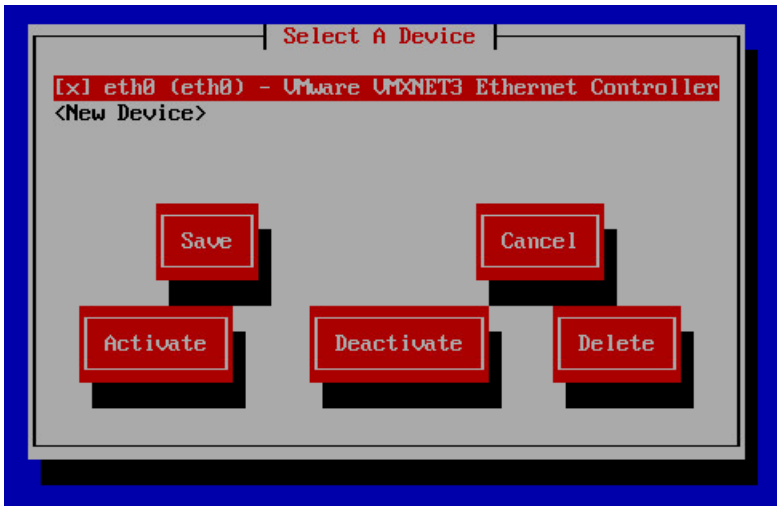
На данном этапе необходимо сконфигурировать сетевое подключение.




Настройка сети имеет две составляющие:

- **Device configuration** - настройка сетевой карты.

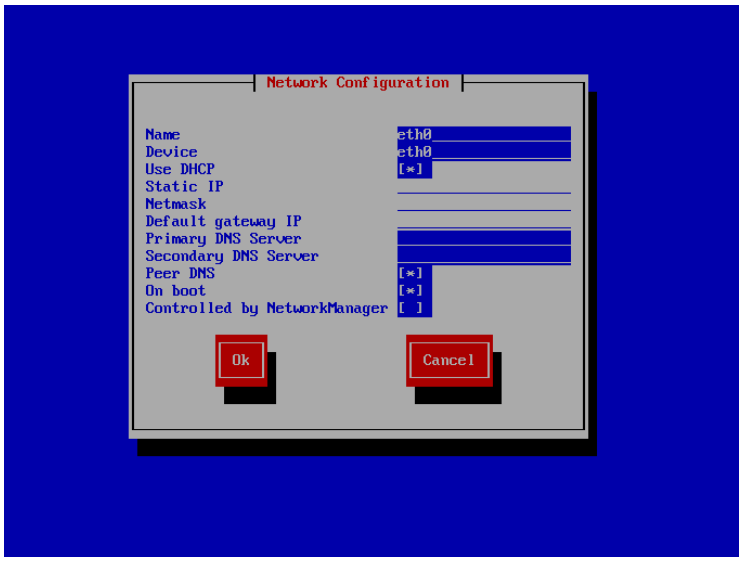
  При настройке **Device configuration** будет предложено выбрать сетевой интерфейс из имеющихся (**eth0** и другие) или создать новый (**<New Device>**).




Признак выбора расположен в начале строки с названием интерфейса и выглядит как **[X]**. Обычно используется **eth0**.

Чтобы активировать или деактивировать интерфейс, нужно установить на нем курсор (строка с названием будет выделена красным), затем по нажатию **Tab** перейти на кнопки управления, расположенные в нижней части экрана, и нажать **Activate** или **Deactivate**, соответственно.

Чтобы настроить интерфейс, нужно установить на нем курсор (строка с названием будет выделена красным) и нажать **Enter**.




Для включения и выключения опций используйте пробел.

Для использования сетевого интерфейса нужно указать его сетевые настройки (статический IP-адрес машины и прочее). Если Система будет получать данные настройки от DHCP-сервера, нужно включить опцию **Use DHCP** (с помощью клавиши проел).

**Важно!**

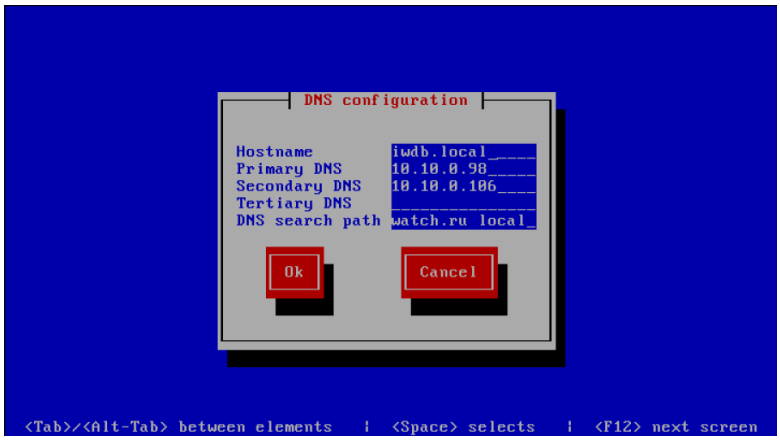
При использовании настройки **Use DHCP** Система будет использовать только данные, полученные от указанных серверов DHCP. Данные, введенные в окне **DNS configuration** (см. далее) будут игнорироваться. Если вручную изменить файл `/etc/resolv.conf`, то его данные при следующей перезагрузке сервера будут заменены на полученные от сервера DHCP.

**Важно!**

Опция **Controlled by NetworkManager** должна быть выключена.

- **DNS configuration** - настройка DNS-конфигурации.

  При настройке **DNS configuration** будет предложено указать необходимые параметры сервера.

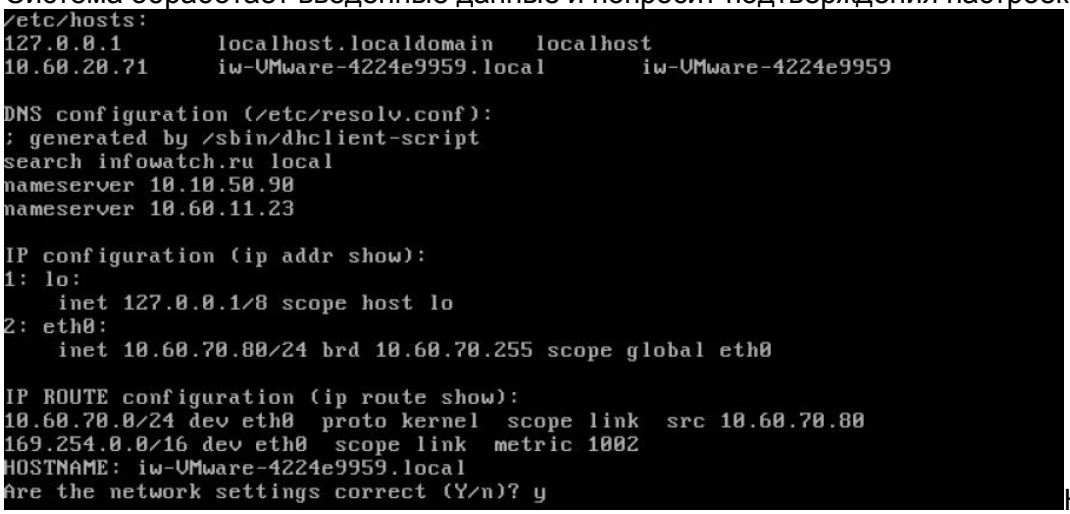



**Важно!**

Если в окне **Network Configuration** был отмечен пункт **Use DHCP**, то вместо этих параметров будут использоваться полученные от указанных серверов DHCP.

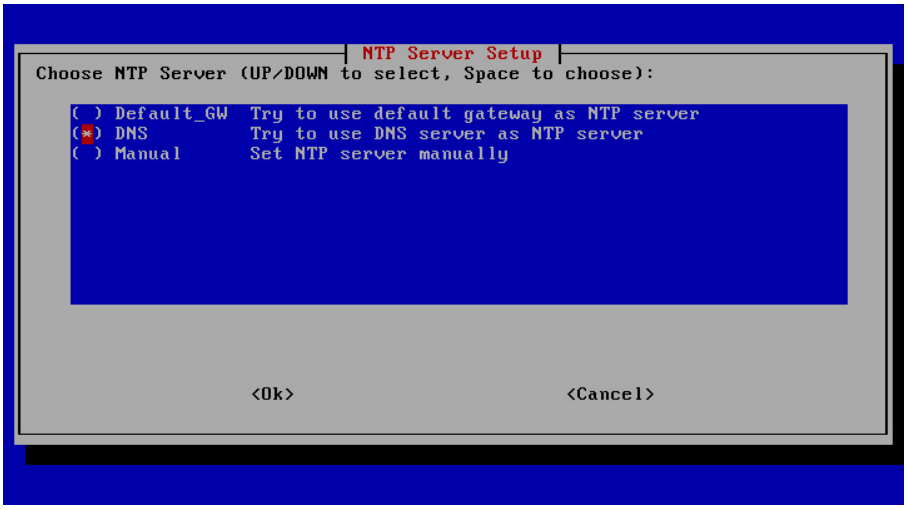
По завершении настроек потребуется нажать **Save&Quit**, чтобы подтвердить изменения.

Система обработает введенные данные и попросит подтверждения настроек.




На данном этапе необходимо проверить указанные сетевые настройки. Если настройки некорректны, введите **N** и укажите правильные параметры (см. предыдущие шаги). Если настройки корректны, введите **Y** для подтверждения и нажмите **Enter**.

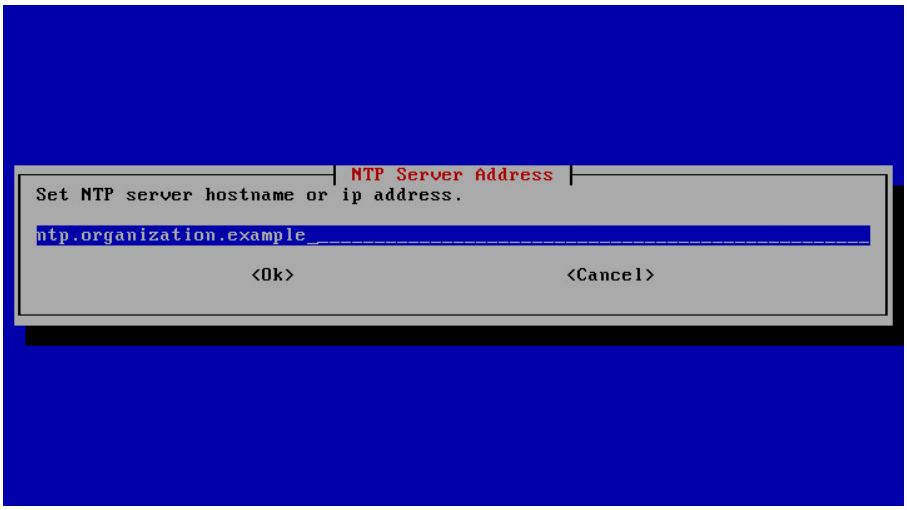
## 3.1.8 Настройка синхронизации времени (NTP-server)




На данном этапе требуется выбрать одну из следующих опций настройки сервера для синхронизации времени (NTP-server):

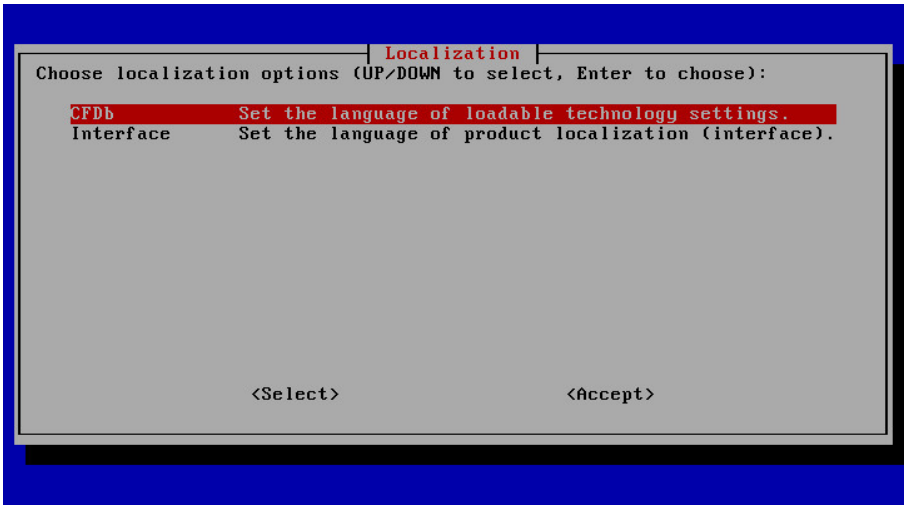
- **Default_GW** - шлюз, используемый компьютером по умолчанию;
- **DNS** - контроллер домена: обычно используется в организациях в качестве сервера времени;
- **Manual** - возможность вручную указать имя сервера или его IP-адрес.

Для выбора опции нужно установить знак астериска ( * ) в необходимом поле и нажать пробел, затем - **OK**.



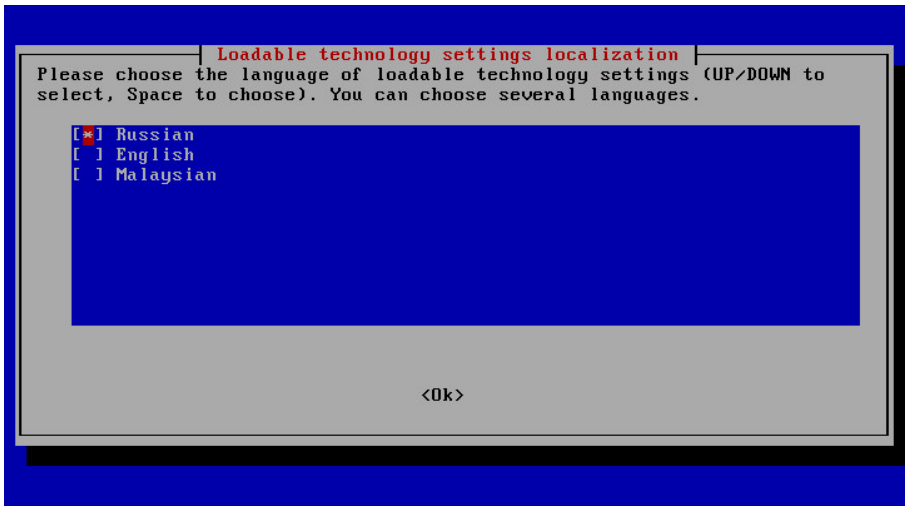

Если по каким-либо причинам указать NTP-сервер не удается, нажмите **Cancel** и выполните данную настройку позднее (подробнее см. в документе «*InfoWatch Traffic Monitor. Руководство администратора*»).

## 3.1.9 Настройка локализации




Система имеет несколько языков локализации. На данном этапе предлагается выбрать:

- **CFDb** - языковые настройки для таких предустановленных сущностей, как категории и термины, списки, предустановленные фильтры и политики по умолчанию.

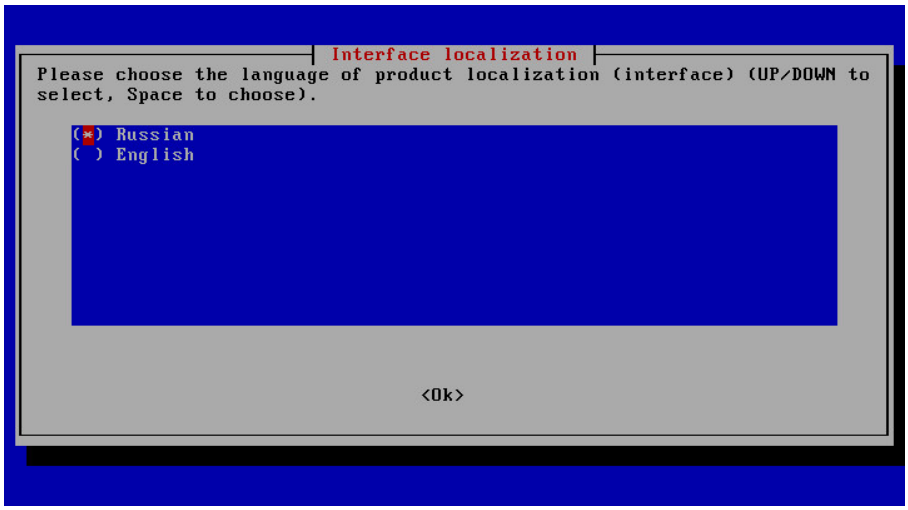



Предлагаются три языка:

- *Russian* – русский;
- *English* – английский;
- *Malaysian* – малайский.

Для выбора нужно установить знак астериска ( * ) в необходимом поле и нажать пробел, затем - **OK**. Вы можете выбрать один, два или три языка.

- **Interface** - язык, на котором будет установлена консоль управления. На выбор предлагаются два языка:
  - *Russian* – для русскоязычного интерфейса;
  - *English* – для англоязычного интерфейса.



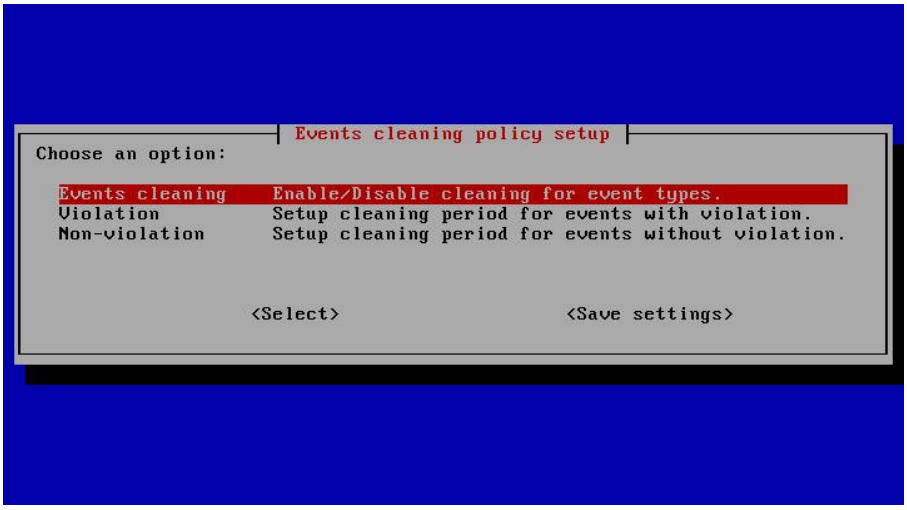

Для выбора нужно установить знак астериска ( * ) в необходимом поле и нажать пробел, затем - **OK**.

После выбора параметров локализации требуется нажать **Accept**.



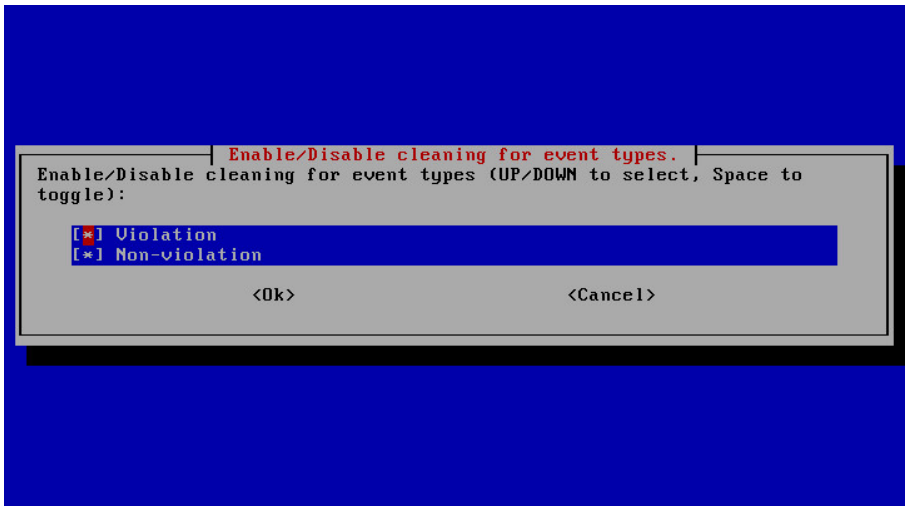

В открывшемся требуется проверить, что выбранные языки для предустановленных сущностей и для интерфейса указаны правильно, затем нажать **Yes**.

## 3.1.10 Настройка автоматического удаления событий из БД



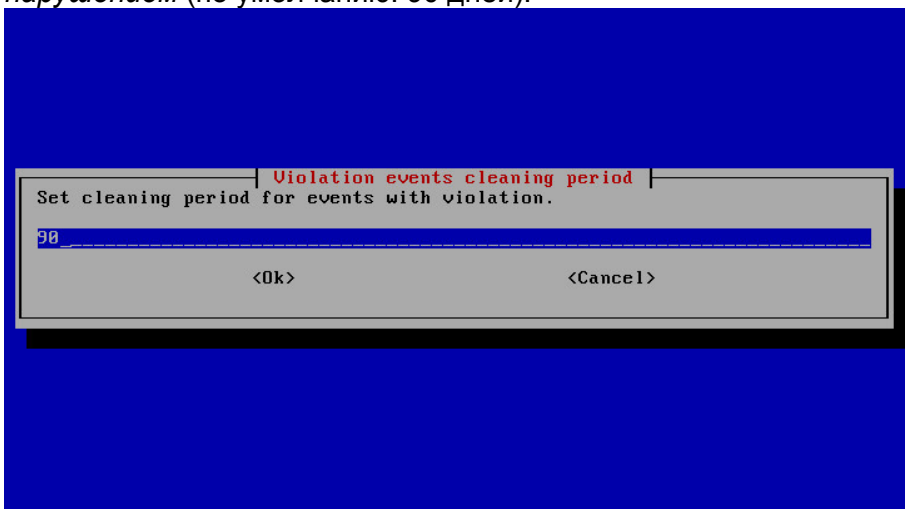

На данном этапе настраиваются параметры автоматического удаления событий из БД. Доступны опции:

- **Events cleaning** – настраивает включение и выключение (по умолчанию: выключено) автоматического удаления событий двух типов:



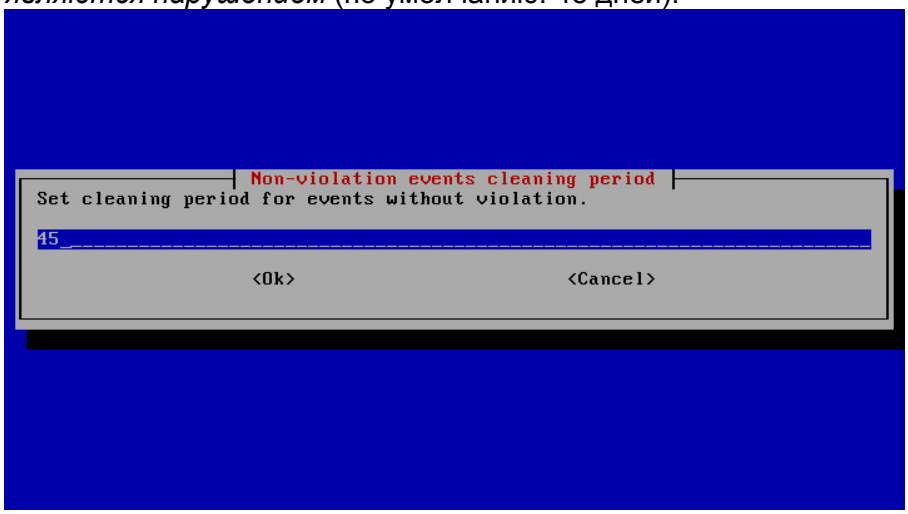

- **Violation** – включение автоматического удаления событий, которые являются нарушением (подробнее о нарушениях см. «*InfoWatch Traffic Monitor. Руководство пользователя*»);
- **Non-violation** – включение автоматического удаления событий, которые не являются нарушением.
  Вы можете выбрать оба пункта, чтобы удалялись объекты как с нарушениями, так и без.
  Для выбора опции требуется установить курсор в нужное поле и нажать пробел до появления в поле значка астериска ( * ).
  По завершении настройки требуется нажать **Ok**.

- **Violation** – настраивает периодичность автоматического удаления событий, которые *являются нарушением* (по умолчанию: 90 дней).




Периодичность удаления указывается в днях. По завершении настройки требуется нажать **Ok**.

- **Non-violation** – настраивает периодичность автоматического удаления событий, которые *не являются нарушением* (по умолчанию: 45 дней).

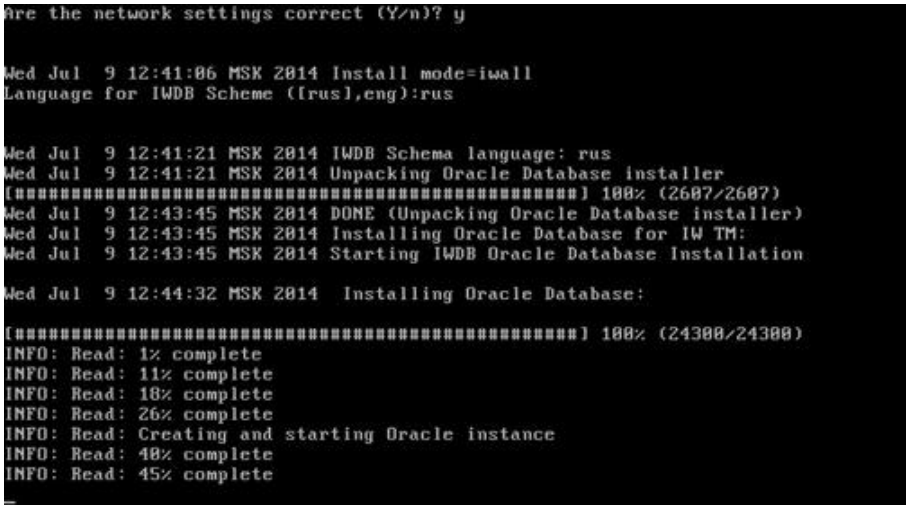



Периодичность удаления указывается в днях. По завершении настройки требуется нажать **Ok**.

По завершении настроек требуется нажать **Save settings**.

## 3.1.11 Завершение установки

По завершении настроек начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране:




В результате установки в Системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

О порядке настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

# 3.2 Установка TM Enterprise и TM Standard в режиме "Все-в-одном" (All-in-one)

Установка «все-в-одном» позволяет установить все компоненты Системы на один компьютер.

**Важно!**

В данной статье приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе «Общие сведения по этапам установки серверных компонентов».

**Чтобы установить Traffic Monitor Enterprise или Traffic Monitor Standard в режиме «Все-в-одном», выполните следующие действия:**

1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.
2. В окне приветствия выберите:
   - **TM Enterprise** – для установки редакции Enterprise;
   - **TM Standard** – для установки редакции Standard.

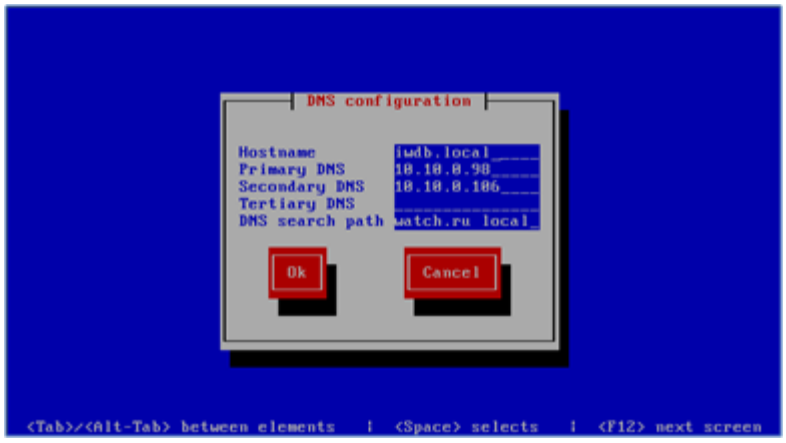
   Нажмите **Enter**.
3. В окне выбора базы данных укажите, какая СУБД должна быть установлена (опция доступна только для **TM Enterprise**):
   a. **Oracle Enterprise**;
   b. **PostgreSQL**.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите **TME All-in-one** или **TMS All-in-one** - в зависимости от выбранной редакции, нажмите **Enter**.

   **Важно!**

   После выбора режима установки на экран может быть выведено предупреждение «*The storage device below may contain data*». Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of file systems**.
5. Укажите настройки часового пояса для сервера, нажмите **Next**.
6. Задайте пароль пользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе "Приложение А. Рекомендации по составлению имен и паролей".

7. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):
    a. Выберите **Use All Space**.
    b. Установите флажок в поле **Review and modify partitioning layout**, расположенном внизу окна, нажмите **Next**.
    c. Убедитесь, что диски разбиты правильно, нажмите **Next**.
8. Для настройки параметров сетевой карты:
    a. Выберите **Device configuration**, нажмите **Enter**.
    b. Выберите сетевой интерфейс **eth0**, нажмите **Enter**.
    c. Убедитесь, что опция **Controlled by Network Manager** *выключена*, а опция **On boot** *включена*.
    d. Если вы хотите, чтобы Система использовала сетевые настройки от DHCP сервера, переведите курсор в поле **Use DHCP** и нажмите пробел. В противном случае вручную введите сетевые настройки сервера (статический IP-адрес машины и прочее). По завершении конфигурирования нажмите **OK**.
    e. Нажмите **Save**, чтобы сохранить сделанные настройки.
9. Для настройки DNS конфигурации выберите **DNS configuration** и укажите необходимые параметры сетевых настроек сервера. Затем нажмите **OK**.




10. Нажмите **Save&Quit**.
11. Проверьте указанные сетевые настройки. Если настройки некорректны, нажмите **N** на клавиатуре и укажите правильные параметры (см. предыдущие шаги). Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
12. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска ( * ) в поле **DNS** и нажмите пробел, затем - **OK**.

**Примечание:**

Если по каким-либо причинам указать NTP-сервер не удается, нажмите **Cancel** и выполните данную настройку позднее (подробнее о настройке NTP-сервера см. в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Настройка синхронизации времени").

13. Настройте параметры локализации:
    a. Укажите язык предустановленных сущностей:
        i. Выберите **CFDb**, нажмите **Enter** .
        ii. Выберите требуемый язык, нажмите **OK**.
        На выбранном языке будут созданы такие предустановленные сущности, как классификатор, запросы, политики по умолчанию. Вы можете выбрать один или несколько языков.
    b. Укажите язык интерфейса:
        i. Выберите **Interface**, нажмите **Enter**.
        ii. Выберите требуемый язык, Нажмите **OK**.
        На выбранном языке будет установлена консоль управления.
    c. Нажмите **Accept**.
    d. В открывшемся окне проверьте, что выбранные языки для предустановленных сущностей и для интерфейса указаны правильно, затем нажмите **Yes**.
14. Настройте параметры автоматического удаления событий из БД (детальное описание см. в статье "Настройка автоматического удаления событий из БД").
15. По завершению настроек нажмите **Save settings**.

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

В результате установки в системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора (**kickstart**). После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера Traffic Monitor.

О порядке дальнейшей настройки Системы см. документ «InfoWatch Traffic Monitor. Руководство администратора».

# 3.3 Распределенная установка TM Enterprise

Traffic Monitor в редакции Enterprise позволяет развернуть Систему так, чтобы сервер Traffic Monitor и СУБД (Oracle Enterprise или PostgreSQL) были установлены на разные компьютеры. Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одном компьютере.

Установка серверов должна производиться в следующем порядке:

- Установка Базы данных (TM DB server);
- Установка Сервера Traffic Monitor (TME Node server).

**Важно!**

Установка в другом порядке (сервер Traffic Monitor устанавливается раньше, чем База данных) не поддерживается и приводит к возниновению ошибок в процессе установки.

Вы можете установить несколько серверов Traffic Monitor. При этом необходимо логически разделить их на основной и второстепенный (второстепенные). Основным сервером называется сервер, на котором будут запущены процессы, необходимые Системе в единственном экземпляре. Порядок настройки описан в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Дополнительные настройки при установке с ключами IWDBX и IWTM".

## 3.3.1 Установка Базы данных (TM DB server)

**Важно!**

В данном разделе приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе "Общие сведения по этапам установки серверных компонентов".

**Чтобы установить Базу данных, выполните следующие действия:**

1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.
2. В окне приветствия выберите **TM Enterprise**, нажмите **Enter**.
3. В окне выбора базы данных укажите, какая СУБД должна быть установлена:
   a. **Oracle Enterprise**;
   b. **PostgreSQL**.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите **TME DB server**, нажмите **Enter**.

**Важно!**

После выбора режима установки на экран может быть выведено предупреждение "*The storage device below may contain any data"*. Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of filesystems**.

5. Укажите настройки часового пояса для сервера, нажмите **Next**.
6. Задайте пароль пользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе "Приложение А. Рекомендации по составлению имен и паролей".
7. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):
    a. Выберите **Use All Space**.
    b. Установите флажок в поле **Review and modify partitioning layout**, расположенном внизу окна, нажмите **Next**.
    c. Убедитесь, что диски разбиты правильно, нажмите **Next**.
8. Выполните настройку параметров сетевой карты и DNS конфигурации (детальное описание см. в статье "Настройка сети"), нажмите **Save&Quit**.
9. Проверьте указанные сетевые настройки. Если настройки некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
10. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска ( * ) в поле **DNS** и нажмите пробел, затем - **Ok**.
11. Настройте параметры локализации:
    a.
        i. Укажите язык предустановленных сущностей:
            1. Выберите **CFDb**, нажмите **Enter** .
            2. Выберите требуемый язык, нажмите **Ok**.
            На выбранном языке будут созданы такие предустановленные сущности, как классификатор, запросы, политики по умолчанию. Вы можете выбрать один или несколько языков.
        ii. Укажите язык интерфейса:
            1. Выберите **Interface**, нажмите **Enter**.
            2. Выберите требуемый язык, Нажмите **Ok**.
            На выбранном языке будет установлена консоль управления.
        iii. Нажмите **Accept**.
        iv. В открывшемся окне проверьте, что выбранные языки для предустановленных сущностей и для интерфейса указаны правильно, затем нажмите **Yes**.
12. Настройте параметры автоматического удаления событий из БД (детальное описание см. в статье "Настройка автоматического удаления событий из БД").
13. По завершении настроек нажмите **Save settings**.

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

В результате установки в Системе будут созданы учетные записи, перечисленные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

О порядке дальнейшей настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».
.

## 3.3.2 Установка Сервера Traffic Monitor (TME Node server)

> **Важно!**
>
> В данной статье приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе "Общие сведения по этапам установки серверных компонентов".

**Чтобы установить Сервер Traffic Monitor, выполните следующие действия:**

1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.
2. В окне приветствия выберите **TM Enterprise**.
3. В окне выбора базы данных в укажите, какая СУБД должна быть установлена:
   a. **Oracle Enterprise**;
   b. **PostgreSQL**.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите **TME Node server**, нажмите **Enter**.

> **Важно!**
>
> После выбора режима установки на экран может быть выведено предупреждение «*The storage device below may contain any data*». Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of file systems**.

5. Укажите настройки часового пояса для сервера, нажмите **Next**.
6. Задайте пароль суперпользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе "Приложение А. Рекомендации по составлению имен и паролей".

7. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):
    a. Выберите **Use All Space**.
    b. Установите флажок в поле **Review and modify partitioning layout**, расположенном внизу окна, нажмите **Next**.
    c. Убедитесь, что диски разбиты правильно, нажмите **Next**.
8. Выполните настройку параметров сетевой карты и DNS конфигурации (детальное описание см. в статье "Настройка сети"), нажмите **Save&Quit**.
9. Проверьте указанные сетевые настройки. Если они некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
10. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска (*) в поле **DNS** и нажмите пробел, затем - **OK**.
11. Укажите статический IP-адрес сервера БД, нажмите **Enter**.

> **Примечание.**
>
> Если используется DHCP, необходимо привязать выдачу определенного IP-адрес к MAC-адресу.

12. Проверьте правильность настроек. Если они некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.

В результате установки в Системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора (**kickstart**). После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера Traffic Monitor.

О порядке дальнейшей настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

## 3.4 Установка подсистемы Краулер

Перехватчик Краулер реализован в виде двух служб Windows:

- `InfoWatch.Crawler.Scanner` – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;
- `InfoWatch.Crawler.Server` – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor;

**Важно!**

С одной схемой БД Traffic Monitor может успешно работать **только один** экземпляр сервера Краулер. Один сервер Краулер в текущей реализации Системы может поддерживать **только один** экземпляр сканера Crawler.

Перед установкой ознакомьтесь с требованиями к аппаратному и программному обеспечению компьютеров, на которые будет выполняться установка компонентов. Для установки обоих компонентов подсистемы Краулер (сервер и сканер) используется единый дистрибутив.

**Важно!**

И сервер, и сканер Краулер должны быть установлены на компьютеры, находящиеся в одном домене: в том, к которому принадлежат компьютеры, которые предполагается сканировать.

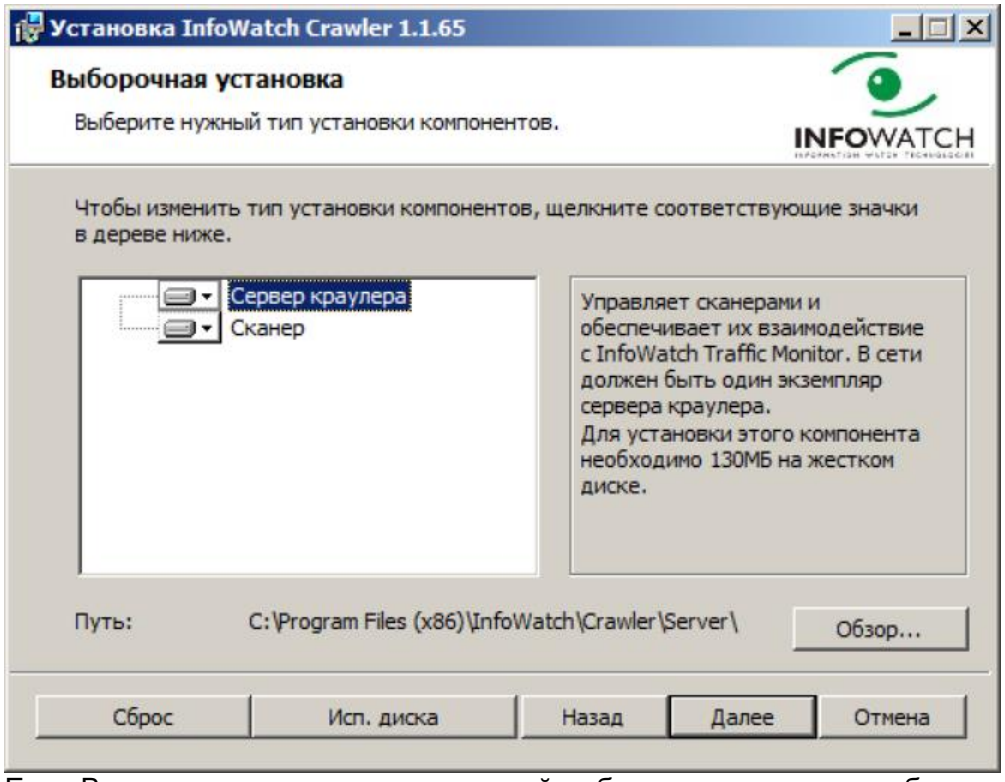
**Чтобы установить Краулер:**

1. Запустите установочный пакет `Crawler_vx.x.xxx.msi`, где x.x.xxx – номер версии.

**Примечание:**

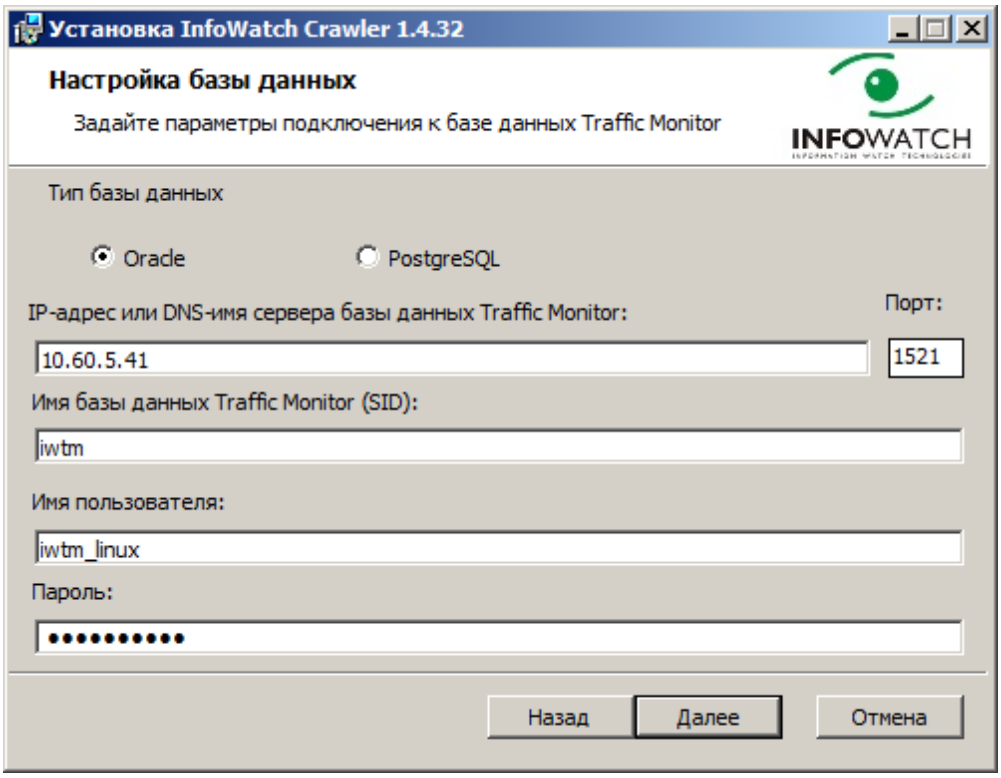
Язык мастера установки определяется автоматически и зависит от выбранного формата (см. **Пуск -> Панель управления -> Язык и региональные стандарты**, вкладка **Форматы**).

2. В окне приветствия мастера установки InfoWatch Crawler нажмите **Далее**.
3. В окне выбора области установки нажмите **Далее**.
4. На шаге **Выборочная установка** определите, какие компоненты Crawler нужно установить и укажите директорию, в которую будет установлен компонент:
   - **Сервер краулера** – установка службы InfoWatch.Crawler.Server, управляющей заданиями сканирования и обеспечивающей взаимодействие с сервером, базой данных и Консолью управления Traffic Monitor.
   - **Сканер** – установка службы InfoWatch.Crawler.Scaner, осуществляющей сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам.




Если Вы не хотите устанавливать какой-либо из компонентов, выберите его и в раскрывшемся списке отметьте пункт ✕ **Этот компонент будет полностью недоступен**.
Укажите путь к директориям, в которые будут установлены компоненты, и нажмите **Далее**.

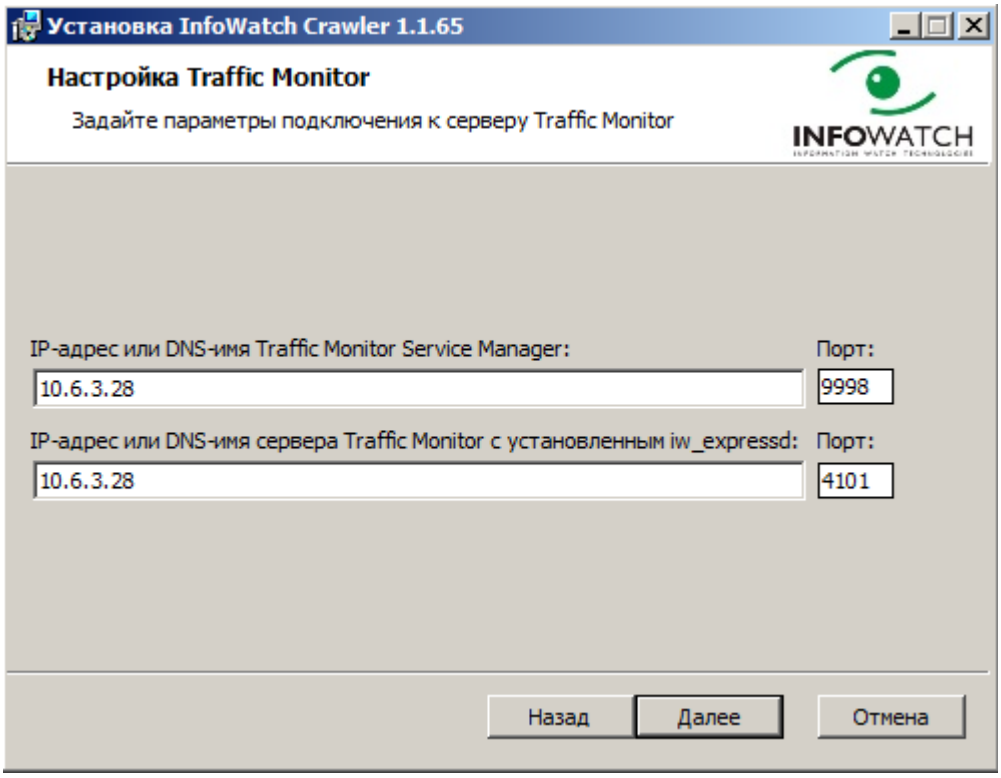
5. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сервер краулера**:
   a. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с базой данных Traffic Monitor, нажмите **Далее**.




В зависимости от используемой СУБД параметры подключения могут различаться:

| Параметр | Oracle | PostgreSQL | Пояснения |
|---|---|---|---|
| IP-адрес или DNS-имя | Соответственно используемому серверу БД ТМ | | |
| Порт | 1521 | 5433 | |
| Имя базы данных | iwtm | postgres | Для PostgreSQL указывается SID или service name. |
| Имя пользователя | iwtm_linux | iwtm_linux | Пользователь Linux части СУБД, от имени которого перехваченные объекты будут загружаться в базу данных. |
| Пароль | xxXX1234 | xxXX1234 | Если не изменялся после установки серверной части Traffic Monitor. |

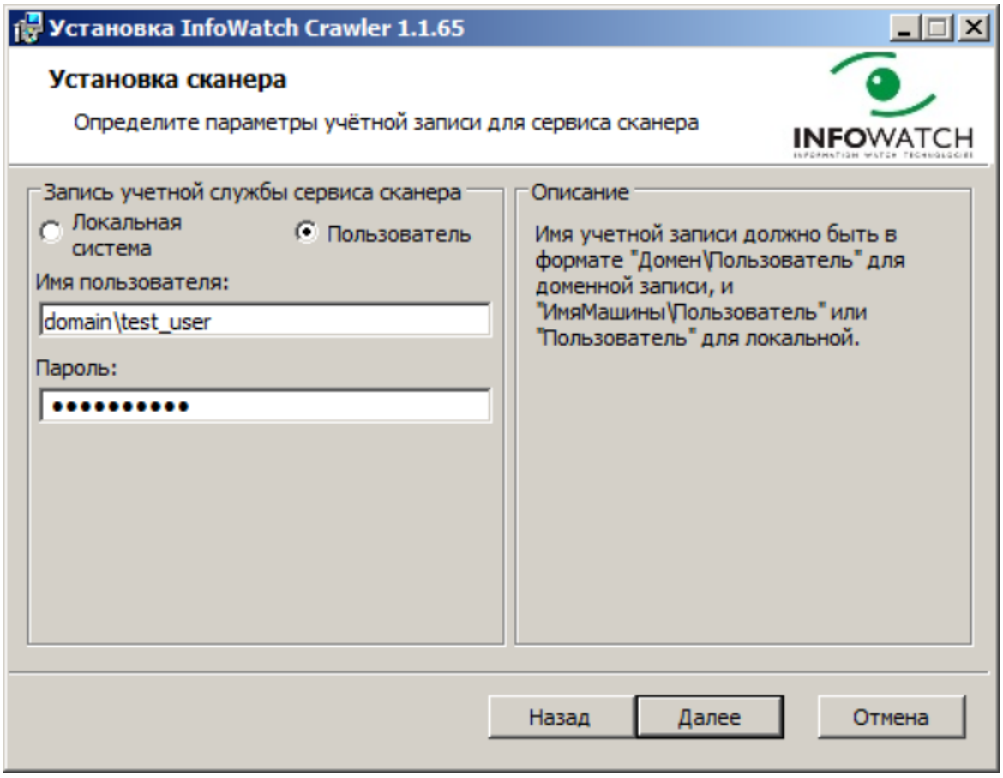
b. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с сервером Traffic Monitor, нажмите **Далее**.




В случае распределенной установки укажите следующие значения:
- в поле **IP-адрес или DNS-имя Traffic Monitor Service Manager** укажите IP-адрес сервера БД ТМ;
- в поле **IP-адрес или DNS-имя сервера Traffic Monitor с установленным iw_expressed** укажите IP-адрес сервера ТМ (TME Node Server).

После окончания установки запустите сервер Краулера. Для этого выполните следующие действия:

6. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**:
   a. укажите, от имени какой учетной записи будет запускаться служба InfoWatch.Crawler.Scaner. Вы можете выбрать стандартную учетную запись Local System (рекомендуется) или ввести параметры учетной записи, имеющей право на выполнение служб в фоновом режиме (настройка данной возможности выполняется в меню **Панель управления –> Администрирование –> Локальная политика безопасности –> Локальные политики –> Назначение прав пользователя –> Вход в качестве службы**). Нажмите **Далее**.

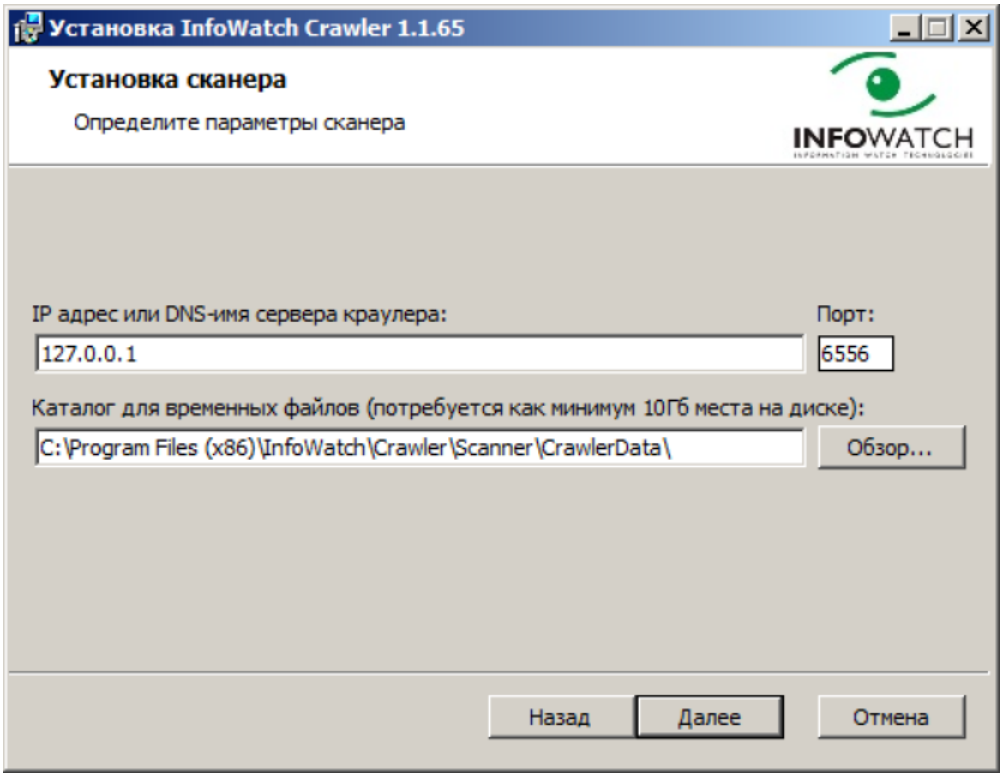



b. укажите:

- IP адрес или DNS имя компьютера, куда установлен компонент **Сервер**;
- номер порта сервера Краулер;
- путь к директории, куда сканер будет временно сохранять файлы, скопированные с проверяемых ресурсов.

**Примечание:**

Если поле **Каталог для временных файлов** оставить пустым, то установщик автоматически выберет последнее использованное в операционной системе значение пути.




7. Нажмите **Далее**.
8. Нажмите **Установить**, чтобы начать установку Краулер. По окончании установки нажмите **Готово**.
9. После установки компонента Сервер запустите его, выполнив следующие действия:
    - подключитесь к серверу, на котором установлен пакет **iwtm-webgui**;
    - в файле **web.conf** измените значение параметра `enabled` секции crawler с "0" на "1";
    - выполните команду `service iwtm restart kicker`.

## 3.5 Предустановленные серверные параметры

В результате установки серверной части Системы создается ряд сущностей, к которым впоследствии может потребоваться обращаться при дальнейшей настройке и эксплуатации Системы.

Имя сервера (hostname): **iwtm-xxxxxxxxxxxxxxxx.local**, где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Директории установки Системы (могут располагаться на разных серверах):

- сервер Traffic Monitor – **/opt/iw**
- БД – **/u01** и **/u02**

> **Примечание.**
>
> При установке Traffic Monitor версии `6.1.100` или ниже БД PostgreSQL устанавливается только в каталог `/u01`.

Параметры базы данных Traffic Monitor:

| **Параметр** | **Oracle** | **PostgreSQL** |
|---|---|---|
| Порт подключения к БД | **1521** | **5433** |
| Имя базы данных / SID или service name | **iwtm** | **postgres** |

Учетные записи:

| **Учетная запись** | **Имя** | **Пароль** |
|---|---|---|
| Суперпользователь OS Linux (root) | **root** | Задается при установке |
| Пользователь Linux, от имени которого будут запускаться серверные процессы Traffic Monitor | **iwtm** | Без пароля |
| Oracle администратор | **sys** | xxXX1234 |
| | **system** | xxXX1234 |
| Владелец схемы базы данных | **iwtm** | xxXX1234 |
| Пользователь Linux части СУБД, от имени которого перехваченные объекты будут загружаться в базу данных (и Oracle, и PostgreSQL) | **iwtm_linux** | xxXX1234 |
| Пользователь, от имени которого веб-интерфейс будет взаимодействовать с БД | **iwtm_web** | xxXX1234 |
| Веб-консоль управления: администратор пользователей | **administrator** | xxXX1234 |
| Веб-консоль управления: офицер безопасности | **officer** | xxXX1234 |

| Учетная запись | Имя | Пароль |
|---|---|---|
| Пользователь Linux, от имени которого будут запускаться серверные процессы БД<br>**Важно!** Настоятельно рекомендуется сразу же по окончании установки сменить пароль этой учетной записи .<br>**Примечание:**<br>При установке базы данных Postgres, данная учетная запись не создается. | **oracle** | xxXX1234 |

Группа владельца инсталляции клиента СУБД Oracle, в состав которой включены пользователи iwtm, oracle - **oinstall**

# 4 ОБНОВЛЕНИЕ СИСТЕМЫ

**Чтобы обновить Систему для типа установки "все-в-одном"**:

1. Обновите пакеты RHEL и IWTM.
2. Обновите схему БД для Oracle или PostgreSQL.
3. Перезагрузите сервер.

**Чтобы обновить Систему для распределенного типа установки**:

1. На сервере ТМ и БД обновите пакеты RHEL и IWTM.
2. На сервере БД обновите схему БД для Oracle или PostgreSQL.
3. Перезагрузите сервер БД.
4. Перезагрузите сервер ТМ.

Перед началом обновления проверьте наличие файла `/opt/iw/tm5/iwks_mode` и соответствие типа установки, указанного в файле, с фактическим типом установки.
Файл может содержать следующие параметры:

| **Параметр** | **Значение** |
|---|---|
| iwall | Все компоненты InfoWatch Traffic Monitor Enterprise устанавливаются на один сервер |
| iwtm | Установка сервера Traffic Monitor на отдельный компьютер |
| iwdb | Установка сервера СУБД со схемой БД Traffic Monitor на отдельный компьютер |
| iwtms | Все компоненты InfoWatch Traffic Monitor Standard устанавливаются на один сервер |

Если файл отсутствует или в нем указана некорректная версия установки, создайте файл и укажите корректный параметр.

**Важно!**

В результате обновления происходит замена конфигурационного файла system.lua, поэтому Система перенастраивается в транспортный режим по умолчанию - в режим копирования. Чтобы вернуть настройки на использовавшийся ранее режим блокировки ("в разрыв"), в конфигурационном файле **system.lua** измените значения параметра **transport_mode** с **Copy** на **Normal**. Подробнее о порядке настройки транспортного режима см. Руководство администратора, раздел "Настройка перехвата трафика", подразделы для того или иного типа трафика.

.

# 4.1 Обновление пакетов RHEL и IWTM

Для обновления Системы требуется подключение дистрибутивного диска **kickstart**. Необходимые для обновления пакеты устанавливаются на сервер с указанного диска.

1. В произвольном разделе жесткого диска компьютера создайте директорию и смонтируйте CD-диск:
   `mkdir -p /mnt/rhel-dvd && mount /dev/cdrom /mnt/rhel-dvd`
2. В директории `/etc/yum.repos.d` создайте файл **rhel-dvd.repo** (этот файл потребуется для указания пути к файлам обновления).
3. Откройте файл **rhel-dvd.repo** для редактирования и вставьте в следующий текст:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=1
gpgcheck=0

[rhel-dvd-iwtm]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux
enabled=1
gpgcheck=0

[rhel-dvd-iwtm-cfdb]name=DVD_IW-CFDBbaseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/enabled=1gpgcheck=0
```

> **Примечание:**
>
> Если в Системе используется нестандартная БКФ, то репозиторий cfdb перед началом обновления добавлять не нужно.

4. Сохраните измененный файл **rhel-dvd.repo**.
5. Очистите кэш менеджера пакетов:
   `yum clean all`
6. Удалите пакет `iwtm-tmcap`:

```
rpm -e --nodeps iwtm-tmcap
```

> **Важно!**
>
> Если не удалить пакет, то в процессе обновления может быть удален модуль ядра tmcap.ko, что потребует переустановку `iwtm-tmcap`.
>
> При обновлении сервера базы данных удаление `iwtm-tmcap` не требуется.

7. Установите `kernel-headers` используемой версии ядра:

```
yum install kernel-headers
```

**Примечание:**

Если после установки Системы не вносились изменения в kernel-headers, пропустите этот шаг.

8. Остановите сервисы iwtm:
   `service iwtm stop`
9. Установите пакет `iwtm-tmcap`:

   ```
   yum install iwtm-tmcap
   ```
10. Запустите процесс обновления пакетов:
    `yum upgrade`

11. Проверьте наличие новых версий конфигурационных файлов с расширением **conf.rpmnew** в каталоге `/opt/iw/tm5/etc/:`
    - Если подобные файлы есть, их нужно корректно объединить со старыми конфигурационными файлами.
12. Проверьте наличие новых версий конфигурационных файлов Nagios с расширением **cfg.rpmnew** в каталоге `/etc/nagios/iwmon:`
    - Если подобные файлы есть, их нужно корректно объединить со старыми конфигурационными файлами.

**Важно!**

В **/opt/iw/tm5/etc/postgresql.conf** значение параметра `Port` должно всегда быть равным `5433`.

13. Если в предыдущей версии вносились изменения в конфигурационный файл **config_manager.conf**, то необходимо скопировать настройки из секции Serman файла **config_manager.conf.rpmsave** в секцию `Serman` файла **agent.conf**. Оба файла расположены в директории `/opt/iw/tm5/etc`.
14. Проверьте каталог `/opt/iw/tm5/etc/scripts/` на наличие скриптов с расширением **.lua.rpmnew**:
    - Если подобные файлы есть, их нужно корректно объединить со старыми конфигурационными файлами.

## 4.2 Обновление схемы БД Oracle

1. Остановите службы:

```
service iwtm stop
service php-fpm stop
service nagios stop
```

**Примечание**

При наличии в Системе подсистемы Crawler потребуется приостановить службы указанной подсистемы (на сервере Crawler).

2. Переключитесь на пользователя: su - oracle.

**Примечание**

Логин владельца схемы по умолчанию: `iwtm` .

3. Убедитесь, что конфигурационный файл **database.conf**, расположенный в директории `/opt/iw/tm5/csw/oracle`, обновился корректно, и в нем указана актуальная версия схемы.
4. Перейдите в директорию `/opt/iw/tm5/csw/oracle`:

   ```
   cd /opt/iw/tm5/csw/oracle
   ```

5. Запустите обновление БД при помощи сценария (скрипта):
   `./update.sh`
6. Запустите остановленные службы (необходимо обратно переключиться на пользователя root):

   ```
   service iwtm start
   service php-fpm start
   service nagios start
   ```

**Примечание**

При наличии в Системе подсистемы Crawler потребуется запустить службы указанной подсистемы (на сервере Crawler).

## 4.3 Обновление схемы БД PostgreSQL

1. Остановите службы:

   ```
   service iwtm stop
   service php-fpm stop
   service nagios stop
   ```

**Примечание**

При наличии в Системе подсистемы Crawler потребуется приостановить службы указанной подсистемы (на сервере Crawler).

2. Переключитесь на пользователя: su - postgres.

**Примечание**

Логин владельца схемы по умолчанию: `iwtm`.

3. Убедитесь, что конфигурационный файл **database.conf**, расположенный в директории `/opt/iw/tm5/csw/postgres`, обновился корректно, и в нем указана актуальная версия схемы.
4. Перейдите в директорию `/opt/iw/tm5/csw/postgres`:

   ```
   cd /opt/iw/tm5/csw/postgres
   ```

5. Запустите обновление БД при помощи сценария (скрипта):
   ```
   ./update.sh
   ```
6. Запустите остановленные службы (необходимо обратно переключиться на пользователя root):
   ```
   service iwtm start
   service php-fpm start
   service nagios start
   ```

**Примечание**

При наличии в Системе подсистемы Crawler потребуется запустить службы указанной подсистемы (на сервере Crawler).

# 5 УДАЛЕНИЕ СИСТЕМЫ

Удаление Системы подразумевает удаление всех пакетов Системы, а также удаление используемой схемы базы данных. Для полного удаления операционной системы и СУБД вы можете, например, выполнить форматирование используемых разделов стандартными средствами.

- О порядке удаления схемы БД (как Oracle, так и PostrgreSQL) см. "Удаление схемы базы данных".
- Подсистема Crawler (как сервер, так и сканер) удаляется стандартными средствами ОС Windows: **Пуск -> Панель управления -> Программы и компоненты**, команда **Удалить**.
- Чтобы удалить отдельный пакет, выполните команду:

  ```
  rpm -e имя_пакета
  ```
- Все серверные компоненты Traffic Monitor (в том числе компоненты веб-консоли, модули Sniffer, IW ICAP, модуль взаимодействия с удаленной базой данных и другие) выполняются при помощи следующей команды:

  ```
  yum remove `rpm -qa | grep iwtm`
  ```

По окончании удаления Сервера Traffic Monitor верните внешнюю инфраструктуру, настроенную на Traffic Monitor, в исходное состояние:

- если выполнялась интеграция с почтовым relay-сервером - убедитесь, что параметры Postfix возвращены в исходное состояние;
- если Система выполняла перехват и фильтрацию SMTP-трафика - настройте доставку SMTP-писем через корпоративный почтовый сервер, минуя InfoWatch Traffic Monitor.

После удаления на компьютере остаются только:

- операционная система;
- конфигурационные файлы, в которые были внесены изменения (измененным файлам присваивается суффикс **.rpmsave** - например, **detector.conf.rpmsave**; файлы, которые не изменялись, будут удалены);
- очередь объектов (о порядке удаления файлов из директории временных файлов операционной системы и данных из директорий файловых очередей Traffic Monitor см. «InfoWatch Traffic Monitor. Руководство администратора», статья "Удаление временных файлов");
- категории и термины;
- файл лицензии;
- учетная запись пользователя – владельца InfoWatch Traffic Monitor, и группа, в состав которой входил этот пользователь.

# 5.1 Удаление схемы базы данных

Данная инструкция актуальна для СУБД Oracle и PostrgreSQL.

**Важно**

Не удаляйте схему базы данных, от которой для архивирования были отключены ежедневные табличные пространства. Иначе Вы не сможете восстановить данные из этих табличных пространств.

1. **Проверка сервера СУБД Oracle**

   Убедитесь, что:

   - версия установленной схемы базы данных соответствует версии программного пакета, используемого для ее удаления;
   - запущен сервер СУБД;
   - в конфигурационном файле **database.conf** корректно указаны имя и пароль учетной записи, обладающей правами SYSDBA (значения параметров `sysdba` и `sysdba_password`).

2. **Остановка TrafficMonitor**

   a. Остановить все процессы Traffic Monitor:
   `service iwtm stop`

   b. Закрыть все экземпляры консоли управления;

   c. Остановить веб-сервис:
   service php-fpm stop

   d. Прекратить все соединения с удаляемой схемой базы данных, осуществляемые из других программ.

3. **Запуск удаления схемы**

   a. Перейдите в директорию
   `/opt/iw/tm5/csw/oracle` или `/opt/iw/tm5/csw/postgres`

   b. Выполните скрипт:
   ./uninstall.sh

**Важно**

При удалении схемы БД из Системы будут также удалены следующие компоненты:

- политики, в том числе предустановленные (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Предустановленные политики");
- плагины и токены (см. "*Infowatch Traffic Monitor. Руководство администратора*", статья "Плагины").

Для восстановления плагина Device Monitor и повторного распространения предустановленных политик выполните следующие действия:

1. Создайте файл **/opt/iw/tm5/www/backend/protected/runtime/first_run** от имени пользователя **iwtm**;
2. Перезапустите процесс **iw_kicker**:
   ```
   service iwtm restart kicker
   ```

   Далее нужно вручную добавить остальные плагины (см. "*Infowatch Traffic Monitor. Руководство администратора*", статья "Добавление плагина") и создать необходимые политики (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статьи "Создание политики защиты данных" и "Создание политики контроля персон").

## 5.2 Crawler

Подсистема Crawler (как сервер, так и сканер) удаляется стандартными средствами ОС Windows: **Пуск -> Панель управления -> Программы и компоненты**, команда **Удалить**.

# 6 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ

**Требования к именам пользователей**

- Длина имени пользователя может составлять от 1 до 20 символов.
- Имя пользователя может состоять из букв латинского алфавита, цифр и символа подчеркивания «_». Должно начинаться с буквы.

**Требования к паролям пользователей**

- Длина пароля может составлять от 1 до 30 символов.
- Пароль пользователя может состоять из букв латинского алфавита, цифр и символов:

«#», «$» или «_».
Может начинаться только с буквы.

- Пароль чувствителен к регистру символов.

**Рекомендации по составлению надежных паролей**

- Рекомендуемая длина пароля: от 10 до 30 символов.
- Пароль должен представлять собой смешанный набор букв верхнего и нижнего регистров, цифр и символов.
- Не рекомендуется:
    - включать в состав пароля слова и словосочетания;
    - включать в состав пароля несколько идущих подряд одинаковых символов;
    - начинать и заканчивать пароль одним и тем же символом;
    - создавать новый пароль путем добавления символов к текущему паролю.

**Общие рекомендации**
Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.
В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

| | | | |
|---|---|---|---|
| ACCESS | EXCLUSIVE | MODE | SELECT |
| ADD | EXISTS | MODIFY | SESSION |
| ALL | FILE | NOAUDIT | SET |
| ALTER | FLOAT | NOCOMPRESS | SHARE |
| AND | FOR | NOT | SIZE |
| ANY | FROM | NOWAIT | SMALLINT |

| | | | |
|---|---|---|---|
| AS | GRANT | NULL | START |
| ASC | GROUP | NUMBER | SUCCESSFUL |
| AUDITBETWEEN | HAVING | OF | SYNONYM |
| BY | IDENTIFIED | OFFLINE | SYSDATE |
| CHAR | IMMEDIATE | ON | TABLE |
| CHECK | IN | ONLINE | THEN |
| CLUSTER | INCREMENT | OPTION | TO |
| COLUMN | INDEX | OR | TRIGGER |
| COMMENT | INITIAL | ORDER | UID |
| COMPRESS | INSERT | PCTFREE | UNION |
| CONNECT | INTEGER | PRIOR | UNIQUE |
| CREATE | INTERSECT | PRIVILEGES | UPDATE |
| CURRENT | INTO | PUBLIC | USER |
| DATE | IS | RAW | VALIDATE |
| DECIMAL | LEVEL | RENAME | VALUES |
| DEFAULT | LIKE | RESOURCE | VARCHAR |
| DELETE | LOCK | REVOKE | VARCHAR2 |
| DESC | LONG | ROW | VIEW |
| DISTINCT | MAXEXTENTS | ROWID | WHENEVER |
| DROP | MINUS | ROWNUM | WHERE |
| ELSE | MLSLABEL | ROWS | WITH |

# 7 ПРИЛОЖЕНИЕ В. ЛИЦЕНЗИИ НА СТОРОННЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При создании Системы были использованы разработки третьих сторон, распространяемые на условиях лицензии MIT (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

Также использовалось программное обеспечение:

- распространяемое на условиях лицензий BSD (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- распространяемое на условиях GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext – http://www.foolabs.com/xpdf/
  - Tnef – http://sourceforge.net/projects/tnef/
  - Unzip – http://www.info-zip.org/UnZip.html
  - libcole.so – arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so – pauljlucas@mac.com