Оглавление

[1. Аннотация 1](#_Toc4079042)

[2. Назначение ПО 1](#_Toc4079043)

[3. Программно-аппаратные среды функционирования ПО 1](#_Toc4079044)

[4. Общие принципы функционирования ПО 3](#_Toc4079045)

[5. Реализация ПО 4](#_Toc4079046)

[Интеграция с сетевым трафиком 5](#_Toc4079047)

[Интеграция с почтовой системой 5](#_Toc4079048)

[Типовые схемы подключения 6](#_Toc4079049)

[Режим анализа копии трафика и файлов из трафика 6](#_Toc4079050)

[Режим анализа копии трафика и файлов из трафика в GRE туннеле 7](#_Toc4079051)

[Режим анализа почты 8](#_Toc4079052)

[Получение писем по SMTP 8](#_Toc4079053)

[Получение писем с помощью механизма скрытой копии (BCC) 9](#_Toc4079054)

[Получение писем по SMTP с блокировкой (inline-режим) 10](#_Toc4079055)

# Аннотация

Настоящий документ содержит описание реализации программного обеспечения «TDS» версии 1.0 (далее – ПО).

# Назначение ПО

ПО - комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования внутри корпоративной инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение TDS существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

# Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

1. Аппаратные среды:
   1. Сервера со следующими техническими требованиями:

Таблица 1 Технические требования для TDS Сенсор

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TDS Сенсор (нагрузка Mbps)** | **250** | **1000** | **5000** | **20000** |
| **CPU** | 3,9 GHz, 4 C, 8 MB | 3,9 GHz, 4 C, 8 MB | 2.4 GHz, 14 C, 35 MB | 2.4 GHz, 14 C, 35 MB |
| **RAM, GB** | 32 | 32 | 64 | 128 |
| **HDD, GB** | 2 х 480 | 2 х 1200 | 2 х 1200 | 2 х 1200 |
| **Network** |  | | | |
| **mgmt Ethernet** | 1 | 1 | 1 | 1 |
| **Span** | до 4 Ethernet | до 4 Ethernet or SFP | до 4 SFP/SFP+ | до 4 SFP+ |

Таблица 2 Технические требования для TDS HuntBox

|  |  |  |  |
| --- | --- | --- | --- |
| **TDS HuntBox** | **Enterprise** | **Performance** | **Storage** |
| **CPU** | 2.4 GHz, 14 C, 35 MB | 2.4 GHz, 28 C, 35 MB | 2.4 GHz, 14 C, 35 MB |
| **RAM, GB** | 96 | 128 | 64 |
| **HDD, GB** | 4 х 1200 | 4 х 1200 | 2 x 1200 HDD + 2 x 960 SSD |
| **Network** |  |
| **mgmt Ethernet** | 1 или более | 1 или более | 1 или более |

Таблица 3 Технические требования для TDS Endpoint

|  |  |  |  |
| --- | --- | --- | --- |
| **Операционная система** | **Windows 7** | **Windows 8/8.1** | **Windows 10** |
| **CPU** | Не ниже Inter core i3 второго поколения | Не ниже Intel core i3 второго поколения | Не ниже Intel core i3 второго поколения |
| **RAM, GB** | 4 | 4 | 4 |
| **HDD, MB** | 100 | 100 | 100 |
| **Network** |  |
|  | Связь с TDS HuntBox | Связь с TDS HuntBox | Связь с TDS HuntBox |

1. Виртуальные среды:
   1. Hyper-V
   2. Vmware Esxi
   3. Qemu
   4. Xen-server
2. Использование браузеров для доступа к системе:
   1. Windows Internet Explorer версии 8.0 и выше
   2. Google Chrome версии 4.0 и выше
   3. Mozilla Firefox версии 3.5 и выше
   4. Apple Safari версии 4.0 и выше
   5. Opera версии 10.5 и выше
   6. iOS Safari версии 3.2 и выше
   7. Opera Mobile версии 11.0 и выше
   8. Google Chrome for Android версии 11.0 и выше
   9. Mozilla Firefox for Android версии 26.0 и выше
   10. Windows Internet Explorer Mobile версии 10.0 и выше

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

# Общие принципы функционирования ПО

На рисунке 1 изображены общие принципы функционирования ПО.

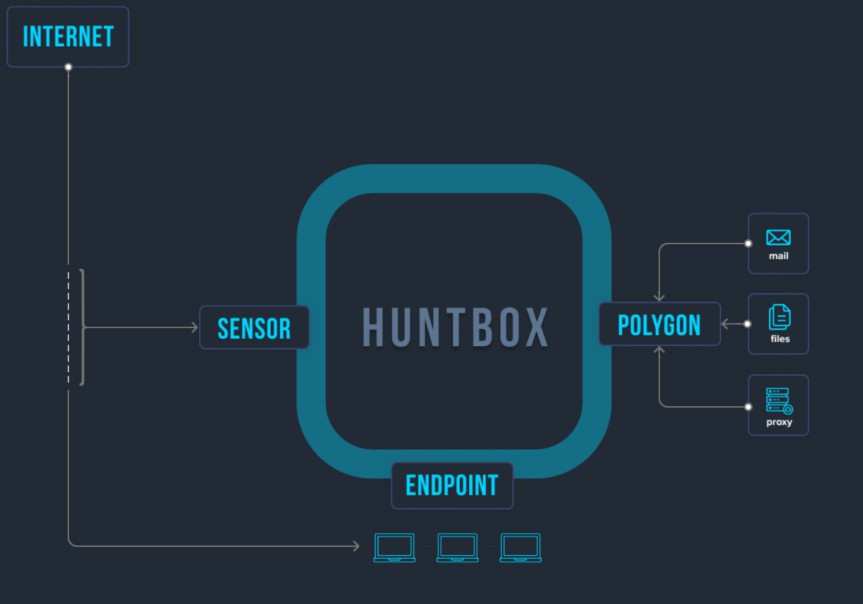


Рисунок 1. Общие принципы функционирования ПО.

TDS HuntBox - система анализа, корреляции, принятия решений и управления всеми компонентами комплекса.

TDS Sensor (Cенсор) - сенсор анализа данных, подключаемый к копии сетевого трафика защищаемой организации. Является так же модулем почтовой интеграции для проведения анализа почтовых сообщений совместно с TDS Polygon

TDS Polygong (песочница) - модуль поведенческого анализа файлов, получаемых из почты, целевых хостов (с помощью TDS Endpoint), файловых хранилищ, ICAP клиентов. Позволяет детектировать неизвестные ранее угрозы и продвинутые целевые атаки.

TDS Endpoint – программное обеспечение для сбора данных о поведении пользователя и программ, обеспечивающее фиксацию полной хронологии событий на системе, блокировку аномального поведения, изоляцию хоста, отправку данных в удаленное хранилище для последующего анализа.

ПО - это комплексное решение, направленное на повышение качества обнаружения новых и неизвестных угроз, атак без использования вредоносных программ, обеспечение процесса threat hunting, оптимизацию процессов реагирования на инциденты и их последующего расследования именно внутри корпоративной инфраструктуры.

# Реализация ПО

**Архитектурно решение состоит из следующих модулей:**

1. **TDS Sensor**

Сенсор предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы сенсор использует собственные сигнатуры и поведенческие правила.

**Особенности системы:**

* Постоянно обновляемые базы – информация из киберразведки и системы криминалистики
* Единый интерфейс с тикет-системой
* Интеграция с почтой/icap
* Анализ трафика до 20 Gb/s
* Возможность виртуальной установки/HW Appliance
* Интеграция с SIEM и другими системами

1. **TDS Polygon**

Данная система предназначена для поведенческого анализа подозрительных объектов в безопасной среде. Полученные по электронной почте или скачанные из интернета файлы проверяются до попадания на компьютеры пользователей. Применение технологий машинного обучения позволяет выявить ранее неизвестные вредоносные программы без использования сигнатур, а также блокировать их доставку пользователям.

**Особенности системы:**

* Запатентованная технология обнаружения обхода песочницы
* Эмуляция действий пользователей
* Специально подготовленные образы для обнаружения 0-Day уязвимостей и различного вида ВПО (вредоносного программного обеспечения).
* Анализ файлов с измененными расширениями
* Запатентованный низкоуровневый монитор, выявляющий все возможные действия в том числе и выполнение кода на уровне CPU.
* Дешифровка запароленных архивов с паролем в теле письма/вложенном файле/по словарю.
* Ретроспективный анализ

1. **Центр управления, мониторинга, хранения событий и обновления**

Специалисты Центра управления мониторинга Group-IB (TDS-SOC) отслеживают и анализируют события, выявленные TDS Sensor и TDS Polygon. Эксперты TDS-SOC немедленно уведомляют специалистов организации о критичных угрозах по электронной почте и телефону, а также дают рекомендации по их устранению. Поддержка работает круглосуточно, 365 дней в году. По умолчанию используется TDS-SOC Group-IB. Центр Управления также может быть развернут внутри сети заказчика в виде TDS HuntBox.

* **TDS HuntBox**

Центр управления, мониторинга, хранения событий и обновлений, устанавливаемый внутри инфраструктуры заказчика. Huntbox интегрируется с другими компонентами комплекса TDS (Sensor, Polygon, Endpoint ) и значительно расширяет функционал решения за счет новых возможностей:

**Особенности системы**

* Оркестрация всех компонентов TDS и управлением ими из единого интерфейса
* Анализ больших данных, выявление новых инструментов и инфраструктуры атакующих
* Хранение логов и аналитической информации по инцидентам
* Визуализация инцидента на ранней стадии атаки
* Удаленное реагирование на конечных станциях
* Внутренний Threat Hunting по логам
* Сбор криминалистических данных для расследования инцидентов
* **Гибкая схема установки**
  + On-Premise / Cloud / Hybrid
  + Различные способы взаимодействия с инфраструктурой Group-IB (см. руководство администратора «Обновления и потоки данных»)

## Интеграция с сетевым трафиком

Система обеспечивает анализ трафика, подаваемого на оборудование TDS Sensor из разных источников:

* SPAN/RSPAN трафик
* SPAN/RSPAN траффик в GRE-туннеле
* ICAP (файлы из трафика)

При интеграции по ICAP возможно настроить режим блокировки - вредоносные вложения не будут доступны для загрузки пользователям.

## Интеграция с почтовой системой

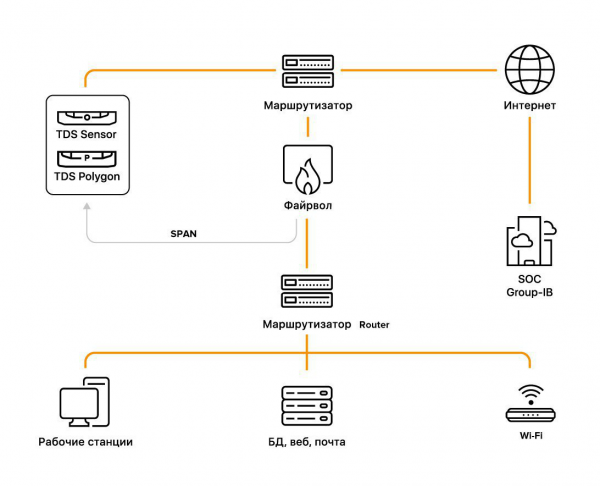
Поддерживаются несколько различных способов получения писем для поведенческого анализа:

* Получение писем по SMTP
* Получение писем с помощью механизма скрытой копии (BCC) через POP3/IMAP

Поддерживается возможность блокировки вредоносных писем посредством интеграции TDS Sensor в режиме MTA (Mail Transfer Agent). Внутренний MTA режим обеспечивает возможность настройки почтовой инфраструктуры любой сложности - с любым количеством почтовых серверов и настройкой различных правил пересылки. При этом обеспечивается отказоустойчивость и балансировка нагрузки.

## Типовые схемы подключения

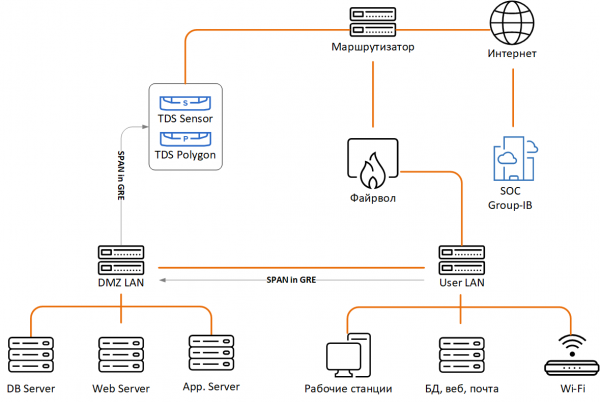
### Режим анализа копии трафика и файлов из трафика

[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Span.png)

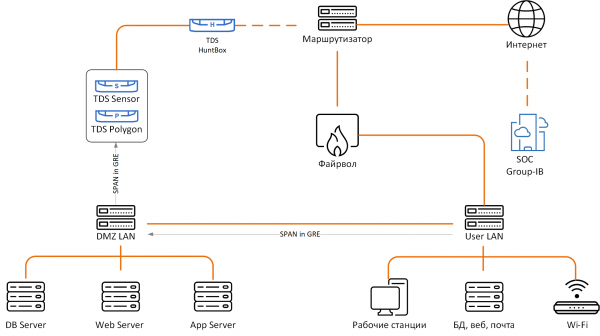
Анализ копии трафика. Работа через TDS SOC

В этом режиме TDS Polygon осуществляет пассивный мониторинг файлов из трафика. Объекты анализа поступают от TDS Sensor и отправляются в облако TDS Polygon Cloud.

### Режим анализа копии трафика и файлов из трафика в GRE туннеле

[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:SPANinGRE.png)

Анализ копии трафика в GRE. Работа через TDS SOC

[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:ERSPAN_with_HuntBox.png)

Анализ копии трафика в GRE. Работа через TDS HuntBox

TDS Sensor поддерживает возможность организовывать GRE-туннели. Когда нет возможности напрямую подать SPAN/RSPAN, поскольку между сенсором и зеркалирующим оборудованием находится L3 оборудование, либо необходимо получить трафик с фермы виртуальных машин, можно использовать GRE-инкапсуляцию, для передачи SPAN трафика в TDS.

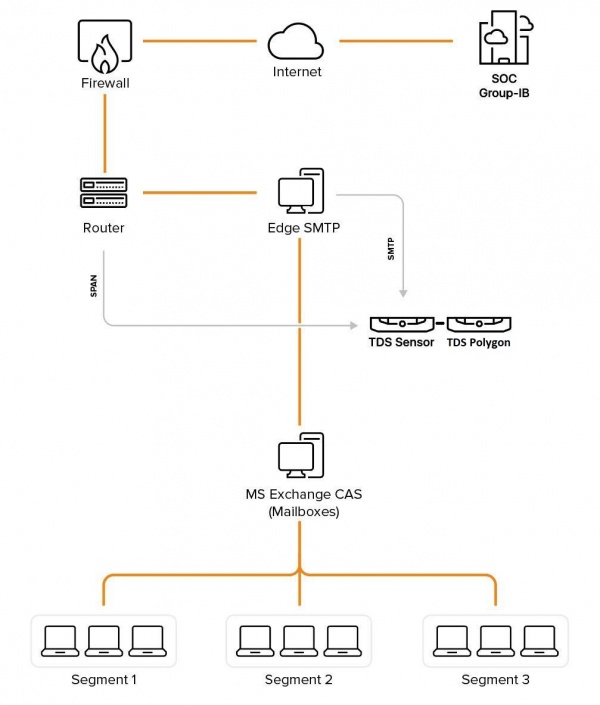
## Режим анализа почты

Поддерживаются несколько различных способов получения писем для поведенческого анализа:

* Получение писем по SMTP.
* Получение писем с помощью механизма скрытой копии (BCC)

### Получение писем по SMTP

При данной интеграции TDS Sensor выступает как MTA (или SMTP Relay), получаю копию всей входящей почты через SMTP. Единственное отличие этого режима, от режима с блокировкой, что письма тут не пересылаются дальше, а просто анализируются.

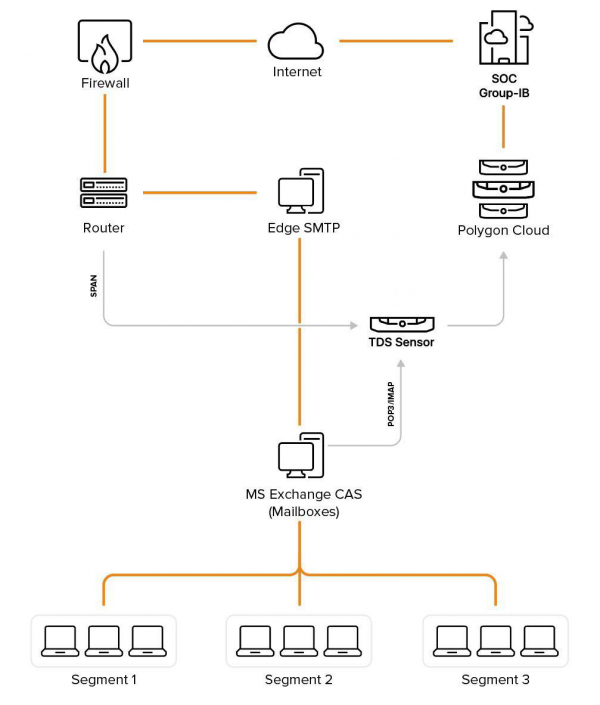
[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:SMTP-copy.jpg)

анализ SMTP копии. Работа через TDS SOC

Схема 3: TDS Sensor + TDS Polygon — анализ копии трафика, копии почты и файлов из канала связи.

### Получение писем с помощью механизма скрытой копии (BCC)

При данной интеграции создаётся дополнительный почтовый ящик, куда осуществляется копирование всей входящей почты. TDS Sensor подключается к подготовленному ящику и забирает письма для анализа.

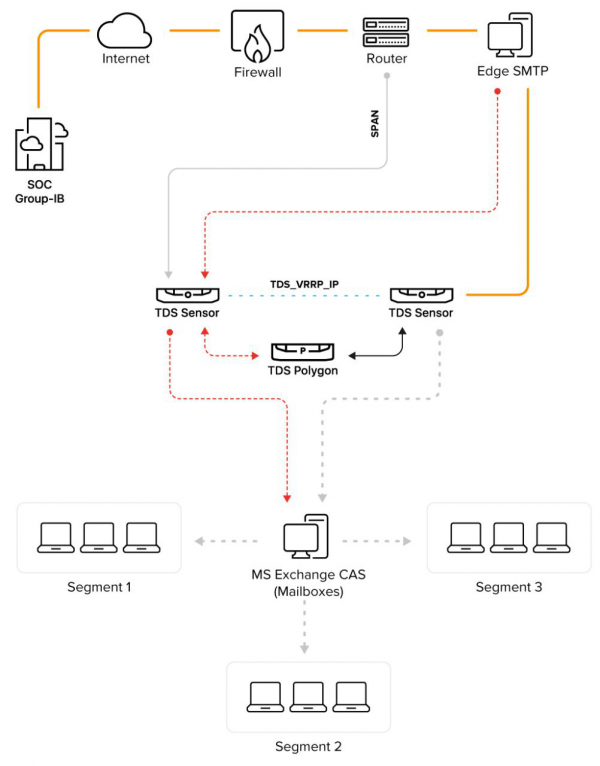
[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Photo_2018-03-21_13-25-07.png)

Анализ BCC. Работа через TDS SOC

Схема 2: TDS Sensor + TDS Polygon — анализ копии трафика, копии почты и файлов из канала связи.

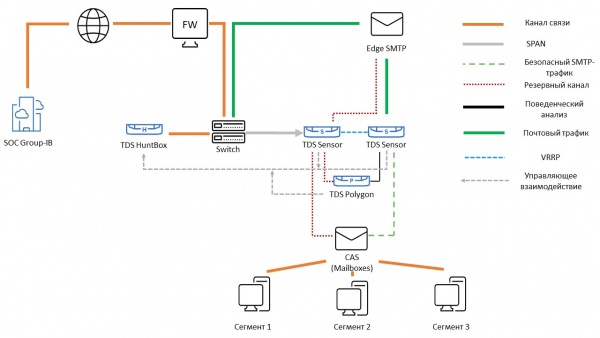
### Получение писем по SMTP с блокировкой (inline-режим)

Основной режим интеграции с почтой, когда почта проходит через TDS Sensor как через SMTP Relay, и доставляется дальше после анализа. Соответственно вредоносные письма блокируются. Отказоустойчивость обеспечивается либо на уровне DNS, либо на уровне SMTP-сервера, где настраивается несколько релеев, либо на уровне VRRP, когда несколько устройств делят виртуальный IP адрес.

[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:Inline.png)

Работа в MTA режиме через TDS SOC

Схема 4: TDS Sensor + TDS Polygon — анализ почты с блокировкой вредоносных объектов.

[](https://tdswiki.group-ib.ru/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB:%D0%A1%D0%BB%D0%B0%D0%B9%D0%B4.JPG)

Анализ почты с блокировкой объектов и работой через TDS HuntBox

Все схемы выше могут реализованы, как с применением TDS HuntBox, так и без него работая напрямую через SOC Group-IB.