



# Гарда БД

Функциональная спецификация  
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. О компании .....  | 4                                      |
| 1.3. Техническая поддержка .....                                 | 4                                      |
| <b>2. Назначение модуля</b> .....                                | <b>4</b>                               |
| <b>3. Функциональные возможности</b> .....                       | <b>4</b>                               |
| <b>3.1. Мониторинг событий информационной безопасности</b> ..... | <b>4</b>                               |
| 3.1.1. Поддерживаемые БД .....                                   | 5                                      |
| 3.1.2. Обнаружение неконтролируемых БД.....                      | 5                                      |
| 3.1.3. Декодирование трафика.....                                | 5                                      |
| <b>3.2. Аудит событий информационной безопасности</b> .....      | <b>7</b>                               |
| 3.2.1. Дополнительные возможности обработки перехваченных данных | 7                                      |
| <b>3.3. Идентификация пользователей (персонификация)</b> .....   | <b>7</b>                               |
| <b>3.4. Блокировка доступа</b> .....                             | <b>Ошибка! Закладка не определена.</b> |
| <b>3.5. Использование таблицы ассоциаций</b> .....               | <b>8</b>                               |
| <b>3.6. Приложение 1. Поддерживаемые БД</b> .....                | <b>8</b>                               |

## 1. Введение

### 1.1. Аннотация

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

### 1.2. 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)

### 1.3. 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. Функциональные возможности

### 3.1. Мониторинг событий информационной безопасности

По умолчанию Система настроена на сбор максимального объема информации, проходящей по сети предприятия. Изначально при разворачивании Комплекса, либо в процессе эксплуатации администратор Комплекса может изменять состав собираемой информации. При необходимости можно исключить из перехвата трафик к определенным базам данных.

В политике тотального перехвата и в политиках безопасности возможен статистический режим работы, при котором не перехватываются переменные и ответы на SQL-запросы и HTTP-запросы. Данный режим снижает нагрузку на хранилище.

При помощи политик безопасности можно настроить мониторинг критичных баз данных в соответствии со следующими критериями:

- Дата/Время;
- IP-адрес:порт;
- Логин БД;
- Таблица/Объект;
- Поле таблицы/объекта;
- Логин ОС;
- Имя программы;
- Имя функции/процедуры;
- SQL-операции;
- Объем запроса;
- Объем ответа;
- Строк в ответе;
- Ключевое слово;
- Аутентификация;
- Экземпляр БД;
- Пользователь.

Значения критериев могут быть объединены в списки. Списки критериев могут быть сгруппированы при помощи логических операций.

### 3.1.1. Поддерживаемые БД

Система позволяет осуществлять мониторинг запросов, получаемых в виде копии трафика, к базам данных. Перечень поддерживаемых баз данных см. в [Приложении 1. Поддерживаемые БД](#). Поддерживается мониторинг запросов к веб-приложениям, доступ к которым осуществляется по протоколам HTTP/HTTPS.

**Примечание:** Мониторинг трафика к базам данных, не указанным в Приложении 1. «Поддерживаемые БД» возможен, но не гарантируется.

### 3.1.2. Обнаружение неконтролируемых БД

Модуль обладает возможностью автоматически обнаруживать неконтролируемые сервера БД, к которым были зафиксированы сетевые запросы.

### 3.1.3. Декодирование трафика

Система способна декодировать трафик, передаваемый по основным протоколам, указанным в следующей таблице:

| Протокол                         | Особенности декодирования  |
|----------------------------------|--|
| Ethernet, TCP/IP                 | <ul style="list-style-type: none"> <li>• протокол Ethernet IEEE 802.3 в полном объеме;</li> <li>• протоколы TCP/IP, UDP/IP в полном объеме;</li> <li>• мониторинг объема данных TCP, UDP в секунду.</li> </ul> |
| БД Oracle (прикладные протоколы) | <ul style="list-style-type: none"> <li>• протокол подключения и обмена данными Oracle;</li> <li>• контроль переключения каналов (сессий) TNS;</li> </ul>   |

|   |  |
|---|--|
|   | <ul style="list-style-type: none"> <li>• автоматическое обнаружение ключей декодирования (с помощью агентов).</li> </ul>   |
| БД MS SQL 2008 и MS SQL 2012 (прикладные протоколы) | протокол TDS версии СУБД 8 и 12  |
| Kerberos (протокол аутентификации)                  |  |
| HTTP и HTTPS  | <ul style="list-style-type: none"> <li>• методы GET, POST;</li> </ul>  |
| HTTPS 1.2   | <ul style="list-style-type: none"> <li>• протоколы: RFC2246 The TLS Protocol Version 1.0, RFC4346 The Transport Layer Security (TLS) Protocol Version 1.1, RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2;</li> <li>• шифронаборы (cipher suites): "0x00,0x01"<br/>TLS_RSA_WITH_NULL_MD5, "0x00,0x02"<br/>TLS_RSA_WITH_NULL_SHA, "0x00,0x04"<br/>TLS_RSA_WITH_RC4_128_MD5, "0x00,0x05"<br/>TLS_RSA_WITH_RC4_128_SHA, "0x00,0x07"<br/>TLS_RSA_WITH_IDEA_CBC_SHA, "0x00,0x09"<br/>TLS_RSA_WITH_DES_CBC_SHA, "0x00,0x0A"<br/>TLS_RSA_WITH_3DES_EDE_CBC_SHA, "0x00,0x2F",<br/>TLS_RSA_WITH_AES_128_CBC_SHA, "0x00,0x35",<br/>TLS_RSA_WITH_AES_256_CBC_SHA, "0x00,0x3B" TLS_RSA_WITH_NULL_SHA256, "0x00,0x3C"<br/>TLS_RSA_WITH_AES_128_CBC_SHA256, "0x00,0x3D"<br/>TLS_RSA_WITH_AES_256_CBC_SHA256, "0x00,0x41"<br/>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA, "0x00,0x84"<br/>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA, "0x00,0x96" TLS_RSA_WITH_SEED_CBC_SHA, "0x00,0x9C"<br/>TLS_RSA_WITH_AES_128_GCM_SHA256, "0x00,0x9D"<br/>TLS_RSA_WITH_AES_256_GCM_SHA384, "0x00,0xBA"<br/>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256, "0x00,0xC0"<br/>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256</li> <li>• алгоритмы обмена ключами: RSA, длина ключа до 4096 бит</li> <li>• алгоритмы сжатия TLS: NULL</li> <li>• расширения TLS: RFC5077 Transport Layer Security (TLS) Session Resumption without Server-Side State, RFC7627 Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension, RFC7366 Encrypt-then-MAC for Transport Layer Security (TLS)</li> </ul> |

Также Система выполняет контентный анализ текстовой информации, анализируя данные файлов. Поддерживаемые форматы файлов указаны в таблице ниже:

| Тип файла                  | Расширение файла                     |
|----------------------------|--------------------------------------|
| текстовые файлы            | .txt, .html, .xml и т.д.             |
| текстовые файлы в архиве   | .zip, .rar                           |
| документы Microsoft Office | .doc, .docx, xls, .xlsx, .ppt, .pptx |
| Adobe Acrobat              | .pdf                                 |

|             |                  |
|-------------|------------------|
| Open Office | .odt, .odp, .ods |
|-------------|------------------|

**Примечание:** Текстовые файлы и офисные документы, содержащиеся в архивах форматов могут быть декодированы до 20 уровня вложенности.

## 3.2. Аудит событий информационной безопасности

### 3.2.1. Дополнительные возможности обработки перехваченных данных

Предварительная обработка данных:

- Обнаружение доступа к данным по регулярным выражениям. Система позволяет создавать собственные регулярные выражения и автоматически проверять их корректность. В Системе доступны предустановленные регулярные выражения.
- Система позволяет маскировать критичные данные в перехватываемых обращениях к персональным данным. Маскирование может производиться по группам регулярных выражений и по количеству символов с конца. Данный параметр настраивается через интерфейс Системы.
- Выделение данных из ответов на http-запросы в заполненных веб-формах. Существует возможность выделения из заголовка HTTP реального IP-адреса web клиента и поле IP Web Клиента.

Обработка данных:

- Идентификация пользователей при трехзвенной архитектуре подключения к БД.

### 3.3. Идентификация пользователей (персонификация)

Если необходима персонификация сетевого трафика (сопоставление IP-адресов с регистрационными именами сотрудников, осуществляющих действия в БД), следует выполнить необходимые настройки. В результате настройки персонификации трафика для каждого перехваченного SQL-объекта будет добавлено поле «Логин ОС», так как данная информация присутствует не во всех протоколах взаимодействия с СУБД.

Персонифицирование трафика осуществляется с помощью контроля протокола Kerberos. Для этого в точку съема необходимо подавать трафик со всех контроллеров домена.

В перехваченных запросах доступна информация об идентификаторах пользователя в зависимости от контролируемой БД:

| БД/тип приложения              | Информация  |
|--------------------------------|---|
| Oracle                         | <ul style="list-style-type: none"> <li>• Логин БД (в.т.ч. прокси-пользователь)</li> <li>• Логин ОС</li> <li>• Имя домена/компьютера,</li> <li>• IP клиента</li> <li>• Порт клиента</li> </ul> |
| MSSQL (Windows-аутентификация) | <ul style="list-style-type: none"> <li>• Логин БД,</li> <li>• Логин ОС,</li> <li>• Имя домена/компьютера,</li> <li>• IP клиента</li> <li>• Порт клиента</li> </ul>                            |
| MSSQL (SQL-аутентификация)     | <ul style="list-style-type: none"> <li>• IP клиента</li> <li>• Порт клиента</li> </ul>  |

|  |   |
|--|---|
| PostgreSQL,<br>MySQL,<br>Sybase,<br>Netezza,<br>DB2,<br>Firebird,<br>Interbase,<br>Apache Hive<br>Informix | <ul style="list-style-type: none"> <li>• Логин БД,</li> <li>• IP клиента</li> <li>• Порт клиента</li> </ul>                 |
| Teradata   | <ul style="list-style-type: none"> <li>• IP клиента</li> <li>• Порт клиента</li> </ul>                                      |
| Веб-приложения   | <ul style="list-style-type: none"> <li>• учетная запись приложения</li> <li>• IP клиента</li> <li>• Порт клиента</li> </ul> |

**Примечание:** Для всех протоколов доступа к БД идентификационная информация может быть дополнена Логинем ОС в случае подачи Kerberos-трафика.

### 3.4. 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 неявные обращения к объектам БД, даже если в политиках безопасности 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.

### 3.5. Приложение 1. Поддерживаемые БД

| Семейство СУБД       | Версии СУБД   |
|----------------------|---|
| Oracle Database      | 10g 11g 12c 18c 19c   |
| Microsoft SQL Server | 2008 2008 R2<br>2012 2014                                   |
| PostgreSQL           | 7.4.5 7.4.6<br>8.4.13 8.4.3<br>9.2.7 9.2.24 9.4.5           |
| Vertica              | 10.0.0  |
| Greenplum            | 6.11.1  |
| MariaDB              | 5.5.60  |
| Teradata             | 14.10.03.02<br>15.10.06.02 15.10.06.05<br>16.00.00.04 16.10 |
| MySQL                | 5.1.39 5.1.63 5.1.73 5.6.21 5.6.19 5.6.27<br>7.11           |
| Apache Hive          | 1.2.1000.2.6.3.0-235  |
| SAP Sybase           | ASE 16.0.0  |
| IBM Netezza          | 7.1.0.0   |
| IBM DB2              | 11.1.0.1527   |
| Firebird             | 2.5.8.27089<br>3.0.2.32703                                  |
| Interbase            | 2017 13.0.0.129   |
| Ред База Данных      | 3.0.3.107   |
| HBase                | 2   |
| Apache Kafka         | 0.11.4<br>1.0.0 1.1.0                                       |
| Cassandra            | 4.0.0.604   |

## Приложение 1. Поддерживаемые БД

---

|                |                            |
|----------------|----------------------------|
| ScyllaDB       | 4.5.3-0.20211223.c8f14886d |
| SAP Hana       | 2.00.033.00.1535711040     |
| Tarantool      | 1.10.3<br>2.1.1 2.2.0      |
| MongoDB        | 3.6.12                     |
| 1С Предприятие | 8.3.15.1830                |
| Spark          | 2.4<br>3.0                 |
| Informix       | 14.10.FC5DE                |