



# Гарда БД

Руководство пользователя

Модуль анализа сетевого трафика

Дата выпуска: 18.11.2022

Статус документа: Released

Версия ПО: 4.21

ООО «Гарда Технологии»

Все права сохраняются за правообладателем.

ООО «Гарда Технологии» оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

#### ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО «Гарда Технологии». Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким-либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО «Гарда Технологии». Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

---

# Содержание

<b>1. Введение</b> .....	<b>4</b>
1.1. Аннотация.....	4
1.2. Типографические соглашения .....	4
1.3. Использование имен, номеров телефонов, сетевых адресов .....	4
1.4. О компании .....	4
1.5. Техническая поддержка .....	4
<b>2. Назначение модуля</b> .....	<b>5</b>
<b>3. Работа с Анализаторами</b> .....	<b>5</b>
3.1. Добавление и редактирование записи об анализаторе.....	5
3.2. Использование таблицы ассоциаций .....	7
3.3. Тестирование источников данных .....	9

## 1. Введение

### 1.1. Аннотация

Данный документ представляет собой Руководство пользователя к программному модулю анализа сетевого трафика, входящего в состав программного обеспечения «Гарда БД» (далее Система, Комплекс).

### 1.2. Типографические соглашения

Обозначения и типографические соглашения, использованные в данном документе, приведены ниже.

#### Соглашения и обозначения

Пример	Обозначение
<u>Примечание: текст</u>	Важная информация, требующая особого внимания
<i>N</i>	Ссылка на документ
<b>Registration</b>	Названия конфигурационных параметров, вкладок и кнопок в граф. интерфейсе
<a href="http://www.example.com/">http://www.example.com/</a>	Гиперссылки

### 1.3. Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

### 1.4. О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов.

Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности:

- защиты от DDoS-атак операторского класса.
- защиты баз данных.
- фрод-мониторинга порядка пропуска трафика операторов связи.
- DLP-систем.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее – на [gardatech.ru](http://gardatech.ru)

### 1.5. Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: [gbd.support@gardatech.ru](mailto:gbd.support@gardatech.ru).

## 2. Назначение модуля

Модуль анализа сетевого трафика (далее модуль «Анализатор», анализатор) предназначен для аудита и съема трафика в соответствии с критериями фильтрации. Средствами модуля выполняется анализ на соответствие настроенным политикам, передача перехваченных в соответствии с политиками событий в модули хранения и обработки данных.

## 3. Работа с Анализаторами

При работе с анализаторами сетевой активности пользователь может добавлять/удалять записи об анализаторах, блокировать и перезапускать анализаторы, а также запрашивать диагностическую информацию с анализаторов путем тестирования. О тестировании анализатора см. в разделе [Тестирование источников данных](#).

---

*Примечание:* При долгом отсутствии поступления трафика на анализатор в журнал **Системные сообщения** будет заноситься следующее сообщение: «На входе Анализатора долгое время нет трафика».


---

### 3.1. Добавление и редактирование записи об анализаторе

Для добавления записи об анализаторе:

1. Перейдите на страницу **Настройки** → **Анализаторы**.
2. Под списком анализаторов в левой части страницы нажмите **Добавить анализатор**.
3. В открывшемся окне **Новый анализатор** заполните следующие поля:
  - **Название** - название анализатора. Значение будет отображаться в списке анализаторов.
  - **Описание** - произвольное описание или комментарий.
  - **IP-адрес управления** - адрес для управления анализатором.
  - **IP-адрес для агентов** - адрес для приема соединений с агента. Для настройки нескольких IP-адресов используйте кнопку **Добавить** (см. рисунок ниже).
  - **Порт**.
  - **Права просмотра** - при необходимости выдать право доступа пользователю раскройте роль и установите флажки напротив отдельных пользователей. При необходимости выдать права доступа целой роли установите флажок напротив роли. Однако, необходимо иметь в виду, что при выдаче прав доступа целой роли новые пользователи с данной ролью также будут иметь доступ к данным анализатора.
  - **Узлы хранилища** - выберите узлы хранилища, на которые будут приходить данные с анализатора.
4. Нажмите **Добавить**. Запись появится в списке анализаторов. Чтобы отменить действие, нажмите **Отмена**.

Для блокировки анализатора активируйте переключатель **Блокировать анализатор**. Зabloкированный анализатор неактивен, т.е. нет связи с хранилищем данных, не ведется мониторинг операций в контролируемых БД. Для перезапуска анализатора нажмите **Перезапустить** (см. рисунок ниже). На время перезапуска анализатора мониторинг операций с контролируемыми БД будет прекращен.

При необходимости отправки уведомления об отсутствии данных в журнал **Системные сообщения** активируйте соответствующий переключатель. По нажатию на пиктограмму  пользователю

становится доступна возможность задать временной период, в течении которого отсутствуют данные.

Возможны три типа состояния анализатора:



- анализатор активен;

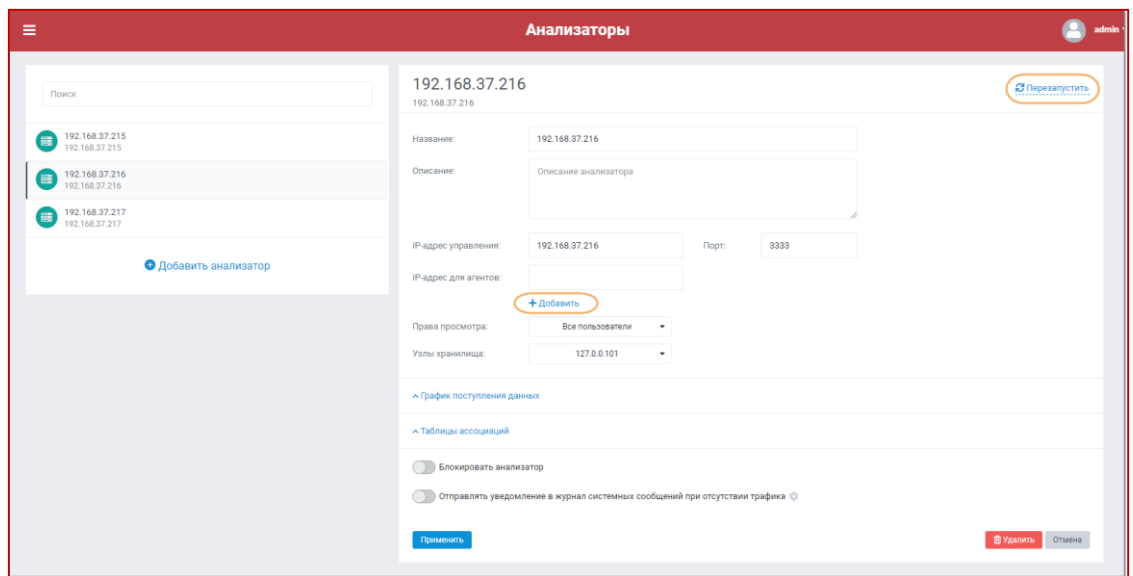


- связь с анализатором отсутствует;



- анализатор заблокирован.

Для изменения свойств анализатора выберите нужную запись в списке, в открывшемся окне отредактируйте необходимые параметры и нажмите кнопку **Применить**. Для удаления анализатора нажмите кнопку **Удалить** (см. рис. ниже).



### Изменение свойств анализатора

Для просмотра таблиц ассоциаций нажмите **Таблицы ассоциаций** и выберите необходимые базы данных (см. [Использование таблицы ассоциаций](#)).

Для просмотра статистики поступления данных нажмите **График поступления данных**.

В левом верхнем углу графика выберите период, за который необходимо построить график (см. рис. ниже). По умолчанию выбран период **За сегодня**.

Система позволяет строить график по 3 показателям:

- **Точка съема** - скорость, с которой данные приходят на анализатор;
- **Анализатор - Хранилище** - скорость, с которой данные идут от анализатора к хранилищу;
- **Количество запросов**.

При активации переключателя **Лицензионное ограничение** на графике показываются следующие пороговые значения:

- трафик, который может обработать анализатор в соответствии с лицензией;
- количество запросов в секунду, которое может обработать анализатор в соответствии с лицензией.

Для детального просмотра выделите необходимую область под графиком (см. рис. ниже).

График поступления данных можно добавить на главную страницу или экспортировать в формате PDF. Для этого нажмите **Сохранить** и выберите соответствующее действие.

При необходимости удаления устаревшей статистики поступления данных выполните следующие действия:

1. Выберите подходящий для вас вариант из списка **Удалять данные старше...**
2. Нажмите **Удалить**.
3. Подтвердите действие во всплывающем окне.

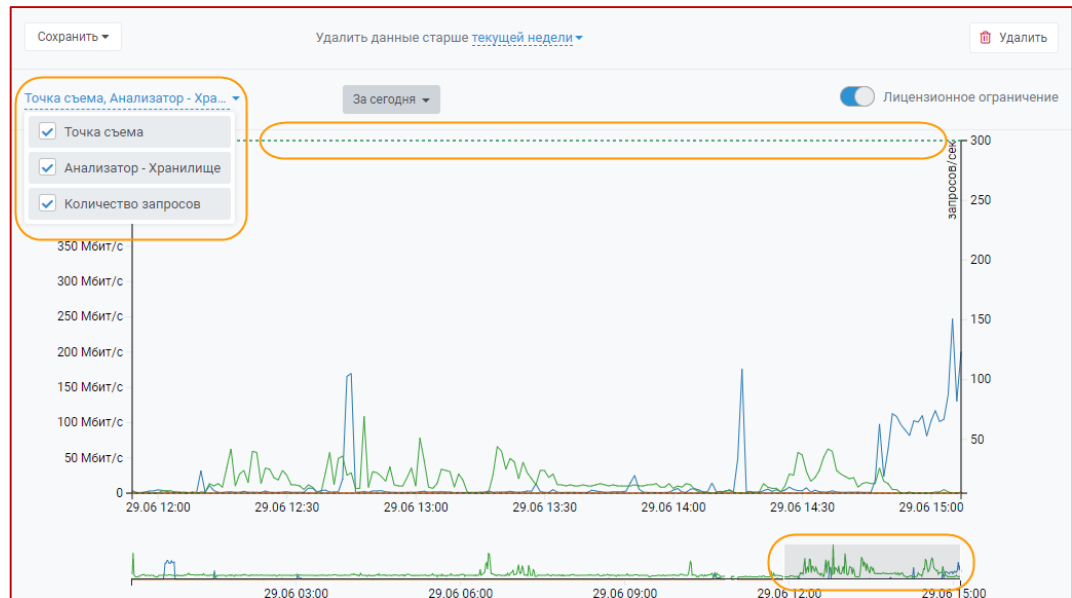


График поступления данных

### 3.2. Использование таблицы ассоциаций

Для выявления фактов неявного обращения пользователей к объектам БД в комплексе предусмотрена функция таблиц ассоциаций.

Под неявным обращением понимается обращение к объекту БД (например, таблице) через синонимы, представления, функции и хранимые процедуры.

Использование таблицы ассоциаций позволяет перехватывать такие запросы, даже если в политиках безопасности явно не были указаны функции/синонимы/представления, обращающиеся к защищаемым объектам, а указаны лишь сами объекты в виде критериев анализа. Это позволяет повысить эффективность перехвата информации.

**Пример:** Предположим, согласно созданным критериям требуется перехватывать обращения к объекту БД EMPLOYEES. У объекта EMPLOYEES есть синоним S\_EMPLOYEES. Если этот синоним внесен в таблицу ассоциаций, то будут перехвачены запросы не только к объекту EMPLOYEES (например, SELECT \* FROM EMPLOYEES), но и к его синониму S\_EMPLOYEES (например, SELECT \* FROM S\_EMPLOYEES).

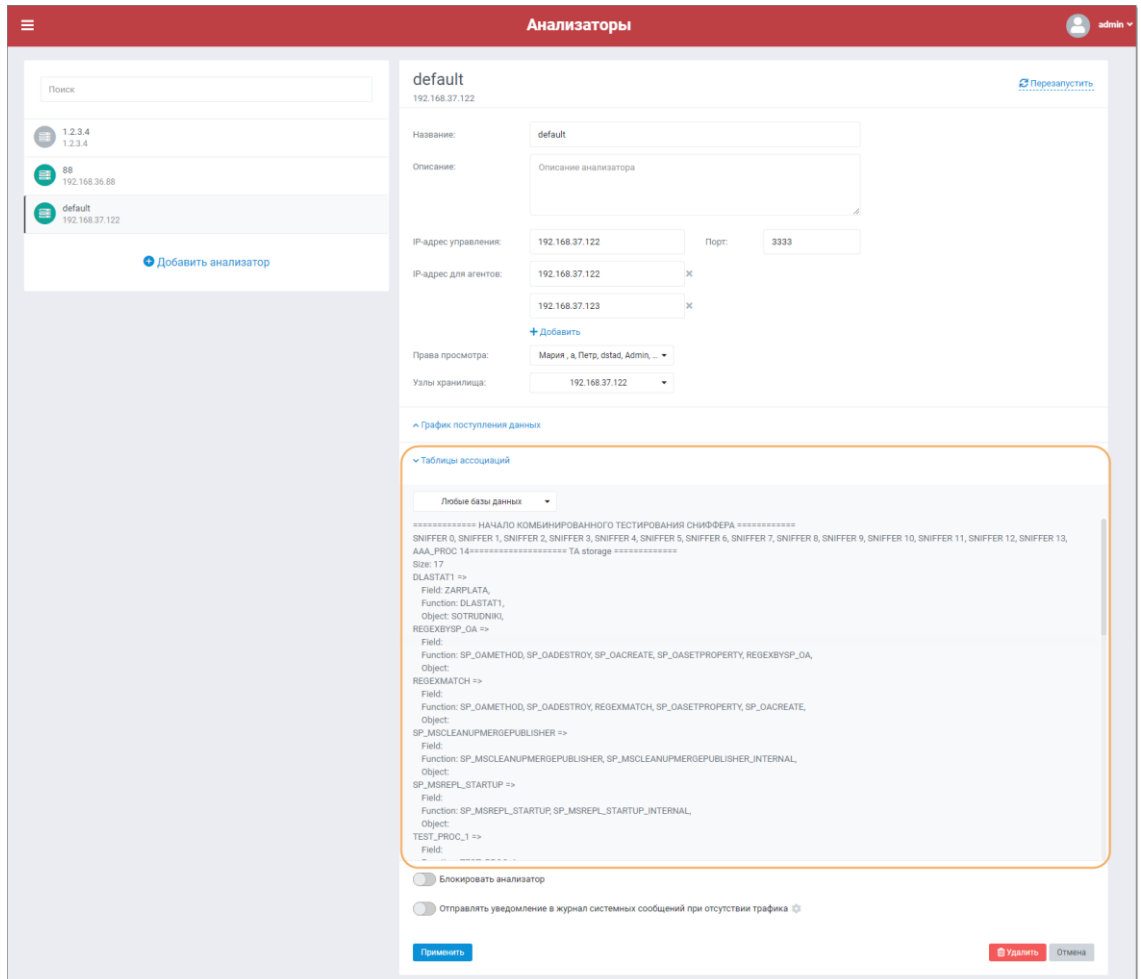
Чтобы использовать таблицы ассоциаций, необходимо выполнить следующие действия:

1. Создать или выбрать политику мониторинга с критериями **Таблица\Объект** или **Поле таблицы\объекта**.
2. Активировать переключатель **Использовать таблицы ассоциаций** в настройках политики.
3. Перейти в раздел **Настройки** → **Базы данных** и активировать переключатель **Синхронизация таблиц ассоциаций** в настройках выбранной БД.

**Примечание:** Синхронизация таблиц ассоциаций происходит посредством выполнения запроса на защищаемый сервер БД.

Для просмотра таблиц ассоциаций:

1. Перейдите в раздел **Настройки** → **Анализаторы**.
2. Выберите необходимый анализатор.
3. В настройках анализатора нажмите **Таблицы ассоциаций** и выберите необходимые базы данных (см. рис. ниже).



### Таблицы ассоциаций

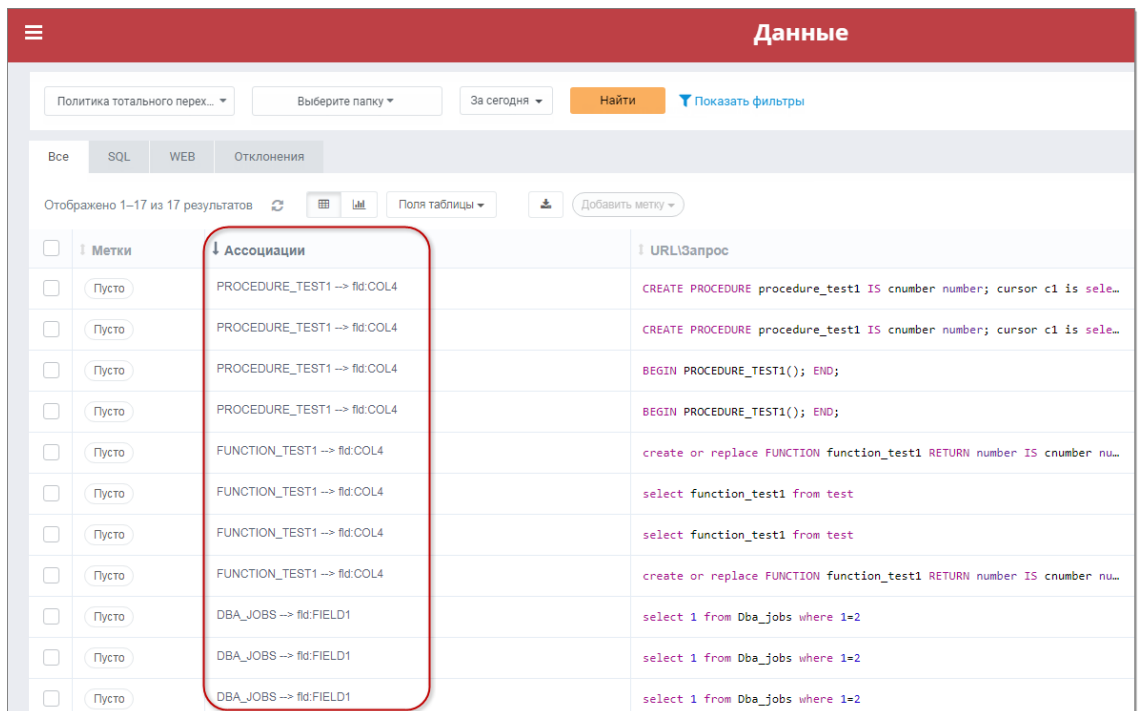
Просмотр ассоциаций, по которым были перехвачены события, доступен в поле **Ассоциации** раздела **Данные** (см. рис. ниже).

Все синонимы, представления, функции и процедуры на объекты контролируемой БД хранятся в таблице ассоциаций на сервере анализатора. Именуемые ассоциации обновляются посредством запроса к контролируемой БД каждую ночь.

Кроме того, Система автоматически отслеживает создание, изменение и удаление синонимов, представлений, функций, процедур пользователями контролируемой БД и обновляет таблицу ассоциаций.

Для каждой контролируемой БД может существовать только одна уникальная таблица ассоциаций.

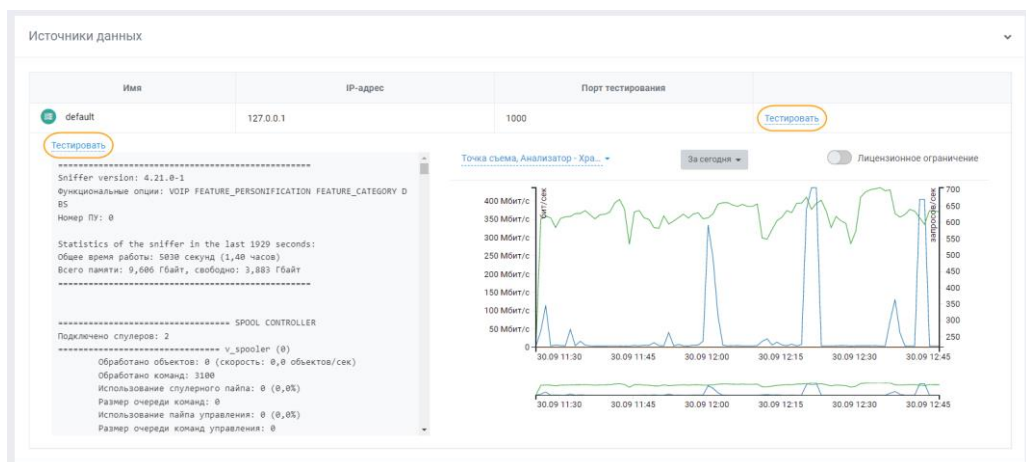




Поле Ассоциации в разделе Данные

### 3.3. Тестирование источников данных

В качестве источника данных в Системе выступает модуль анализа сетевого трафика (анализатор). Тестирование анализатора служит для определения параметров его работы. Для тестирования анализатора нажмите **Тестировать** в таблице **Источники данных**. Ниже появится график поступления данных на анализатор. Для получения информации о тестировании нажмите **Тестировать** в левом верхнем углу, как показано на рисунке ниже.



Тестирование анализатора