**ПРОГРАММНО АППАРАТНОЕ ОБЕСПЕЧЕНИЕ «TDS»**

**Версия 1.0**

**РУКОВОДСТВО АДМИНИСТРАТОРА**

**СОДЕРЖАНИЕ**

[Аннотация 5](#_Toc4073568)

[1. Назначение ПО 5](#_Toc4073569)

[2. Программно-аппаратные среды функционирования ПО 5](#_Toc4073570)

[3. Общие принципы функционирования ПО 8](#_Toc4073571)

[4. Обязанности и функции администратора заказчика 9](#_Toc4073572)

[5. Порядок встраивания 9](#_Toc4073573)

[5.1. Выбор схемы встраивания в инфраструктуру 9](#_Toc4073574)

[5.1.1. Почтовая интеграция 10](#_Toc4073575)

[5.1.2. Сетевая интеграция 13](#_Toc4073576)

[5.1.3. Файловая интеграция 13](#_Toc4073577)

[5.2. Выбор типа взаимодействия ПО c АС ООО «Группа АйБи» (далее Group-IB); 14](#_Toc4073578)

[5.3. Определение точек съёма трафика в инфраструктуре заказчика для сигнатурного анализа 15](#_Toc4073579)

[5.4. Определение способа интеграции с почтовыми серверами заказчика 15](#_Toc4073580)

[5.5. Определение необходимости подключения ПО к файловым хранилищам заказчика для поведенческого анализа файлов 16](#_Toc4073581)

[5.6. Встраивание TDS HuntBox с выбранным режимом работы в инфраструктуру заказчика 16](#_Toc4073582)

[5.6.1. HuntBox активация 16](#_Toc4073583)

[5.6.2. Подключение к консоли HuntBox 20](#_Toc4073584)

[5.6.3. Главное меню TDS HuntBox 21](#_Toc4073585)

[5.7. Встраивание TDS Sensor с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки TDS HuntBox 23](#_Toc4073586)

[5.7.1. Подключение к сети и захват трафика 23](#_Toc4073587)

[5.7.2. Активация сенсора и синхронизация с HuntBox 25](#_Toc4073588)

[5.7.3. Подключение к консоли TDS-Sensor 30](#_Toc4073589)

[5.7.4. Меню CLI TDS Sensor 31](#_Toc4073590)

[5.7.5. Настройка сети TDS Sensor 32](#_Toc4073591)

[5.8. Установка TDS Endpoint на защищаемых хостах заказчика 36](#_Toc4073592)

[5.9. Встраивание TDS Polygon с учётом установки TDS Sensor, TDS Endpoint, TDS HuntBox 37](#_Toc4073593)

[5.10. Обеспечение связности всех модулей с TDS HuntBox; 38](#_Toc4073594)

[5.11. Определение перечня IP-подсетей заказчика, которые будут определены как защищаемые и ввод этих данных в ПО 38](#_Toc4073595)

[5.12. Интеграция почтовой системы 39](#_Toc4073596)

[6. Интерфейс администратора 39](#_Toc4073597)

[6.1. Dashboard 40](#_Toc4073598)

[6.1.1. Состояние устройства 40](#_Toc4073599)

[6.1.2. Последние алерты 41](#_Toc4073600)

[6.1.3. Статистика алертов по классификатору и критичности 42](#_Toc4073601)

[6.1.4. Статистика событий по классификатору 44](#_Toc4073602)

[6.1.5. График событий по классификатору 45](#_Toc4073603)

[6.1.6. График SPAN интеграции 46](#_Toc4073604)

[6.1.7. Статистика SPAN интеграции 48](#_Toc4073605)

[6.1.8. График электронной почты 49](#_Toc4073606)

[6.1.9. Статистика почтовой интеграции 51](#_Toc4073607)

[6.1.10. График числа online-хостов с TDS Endpoint 52](#_Toc4073608)

[6.1.11. График числа системных событий TDS Endpoint 52](#_Toc4073609)

[6.2. Алерты 53](#_Toc4073610)

[6.2.1.Алерт 53](#_Toc4073611)

[6.2.2. Информация об алерте 55](#_Toc4073612)

[6.2.3. Фильтры 65](#_Toc4073613)

[6.3. Расследование 67](#_Toc4073614)

[6.3.1. Письма 68](#_Toc4073615)

[6.3.2. Файлы 72](#_Toc4073616)

[6.3.3. Компьютеры 74](#_Toc4073617)

[6.4. Настройки 79](#_Toc4073618)

[6.4.1. Устройства 79](#_Toc4073619)

[6.4.1.1 Общие данные по устройствам 79](#_Toc4073620)

[6.4.1.2. Фильтр 80](#_Toc4073621)

[6.4.1.3. Добавить устройства 81](#_Toc4073622)

[6.4.2. Редактирование настроек TDS HuntBox 83](#_Toc4073623)

[6.4.2.1. Обновления и потоки данных 84](#_Toc4073624)

[6.4.2.2. Прокси-сервер 85](#_Toc4073625)

[6.4.2.3. Сервер времени 85](#_Toc4073626)

[6.4.2.4. Сертификат web-сервера 86](#_Toc4073627)

[6.4.2.5. Настройки почтового сервера 86](#_Toc4073628)

[6.4.2.6. Сервер событий TDS Endpoint 87](#_Toc4073629)

[6.4.3. Редактирование настроек TDS Sensor 87](#_Toc4073630)

[6.4.3.1. Интеграция с Polygon 88](#_Toc4073631)

[6.4.3.2. Почтовый сервер 89](#_Toc4073632)

[6.4.3.3. Почтовый клиент 92](#_Toc4073633)

[6.4.3.4. Стратегия работы со ссылками 93](#_Toc4073634)

[6.4.3.5. ICAP сервер 94](#_Toc4073635)

[6.4.3.6. Анализ файлов из трафика 95](#_Toc4073636)

[6.4.3.7. Анализ сетевого трафика 95](#_Toc4073637)

[6.4.3.8. Экспорт данных 96](#_Toc4073638)

[6.4.3.9. Сервер времени TDS Sensor 96](#_Toc4073639)

[6.4.3.10. Белый список 97](#_Toc4073640)

[6.4.3.11. Настройки разрешения имён 99](#_Toc4073641)

[6.4.4. PKI 100](#_Toc4073642)

[6.4.4.1. Данные по сертификатам 101](#_Toc4073643)

[6.4.4.2. Изменение сертификатов 102](#_Toc4073644)

[6.4.4.3. Фильтры 102](#_Toc4073645)

[6.4.5. Пользователи 103](#_Toc4073646)

[6.4.5.1. Полная информация по пользователю 103](#_Toc4073647)

[6.4.5.2. Добавить пользователя 105](#_Toc4073648)

[6.4.5.3. Удаление пользователя 105](#_Toc4073649)

[6.4.5.4. Фильтры 106](#_Toc4073650)

[6.4.6. Компании 107](#_Toc4073651)

[6.4.6.1. Общий список компаний 107](#_Toc4073652)

[6.4.6.2. Информация о компании 107](#_Toc4073653)

[6.4.6.3. Добавление новой компании 109](#_Toc4073654)

[6.4.6.4. Архивирование компании 109](#_Toc4073655)

[6.4.6.5. Фильтры 109](#_Toc4073656)

# Аннотация

Настоящий документ содержит руководство администратора по встраиванию программного комплекса «TDS» версии 1.0 (далее – ПО) в защищаемую инфраструктуру.

# 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.

Описание реализации ПАК представлено в документе «Описание реализации».

# 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.

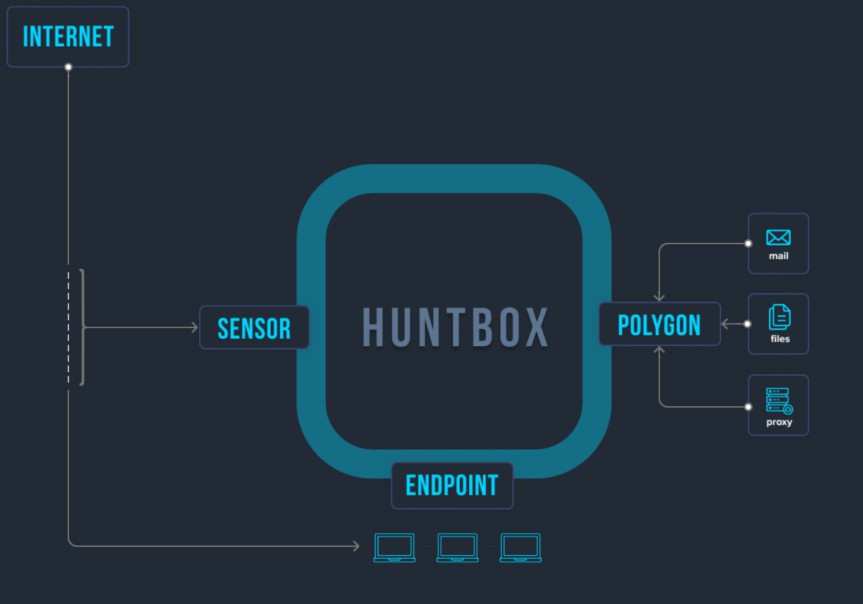


Рисунок 1. Общие принципы функционирования ПО.

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.

Детальная информация о реализации ПО представлена в руководстве «Описание реализации».

# Обязанности и функции администратора заказчика

В обязанности администратора входит следующее:

* Произвести встраивание ПО в защищаемую инфраструктуру
* Поддерживать функционирование ПО

# Порядок встраивания

Для встраивания ПО в защищаемую инфраструктуру необходимо выполнить следующие шаги:

* Выбор схемы встраивания в инфраструктуру;
* Выбор типа взаимодействия ПО c АС ООО «Группа АйБи» (далее Group-IB);
* Определение точек съёма трафика в инфраструктуре заказчика для сигнатурного анализа;
* Определение способа интеграции с почтовыми серверами заказчика;
* Определение необходимости подключения ПО к файловым хранилищам заказчика для поведенческого анализа файлов
* Встраивание TDS HuntBox с выбранным режимом работы в инфраструктуру заказчика;
* Встраивание TDS Sensor с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки TDS HuntBox;
* Установка TDS Endpoint на защищаемых хостах заказчика;
* Встраивание TDS Polygon с учётом установки TDS Sensor, TDS Endpoint, TDS HuntBox;
* Обеспечение связности всех модулей с TDS HuntBox;
* Определить перечень IP-подсетей заказчика, которые будут определены как защищаемые и ввести эти данные в ПО;
* Интеграция почтовой системы;
* Интеграция файлового хранилища;

## 5.1. Выбор схемы встраивания в инфраструктуру

Существует следующие критерии встраивания в инфраструктуру:

1. Почтовая интеграция:
   1. BCC
   2. Inline
2. Сетевая интеграция:
   1. SPAN
   2. RSPAN
   3. SPAN over GRE
3. Файловая интеграция:
   1. ICAP
   2. Файловые хранилища
   3. Анализ файлов из трафика

### 5.1.1. Почтовая интеграция

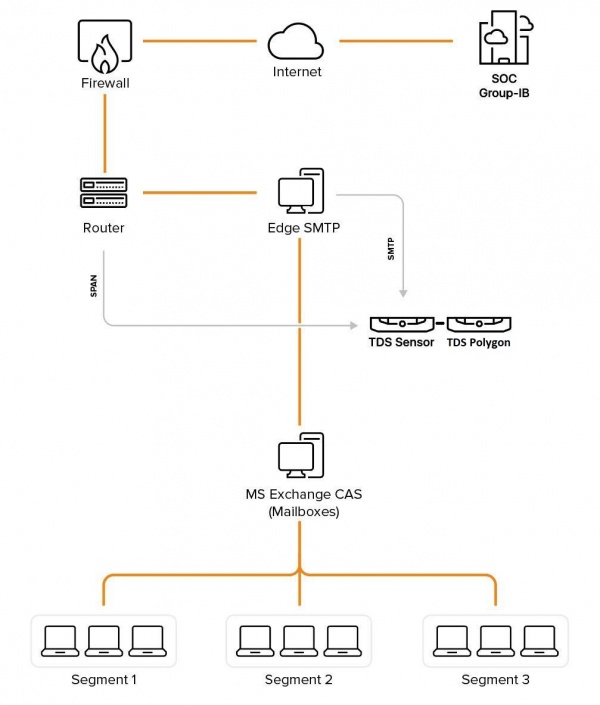
Поддерживаются несколько различных способов получения писем для поведенческого анализа:

1. BCC – анализ копии писем
   1. Получение писем по SMTP.
   2. Получение писем с помощью механизма скрытой копии (BCC)
2. Inline – анализ оригинальных писем. Получение писем по SMTP с блокировкой.

**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.

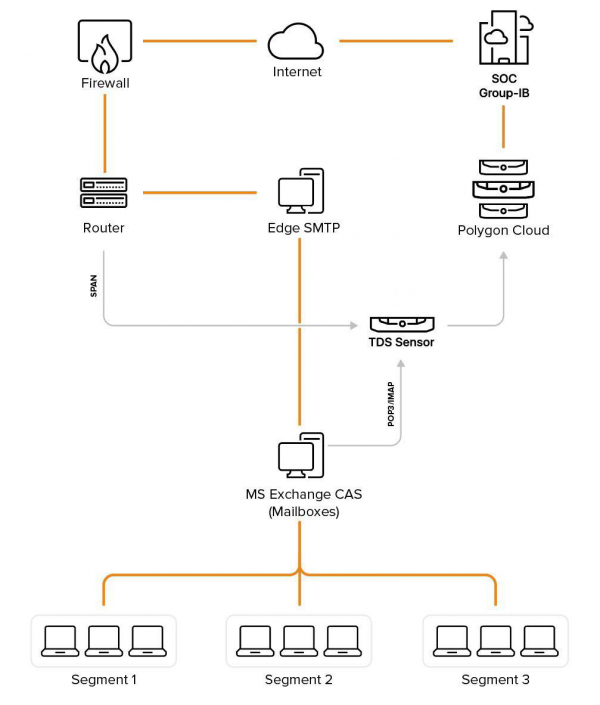
Получение писем по SMTP



**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.

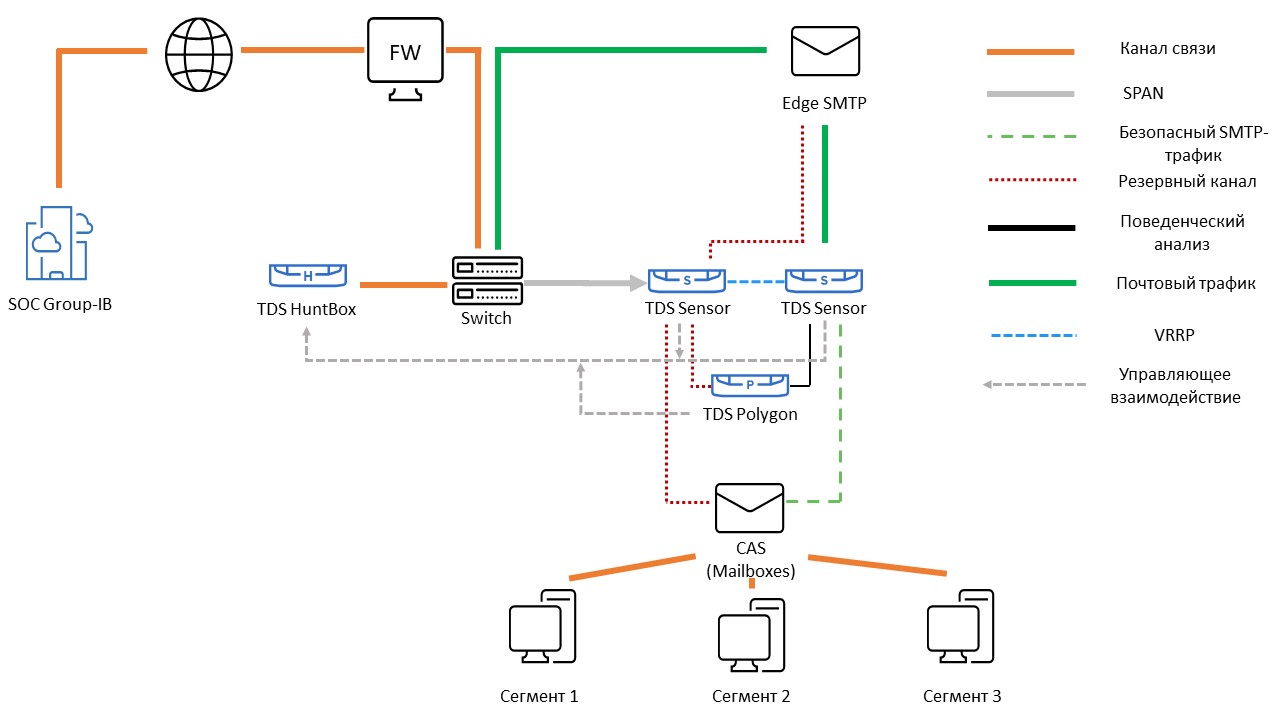
Получение писем с помощью механизма скрытой копии (BCC)



**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.

Получение писем по SMTP с блокировкой (inline-режим)



### 5.1.2. Сетевая интеграция

Съём трафика осуществляется с коммутаторов заказчика либо с маршрутизаторов с наличием SPAN функций. Система обеспечивает анализ трафика, подаваемого на оборудование TDS Sensor из разных источников:

* SPAN
* RSPAN трафик
* SPAN/RSPAN траффик в GRE-туннеле

SPAN и RSPAN определяют копирование трафика на уровне L2 модели OSI.

SPAN/RSPAN over GRE определяют копирование трафика на уровне L3 модели OSI.

### 5.1.3. Файловая интеграция

По мимо получения файлов для поведенческого анализа из почтового трафика, имеется следующие возможности:

1. ICAP
2. Файловые хранилища
3. Анализ файлов из трафика

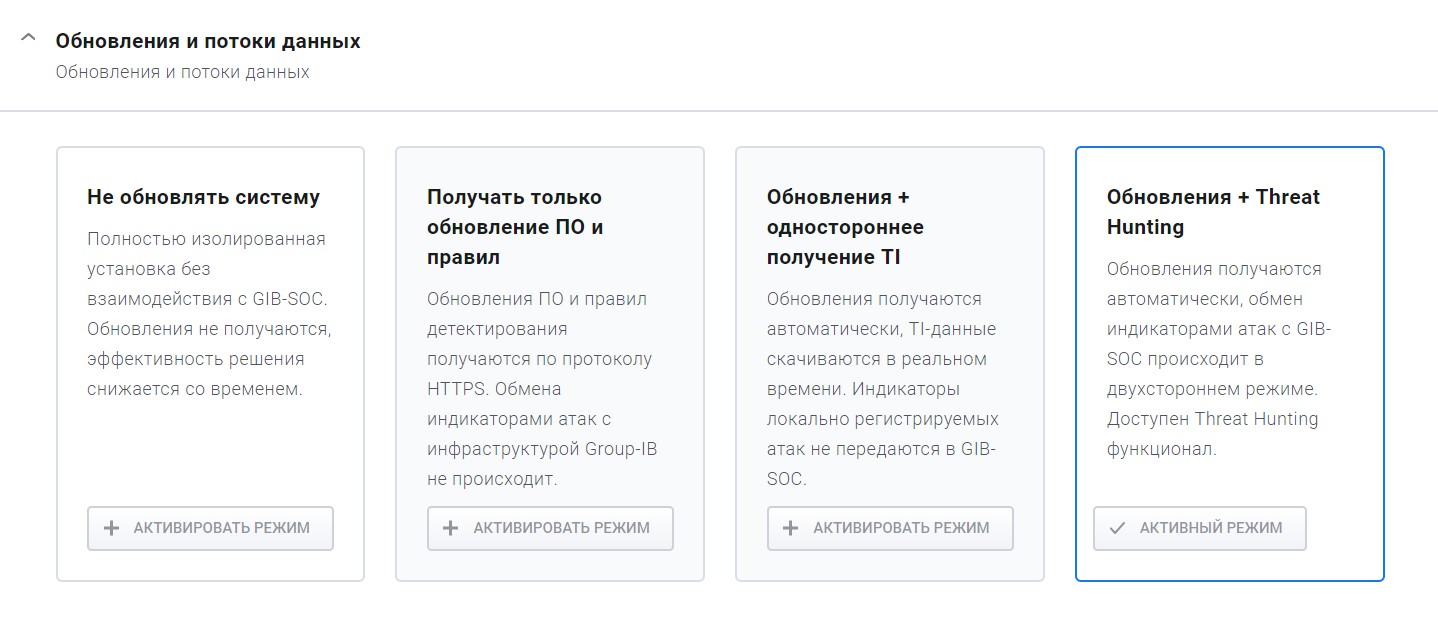
ICAP обеспечивает интеграцию с проксирующими решениями для получения скачиваемых файлов и их последующего анализа в модуле TDS Polygon

Интеграция с файловыми хранилищами обеспечивает поведенческий анализ файлов и автоматическое удаление найденного вредоносного программного обеспечения (ВПО).

Анализ файлов из трафика позволяет собирать из анализируемого SPAN трафика файлы для поведенческого анализа, в случае если трафик нешифрованный.

## 5.2. Выбор типа взаимодействия ПО c АС ООО «Группа АйБи» (далее Group-IB);

Тип взаимодействия ПО с АС ООО «Группа АйБи» определяет список обмениваемых данных между заказчиком и производителем. Расположение настройки описано в одноимённом разделе в пунктах описывающих интерфейс ПО.



Описание режимов:

* **Не обновлять систему**

Данный режим подразумевает полностью закрытую инсталляцию. HuntBox никак не взаимодействует с серверами Group-IB.  
Обновление программного обеспечения, IOC и сетевых сигнатур не производится.

* **Получать только обновление ПО и правил**

Данный режим позволяет оборудованию получать обновления ПО для HuntBox и всех подключённых к нему устройств.  
Обновление индикаторов и сигнатур не производится.  
В данном режиме нет возможности загружать данные по инфраструктуре атакующих и отсутствует взаимодействие с SOC Group-IB для получения поддержки по инцидентам в режиме 24/7.  
Обновления доставляются с сервера Group-IB - 92.53.76.98:443/tcp

* **Обновления + одностороннее получение TI**

Данный режим дополняет предыдущий и позволяет получать обновление индикаторов атак и сигнатур для подключённых к Huntbox устройств.  
В данном режиме не возможно получать мониторинг и поддержку от CERT (SOC Group-IB).  
В данном режиме имеется возможность загружать данные по инфраструктуре атакующих вручную.  
Для получения данных по инфраструктуре атакующих HuntBox необходим доступ до сервера - tdsi.group-ib.com:443/tcp

* **Обновление + двухсторонний обмен индикаторами**

Данный режим дополняет предыдущий и позволяет выгружать данные об обнаруженных инцидентах в сервера Group-IB.  
Имеется возможность автоматически получать информацию по инфраструктуре атакующих.  
В данном режиме имеется имеется возможность мониторинга и поддержки от CERT Group-IB в режиме 24/7.  
Для получения данных по инфраструктуре преступников и связи с SOC Group-IB,а так же для получения обновлений - tdsi.group-ib.com:443/tcp

## 5.3. Определение точек съёма трафика в инфраструктуре заказчика для сигнатурного анализа

При организации зеркалирования следует учитывать, что трафик пользователей корпоративных прокси-серверов и сегментов сети, расположенных за NAT’ом, должен зеркалироваться до проксирования/натирования, как можно ближе к пользовательскому сегменту, до любого фильтрующего оборудования, чтобы в заголовках пакетов были видны оригинальные IP-адреса клиентов, а также для исключения фильтрации части трафика средствами межсетевых экранов. Это упростит реагирование на выявленные сетевые инциденты.

## 5.4. Определение способа интеграции с почтовыми серверами заказчика

Доступные способы интеграции:

* BCC via POP3/IMAP
* BCC via SMTP
* Inline режим via SMTP

Выбор почтовой интеграции определяется следующими критериями:

1. Особенности почтовой инфраструктуры клиента – общая рекомендация, использовать BCC via SMTP интеграцию – самую простую в реализации и наиболее эффективную при организации мониторинга атак через почтовую систему.
2. Необходимость автоматической блокировки опасных писем – использование inline режима.

## 5.5. Определение необходимости подключения ПО к файловым хранилищам заказчика для поведенческого анализа файлов

ПО имеет возможность проводить поведенческий анализировать файлов, хранящихся на файловых хранилищах заказчика в момент их изменения или запроса пользователями.   
Поддерживаемые протоколы подключения:

* SMB
* FTP
* WebDav

## 5.6. Встраивание TDS HuntBox с выбранным режимом работы в инфраструктуру заказчика

Для работы должен быть доступен для подключения сетевой адрес:

* Для получения обновлений используется адрес - 92.53.76.98:443/tcp
* Для получения данных по инфраструктуре преступников и использования преимуществ SOC Group-IB - tdsi.group-ib.com:443/tcp

При необходимости работа TDS HuntBox с Group-IB SOC может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT. Дополнительные сетевые настройки доступны в разделах Huntbox активация и Прокси-сервер

### 5.6.1. HuntBox активация

Перед настройкой решение необходимо активировать, то есть зарегистрировать лицензионный ключ, полученный при покупке или тестировании решения на серверах Group-IB.

Для первичной активации HuntBox должен иметь доступ до инфраструктуры Group-IB - https://soc.group-ib.com:40500

Сетевые настройки для присваивания IP адреса доступны в консоли HuntBox. Обратитесь в раздел Подключение к консоли HuntBox

Web-интерфейс доступен по адресу https://ip\_addr\_huntbox.

При открытии web-интерфейса вас будет приветствовать меню активации HuntBox (рис.1)

Шаг 1: Информация о компании

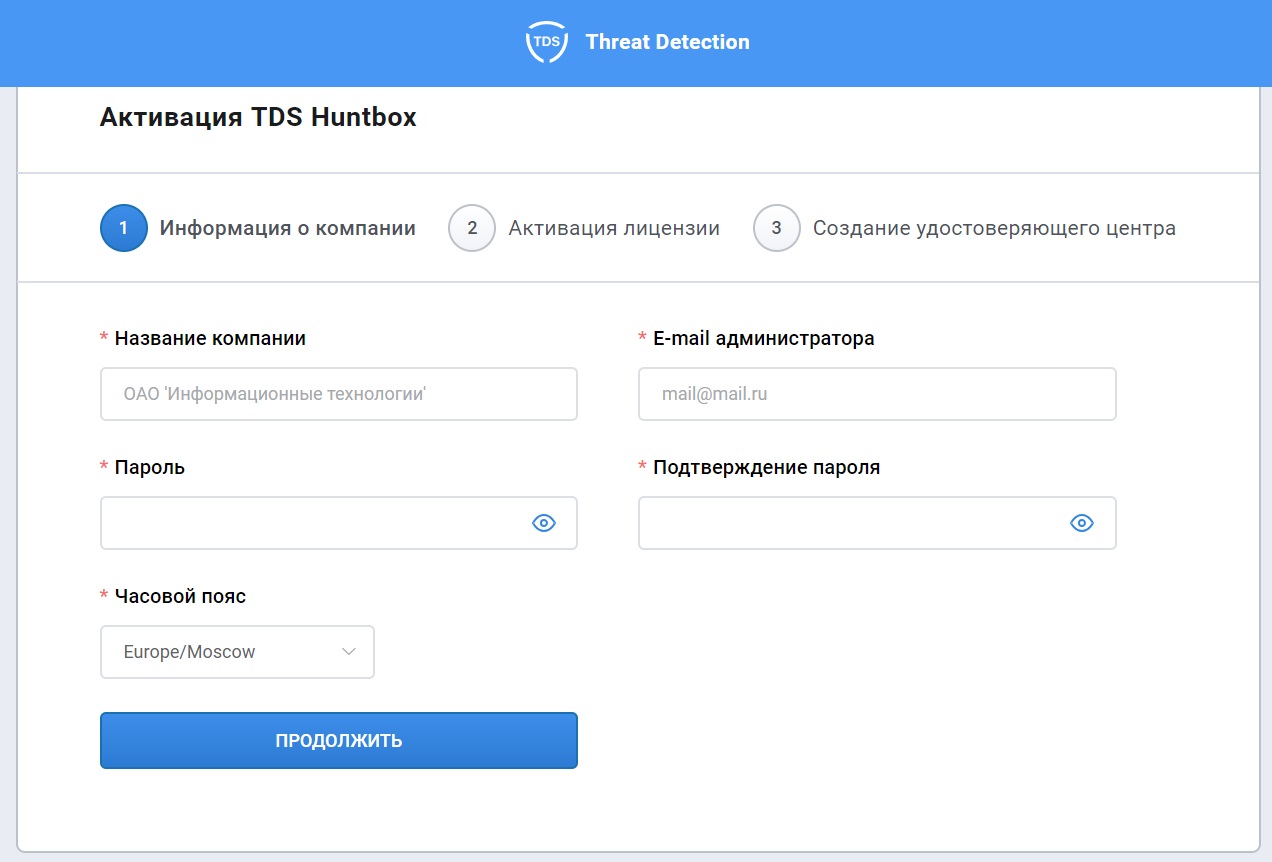


Рис. 1: Информация о компании

Данные занесённые в разделе Информация о компании(рис.1) будут использованы для активации лицензии и должны соответствовать реальным данным клиента.

* Название организации
* E-mail администратора - будет использоваться в качестве имени пользователя при аутентификации в системе
* Пароль / Подтверждение пароля - пароль администратора для входа в систему
* Часовой пояс

Шаг 2: Активация лицензии

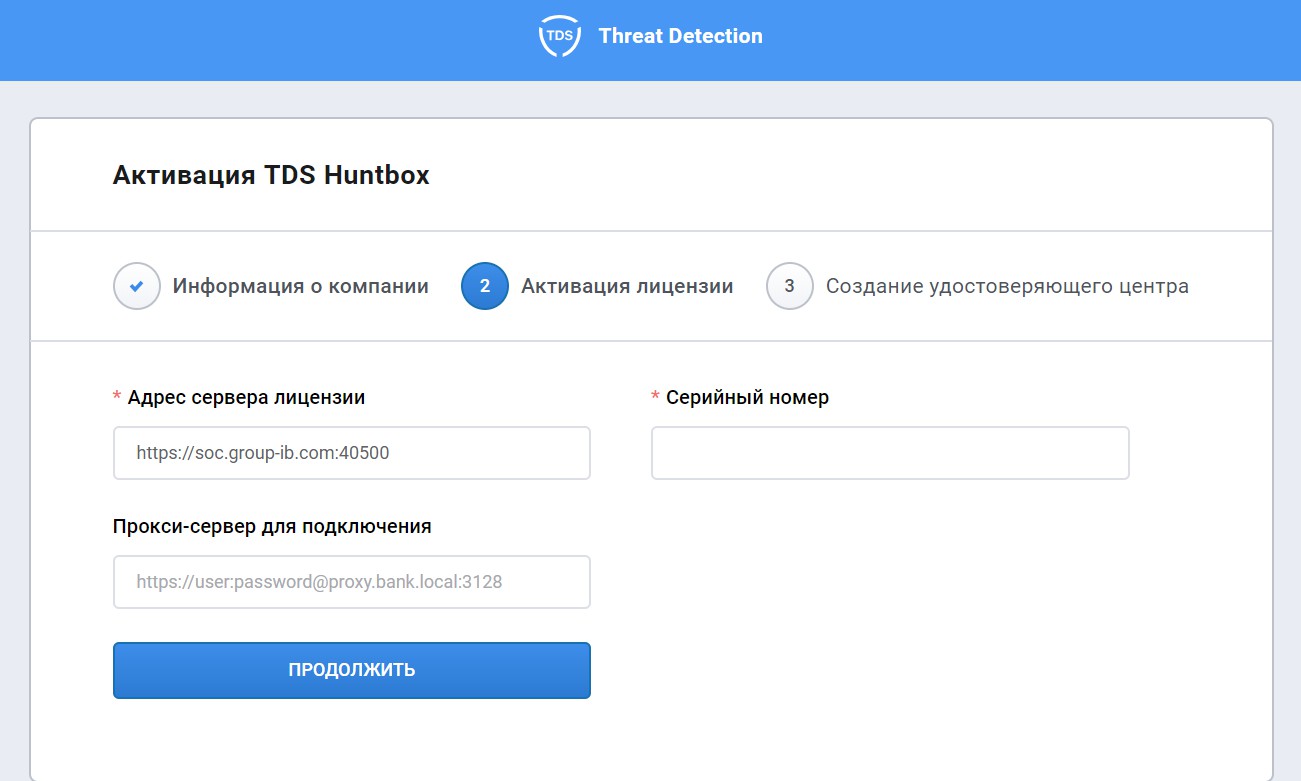


Рис. 2: Активация лицензии

* Адрес сервера лицензии - https://soc.group-ib.com:40500
* Серийный номер - номер выданный при покупке или тестировании HuntBox
* (Опционально) - прокси-сервер в формате http(s)://user:password@proxyFQDN:port

Шаг 3: Создание удостоверяющего центра

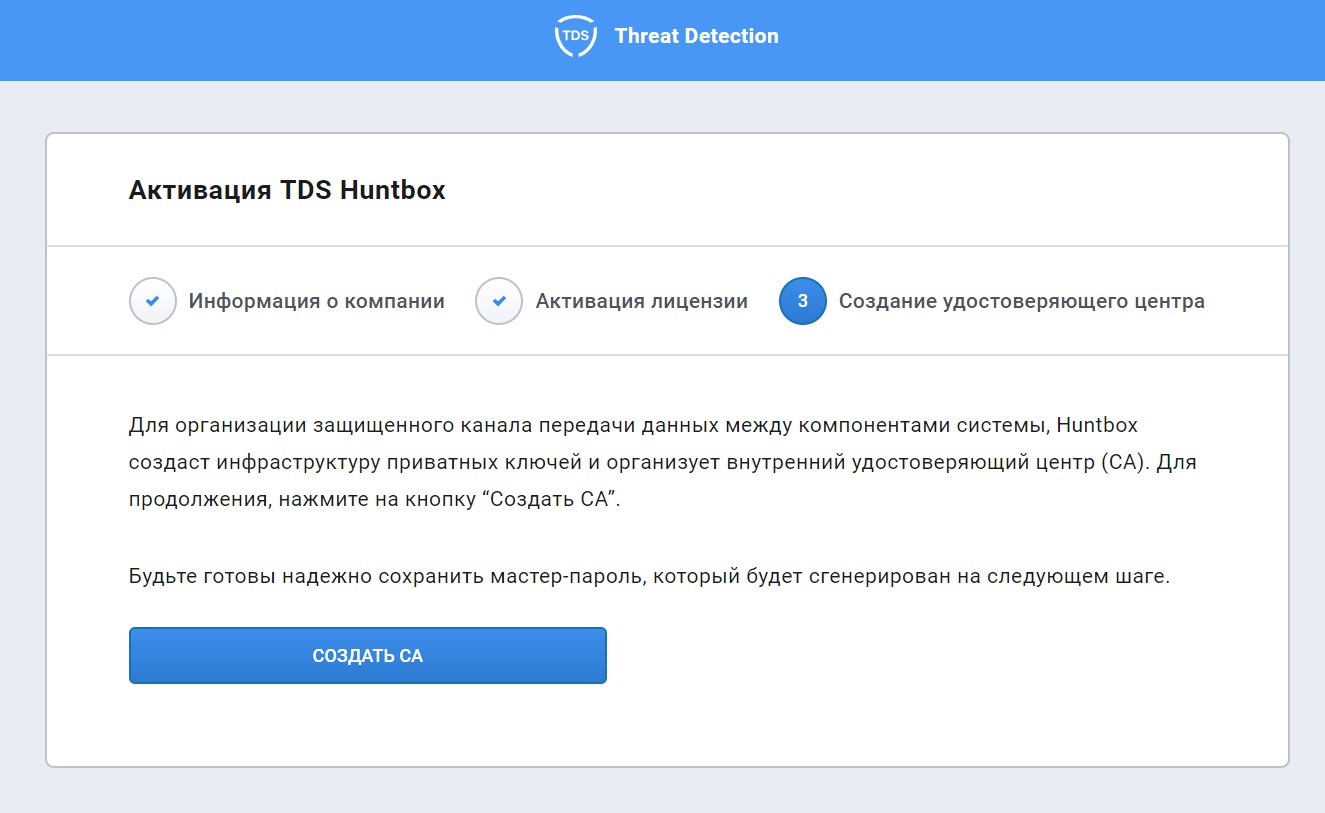


Рис. 3: Создание удостоверяющего центра

**Создать СА** - запускает процесс генерации мастер-пароля для дальнейшей настройки и добавления оборудования (сенсоров и Polygon) (рис.4)

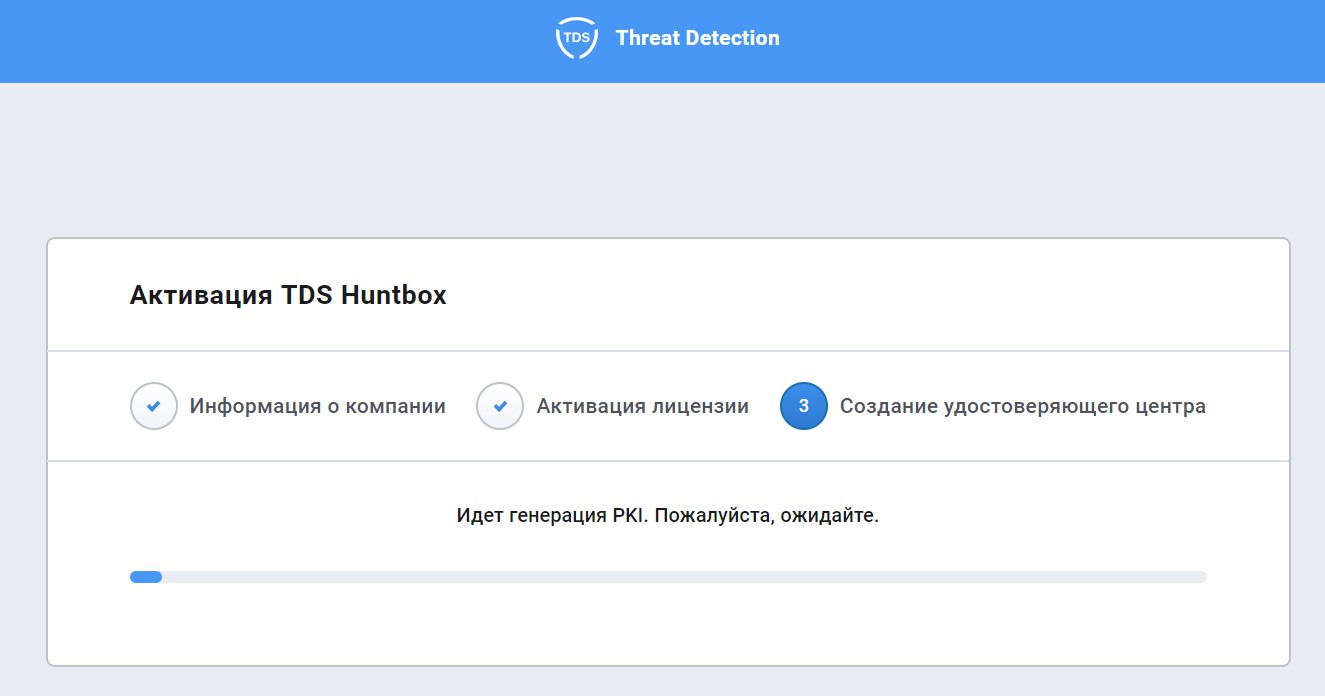


Рис. 4: Генерация ключей

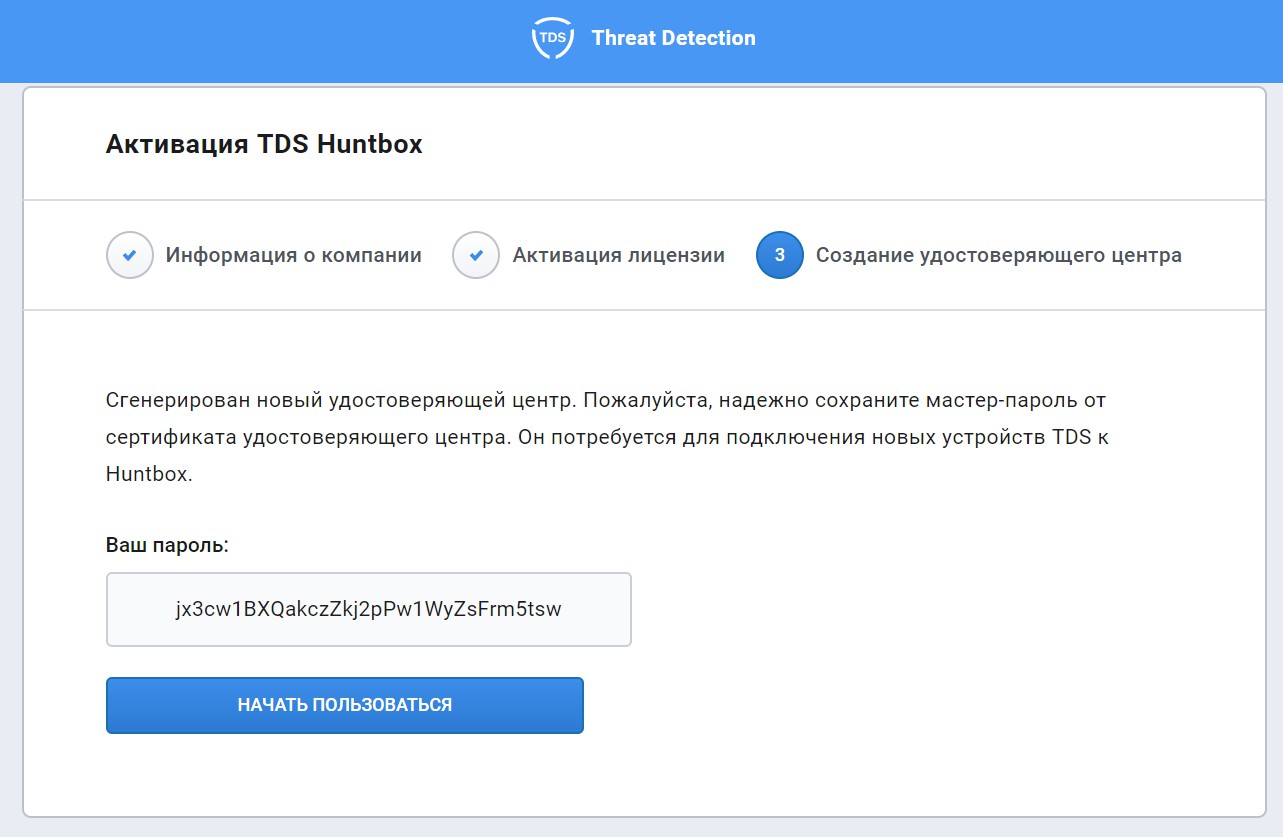


Рис. 5: Созданный пароль

Сохраняйте ваш мастер-пароль в надёжном месте - он будет использоваться при подключении компонентов TDS Sensor, TDS Polygon, TDS Endpoint.

Начать Пользоваться - позволяет завершить процесс активации HuntBox.

### 5.6.2. Подключение к консоли HuntBox

Консоль TDS HuntBox доступна администратору следующими способами:

* С помощью KVM (D-SUB для видео и USB для клавиатуры).
* С помощью последовательного порта:
  + Baudrate: 115200
  + 8-bit
  + Flow control: ON
* Через SSH при условии настроенного сетевого подключения.

Логин / Пароль консоли TDS HuntBox

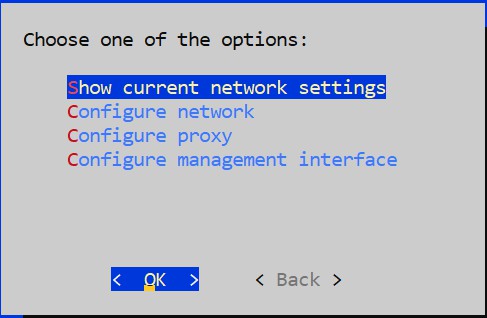
Для управления сервером используйте учетную запись с логином tds и паролем tds.

После ввода логина и пароля на экран будет выведена основная информация о TDS HuntBox.

Для входа в главное меню выберите Enter the Shell.

Не забудьте изменить пароль по умолчанию!

### 5.6.3. Главное меню TDS HuntBox



Главное меню TDS HuntBox

Пункты главного меню:

Show current network settings: просмотр и изменение настройки сети.

1. Configure network:
2. Configure proxy:
3. Configure managment interface:
4. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

Configure network

Доступны следующие варианты настроек:

1. DHCP: автоконфигурация адреса и прочих настроек по протоколу DHCP. Производится автоконфигурация интерфейса и перезапуск сети.
2. Static: статическая конфигурация параметров. Требуется ввод всех сетевых параметров вручную, после чего производится перезапуск сети. Для отмены ввода параметров в любой момент используется сочетание Ctrl+C.
3. Cancel: возврат на уровень меню выше.

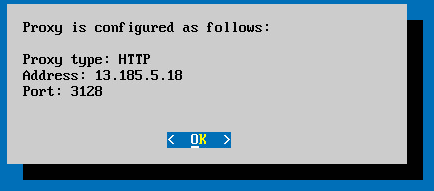
Configure proxy

Настройка прокси-сервера для доступа к обновлениям и облачному сервису Group-IB. TDS HuntBox позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика для всех компонент TDS. В процессе настройки устройство запрашивает конфигурационную строку в следующем формате: Login:pass@domen\_proxy:port

При этом необходимо выбрать тип проксирования: http-proxy или socks-proxy.

Проверьте введенные значения:

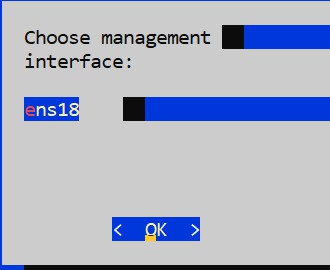
Proxy Settings -> Show current proxy settings



Для успешного использования прокси-сервера, он должен поддерживать метод CONNECT с открытием соединений на 443 порт.

Configure managment interface

В данном меню предоставляется возможность выбора из доступных на TDS HuntBox интерфейсов управляющий. Управляющий интерфейс будет использоваться всеми компонентами для работы с TDS HuntBox.



Выбор управляющего интерфейса

## 5.7. Встраивание TDS Sensor с учётом точек съёма трафика, почтовой интеграции, интеграции с файловыми хранилищами и с учётом установки TDS HuntBox

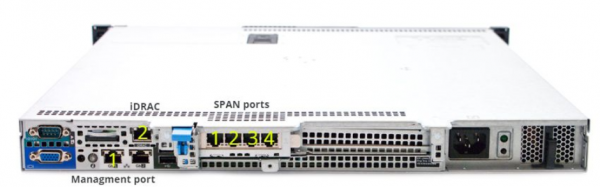
В базовой комплектации TDS Sensor имеет четыре сетевых интерфейса для приема трафика и один порт для подключения к сети и управления. Для обновления ПО и использования преимуществ облачного центра Group-IB SOC через порт управления TDS Sensor,в зависимости от выбранного типа инсталляции, должен быть доступен для подключения сетевой адрес:

* tdsi.group-ib.com:443/tcp - При использовании SOC Group-IB
* IP адрес TDS HuntBox:1443/udp - При использовании TDS HuntBox

При необходимости работа TDS Sensor с Group-IB SOC / TDS HuntBox может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод CONNECT для установления подключений на 443 порт.

### 5.7.1. Подключение к сети и захват трафика

На Изображении 1, отмечены все необходимые интерфейсы, используемые при интеграции и нормального функционирования:



Изображении 1. Интерфейсы TDS-Sensor

**Порт управления**

Интерфейс №1 (см. Изображении 1) расположены на задней панели и используется для управления устройством и связи с Group-IB SOC / TDS HuntBox, а также для коммуникации с модулем TDS Polygon. По умолчанию интерфейс сконфигурирован для получения настроек сети по протоколу DHCP. Сетевые настройки порта управления можно поменять при помощи технической консоли

**Захват трафика**

Интерфейсы для захвата трафика расположены справа от порта управления и нумеруются от 1 до 4. (см. Изображение 1).

Для работы устройства один или несколько портов захвата трафика должны быть соединены кабелем с источником трафика. Таким источником может быть сетевое устройство с настроенным зеркалированием (SPAN/RSPAN в терминах оборудования CISCO), либо TAP-устройство, копирующее ethernet-кадры на самом низком уровне, либо GRE-туннель со SPAN-траффиком.

TDS захватывает зеркалированый трафик на уровне L2.

L3 mirroring, включая ERSPAN не поддерживается устройством и не является допустимым способом зеркалирования трафика на устройство.

TDS сенсор поддерживает SPAN in GRE: Когда необходимо пропустить SPAN-трафик через несколько устройств уровня L3, либо взять его с фермы виртуальных машин, возможно создать GRE-туннель между TDS и источником SPAN-трафика.

При организации зеркалирования следует учитывать, что трафик пользователей корпоративных прокси-серверов и сегментов сети, расположенных за NAT’ом, должен зеркалироваться до проксирования/натирования, как можно ближе к пользовательскому сегменту, до любого фильтрующего оборудования, чтобы в заголовках пакетов были видны оригинальные IP-адреса клиентов, а также для исключения фильтрации части трафика средствами межсетевых экранов. Это упростит реагирование на выявленные сетевые инциденты.

**iDRAC**

На задних панелях серверов TDS, правее от порта управления, расположены порты iDRAC. (см. Изображении 1 и Изображении 2). Данный интерфейс позволяет реализовать такие функции, как развертывание, обновление, мониторинг и обслуживание серверного оборудования.

### 5.7.2. Активация сенсора и синхронизация с HuntBox

Активация сенсора - включает функционал сенсора.

Синхронизация сенсора - привязывает сенсор к HuntBox либо к SOC, тем самым предоставляя возможность управления сенсором через обозначенные системы.

Для взаимодействия сенсора с HuntBox необходимы следующие порты:

* 443/tcp - для первичной активации и привязки сенсора (единоразово)
* 1443/udp - для дальнейшего взаимодействия сенсора с HuntBox
* 3000/tcp - для взаимодействия сенсора с Polygon

Активация и синхронизация осуществляется через консоль TDS Sensor.

На данном этапе статус Galaxy Connection равен Fail. Так как сенсор не привязан к HuntBox.

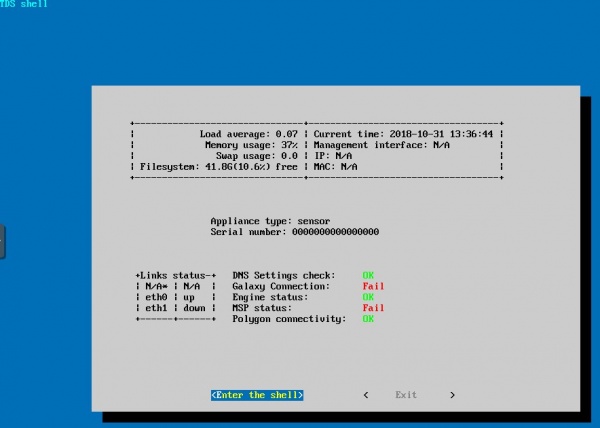


Рис. 1: Galaxy Connection fail

После нажатия Enter the Shell(рис.1) в открывшемся меню пункт Activation(рис.2) отвечает за активацию и синхронизацию.

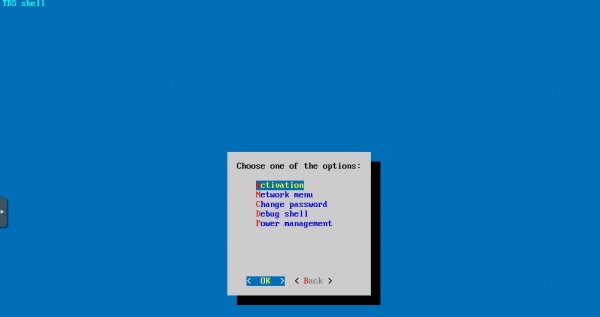


Рис. 2: Activation menu

В меню выбора Central Authority задаётся сервер синхронизации(рис.3). Он определяет дальнейший режим работы сенсора: on-premise или on-cloud. Доступные пункты меню:

* GIB CA - on-cloud инсталляция. Оркестрация сенсором осуществляется через SOC Group-IB
* Private TDS Galaxy - on-premise инсталляция. Оркестрация сенсором осуществляется через TDS HuntBox

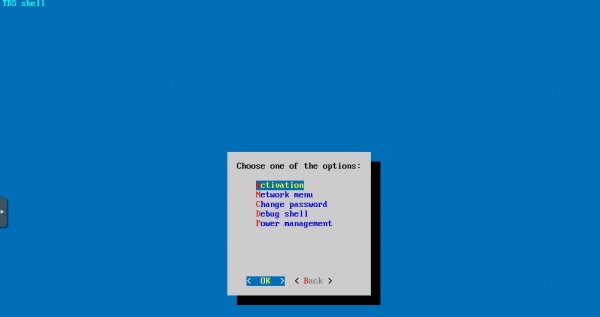


Рис. 3: Central Authorithy

При выборе Ptivate TDS Galaxy(рис.4) необходимо задать доменное имя или IP адрес TDS HuntBox.

При выборе GIB CA необходимо задать доменное имя или IP адрес SOC Group-IB. (задано по умолчанию)



Рис. 4: TDS HuntBox addresses

При работе сенсора(рис.5) через прокси сервер задайте адрес прокси в формате:

Login:pass@domen\_proxy:port



Рис. 5: Proxy Addresses

В пункте Device UUID задаётся номер лицензии (UID) полученного в пункте добавления нового оборудования в соответствующем меню TDS HuntBox



Рис. 6: Device UUID

При нажатии OK запускается процесс регистрации и синхронизации сенсора с выбранным сервером. Внимание: после данной операции мигрировать сенсор с одной инфраструктуры на другую невозможно без вмешательства технической поддержки Group-IB.

После регистрации сенсора консоль будет приветствовать пользователя своим UUID введённым на предыдущем шаге. (рис.7)



Рис. 7: Регистрация окончена

Панель инструментов в консоли сенсора будет отображать Galaxy Connection со статусом OK. (рис.8)

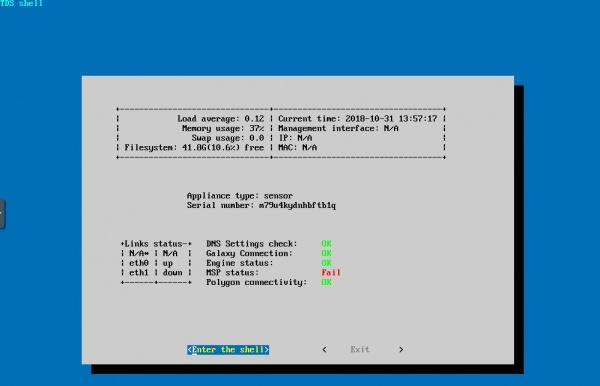


Рис. 8: Galaxy connection - ok

Меню Настройки -> Устройства -> Сенсор в веб интерфейсе HuntBox будет предоставлять информацию по состоянию подключенного устройства. Как указано на рис.9.

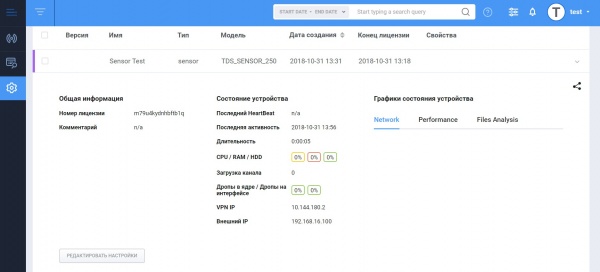


Рис. 9: Статус состояния подключённого сенсора в HuntBox

### 5.7.3. Подключение к консоли TDS-Sensor

Подключение к консоли TDS Sensor-a

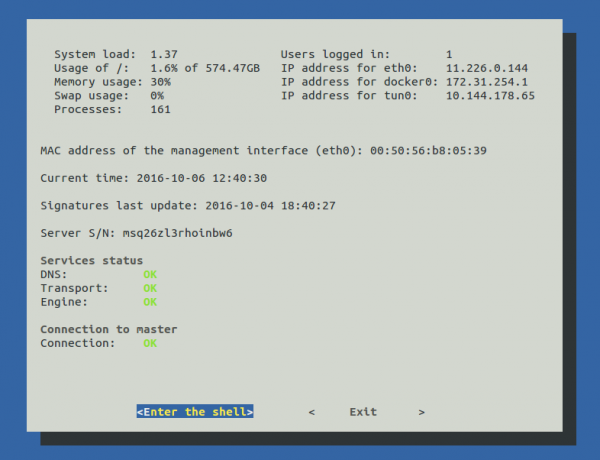
Доступ к консоли TDS Sensor можно получить любым из нижеперечисленных способов:

* С помощью KVM (D-SUB для видео и USB для клавиатуры).
* С помощью последовательного порта:
  + Baudrate: 115200
  + 8-bit
  + Flow control: ON
* Через SSH при условии настроенного сетевого подключения.

Для управления сервером используйте учетную запись с логином tds и паролем tds.

После ввода логина и пароля на экран будет выведена основная информация о TDS Sensor. Для входа в главное меню выберите Enter the Shell.

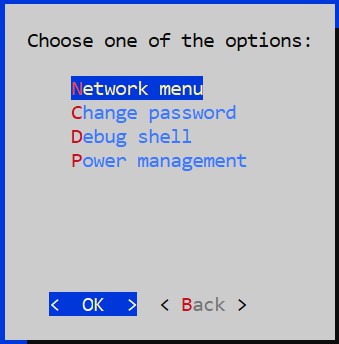
Не забудьте изменить пароль по умолчанию!



Изображение 4. Основная информация о TDS Sensor

### 5.7.4. Меню CLI TDS Sensor

Главное меню TDS Sensor



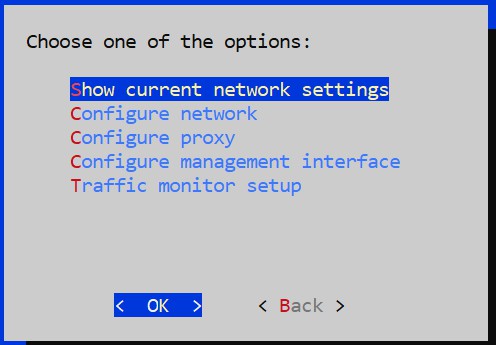
Изображение 5. Главное меню TDS Shell

Пункты главного меню:

1. Network menu: просмотр и изменение настройки сети.
2. Change password: меню изменения административного пароля пользователя tds.
3. Debug shell: доступ до инструментов отладки в режиме командной строки
4. Power management: меню выключения или перезагрузки устройства.
5. Back: вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

### 5.7.5. Настройка сети TDS Sensor

Настройки сети TDS Sensor



Изображение 6. Меню настройки сети

Пункты меню настройки сети:

1. Show current network settings: вывод текущий настройки сетевого интерфейса управления.
2. Configure network: настройка сетевого интерфейса.
3. Configure proxy: настройки прокси для работы с SOC Group-IB / TDS HuntBox.
4. Configure managment interface: настройки управляющего интерфейса.
5. Traffic monitor Setup: меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
6. Back: возврат на уровень меню выше.

**Configure network**

Доступны следующие варианты настроек:

1. DHCP: автоконфигурация адреса и прочих настроек по протоколу DHCP. Производится автоконфигурация интерфейса и перезапуск сети.
2. Static: статическая конфигурация параметров. Требуется ввод всех сетевых параметров вручную, после чего производится перезапуск сети. Для отмены ввода параметров в любой момент используется сочетание Ctrl+C.
3. Cancel: возврат на уровень меню выше.

**Configure proxy**

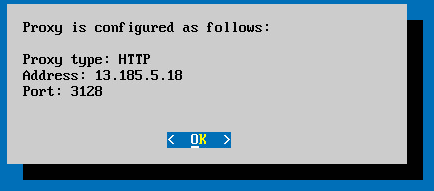
Настройка прокси-сервера для доступа к обновлениям и облачному сервису Group-IB или локальному сервису TDS HuntBox. TDS Sensor позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а также связи с облачным сервисом Group-IB или локальным сервисом TDS HuntBox. В процессе настройки устройство запрашивает конфигурационную строку в следующем формате:

Login:pass@domen\_proxy:port

При этом необходимо выбрать тип проксирования: http-proxy или socks-proxy.

Проверьте введенные значения:

Proxy Settings -> Show current proxy settings



Изображение 10. Результат настройки прокси-сервера.

Для успешного использования прокси-сервер должен поддерживать возможность осуществления запросов методом CONNECT с открытием соединений на 443 порт.

**Configure managment interface**

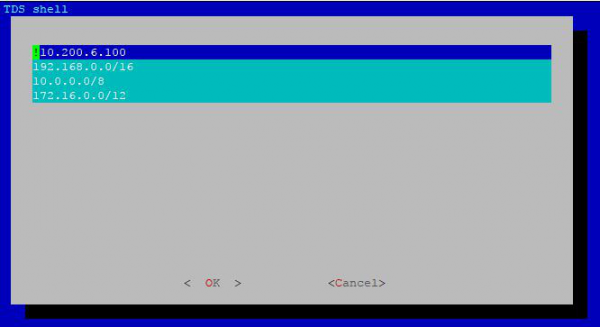
Предоставляет возможность задания управляющего интерфейса в TDS Sensor. Для задания выберите из списка интерфейсов нужны и нажмите ок.

**Traffic Monitor Setup**

Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE:

* Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.

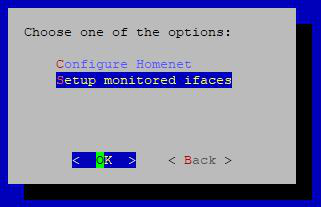
Configure network -> Configure Homenet

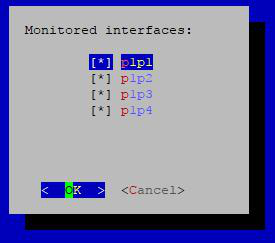


Изображение 7. Ввод локальных адресов.

* Выберите SPAN-интерфейсы:

Configure network -> Setup monitored ifaces





Изображение 8. Выбор SPAN-интерфейсов

## 5.8. Установка TDS Endpoint на защищаемых хостах заказчика

Установка TDS Endpoint перед началом установки необходимо получить файл:

* gibep.msi

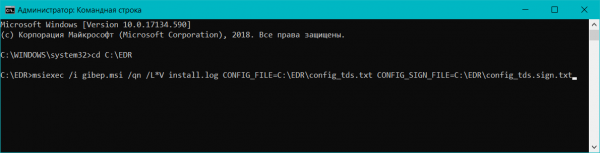
и 2 конфигурационных файла:

* config\_tds.txt
* config\_tds.sign.txt

Эти файлы необходимо поместить в локальную директорию. Важно, что полный путь до директории не должен содержать кириллических символов и пробелов. Для примера поместим эти файлы в C:\EDR

После этого необходимо запустить cmd.exe с правами Администратора, перейти в директорию с установочным и конфигурационными файлами и выполнить команду:

* msiexec /i gibep.msi /qn /L\*V install.log CONFIG\_FILE=C:\EDR\config\_tds.txt CONFIG\_SIGN\_FILE=C:\EDR\config\_tds.sign.txt



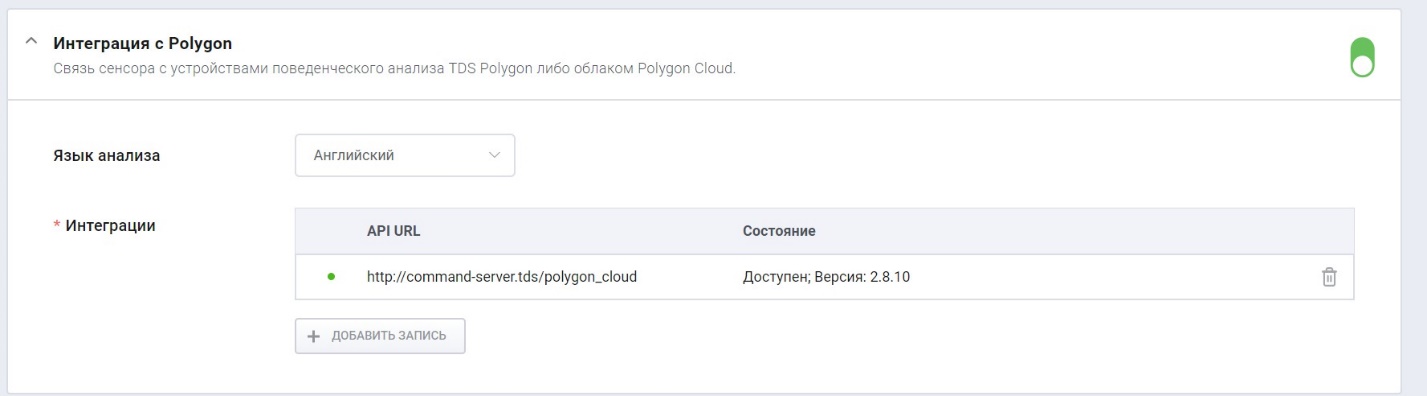
Установка TDS Endpoint локально

## Встраивание TDS Polygon с учётом установки TDS Sensor, TDS Endpoint, TDS HuntBox

Настройка TDS Polygon производится в настройках TDS Sensor, а для TDS Endpoint обеспечивается TDS HuntBox-ом после синхронизации.

Настройка располагается по адресу WUI ->Настройки -> Устройства -> Сенсор -> Редактировать настройки и предлагает возможность интегрировать выбранный TDS Sensor c определенным TDS Polygon для осуществления функций поведенческого анализа.

Интеграция TDS Sensor с TDS Polygon



**Интеграции**

В меню задаётся запись в виде доменного имени или IP адреса TDS Polygon. Возможно задать больше чем одну запись, дабы обеспечить распределение нагрузки по поведенческому анализу. Управление очередью производится на стороне сенсора. Сенсор делает опрос всех подключённых к нему TDS Polygon на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

**Язык анализа**

Задаёт использование определённых образов операционных систем внутри подключённых TDS Polygon. Данные операционные системы будут настроены для поддержания защиты от актуальных угроз в регионах с выбранной языковой системой (По умолчанию поддерживаются Русский и Английский языки).

**Использование облачного TDS Polygon**

Для использования Polygon Cloud (облачной версии TDS Polygon) используется следующая запись:

<http://command-server.tds/polygon_cloud>

## Обеспечение связности всех модулей с TDS HuntBox;

Для работы ПО необходима связность на сетевом уровне всех модулей, а также связь на уровне протоколов ниже:

**TDS Huntbox**

* Для доступа к инфраструктуре Group-IB:
  + tdsi.group-ib.com:443/tcp - режим "TI Feed", т.е. с туннелем
  + 92.53.76.98:443/tcp (для режима доставки обновлений через https)
* Для доступа к устройствам Sensor и Polygon для их обновления и поддержки:
  + 22/tcp каждого из устройств
* Прямой NAT наружу в интернет для выпуска виртуальных машин Polygon, если он происходит через Huntbox

**TDS Sensor**

* Для связи с Huntbox:
  + 1443/udp на ip-адрес Huntbox
* Доступ к Proxy-серверу, либо прямой NAT наружу для скачивания ссылок

**TDS Polygon**

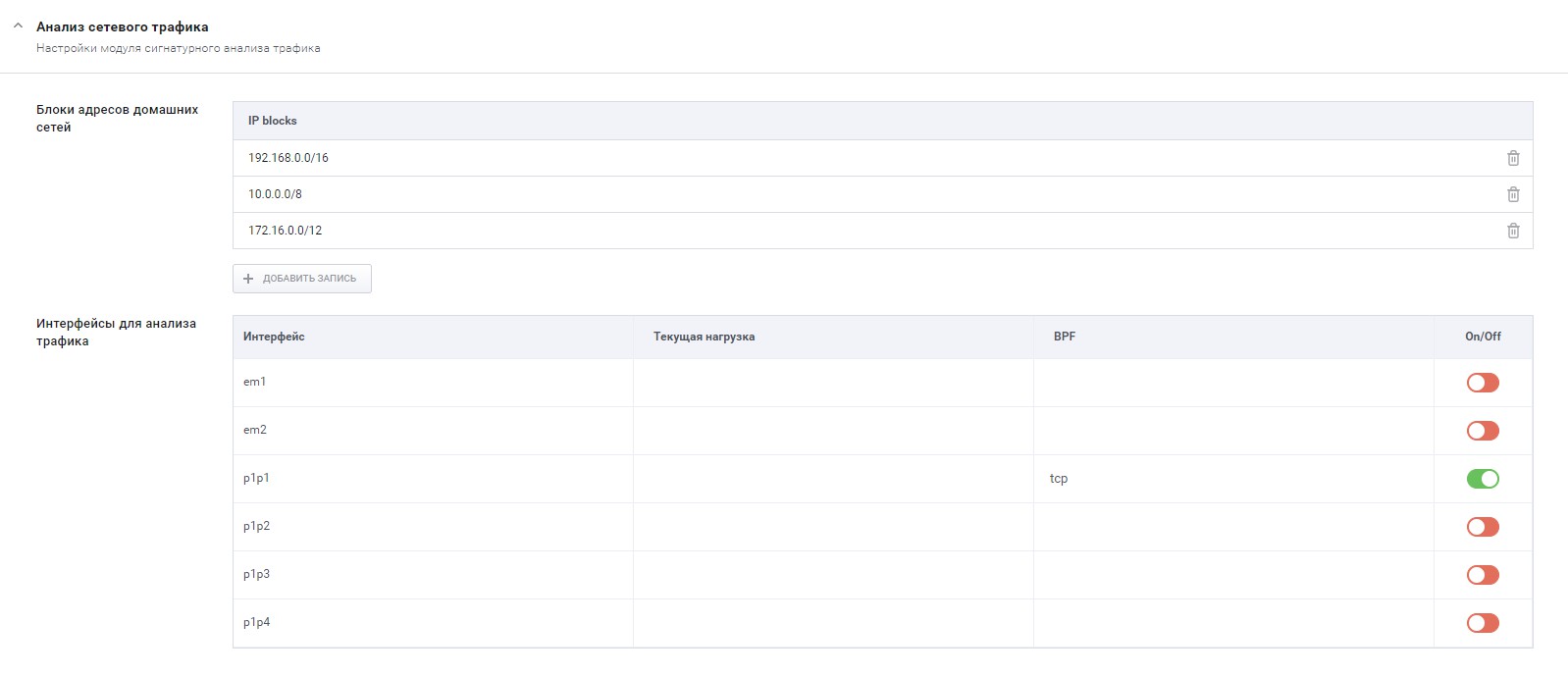
* Для связи с Huntbox:
  + 1443/udp на ip-адрес Huntbox
* Прямой NAT наружу в интернет для выпуска виртуальных машин Polygon, если он происходит автономно, мимо HuntBox

## Определение перечня IP-подсетей заказчика, которые будут определены как защищаемые и ввод этих данных в ПО

Настройка находится по адресу WUI -> Настройки -> Устройства -> Сенсор –> Редактировать настройки -> Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа. Данный раздел даёт системе понимание "инородного" трафика относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGR.

Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.



Анализ сетевого трафика

## Интеграция почтовой системы

Настройки по выбранному типу интеграции находятся в разделах:

Интеграция TDS-Sensor с почтовой системой

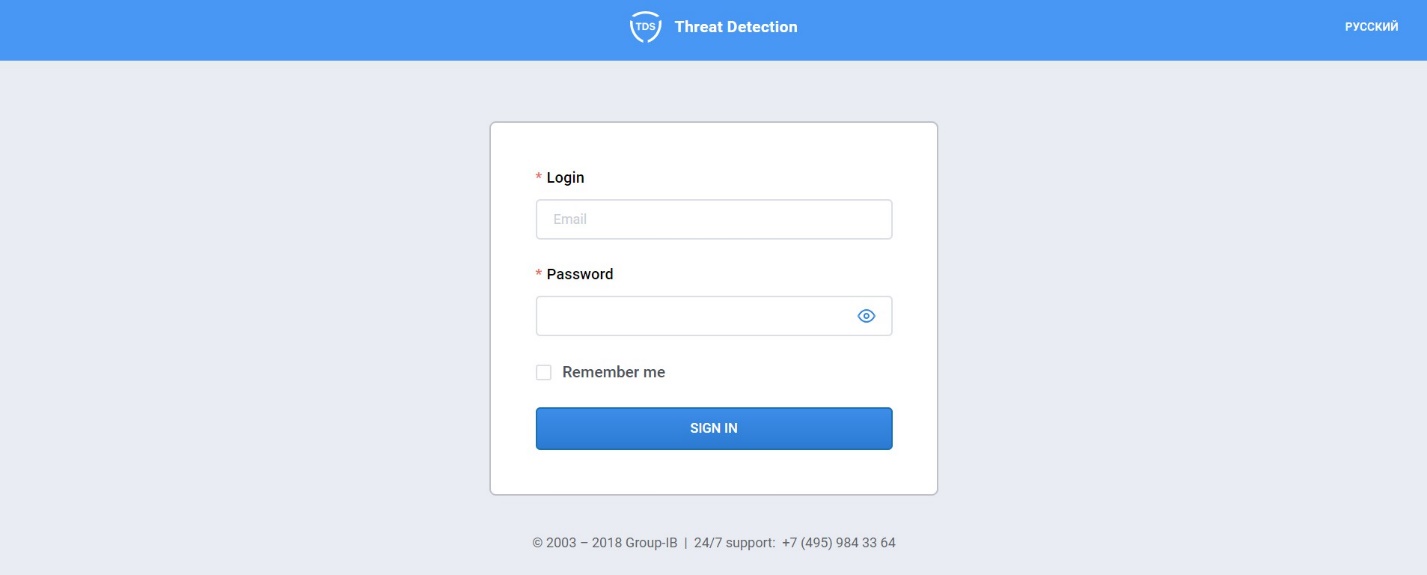
* Интеграция по POP3/IMAP
* Интеграция по SMTP

Inline-режим почтовой интеграции

* Требования к Inline интеграции
* Включение MTA-режима

# Интерфейс администратора

Интерфейс доступен при открытии в браузере страницы <https://ip_addr_TDS_HuntBox>. Пользователю будет предложена форма аутентификации. Для входа в систему используйте логи/пароль администратора, заданные в процессе активации TDS HuntBox или выданные вам данные, созданные в разделе Пользователи.



Страница аутентификации

**Смена языка**

Смена языка интерфейса доступна на странице ввода имени пользователя и пароля в верхнем правом углу. А также в меню настроек пользователей.

## 6.1. Dashboard

Меню предоставляет возможность наблюдения за общими показателями всех компонент системы в графическом виде. Каждый виджет предоставляет возможность наблюдать различные показатели подсистем и настраивается под нужды пользователя.

Для создания нового виджета кликните по кнопке **Добавить виджет** в правом верхнем углу панели и выберите тип из выпадающего списка. Виджеты возможно реорганизовывать в необходимом пользователю порядке. Для этого зажмите кнопку в виде пересекающихся стрелок в правом верхнем углу виджета и перетащите виджет в нужное место. Для удаления виджета выберете кнопку **Удалить**.

Описание виджетов ниже

### 6.1.1. Состояние устройства

Виджет предоставляет данные о CPU,RAM,HDD по всем подключенным к TDS HuntBox устройствам. Данные по нагрузке предоставляются в режиме онлайн. По отключенным / несинхронизированным устройствам данные будут пустыми.

По каждому устройству доступно:

* Тип устройства

Тип компоненты решения TDS

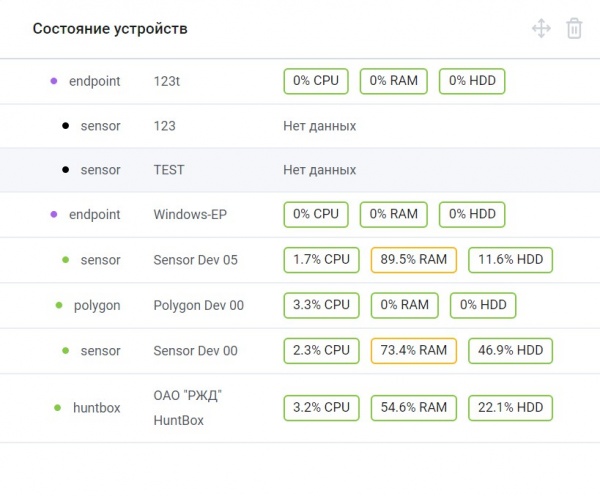
* Имя устройства

Имя заданное при создании заведении нового устройства в разделе настройки

* CPU/RAM/HDD

Нагрузка на оборудование в данный момент

Примечание: нагрузка по ПК с установленными TDS Endpoint не выдаётся. Вместо неё описывается количество хостов с онлайн статусом



Состояние устройств

### 6.1.2. Последние алерты

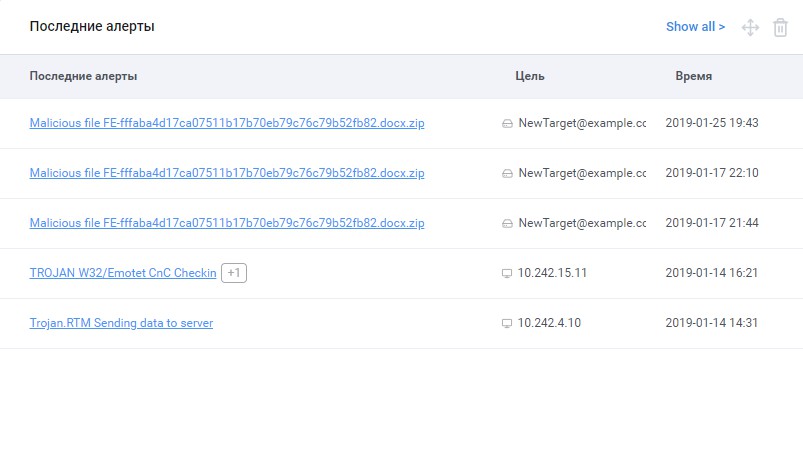
Виджет предоставляет список крайних по дате алертов возникших в системе. По щелчку на алерте происходит переход к полному описанию в разделе Алерты. Что бы перейти к списку всех алертов нажмите Show All в правом верхнем углу виджета. По каждому алерту доступно:

* Цель

Сущность, участвующая в инциденте в качестве жертвы (IP, domainname, email)

* Время

Время первого события связанного с данным алертом в формате гггг-мм-дд чч:мм

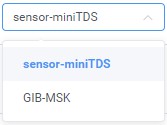


Последние алерты

### 6.1.3. Статистика алертов по классификатору и критичности

Виджет предоставляет диаграмму с количеством алертов за выбранный период по выбранному сенсору.

В правом верхнем углу виджета находится меню выбора классификатора

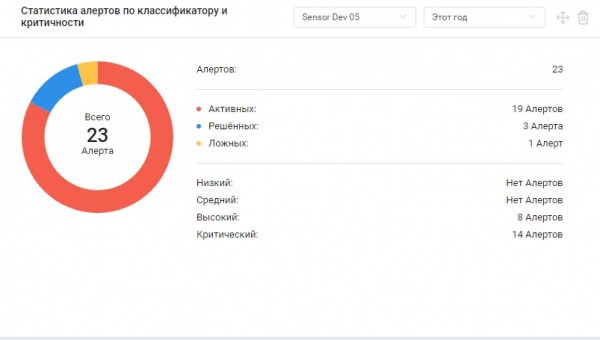


Меню выбора сенсора

и отчётного периода.



Охватываемый период статистики



Статистика алертов

Доступные данные по выбранному классификатору:

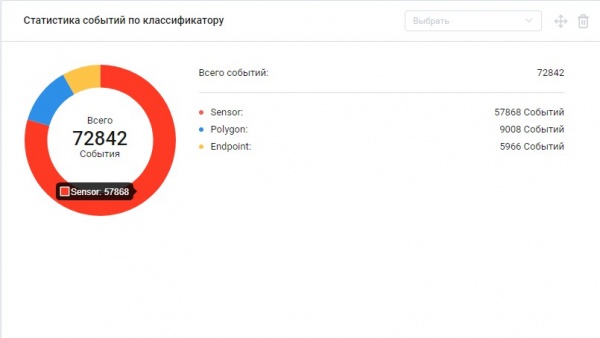
* Алертов - общее количество алертов
  + Активных - в процессе разрешения
  + Решенных - решенные инциденты
  + Ложных - ложные срабатывания
* Критичность
  + Низкий
  + Средний
  + Высокий
  + Критический

### 6.1.4. Статистика событий по классификатору

Предоставляет данные по количеству событий сразу по всем классификаторам за выбранный временной период в виде диаграммы.



Охватываемый период статистики



Статистика событий по классификатору

### 6.1.5. График событий по классификатору

Представляет график количества событий по каждому классификатору за выбранный период времени. Каждая кривая описывает статистику одного классификатора по всем подключенным к TDS HuntBox компонент данного типа (классификатора).

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается).

Доступные фильтры:

* Polygon

Количество событий от всех компонент типа TDS Polygon подключенных к TDS HuntBox.

* Sensor

Количество событий от всех компонент типа TDS Sensor подключенных к TDS HuntBox.

* Endpoint

Количество событий от всех компонент типа TDS Endpoint подключенных к TDS HuntBox.



Охватываемый период статистики

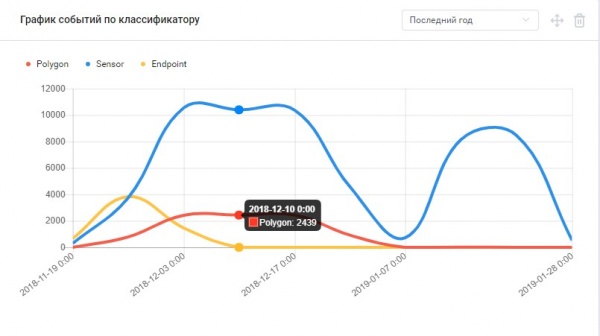
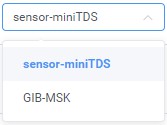


График событий с разбивкой по классификатору

### 6.1.6. График SPAN интеграции

График зависимости общей нагрузки на всех SPAN интерфейсах выбранного сенсора к выбранному периоду времени. Так же предоставляет данные по дропам ядра в том же масштабе. Для отображения данных задайте сенсор через меню выбора сенсора.



Меню выбора сенсора

А также выберите требуемый промежуток времени.



Охватываемый период статистики

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается).

Доступные фильтры:

* Мбит/сек

Нагрузка на всех SPAN интерфейсах

* Дропы в ядре

Потери пакетов на уровне ядра операционной системы.

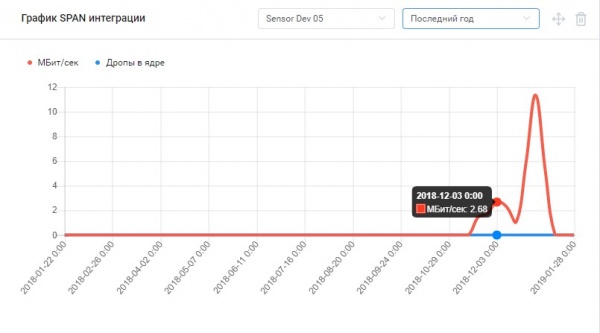


График SPAN интеграции

### 6.1.7. Статистика SPAN интеграции

Предоставляет диаграмму с данными по нагрузке на SPAN интерфейсы выбранного сенсора в режиме онлайн. Отображаемые данные:

* Лицензионное ограничение

Максимально допустимая нагрузка на сенсор в соответствии с приобретённой лицензией (Мбит/с).

* Текущая нагрузка

Нагрузка к данному моменту времени.

* Свободный канал

Свободная нагрузочная полоса для приёма SPAN трафика. Разница между первым и вторым пунктами.

* Минимальная нагрузка

Минимальная нагрузка с момента заведения SPAN трафика на анализ в выбранный сенсор.

* Максимальная нагрузка

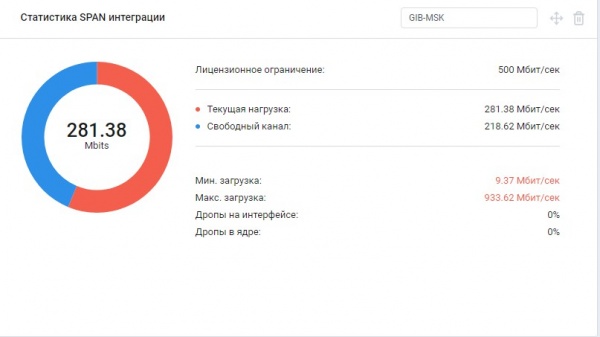
Максимальная нагрузка с момента заведения SPAN трафика на анализ в выбранный сенсор.

* Дропы на интерфейсе

Потери пакетов в физической среде передачи SPAN трафика.

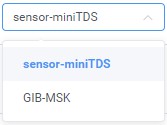
* Дропе в ядре

Потери пакетов на уровне операционной системы сенсора.

Загрузка SAPN интерфейсов

### 6.1.8. График электронной почты

График отображает статистику по принятым почтовым сообщениям и проанализированным вложениям у выбранного сенсора на указанном отчётном периоде. По меню выбора сенсора доступны подключенные к TDS HuntBox сенсоры:



Меню выбора сенсора

Охватываемый период



Охватываемый период статистики

График возможно фильтровать - отображать на нём отдельные кривые. По умолчанию все фильтры отключены. При выборе одного из фильтров кривая соответствующая названию фильтра перестаёт отображаться (вычёркивается). Доступные фильтры:

* Envelope

Количество входящих (принятых) письменных сообщений.

* File

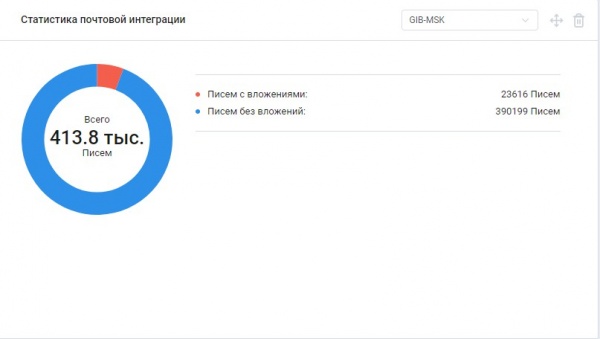
Количество вложенных в принятых почтовых сообщениях файлов.



График почтовых сообщений и вложений

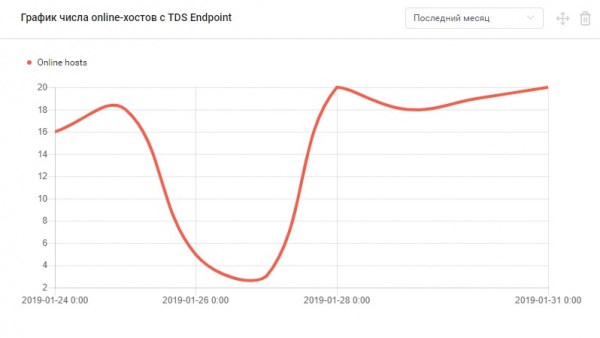
### 6.1.9. Статистика почтовой интеграции

Предоставляет диаграмму с данными по количеству принятых письменных сообщений и письменных сообщений с вложениями на выбранном сенсоре.

 Статистика почтовых сообщений

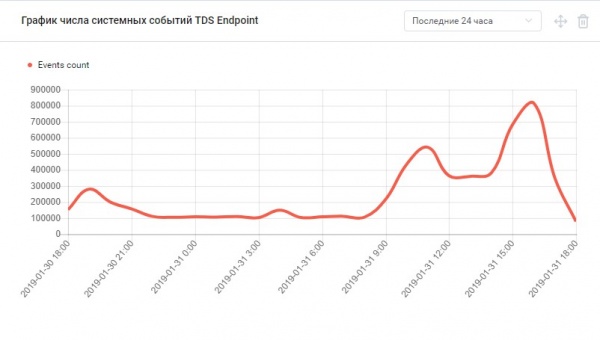
### 6.1.10. График числа online-хостов с TDS Endpoint

График отображает количество ПК с установленными на них TDS Endpoint со статусом онлайн на временной шкале. Временная шкала задаётся в меню выбора отчётного периода.

 График числа TDS Endpoint

### 6.1.11. График числа системных событий TDS Endpoint

График отображает статистику по числу событий на всех TDS Endpoint обнаруженных за указанный отчётный период.

 График числа событий на TDS Endpoint

## 6.2. Алерты

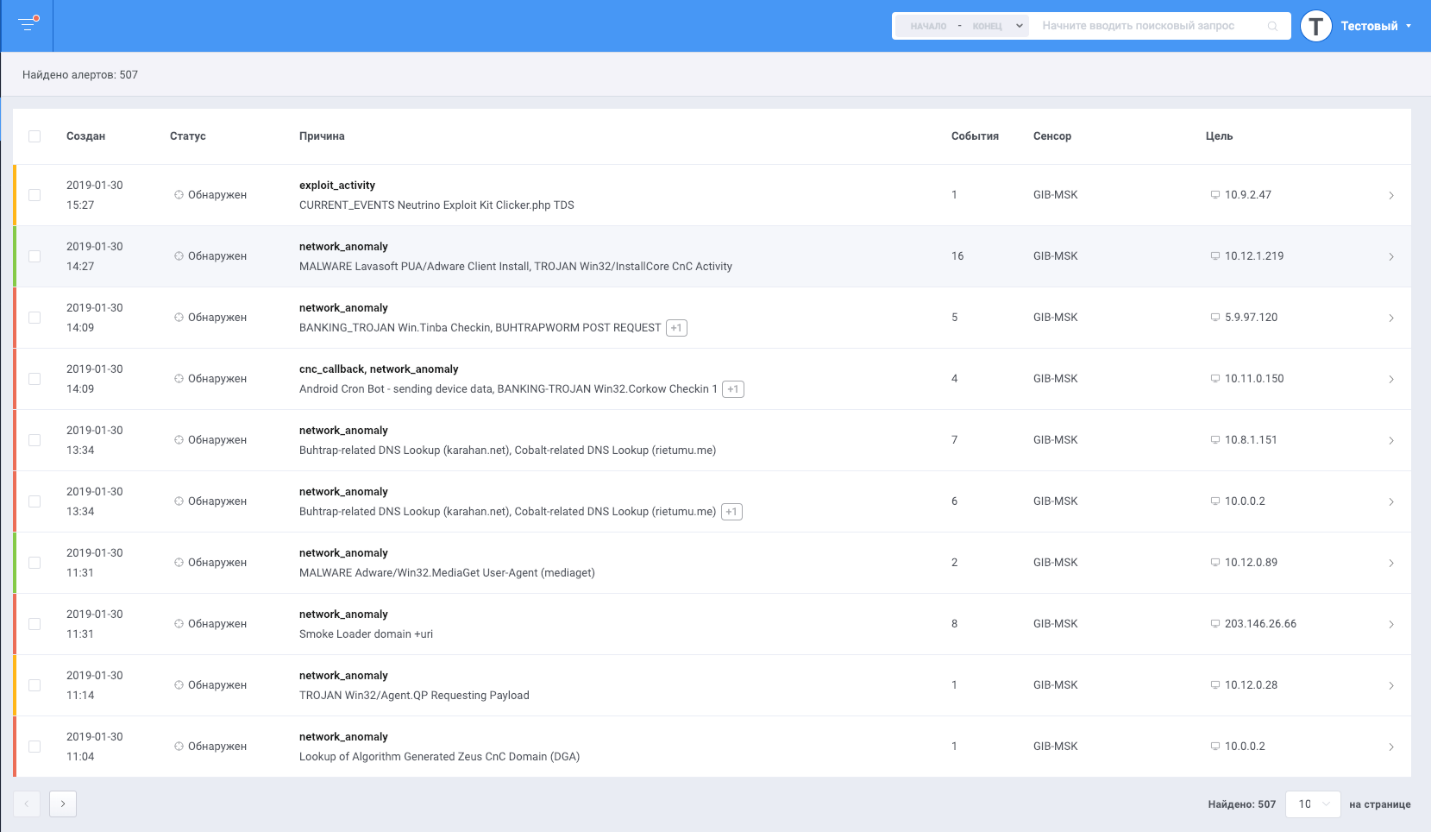
Данный раздел предоставляет информацию о всех происходящих потенциальных инцидентах, детектируемых компонентами TDS Sensor, TDS Polygon, TDS Endpoint подключенными к TDS HuntBox. Таким образом в разделе реализуются функции мониторинга и реагирования на события информационной безопасности. Система предоставляет список алертов с общими данными. Внутри каждого алерта доступна подробная информация, а именно:

* График активности - граф связности событий по данному алерту
* События с полным описанием релевантной данному алерту информацией
* Хронология событий - комментарии и история работы по алерту.
* Информация по инфраструктуре атакующих связанная с данным алертом
* Инструменты для блокирования хостов - если на них установлены TDS Endpoint

### 6.2.1.Алерт

Алерт - потенциально зловредное воздействие на инфраструктуру клиента. Состоит из множества событий скоррелированных из различных подсистем TDS и атрибутированных определенной угрозе и (возможно) группе злоумышленников. В алертах отображаются события, зарегистрированные подсистемами:

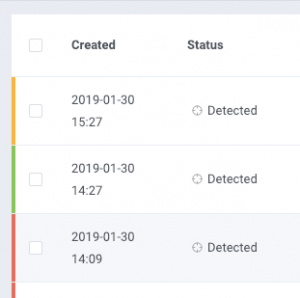
* Сигнатурного анализа: TDS Sensor выявляет случаи совпадения содержимого сетевых сессий с известными шаблонами вредоносного трафика;
* Поведенческого анализа: TDS Polygon - технология анализа поведения файлов. Поведенческие маркеры и классификатор позволяет выявить вредоносную активность файла;
* Агент контроля рабочих станций: TDS Endpoint - установленный агент на ПК.

Список алертов

Каждый пункт представляет из себя алерт состоящий из множества событий различных подсистем TDS (рис. Список алертов).

Общие данные по алертам:

1. Создан - время и дата создания алерта. То есть формальная дата обозначения набора событий, как потенциально вредоносных. Вообще говоря, может быть позже, чем даты событий, породивших данный алерт.
2. Статус - атрибут, служащий для отображения информации о текущем статусе работ по решению заявки.
   1. Обнаружен - выявлена потенциально вредоносная активность, требуется реакция.
   2. Заблокирован - вредоносная активность была заблокирована системой TDS HuntBox.
3. Причина - отображаются модули системы TDS:
   1. endpoint\_activity - активность агента контроля рабочей станции;
   2. network\_anomaly - сигнатурный анализ;
   3. malicious\_file - файл, проанализированный модулем поведенческого анализа.
4. События - количество событий.
5. Сенсор - наименование сенсора.
6. Цель - в данном столбце указывается адрес назначения и адрес источника, IP-адрес, наименование компьютера. Символизирует цель атаки злоумышленников.
7. Уровень опасности - цветовая индикация на левой границе алерта (рис. Уровень опасности)



Уровень опасности

Каждому алерту выдаётся уровень опасности. Уровень опасности определяет степень критичности алерта в соответствии с классификатором уровней угроз Group-IB.

Доступные уровни опасности:

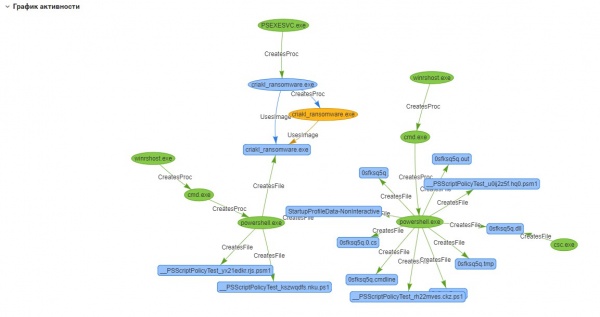
* Критический - события с красным уровнем угроз, указывающие на таргетированные атаки и критические заражения устройств в сети, требующие моментального реагирования.
* Средний - события с желтым уровнем угроз, также могут свидетельствовать о потенциально выявленных угрозах.
* Низкий - события с зеленым уровнем угроз, нарушающие политику безопасности в организации, например, нежелательное ПО, легальные шпионские плагины и т.д.

### 6.2.2. Информация об алерте

После раскрытия алерта предоставляется полная информация по потенциальному инциденту и инструменты по работе с обнаруженными событиями.

#### 6.2.2.1. График активности

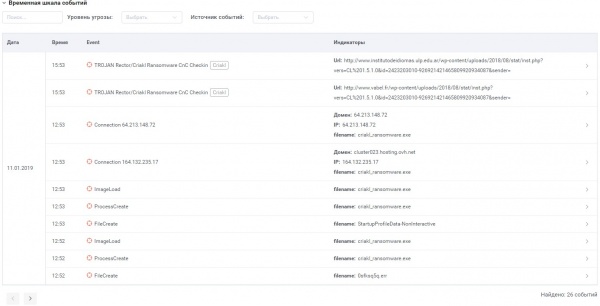
График активности представляет из себя связный направленный граф, в котором узлами являются задействованные в алерте артефакты событий, а ребрами указывается воздействие или взаимодействие артефактов событий друг с другом. График активности предоставляет ретроспективный взгляд на развитие алерта во времени. По графику возможно определить точку начала атаки, а так же дальнейшие пути её распространения со всеми затронутыми артефактами на ПК, в случае, если используется компонент TDS Endpoint. Граф возможно масштабировать, а так же менять в нём абсолютное расположение вершин не меняя связности графа для более удобного изучения аналитиком.



#### 6.2.2.2. Временная шкала событий

Временная шкала событий представляет из себя формальное описание всех событий, связанных с алертом. Источником данных событий могут служить:

* TDS Sensor
* TDS Polygon
* TDS Endpoint
* Внешний threat hunting



**Фильтрация временной шкалы событий**

События выстроены в виде убывающего по времени списка (крайние по времени события отображаются первыми).

Листать события возможно с помощью кнопок Button for list time incidents.jpg в левом нижнем углу. По мимо этого имеется возможность фильтрации событий следующими инструментами:

* Поиск - текстовый поиск по всем полям событий
* Уровень угрозы - отображает только события заданного уровня угроз. Не путайте уровень угроз события и уровень угроз алерта - это разные показатели!
  + Низкий
  + Средний
  + Критический
* Источник событий - отображает только события полученные из выбранной компоненты.
  + Сенсор
  + Полигон
  + Endpoint

**Описание временной шкалы событий**

Общие данные по временной шкале событий:

* Дата

Дата возникновения события в ПК, трафике, почте или при проверке передаваемых файлов.

* Время

Время возникновения события в ПК, трафике, почте или при проверке передаваемых файлов.

* Event

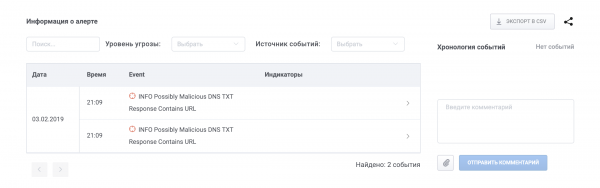
Событие, связанное с выбранным алертом в сокращённом виде. Подразумевает под собой потенциально вредоносное, вредоносное или связанное с вредоносным воздействие, выявленное одной из компонент системы.

* Индикаторы

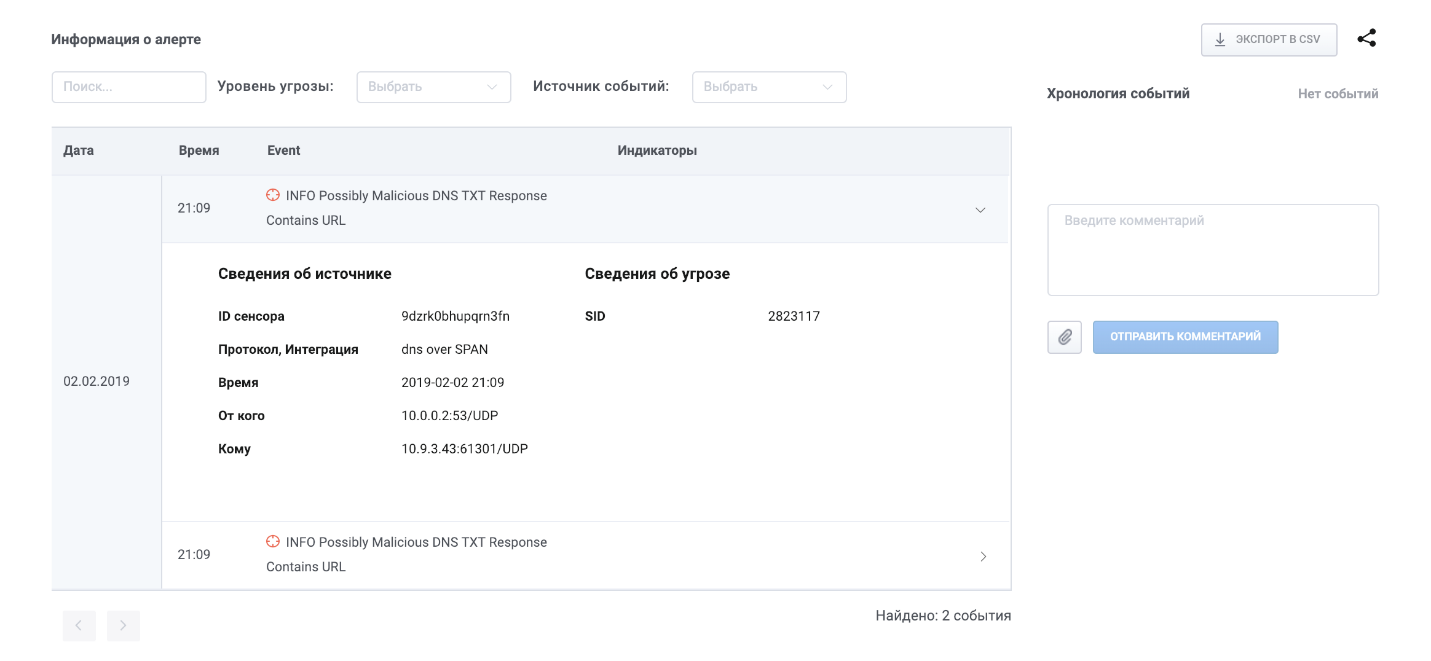
Индикатор события. Краткий перечень важных артефактов события (IP адреса, домены, ссылки, файлы). Полный перечень доступен при раскрытии события. Временная шкала событий может содержать различное количество различных событий от различных источников (компонент) системы. Ниже описываются три типа событий (по типу источника).

##### 6.2.2.2.1. Сигнатурный анализ

События, зарегистрированные системой сигнатурного анализа - это случаи совпадения содержимого сетевых сессий с известными шаблонами вредоносного трафика (рис. Сигнатурные алерты). По клику на любое из событий открывается более подробная информация о каждом из событий.



Сигнатурные события



Подробная информация о событии

По клику на любое из событий открывается подробная информация о событии (рис. Подробная информация о событии), которая включает:

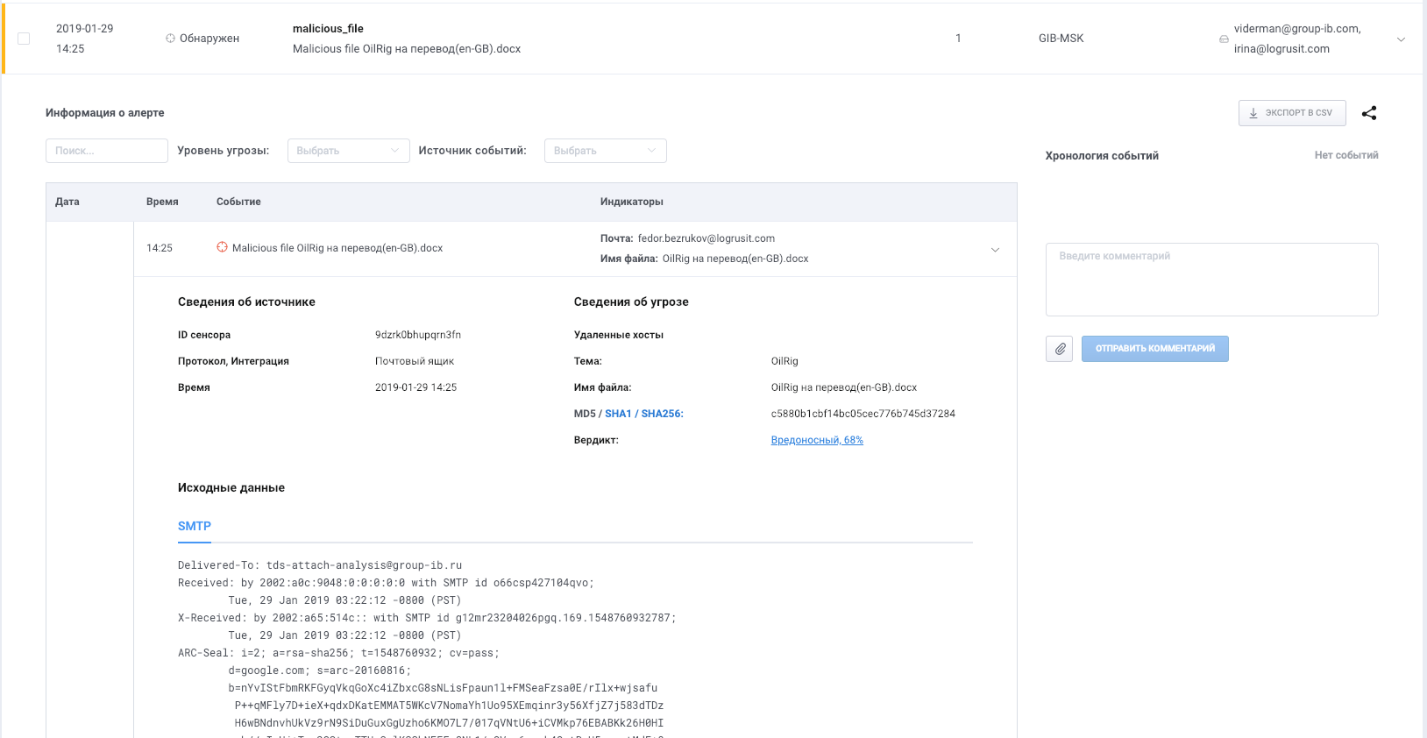
* Сведения об источнике
  + ID сенсора - уникальный номер оборудования TDS Sensor;
  + Протокол, Интеграция - указывает на способ интеграции и протокол реализации;
  + Время - время и дата сработки;
  + От кого - источник, инициировавший коммуникацию;
  + Кому - адрес назначения;
* Сведения об угрозе
  + URLs - запрошенный URI участвующий в зловредной коммуникации
  + SID - уникальный номер сигнатуры
  + Удаленные хосты - хосты использовавшиеся для проведения атаки
* Исходные данные

Предоставляет заголовок коммуникаций, относящихся к данному событию в различных форматах. (рис. HTTP заголовки) При анализе события существует возможность увидеть данные в формате: HTTP, ASCII, HEX

##### 6.2.2.2.2. Поведенческий анализ

Данный тип событий предоставляет базовые детали об объекте анализа.

* Сведения об источнике - состав сведений меняется в зависимости от типа интеграции и используемого протокола
  + ID сенсора - идентификатор сенсора через который объект анализа был отправлен на TDS Polygon
  + Протокол, Интеграция - протокол и способ интеграции по средствам которого был получен объект анализа
  + Время - время получения объекта анализа
  + От кого - источник коммуникации из которого получен объект анализа
  + Кому - получатель коммуникации из которой получен объект анализа
* Сведения об угрозе - состав зависит от типа интеграции и используемого протокола
  + Удалённые хосты - хост используемый для атаки в результате которой был получен объект анализа
  + URI - полная ссылка на ресурс, из-за обращения на которую был получен объект анализа
  + Тема - Тема письма из которого был получен объект анализа
  + Имя файла
  + MD5/SHA1/SHA256 - Значение хешей объекта анализа
  + Вердикт - результат анализа (подробнее в разделе Вердикт ниже)
  + SID
* Исходные данные



##### 6.2.2.2.3. Вердикт поведенческого анализа

При клике на Вердикт страница перенаправляет пользователя на детальный анализ семпла в песочнице TDS Polygon. В блоке “Видео” содержится видео выполнения (открытия) объекта анализа так, как оно выглядело бы на мониторе при открытии на полноценном компьютере. По данному видео часто можно судить о природе атаки и даже о достоверности зарегистрированного события. Следует учесть, что некоторые виды вредоносного ПО скрывают всю свою вредоносную активность от пользователя.

**Общие данные**

* Доступные данные:
* Оценка вредоносности

Вероятностная оценка степени вредоносности анализируемого объекта. Высчитывается методами машинного обучения исходя из выявленных в ходе поведенческого анализа индикаторов.

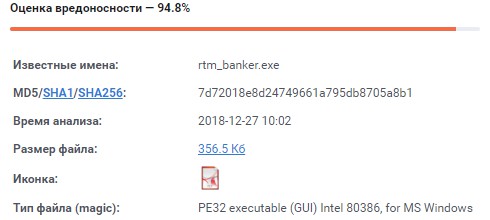
* Известные имена

Имена ВПО под которыми оно может быть известно

* MD5/SHA1/SHA256
* Время анализа

Время окончания анализа объекта

* Размер файла
* Иконка
* Тип файла



Общие данные по отчёту TDS Polygon

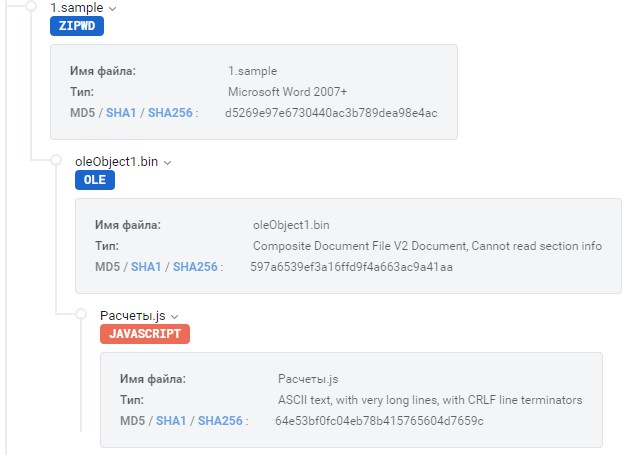
**Файловая структура**

Блок определяет способ организации, хранения и именования файлов в анализируемом объекте.



Файловая структура

Таким образом объект может состоять из нескольких объектов анализа. Каждый объект в данной структуре может быть раскрыт для более детального рассмотрения информации по нему (рис. Детали файловой структуры)



Детали файловой структуры

Для удобства восприятия в файловой структуре применяется цветовое различие типов объектов:

* Оранжевый – исполняемые объекты
* Жёлтый – контейнеры
* Голубой – документы
* Чёрный – прочие файлы

**Поведенческие маркеры**

Блок перечисляет причины, почему данный объект был отнесен к вредоносным. Большинство маркеров имеют индикаторы, подтверждающие вредоносность поведения - например, изменяемые ключи реестра, создаваемые файлы, изменения в чужих процессах и т.д. Индикаторы должны использоваться аналитиком для подтверждения угрозы.



Поведенческие маркеры

Каждый маркер раскрывается для получения конкретной информации по анализируемому объекту относительно данного маркера.

Разделяют следующие типы маркеров:

* Вредоносные

Однозначно вредоносные

* Прочие

Макеры не являющиеся вредоносные, но которые могут помочь при детальном анализе ВПО аналитиком

**Сетевая активность**

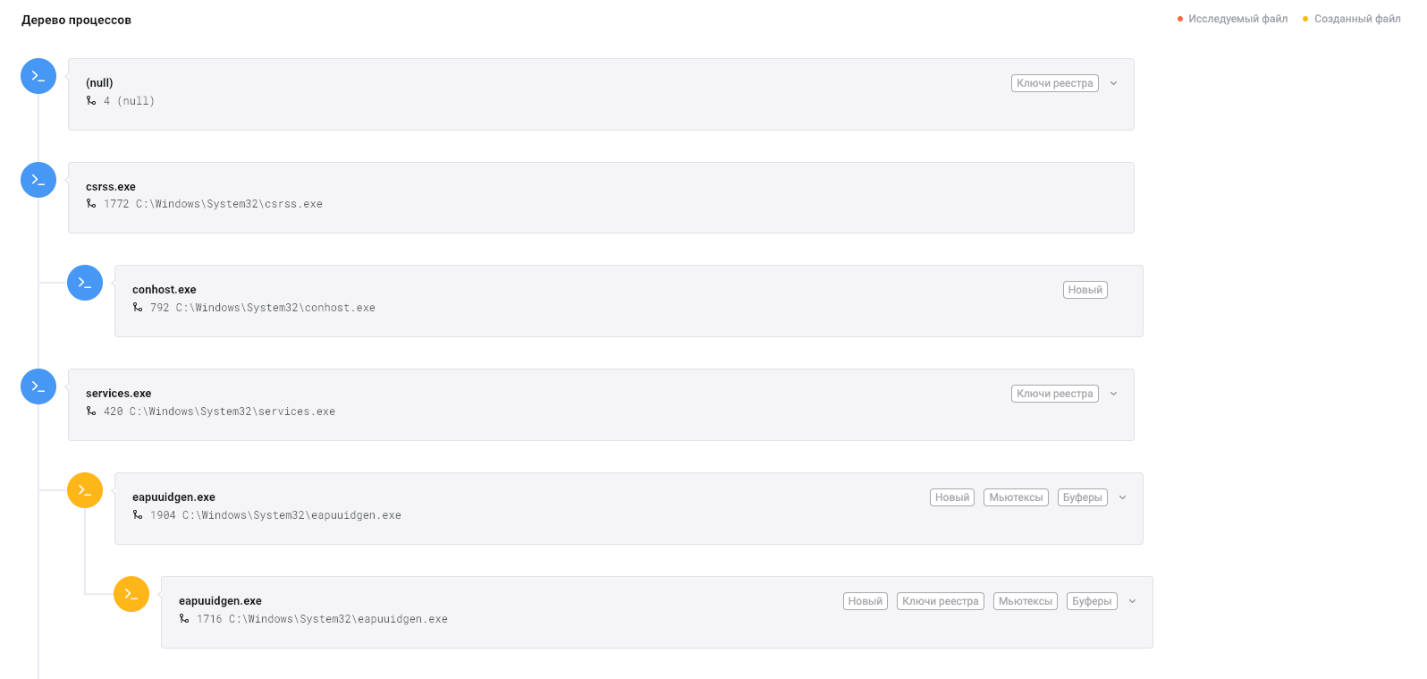
В блоке фиксируются детали о сетевом трафике, сгенерированном после открытия (выполнения) анализируемого объекта. В частности, в нем содержится информация о DNS- и HTTP-запросах и доступна возможность скачивания PCAP-файла с полным дампом данных запросов.



Сетевая активность

**Дерево процессов**

В блоке содержится дерево процессов в состоянии после запуска объекта анализа. Применяется цветовая легенда: Красным цветом выделяются процессы исследуемого объекта, желтым - процессы созданных (дропнутых) файлов. При клике на любой из процессов можно получить детали по активности процесса и вносимых системных изменениях.



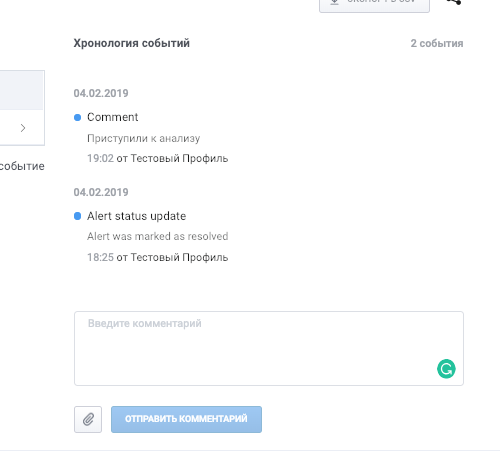
Дерево процессов

#### 6.2.2.3. Хронология событий

Описывает общие события по алерту, начиная с первого события связанного с алертом и продолжая последующей работой ведущейся по данному инциденту. Включает в себя комментарии по работе с данным инцидентом.

**Реагирование на инциденты**

При реагировании на алерт, рекомендуется оставлять комментарии. Для добавления вложений необходимо нажать на кнопку Attach.png (37Ã38)



Фильтры алертов

Для закрытия тикета, требуется отметить галочкой напротив события и нажать на **пометить решенными.**

Если же событие является ложноположительным, то необходимо нажать на **пометить ложными.**

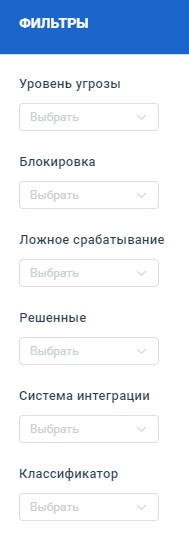
**Блокировать заражённый хост**

Данный функционал доступен только при наличии TDS Endpoint установленного на ПК. После активации блокирует все входящие и исходящие сетевые соединения ПК за исключением общения с TDS HuntBox.

### 6.2.3. Фильтры

**Фильтры типов**

По кнопке фильтры в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтры алертов

**Доступные фильтры для алертов:**

* Уровень угрозы - выбор алертов с выбранным уровнем угроз:
  + Низкий.
  + Средний.
  + Критический.
  + Пусто.
* Блокировка - статус файлов:
  + Да - отображать только заблокированные файлы.
  + Нет - отображать только незаблокированные файлы.
* Ложное срабатывание - false-postitive срабатывания.
  + Да - отобразить только срабатывания помеченные как ошибочные.
  + Нет - убрать все ложные срабатывания из выборки алертов.
  + Пусто - отображать ложные алерты в общей выборке.
* Решенные - отображение разрешенных алертов:
  + Да - отображать только решённые.
  + Нет - убрать все решенные из общей выборки алертов.
  + Пусто - отображать решенные алерты в общей выборке.
* Система интеграции - выбор алертов содержащих в себе события выбранного способа интеграции:
  + Сетевой трафик - события из анализируемого SPAN трафика.
  + Endpoint - события с ПК с установленной компонентой TDS Endpoint.
  + Почтовый сервер - события полученные после анализа почтовых сообщений при SMTP интеграции
  + Почтовый ящик - события полученные после анализа почтовых сообщений при BCC интеграции
  + ICAP-сервер - события полученные при анализе файлов от ICAP клиентов
  + Файловый сканер - события полученные при анализе файлов файловых хранилищ
  + Пусто - отображать алерты всех типов событий в выборке.
* Классификатор - выбор алертов содержащих события от выбранной подсистемы(компоненты) TDS :
  + Sensor - события от сенсоров.
  + Polygon - события из "песочницы" TDS Polygon.
  + Endpoiont - события с хостов с установленной компонентов TDS Endpoint.
  + Пусто - отображать алерты всех типов подсистем в выборке.

**Фильтры дат и текста**

По мимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям алертов и событий. (рис. Фильтр по датам и полям событий)

Data_text_filtering.jpg (519Ã36)

Фильтр по датам и полям событий

## 6.3. Расследование

Данный раздел предоставляет информацию о всех обработанных письмах и файлах в TDS Polygon, подключенными к TDS HuntBox, а также предоставляет информацию о хостах, на которых установлен TDS Endpoint. Раздел состоит из следующих подразделов:

* Письма
* Файлы
* Компьютеры

### 6.3.1. Письма

Раздел содержит всю информацию по почтовому трафику. В разделе отображаются все почтовые сообщения, прошедшие анализ в системе, в том числе и не имеющие вредоносных показателей. Раздел предоставляет возможность управлять карантином писем, в случае использования MTA-режима.

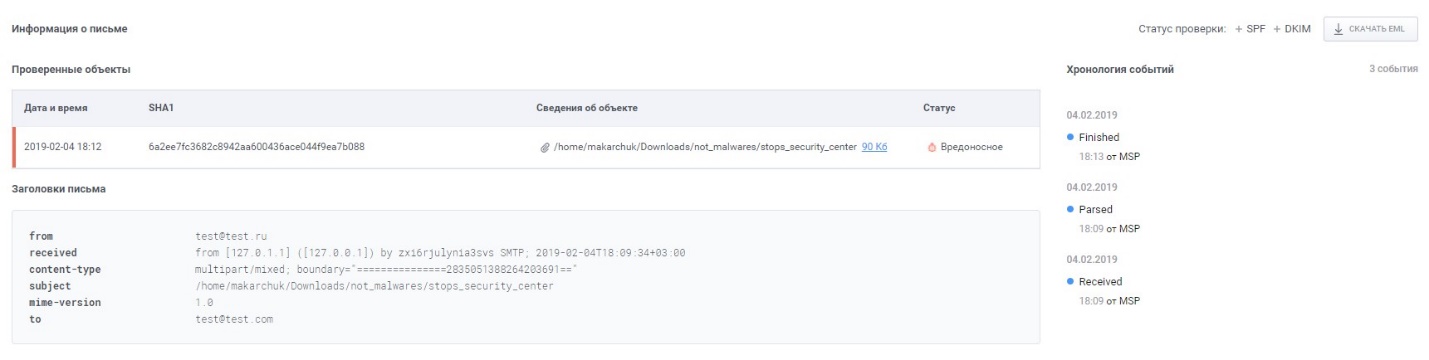
#### 6.3.1.1. Общие данные по письмам

Раздел состоит из списка, каждый пункт которого представляет из себя почтовое сообщение. В списке предоставляются общие данные по письмам:

* Дата создания - время и дата письма, полученного на анализ.
* Сенсор - наименование сенсора через который происходит анализ письма. Рядом с именем сенсора указывает тег, указывающий на способ почтовой интеграции данного сенсора (BCC, MTA, MAILBOX, SPAN)
* От кого - источник письма.
* Кому - адрес назначения письма.
* Тема - Тема письма.
* Статус - атрибут, служащий для отображения информации о текущем статусе по анализу письма:
  + Безопасный - в ходе поведенческого анализа, признаки вредоносной активности не выявлены.
  + Проверяется - письмо находится в процессе анализа.
  + Вредоносный - в поведенческих маркерах письма были выявлены признаки вредоносного программного обеспечения.
  + Заблокированное - письмо заблокировано и находится в карантине (применяется при MTA интеграции)
  + Принудительное - письмо выведено из карантина администратором комплекса и отправлено оригинальному получателю (применяется при MTA интеграции)

**Информация о письме**

Раскрывая отдельный пункт списка писем, становится доступным детальная информация о почтовом сообщении. А также в правом верхнем углу находятся данные о проверке SPF, DKIM записей и возможность скачать почтовое сообщение в формате EML (кнопка скачать eml), в случае если письмо признано вредоносным.



Информация о письме

* **Проверенные объекты**

Предоставляет список проверенных объектов, вложенных в почтовое сообщение. Данные по объектам:

* + Дата и время - время окончания проверки данного объекта системой поведенческого анализа.
  + SHA1 - хэш сумма объекта в формате SHA1.
  + Сведения об объекте - имя объекта и его размер. В случае если объект признан вредоносным, размер объекта становится активной ссылкой на сам объект. По нему можно получить файл для дополнительного анализа.
  + Статус - вредоносное или безопасное вложение.
* **Заголовки письма**

В данном подразделе описываются все технические SMTP заголовки почтового сообщения.

* **Хронология событий**

Предоставляет список важных событий, по почтовому сообщению, начиная с момента получения данного письма сенсором.

#### 6.3.1.2. Управление карантином

При реализации MTA режима письма, заблокированные системой попадают в карантин TDS HuntBox. Данные письма отображаются в настоящем разделе со статусом Заблокированное.

Для управления заблокированными письмами в карантине:

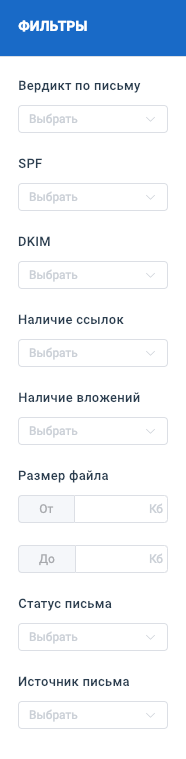
1. Выберите письма - разметив необходимое количество в крайней левой колонке.
2. Нажмите на кнопку **Принудительная отправка** в правом верхнем углу раздела.

После этого письма будут принудительно отправлены оригинальным получателям. Статус письма изменится с Вредоносное Заблокированное на Вредоносное Принудительное. О данном изменении так же будет запись в Хронологии событий.

#### 6.3.1.3. Фильтры

**Фильтры типов**

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтры писем

Доступные фильтры для алертов:

* Вердикт по письму - выбор вердикта писем:
  + Вредоносный.
  + Безопасный.
  + Проверяется.
  + Пусто.
* SPF - статусы проверки записи SPF
  + Пройдена - отображать только письма, отправители которых прошли SPF.
  + Не пройдена - отображать только незаблокированные файлы.
  + Отсутствует - SPF запись у отправителя отсутствует.
  + Пусто - отображать все.
* DKIM - статусы проверки записи DKIM
  + Пройдена - отображать только письма, отправители которых прошли SPF.
  + Не пройдена - отображать только незаблокированные файлы.
  + Отсутствует - DKIM запись у отправителя отсутствует.
  + Пусто - отображать все.
* Наличие ссылок - отображение писем в которых есть ссылки.
  + Есть - ссылки в письме присутствуют.
  + Отсутствует - ссылки в письме отсутсвуют.
  + Пусто - отображать все.
* Наличие вложений - отображение писем в которых есть вложения.
  + Есть - вложения в письме присутствуют.
  + Отсутствует - влодения в письме отсутсвуют.
  + Пусто - отображать все.
* Размер файла - указать размер вложений:
  + От
  + До
* Статус письма
  + Получено - письмо получено сенсором.
  + Не обработано - письмо находится в очереди на обработку.
  + Обработано - письмо обработано и готово к отправке на анализ в песочницу.
  + Отправлено - файл отправлен в песочницу на анализ.
  + Проанализировано - файл проанализирован.
  + Байпасс - письмо слишком долго висело в системе(настройка “Таймаут проверки писем (мин.) и было отправлено адресату до завершения работы с ним.
  + Принуд. доставка - письмо было доставлено пользователю принудительно, с помощью на
  + Анализ завершен - работа с письмом в системе завершена. Событие Finished в ленте.
  + Белый список - письма не были проанализированы, т.к. отправитель находится в белом списке.
  + Ошибка - любая ошибка с письмом. В событии обозначена причина этой ошибки.
* Источник - фильтрация писем по способу почтовой интеграции
  + SPAN - попытки сбора почтовых сообщений из SPAN трафика
  + MAILBOX - интеграция системы через почтовый ящик по POP3/IMAP, на который предварительно перенаправляются копии почтовых сообщений для анализа
  + MTA - интеграция в inline-режиме
  + BCC - интеграция через приём SMTP копии входящего потока почтовых сообщений

**Фильтры дат и текста**

По мимо данного типа фильтров доступен общий фильтр по датам с возможностью текстового запроса по всем полям почтовых событий. (рис. Фильтр по датам и полям событий)

Data_text_filtering.jpg (519Ã36)

Фильтр по датам и полям событий

### 6.3.2. Файлы

Раздел содержит всю информацию о файлах, которые были пережданы системе TDS для поведенческого анализа.

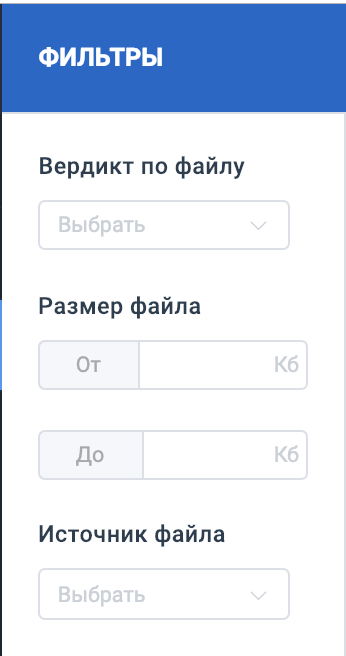
#### 6.3.2.1. Общие данные по файлам

Раздел состоит из списка, каждый пункт которого представляет из себя объект поведенческого анализа (файл). В списке предоставляются общие данные по файлам:

* Дата создания - время и дата файла, полученного на анализ.
* Сенсор - наименование сенсора через который происходит анализ файла. Рядом с именем сенсора указывает тег, указывающий на способ почтовой интеграции данного сенсора (BCC, MTA, MAILBOX, SPAN)
* Источник файла - указывается тег, указывающий на способ получения файла (смотри Фильтры файла)
  + От - источник файла.
  + Кому - адрес назначения.
* Имя файла - имя объекта.
* SHA1 - хеш-сумма файла.
* Статус - атрибут, служащий для отображения информации о текущем статусе по анализу файла:
  + Безопасный - в ходе поведенческого анализа, признаки вредоносной активности не выявлены.
  + Обработка - файл находится в процессе анализа.
  + Вредоносный - в поведенческих маркерах письма были выявлены признаки вредоносного программного обеспечения.

#### 6.3.2.2. Фильтр

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтры файлов

Доступные фильтры для файлов:

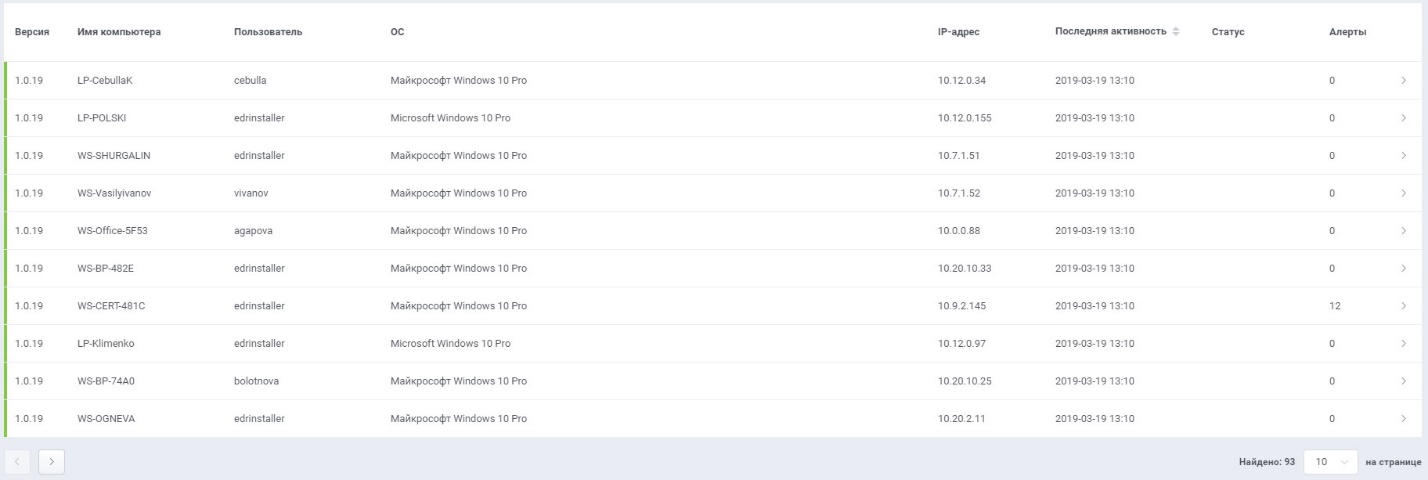
* Вердикт по файлу:
  + Безопасный
  + Вредоносный
  + Проверяется
* Размер файла
  + От
  + До
* Источник файла - фильтрация по типу используемого протокола при перехвате файла в сетевом потоке
  + BRO - используется BRO фильтр
  + HTTP
  + FTP
  + ICAP
  + MAIL - используется один из протоколов почтовой интеграции
  + SMB

### 6.3.3. Компьютеры

В данном разделе представлен список компьютеров, подключенных с помощью TDS Endpoint к HuntBox. По каждому ПК предоставляются общие данные по системе и используемому оборудованию, а также алерты в чьих артефактах участвовал данный ПК.

#### 6.3.3.1. Список компьютеров - общие сведения

В списке представлены все когда-либо подключавшиеся ПК к HuntBox.



Список компьютеров

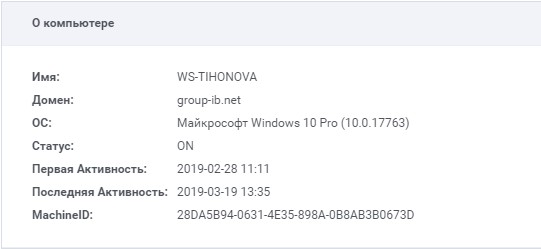
Общая информация по компьютерам:

* Версия - версия TDS Endpoint установленного на ПК
* Имя компьютера - сетевое / доменное имя ПК
* Пользователь - последний авторизованный пользователь ОС ПК
* ОС - используемая версия операционной системы ПК
* IP-адрес - первый адрес в списке сетевых адресов ПК
* Последняя активность - дата последней активности endpoint
* Статус
* Алерты - количество связанных с данным ПК алертов

#### 6.3.3.2. Информация о компьютере

При открытии выбранного компьютера система предоставляет все данные собранные о системе.

##### 6.3.3.2.1. О компьютере

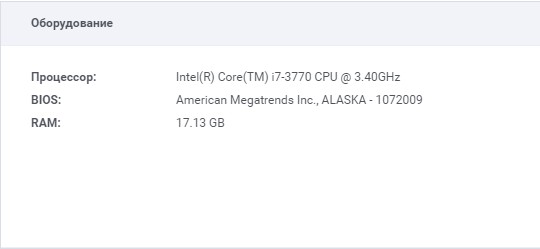


О компьютере

Доступная информация:

* Имя - сетевое / доменное имя ПК
* Домен - домен ПК в Active Directory
* ОС - полная версия используемой операционной системы
* Статус - ON/OFF состояние ПК
* Первая активность - первый отстук TDS Endpoint в систему HuntBox
* Последняя активность - последний зафиксированный отстук TDS Endpoint
* MachineID - идентификатор ПК в системе HuntBox. Формируется TDS Endpoint-ом.

##### 6.3.3.2.2. Оборудование

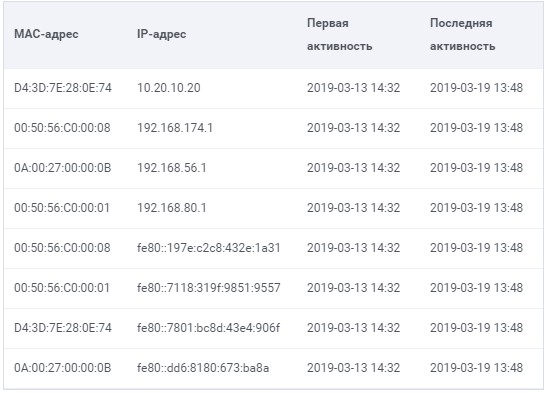


Оборудование

Доступная информация:

* Процессор - полное техническое наименование используемого центрального процессора
* BIOS - наименование BIOS
* RAM - количество оперативной памяти

##### 6.3.3.2.3. Сеть

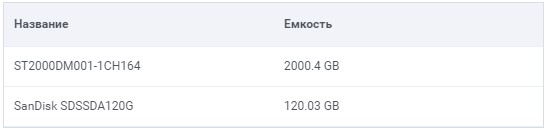


Сеть

Доступная информация:

* МАС-адрес
* IP-адрес
* Первая активность - первая сетевая активность интерфейса, зафиксированная с момента установки TDS Endpoint
* Последняя активность - крайняя сетевая активность интерфейса, зафиксированная с момента установки TDS Endpoint

##### 6.3.3.2.4. Хранилище

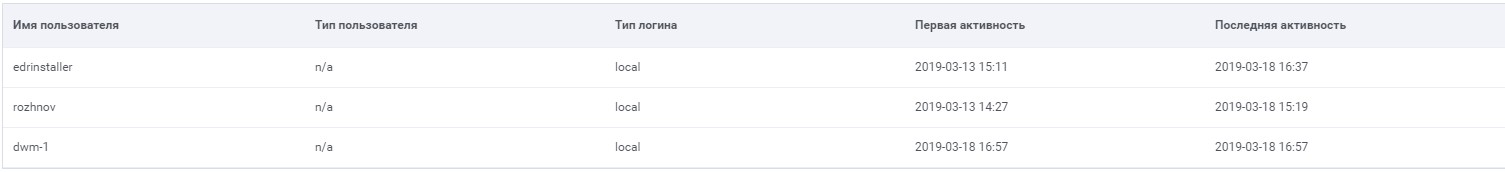


Хранилище

Доступная информация: Предоставляет данные об установленных накопителях в системе

##### 6.3.3.2.5. Пользователи

Список авторизованных, с момента установки Endpoint, пользователей.



Пользователи

Доступная информация:

* Имя пользователя
* Тип пользователя - Доменный/не доменный пользователь
* Тип логина - локальный или удалённый логин
* Первая активность
* Последняя активность

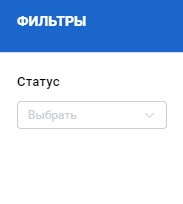
##### 6.3.3.2.6. Алерты

Представляет список алертов в чьих событиях встречался MachineID данного ПК. (Полностью идентичен одноимённому разделу)

#### 6.3.3.3. Фильтры

**Фильтры типов**

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтры компьютеров

Доступные фильтры для компьютеров:

* Статус - статус работы endpoint на компьютере:
  + Online
  + Offline

**Фильтры текста**

По мимо данного типа фильтров доступен общий фильтр c возможностью текстового запроса по всем полям компьютеров. Например, по имени пользователя. (рис. Фильтр по полям)

Text_filter.jpg (310Ã38)

Фильтр по полям

## 6.4. Настройки

В данном разделе расположены настройки управления всех модулей ПО.

### 6.4.1. Устройства

Пункт Apppliances служит для предоставления возможности настроек всех компонентов TDS подключённых к TDS HuntBox.

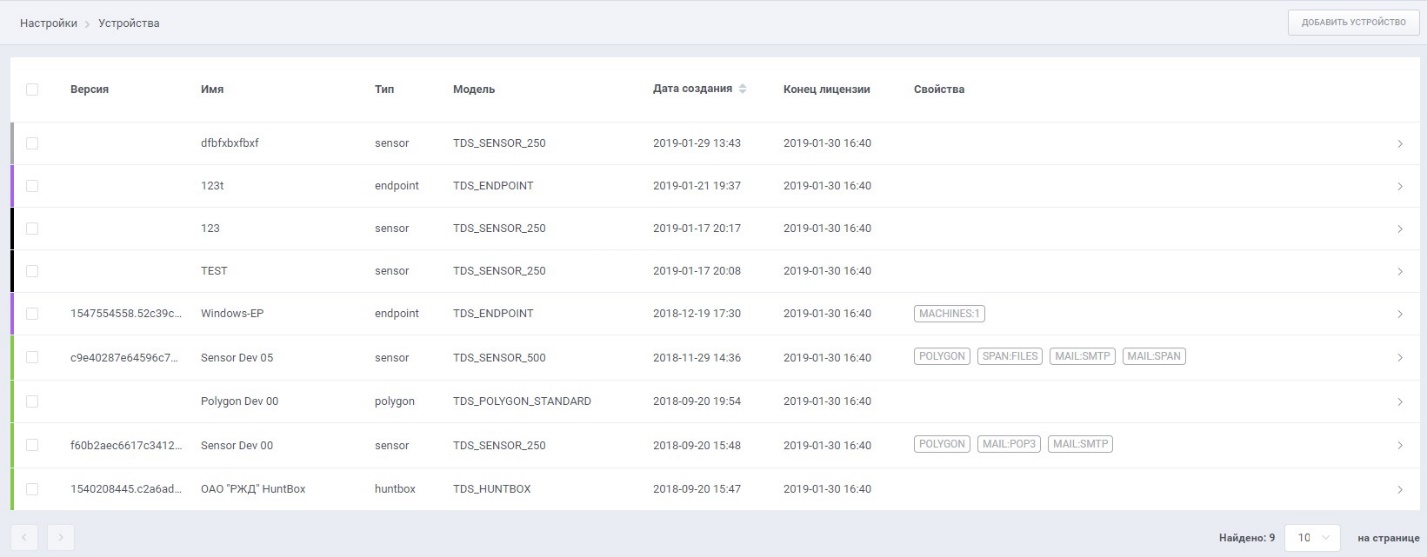
Доступные компоненты:

* TDS Sensor
* TDS Polygon
* TDS HuntBox
* TDS Endpoint

### 6.4.1.1 Общие данные по устройствам

Доступные данные:

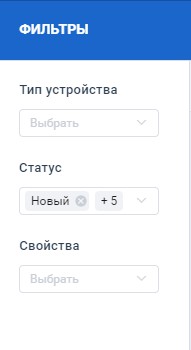
* Версия - версия установленного ПО компоненты TDS
* Имя
* Тип - определяется типом компоненты TDS
* Модель - лицензия, заданная исходя из типа компоненты TDS
* Дата создания - дата создания новой сущности в HuntBox
* Конец лицензии - дата окончания действия лицензии
* Свойства - теги определяющие активированные настройки компоненты TDS



Общие данные по устройствам

### 6.4.1.2. Фильтр

По кнопке фильтра в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Меню фильтрации устройств

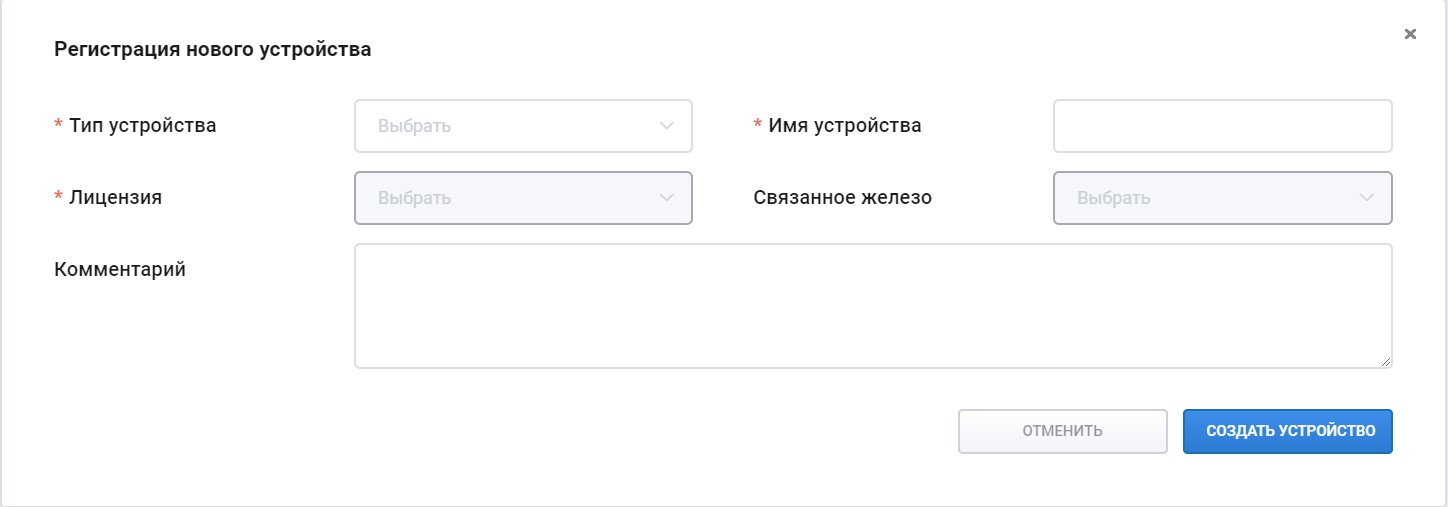
Параметры Статус и Свойства аддитивные - возможен выбор нескольких значений в рамках одного параметра. Доступные фильтры:

* Тип устройства
  + Sensor
  + Polygon
  + Huntbox
  + Endpoint
* Статус
  + Новый
  + Активен
  + В архиве
  + Выключен
  + Проблемы с подключением
  + Проблемы с производительностью
  + Проблемы с интеграцией
* Свойства
  + POLYGON - указывает на интеграцию TDS Sensor с TDS Polygon для поведенческого анализа
  + SPAN:FILES - указывает на попытку сенсора на сбор файлов из SPAN сессий для поведенческого анализа
  + MAIL:SMTP - указывает на интеграция TDS Sensor с почтовым сервером по протоколу SMTP
  + MAIL:SPAN - указывает на попытку сенсора на сбор почтовых сообщений из SPAN сессий
  + MAIL:POP3 - указывает на интеграцию TDS Sensor с почтовым сервером по протоколу POP3
  + MAIL:IMAP - указывает на интеграцию TDS Sensor с почтовым сервером по протоколу IMAP
  + MAIL - указывает на включенный анализ почтовых сообщений в TDS Sensor

### 6.4.1.3. Добавить устройства

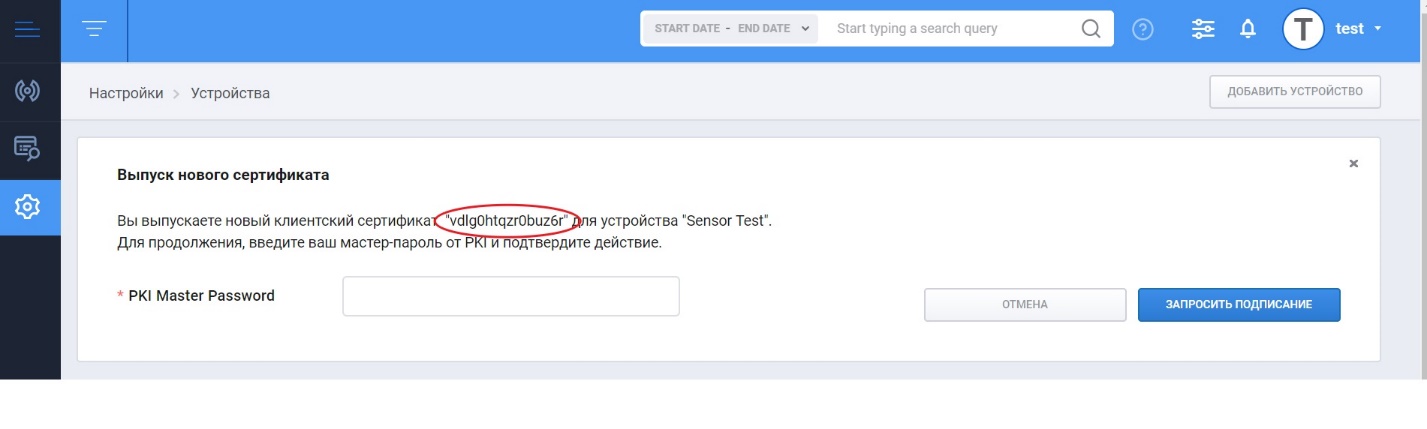
Для регистрации нового устройства нажмите кнопку **добавить устройство**

* Тип устройства - Sensor / Polygon
* Лицензия - от выбора типа лицензии зависит производительность зарегистрированного устройства
* Имя устройства
* Связанное железо(опционально) - связать с устройством из тех что ещё не зарегистрированы на HuntBox
* Комментарий



Регистрация нового устройства

При нажатии на кнопку Создать Устройство диалоговое окно предложит ввести мастер пароль для получения уникального идентификатора(UID) создаваемого устройства.

 Создание UUID для нового устройства

**Запросить Подписание** подписывает UUID нового устройства мастер-паролем.

Таким образом после создания устройства в интерфейсе HuntBox становится доступным ряд настроек и параметров новой сущности. Главным параметром является UUID (или **Номер лицензии**). UUID используется для активации нового устройства и его синхронизации с HuntBox. Остальные настройки и параметры описываются в разделе Редактирования настроек соответствующего модуля.

При регистрации нового устройства необходимо различать создание устройства и "активация и подключение" к HuntBox:

* Создание устройства - это процесс создания новой сущности внутри web-интерфейса HuntBox, а также подписания UID мастер-паролем
* Активация и подключение устройства к HuntBox - это процесс настройки на TDS Sensor/ TDS Polygon - его активации и подключения к HuntBox.

## 6.4.2. Редактирование настроек TDS HuntBox

На странице представлены общие показатели по работе TDS HuntBox:

**Общая информация**

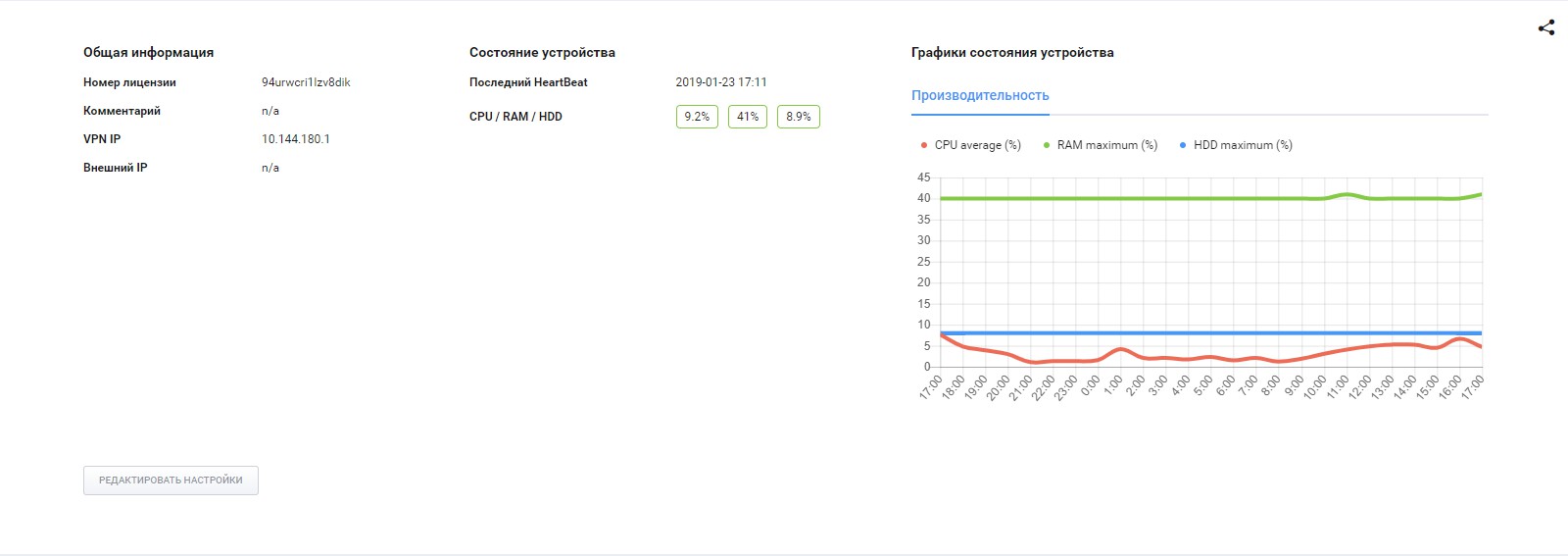
* Номер лицензии - получен при покупке или тестировании решения
* Комментарий
* VPN IP - адрес VPN сервера для коммуникации HuntBox с подключаемыми модулями
* Внешний IP - адрес управляющего интерфейса

**Состояние устройства**

* Последний HeartBeat
* CPU / RAM / HDD

**Графики состояния устройства**

* CPU average (%)
* RAM maximum (%)
* HDD maximum (%)



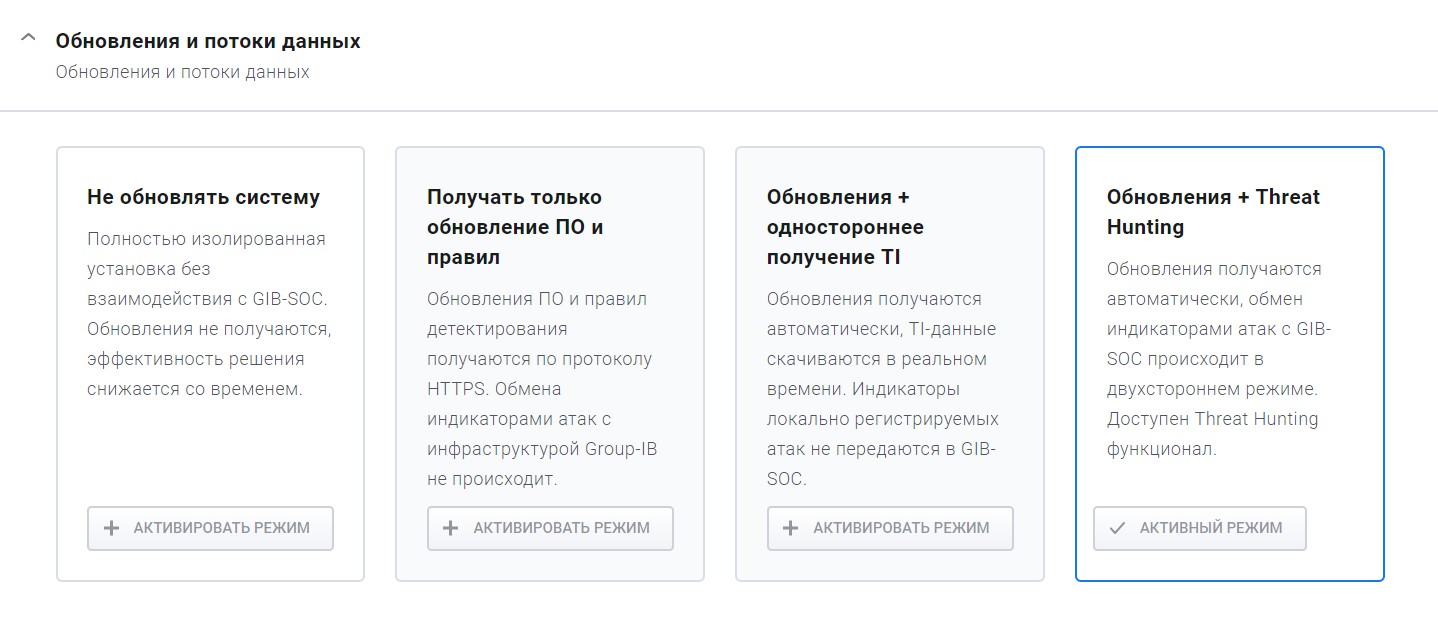
Общие показатели TDS HuntBox

По кнопке **Редактировать Настройки** доступны расширенные настройки:

* Обновления и потоки данных
* Прокси-сервер
* Сервер времени
* Сертификат web-сервера
* Настройки почтового сервера
* Сервер событий TDS Endpoint

### 6.4.2.1. Обновления и потоки данных

Данная настройка предоставляет режимы работы HuntBox определяющие принцип взаимодействия с серверами и сервисами Group-IB. Настройка определяет типы данных которыми будут обмениваться инфраструктура клиента с инфраструктурой Group-IB. Возможно задать как полностью закрытую инсталляцию, так и полностью открытую.



Описание режимов:

* **Не обновлять систему**

Данный режим подразумевает полностью закрытую инсталляцию. HuntBox никак не взаимодействует с серверами Group-IB.

Обновление программного обеспечения, IOC и сетевых сигнатур не производится.

* **Получать только обновление ПО и правил**

Данный режим позволяет оборудованию получать обновления ПО для HuntBox и всех подключённых к нему устройств.

Обновление индикаторов и сигнатур не производится.

В данном режиме нет возможности загружать данные по инфраструктуре атакующих и отсутствует взаимодействие с SOC Group-IB для получения поддержки по инцидентам в режиме 24/7.

Обновления доставляются с сервера Group-IB - 92.53.76.98:443/tcp

* **Обновления + одностороннее получение TI**

Данный режим дополняет предыдущий и позволяет получать обновление индикаторов атак и сигнатур для подключённых к Huntbox устройств.

В данном режиме невозможно получать мониторинг и поддержку от CERT (SOC Group-IB).

В данном режиме имеется возможность загружать данные по инфраструктуре атакующих вручную.

Для получения данных по инфраструктуре атакующих HuntBox необходим доступ до сервера - tdsi.group-ib.com:443/tcp

* **Обновление + Threat Hunting**

Данный режим дополняет предыдущий и позволяет выгружать данные об обнаруженных инцидентах в сервера Group-IB.

Имеется возможность автоматически получать информацию по инфраструктуре атакующих.

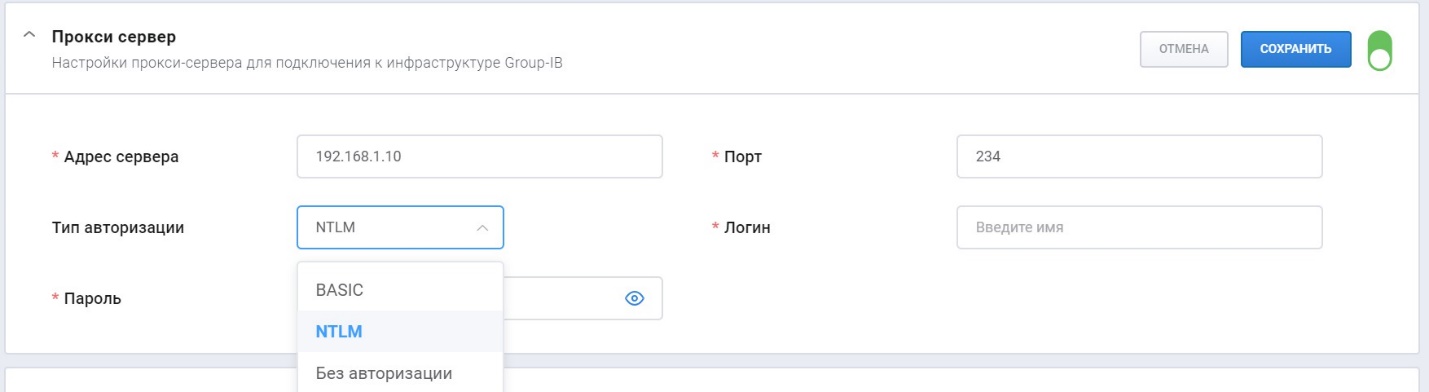
В данном режиме имеется имеется возможность мониторинга и поддержки от CERT Group-IB в режиме 24/7.

Для получения данных по инфраструктуре преступников и связи с SOC Group-IB,а так же для получения обновлений - tdsi.group-ib.com:443/tcp

### 6.4.2.2. Прокси-сервер

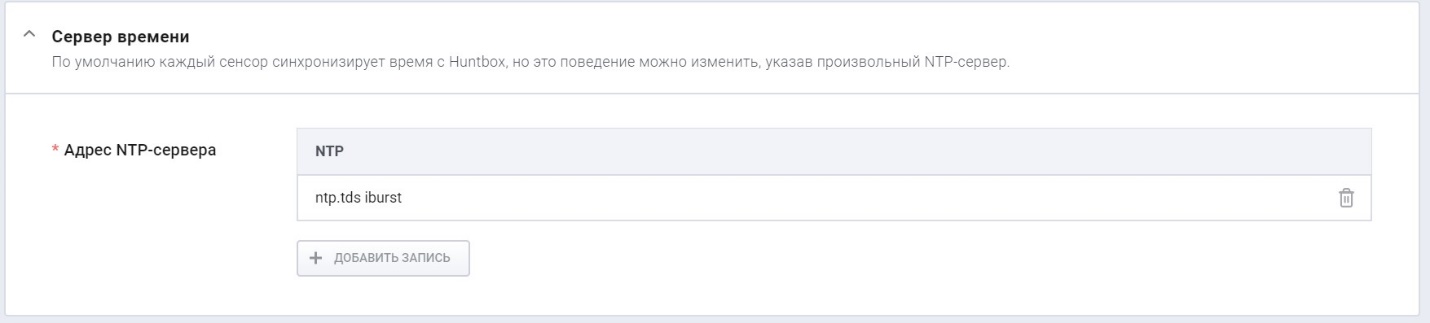
Для работы HuntBox во всех режимах исключая первый (Не обновлять систему) системе необходима связь с серверами Group-IB. Данное подключение может осуществляться через прокси сервера. Доступные настройки:

* Адрес сервера - IP адрес прокси
* Порт
* Тип авторизации - поддерживается базовая и NTLM аутентификации. Так же возможно выбрать прокси без авторизации.
* Задайте логин и пароль при выборе базовой или NTLM аутентификации.



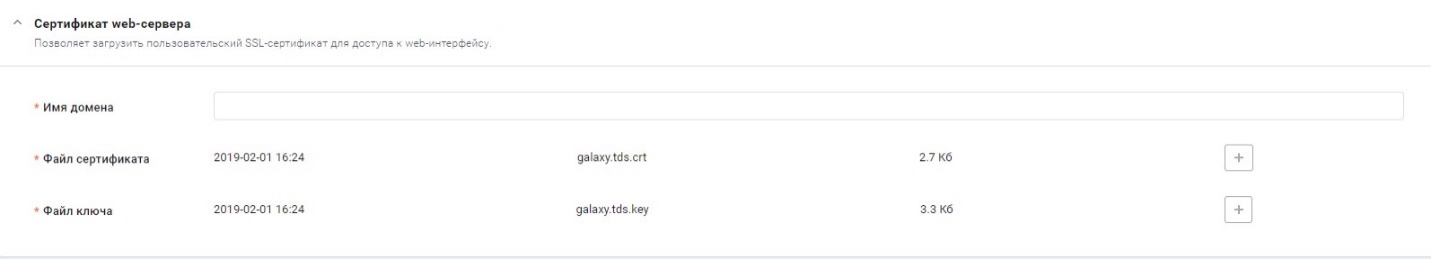
### 6.4.2.3. Сервер времени

В настройках сервера NTP возможно задать адрес сервера синхронизации времени для всех сенсоров, подключенных к данному HuntBox серверу. Все подключенные TDS Sensor и TDS Polygon синхронизируют своё время с HuntBox.



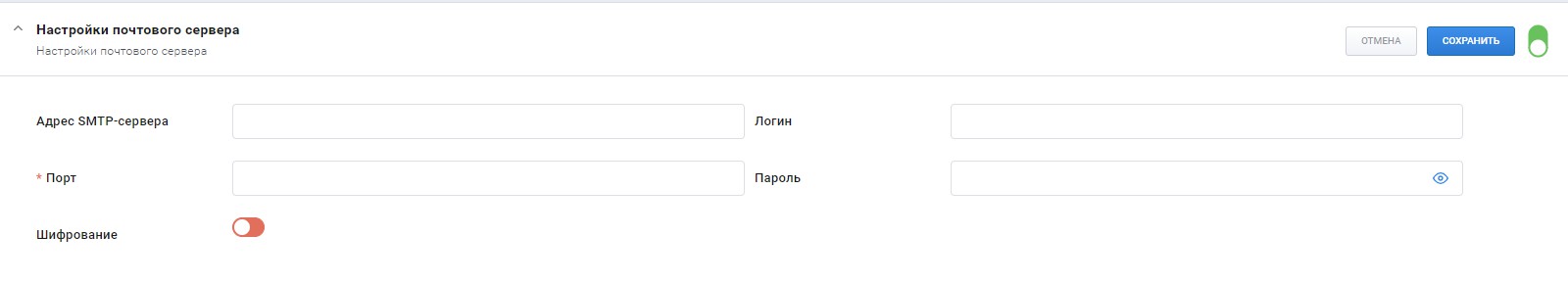
### 6.4.2.4. Сертификат web-сервера

Для доступа в веб-интерфейс возможно задать пользовательские SSL-сертификаты. Сертификат и ключ загружается в форматах .crt и .key



### 6.4.2.5. Настройки почтового сервера

Данная настройка задаёт почтовый сервер и аккаунт для рассылки сообщений для администраторов комплекса. Рассылка осуществляется индивидуально по сработанным инцидентам. Рассылка настраивается в соответствующих настройках аккаунта администратора в разделе Пользователи.

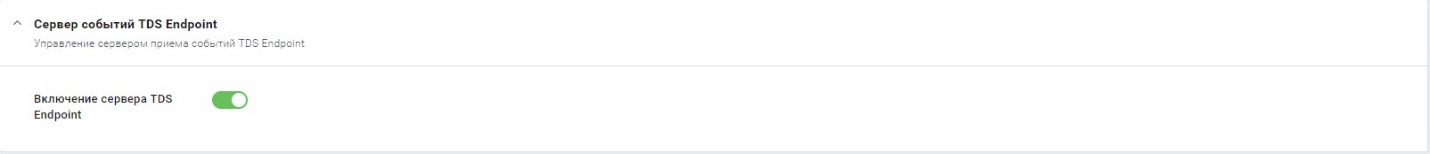


SMTP сервер для оповещений администратора

### 6.4.2.6. Сервер событий TDS Endpoint

Сервер управления TDS Endpoint.

Активирует сервер для агентов на конечных станциях с ОС Windows, следящих за системной активностью и отправляющих события на TDS HuntBox для анализа и последующей реакции. Является решением типа endpoint detection and response.



## 6.4.3. Редактирование настроек TDS Sensor

На странице представлены общие показатели по работе подключенного TDS Sensor. Данные по каждому сенсору доступны при раскрытии карты сенсора в списке подключённых устройств.

**Общая информация**

* Номер лицензии - получен при покупке или тестировании решения
* Комментарий
* VPN IP - адрес внутри VPN туннеля, получаемый при подключении TDS Sensor к TDS HuntBox для управляющих коммуникаций
* Внешний IP - адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)

**Состояние устройства**

* Последний HeartBeat - последний замеченный heartbeat с данного устройства
* Последняя активность - крайнее время активности VPN между сенсором и управляющим HuntBox
* Длительность - временной отрезок в течении, которого между сенсором и HuntBox был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
* CPU / RAM / HDD
* Загрузка канала
* Дропы в ядре / на интерфейсе

**Графики состояния устройства**

Предоставляют двумерный график на временном отрезке в 24 часа по следующим показателям:

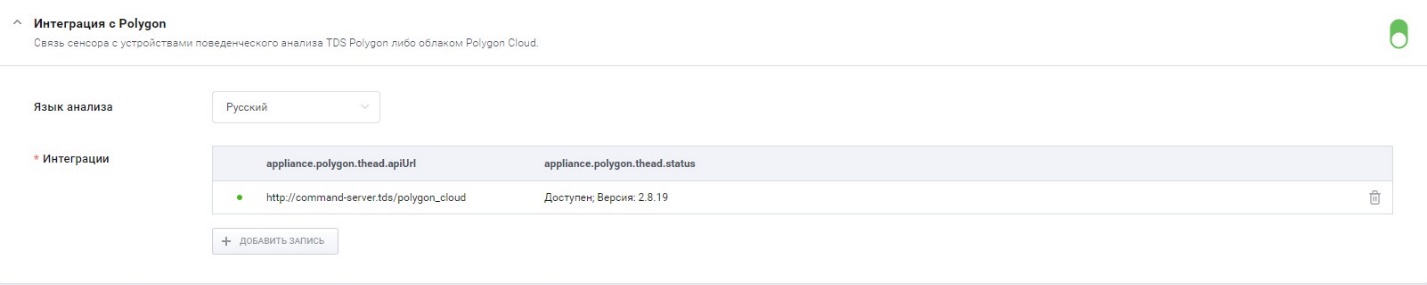
* Производительность - задействованные ресурсы системы
  + CPU average (%)
  + RAM maximum (%)
  + HDD maximum (%)
* SPAN - средняя загрузка канала приёма копии трафика, аккумулированная по всем SPAN интерфейсам сенсора
* MSP - статистика по количеству принятых для анализа почтовых сообщений при наличии почтовой интеграции
  + Envelopers - статистика по принятым письмам
  + Files - статистика файлов, приложенных к данному количеству писем
  + Polygon Queue - размер очереди на TDS Polygon к выбранному моменту времени
* DROPS - отбрасываемые пакеты на физическом интерфейсе приёма копии трафика



Общие показатели TDS Sensor

### 6.4.3.1. Интеграция с Polygon

Данная настройка предлагает возможность интегрировать выбранный TDS Sensor c определенным TDS Polygon для осуществления функций поведенческого анализа.



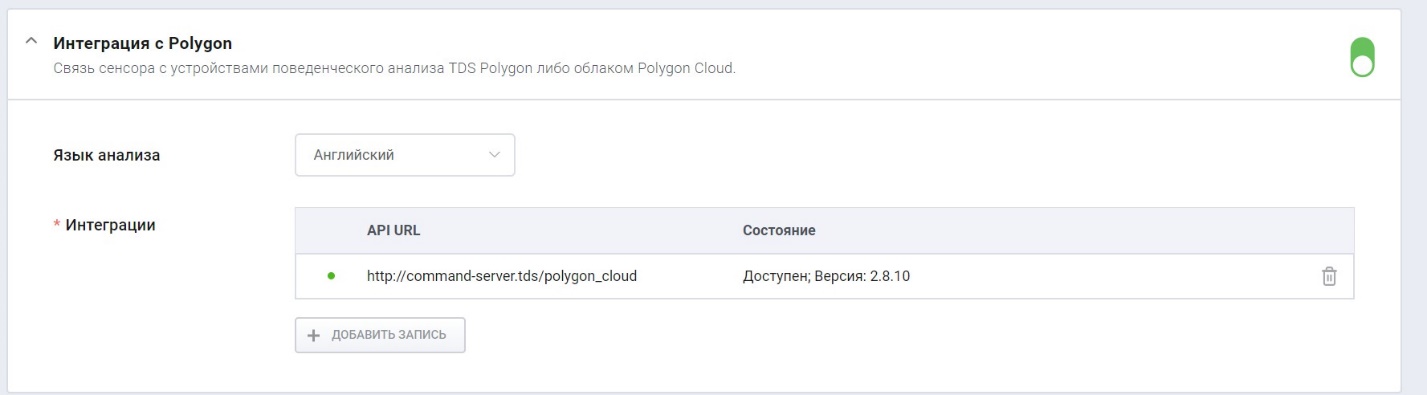
Интеграция TDS Sensor с TDS Polygon

* **Интеграции**

В меню задаётся запись в виде доменного имени или IP адреса TDS Polygon. Возможно задать больше чем одну запись, дабы обеспечить распределение нагрузки по поведенческому анализу. Управление очередью производится на стороне сенсора. Сенсор делает опрос всех подключённых к нему TDS Polygon на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

* **Язык анализа**

Задаёт использование определённых образов операционных систем внутри подключённых TDS Polygon. Данные операционные системы будут настроены для поддержания защиты от актуальных угроз в регионах с выбранной языковой системой (По умолчанию поддерживаются Русский и Английский языки).



Интеграция TDS Sensor с TDS Polygon прошла успешно

**Использование облачного TDS Polygon**

Для использования Polygon Cloud (облачной версии TDS Polygon) используется следующая запись:

<http://command-server.tds/polygon_cloud>

### 6.4.3.2. Почтовый сервер

Настройка позволяет задать основной способ интеграции приёма почтовых сообщений.

**Глубина хранения писем (дни)**

Вне зависимости от выбора способа интеграции необходимо задать параметр глубины хранения.

Он определяет время в сутках в течении которого почтовые сообщения будут храниться на TDS Sensor для ретроспективного анализа почтовых сообщений и вложений в них.

#### 6.4.3.2.1. Приём копии сообщений по SMTP

В данном режиме сенсор не будет являться точкой пересылки почтовых сообщений. И будет ожидать приёма копии почтовых сообщений от почтовых серверов клиента. Режим анализирует почтовый поток клиента, принимаемый по протоколу SMTP.

Для анализа почтовых сообщений по протоколу POP3/IMAP перейдите в раздел настройки 6.4.3.3. Почтовый клиент



Приём копии писем

#### 6.4.3.2.2. МТА режим

В данном режиме сенсор будет являться частью почтовой системы во внедряемой инфраструктуре. И будет анализировать реальный почтовый поток клиента.

Доступные настройки:

* **Блокировать**

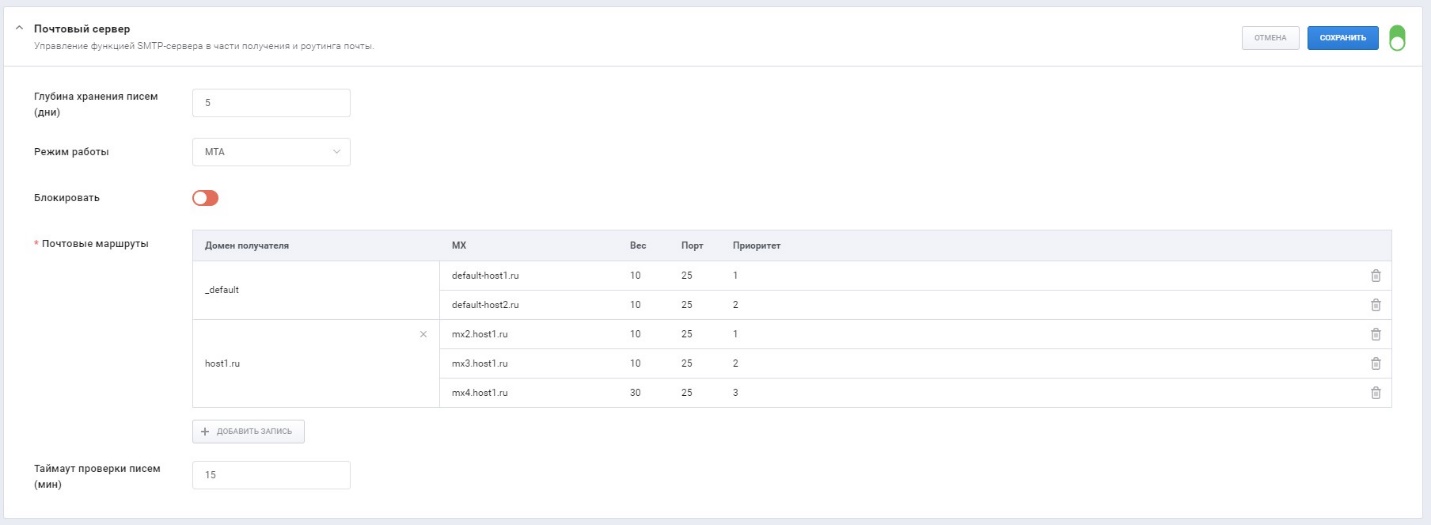
При активации блокирует письма с подозрением на целевую атаку и отправляет их в карантин сенсора. Таким образом возможно интегрировать TDS в почтовую систему в режиме MTA как с блокировкой (для обеспечения превентивной защиты от целевых атак), так и без (для обеспечения бесперебойности бизнес процессов в случае false-postivie срабатываний). Примечание: в случае использования режима работы с блокировкой, оповещения от SOC Group-IB не будут производиться при успешном блокировании письма содержащего вредоносный контент. Управление карантином осуществляется в подразделе раздела Расследования - Письма -> Управление карантином

* **Почтовые маршруты**

Позволяет задать маршрутизацию почтового трафика для следующих MTA или почтовых серверов. Таким образом возможно обеспечить приоритизацию дальнейшей пересылки почтовых сообщений, в случае наличия более одного приёмщика почтовых сообщений (MTA, EDGE, CAS).

* **Таймаут проверки писем**

Время удержания почтовых сообщений на сенсоре до отправки его следующему MTA или почтовому серверу в соответствии с настроенными почтовыми маршрутами. По умолчанию TDS Sensor ограничивает передачу сообщений до получения вердикта от TDS Sensor и TDS Polygon. Таймаут ограничивает сверху время затрачиваемое на данный процесс. Таким образом, в случае если почтовое сообщение не было проверено по истечению заданного таймаута, оно будет отправлено по почтовому маршруту без решения по анализу и будет проанализировано в ретроспективе.



МТА интеграция

**Требования к Inline интеграции**

При реализации Inline-режима необходимо учитывать критерий отказоустойчивости, поэтому реализация выглядит следующим образом:

* Установка двух TDS Sensor, служащих для приема почты по протоколу SMTP.
* При помощи протокола VRRP TDS Sensors делят один виртуальный адрес, на который поступает входящая почта.
* Один из TDS Sensor всегда находится в режиме Master (TDS Sensor, свободный от анализа сетевого трафика SPAN), второй TDS Sensor находится в режиме Backup (он же занят SPAN-трафиком).
* В случае выхода из строя основного TDS Sensor, резервный TDS Sensor в течении 2 секунд регистрирует проблему и переключается в MASTER-режим, забирая виртуальный IP-адрес себе и продолжая полноценную работу системы в части приёма почты.
* Выход из строя основного узла регистрируется в системном журнале, который передается в службу мониторинга CERT-GIB и локально по сети через Syslog в систему учета логов заказчика.

Каждое устройство должно иметь доступ к TDS HuntBox, для чего должен быть доступен следующий адрес:

IP\_address\_TDS\_HuntBox:1443/udp

Система реализует гарантированную доставку писем в течении настраиваемого времени (по умолчанию 5 минут), жестко ограничивая время анализа сверху. Если из-за образовавшейся очереди на анализ проверка писем начинает занимать больше установленного порога времени, осуществляется прямая доставка писем. При этом анализ будет завершен в любом случае.

Перед переключением входящего почтового сервера на TDS-Sensor необходимо проверить работу цепочки доставки писем. Для этого рекомендуется использовать скрипт, который предоставляют специалисты отдела внедрения Group-IB.

### 6.4.3.3. Почтовый клиент

Настройка почтового клиента позволяет TDS Sensor подключаться к почтовым серверам, хранящим клиентские письма и анализировать содержимое почтового ящика. Обратите внимание, сенсор подключается только к одному ящику почтового сервера - на данный ящик необходимо направлять копии почтовых сообщений для анализа (Организуется через внутренние BCC функции почтовых серверов или почтовых сервисов). Дополнительную информация по режиму работы возможно почерпнуть по ссылке Интеграция по POP3/IMAP.

Доступные настройки:

* **Почтовый сервер**

FQDN или сетевой адрес почтового сервера, к которому будет подключаться сенсор по протоколу POP3/IMAP.

* **Порт**

Задаётся в случае использования нестандартных портов на сервере клиента.

* **Имя пользователя**

Логин от почтового ящика, на котором агрегируется копии почтовых сообщений для анализа.

* **Пароль**

Пароль от почтового ящика

* **Протокол**

Внимание! задавая тип протоколов необходимо иметь ввиду особенности работы данных протоколов относительно хранимой на почтовом ящике корреспонденции. Подробнее ниже.

Поддерживаемые протоколы:

* **POP3**

При использовании данного протокола, вся проанализированная почта будет автоматически удаляться сенсором после скачивания почтовых сообщений из ящика. Почта удаляется безвозвратно, только при наличии достаточных прав у используемого сенсором аккаунта.

* **IMAP**

При использовании протокола, используются стандартные команды протокола на удаление закаченных из ящика почтовых сообщений.

* **Шифрование**

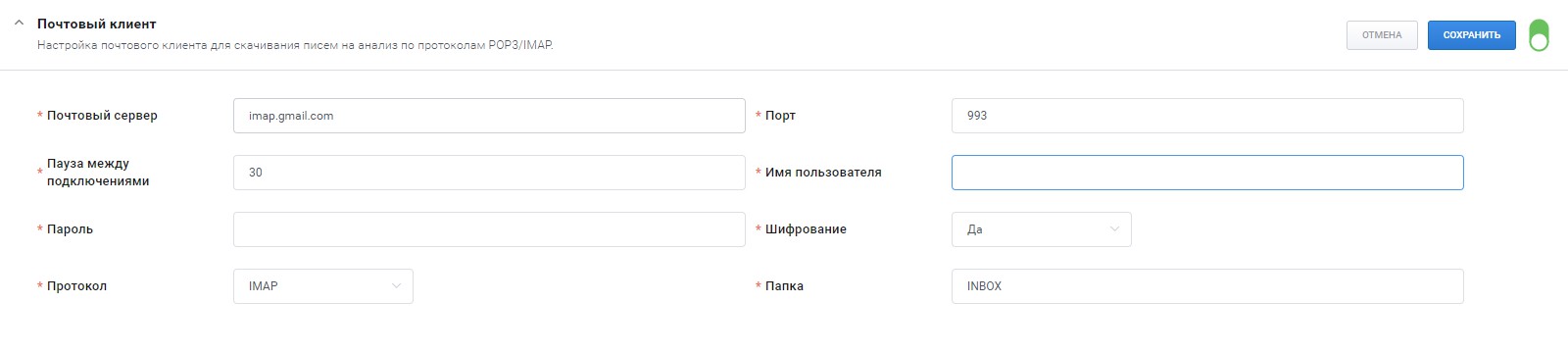
Поддерживаемые версии протоколов шифрования SSLv2, SSLv3, TLS, TLSv1, TLSv1.1, TLSv1.2. Дополнительная информация по поддержке протоколов со стороны клиентов доступна по запросу к специалистам Group-IB.

* **Пауза между подключениями**

Таймаут между подключением к почтовому ящику для скачивания почтовых сообщений. По умолчанию TDS Sensor запрашивает с почтового сервера первые 100 доступных сообщений (вне зависимости от выбранного протокола). Таким образом, если почтовый сервер не корректно обрабатывает команды на удаление от сенсора, возникнет петля.

* **Папка**

Доступно при выборе протокола IMAP. Задаёт имя папки в подключаемом почтовом ящике для скачивания сообщений.



Интеграция с почтовым ящиком

### 6.4.3.4. Стратегия работы со ссылками

При интеграции с почтовой системой сенсор будет осуществлять анализ почтовых сообщений на предмет содержания в нём ссылок на внешние ресурсы. При обнаружении ссылок TDS Sensor будет производить переходы по данным ссылкам. Переход по ссылке ограничивается только ресурсом, указанным в ссылке и не производит дальнейшее изучение ресурсы на предмет ссылок. Поэтому необходимо выбрать стратегию работы со ссылками.

Предлагаемые стратегии:

* **Консервативная**

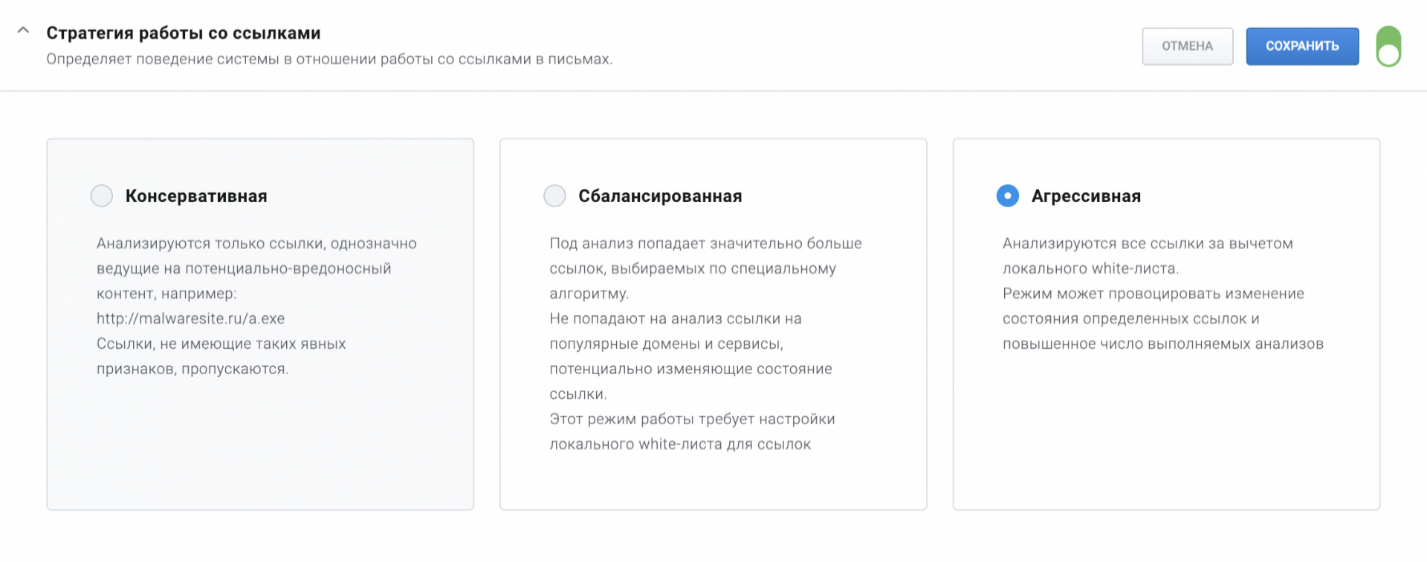
Анализируются только ссылки, однозначно ведущие на потенциально-вредоносный контент, например, http://malwaresite.ru/a.exe. Ссылки, не имеющие таких явных признаков, пропускаются.

* **Сбалансированная**

Под анализ попадает значительно больше ссылок, выбираемых по специальному алгоритму. Не попадают на анализ ссылки на популярные домены и сервисы, потенциально изменяющие состояние ссылки. Этот режим работы требует настройки локального white-листа для ссылок.

* **Агрессивная**

Анализируются все ссылки, за вычетом локального white-листа. Режим может провоцировать изменение состояния определенных ссылок и повышенное число выполняемых анализов.



### 6.4.3.5. ICAP сервер

TDS Sensor может взаимодействовать по протоколу ICAP в качестве сервера с сетевым оборудованием поддерживающий данный протокол в качестве клиентов. Например: Web Proxy, UTM, NGFW, и т.п. При таком взаимодействии ICAP сервер в пассивном режиме ожидает подключение клиентов. ICAP-клиент передает файлы для проведения поведенческого анализа с ожиданием вердикта, либо без ожидания (в зависимости от настройки блокировки). Доступные настройки:

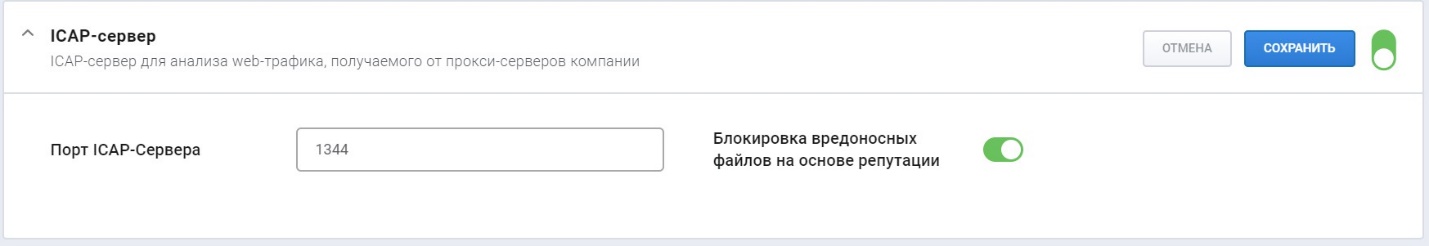
* **TCP-порт**

Порт для подключения ICAP-клиентов. На данном порту будет работать сервис ICAP-сервера.

* **Блокировать скачиваемые вредоносные файлы**

Позволяет активировать режим блокировки для ICAP-клиентов. В данном режиме ICAP-клиенты ожидают от TDS Sensor ответа по вердикту для файла по итогам поведенческого анализа на TDS Polygon. В случае, если файл вредоносный, TDS Sensor присылает ICAP-клиенту команду на блокировку проанализированного файла.

Примечание. В случае получения от ICAP-клиентов архивов или зашифрованных архивов, TDS Sensor разархивирует или попытается разархивировать шифрованный архив произведя подбор пароля по встроенному словарю. Дальнейший анализ будет производиться штатно.



### 6.4.3.6. Анализ файлов из трафика

При активации данной настройки сенсор будет пытаться получать файлы из анализируемой копии трафика и отправлять их на поведенческий анализ. При подобном способе интеграции необходимо учитывать следующие моменты:

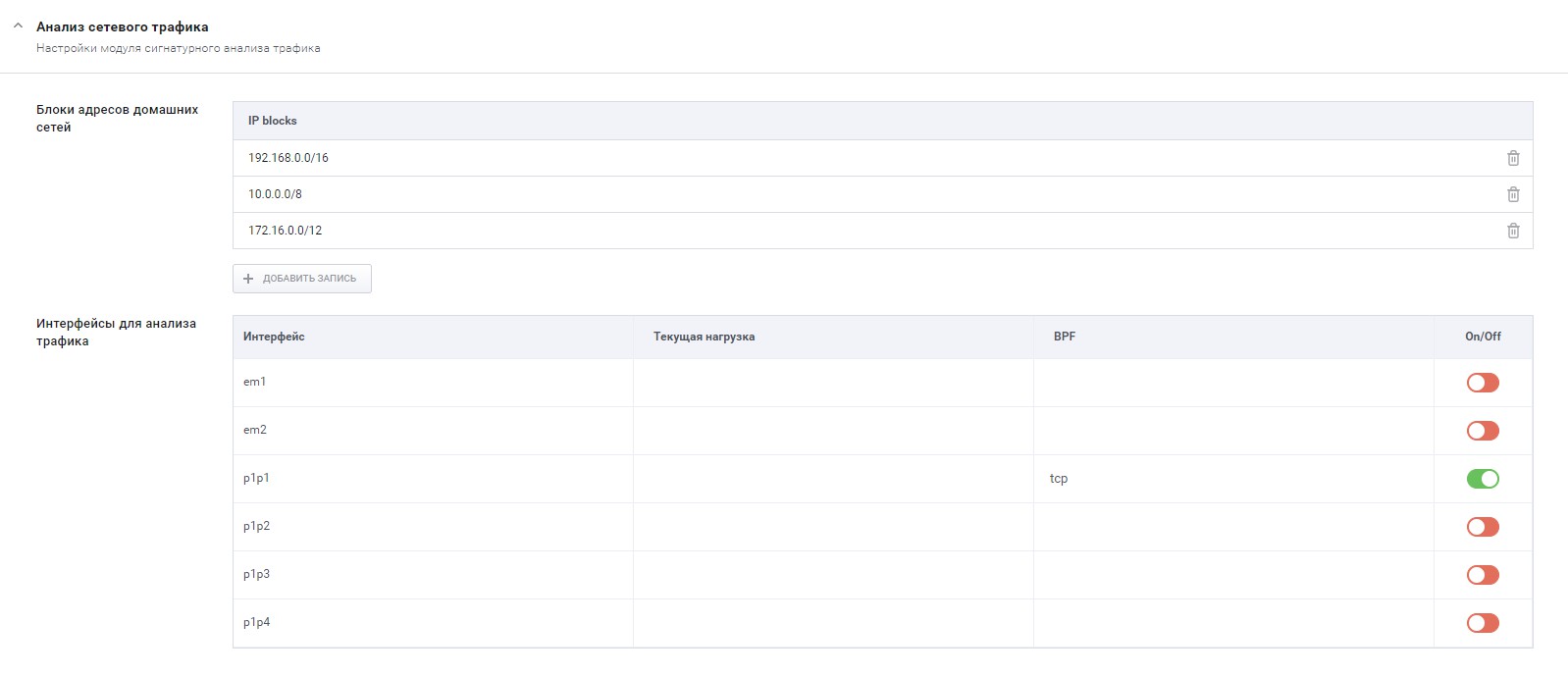
* Дропы - если зеркалирующее устройство (с которого поступают SPAN сессии) будет дропать пакеты при формировании копии трафика, то высока вероятность невозможности собрать из SPAN сессий почтовых сообщений.



### 6.4.3.7. Анализ сетевого трафика

Важнейший раздел при настройке сигнатурного анализа. Данный раздел даёт системе понимание "инородного" трафика относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGR.

Укажите локальные адреса, принадлежащие сети, а также адреса локальных Proxy. Введите список локальных подсетей и исключите из них адреса Proxy-серверов (!proxy-ip). Это позволит отличить взаимодействие с внешними узлами.



### 6.4.3.8. Экспорт данных

По умолчанию логи работы TDS Sensor отправляются и хранятся в TDS HuntBox и SOC Group-IB (в зависимости от заданного режима работы TDS HuntBox). Данная настройка позволяет дополнительно отправлять логи работы сенсора на внешние аналитические системы. Логи будут отправляться напрямую от TDS Sensor до указанных в настройке серверов. Для экспорта логов во внешние системы необходимо задать сетевой адрес, порт и протокол (UDP/TCP) сервера напротив выбранного формата. Возможно задать только один сервер для каждого доступного формата. Логи работы TDS Sensor формируются в формате syslog и затем упаковываются в указанные ниже форматы. Таким образом возможно интегрировать TDS с любой аналитической системой, которая может обрабатывать стандартный формат syslog. Доступные форматы:

* **CEF**

CEF (нативный для SIEM ArcSight), с уровнями угроз Low (1-2), Medium (3), High (4) и Very-High (5).

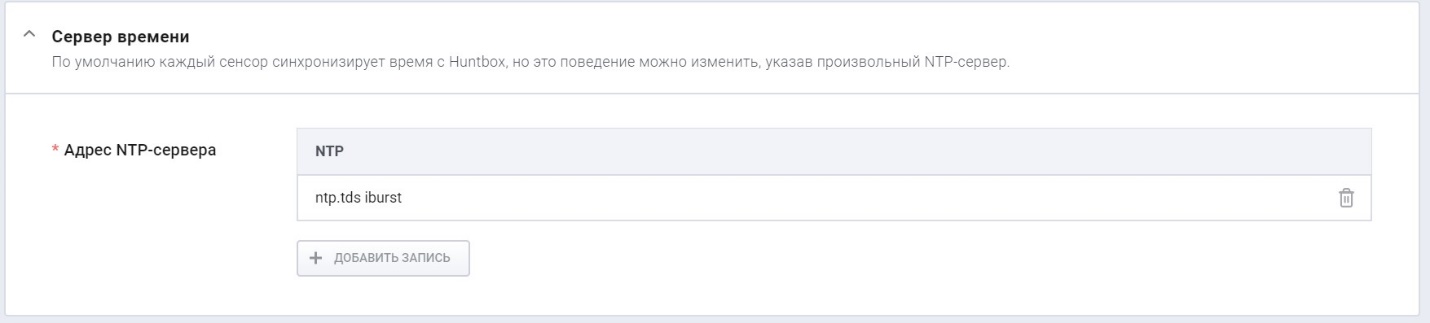
* **JSON**

json, с уровнем угрозы (severity) от 1 до 5.



### 6.4.3.9. Сервер времени TDS Sensor

По умолчанию каждый сенсор синхронизирует время с Huntbox, но это поведение можно изменить, указав произвольный NTP-сервер. Для того чтобы добавить новый произвольный NTP-сервер, необходимо нажать на кнопку **Добавить запись** и внести адрес NTP-сервера в формате FQDN или сетевой IP-адрес.



### 6.4.3.10. Белый список

Белые списки позволяют исключить из анализа внесенные в них объекты в компонентах TDS Sensor и TDS Polygon. Оптимизация работы решения с помощью данного инструмента - обязательное условие высоко качества обнаружения атак.

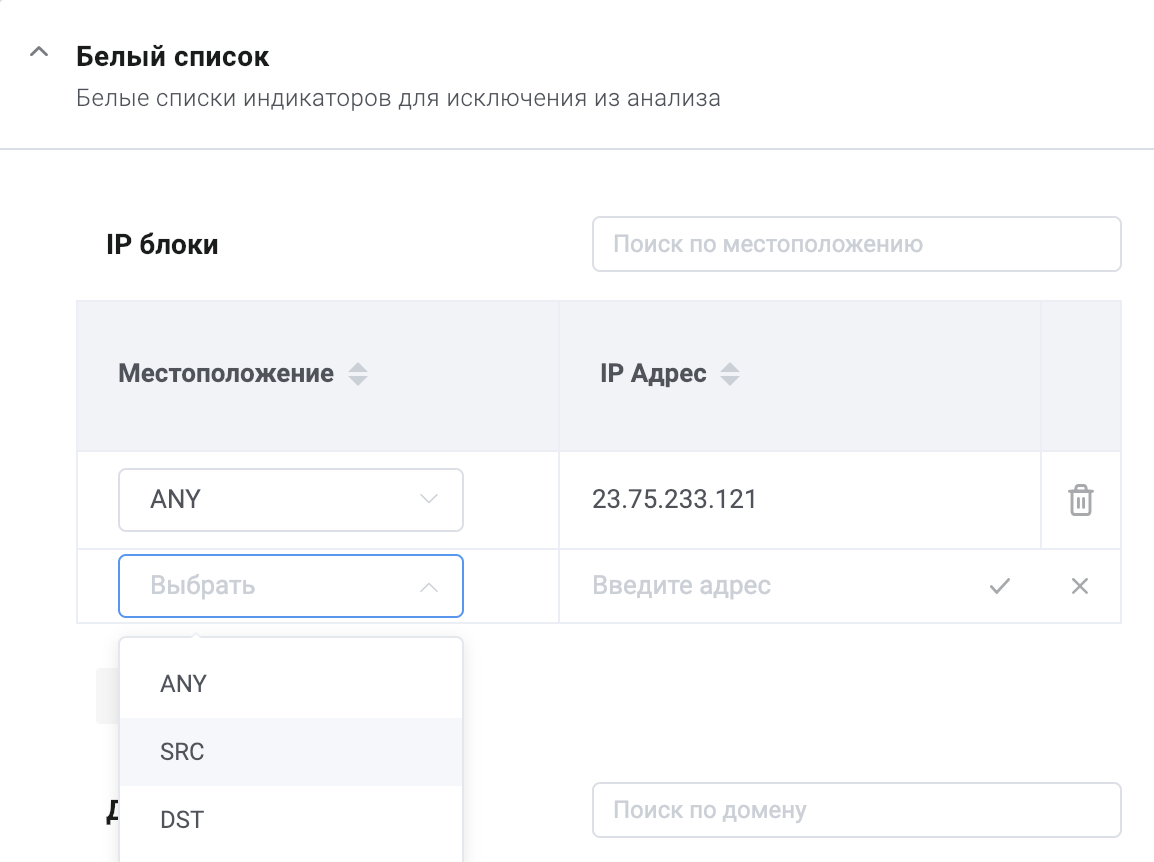
#### 6.4.3.10.1. IP блоки

Позволяет исключать потоки данных на сетевом уровне в различных направлениях (от и/или к целевым,защищаемым, хостам).

В первую очередь необходимо задать направление для фильтрации:

* SRC - Источник.
* DST - Назначение.
* ANY - Источник и Назначение.

Далее необходимо ввести IP-адрес. Система поддерживает IPv4 и IPv6. В ближайшем будущем появится возможность вводить целые подсети.



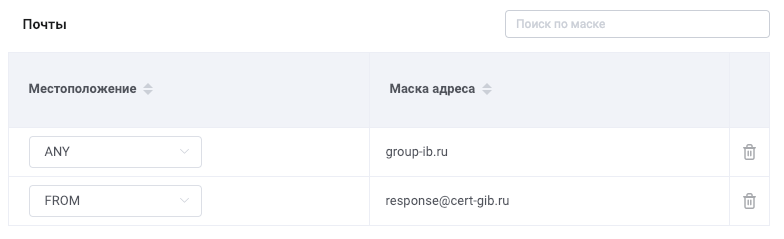
IP блоки

#### 6.4.3.10.2. Почты

Фильтрация почты может позволить значительно уменьшить нагрузку на TDS Polygon. В первую очередь необходимо задать направление для фильтрации:

* TO - адрес назначения.
* FROM - адрес отправителя.
* ANY - адрес назначения и отправителя.

Система поддерживает ввод, как единичных аккаунтов, так и целых доменов. Например, можно добавить в whitelist один аккаунт response@cert-gib.ru или все почтовые аккаунты в домене.\*@group-ib\.com c помощью регулярных выражений.



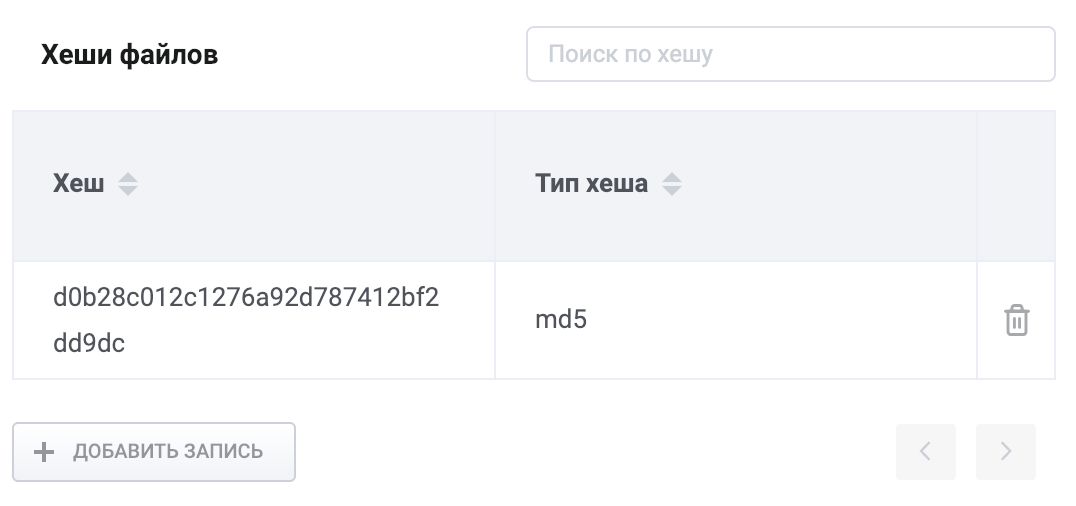
Белый список почты

#### 6.4.3.10.3. Хеши файлов

Система поддерживает фильтрацию файлов в следующих форматах:

* MD5
* SHA1
* SHA256

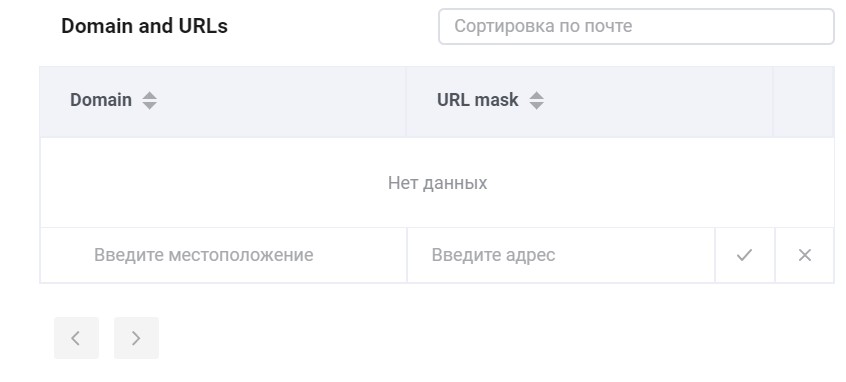
Например, выбрав алгоритм хеширования: MD5 и хеш-сумму файла: d0b28c012c1276a92d787412bf2dd9dc данный файл будет включен в whitelist и не будет анализироваться песочницей.



#### 6.4.3.10.4. Домены и URL-ы

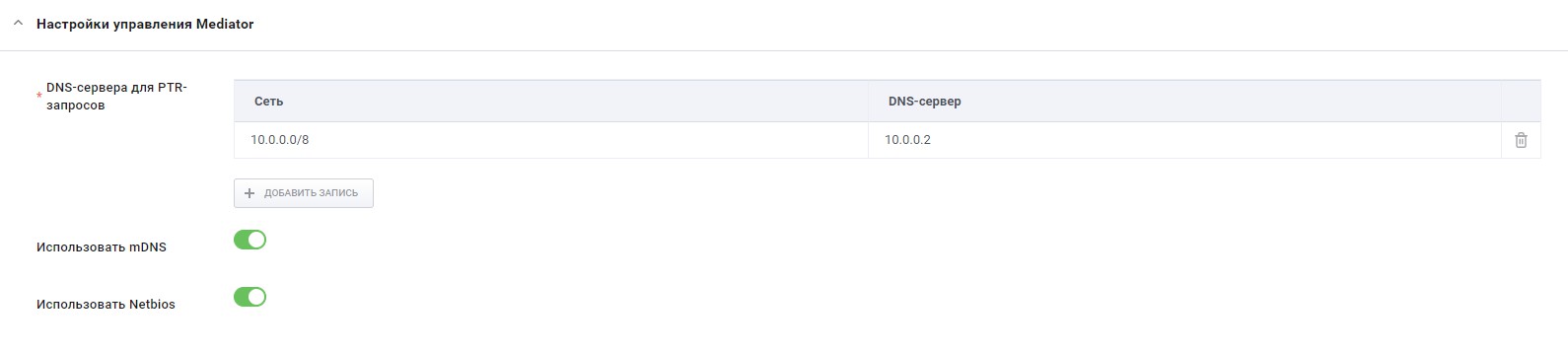
Указанные в данном списке домены и URL будут опускаться при анализе сенсором подозрительных ссылок в почтовых сообщениях и сетевом трафике. В каждой записи необходимо задать:

* Domain - общий домен необходимого уровня
* URL mask - регулярное выражение для анализа ссылок из указанного домена



### 6.4.3.11. Настройки разрешения имён

Данный раздел активирует возможности сенсора по разрешению сетевых адресов в доменные и сетевые имена. Таким образом, аналитикам предоставляется удобный инструмент для быстрого определения принадлежности хостов к обнаруженным инцидентам и тем самым сокращается время реагирования.



**DNS-сервера для PTR запросов**

Настройка позволяет изменить стандартные маршруты по выполнению PTR (reverse DNS) запросов и позволяет задать статические маршруты для выполнения подобных запросов. Чтобы настроить нестандартные маршруты PTR-запросов заполните записи в формате:

* **Сеть**

Подсеть/сеть/IP адрес. - Настройка задаёт подсеть/сеть/адрес для которых необходимо разрешать IP адреса в доменные имена.

* **DNS-сервер**

Настройка задаёт сервер, который будет отвечать за обслуживание PTR запросов для указанных подсетей/сетей/адресов.

**Использование mDNS**

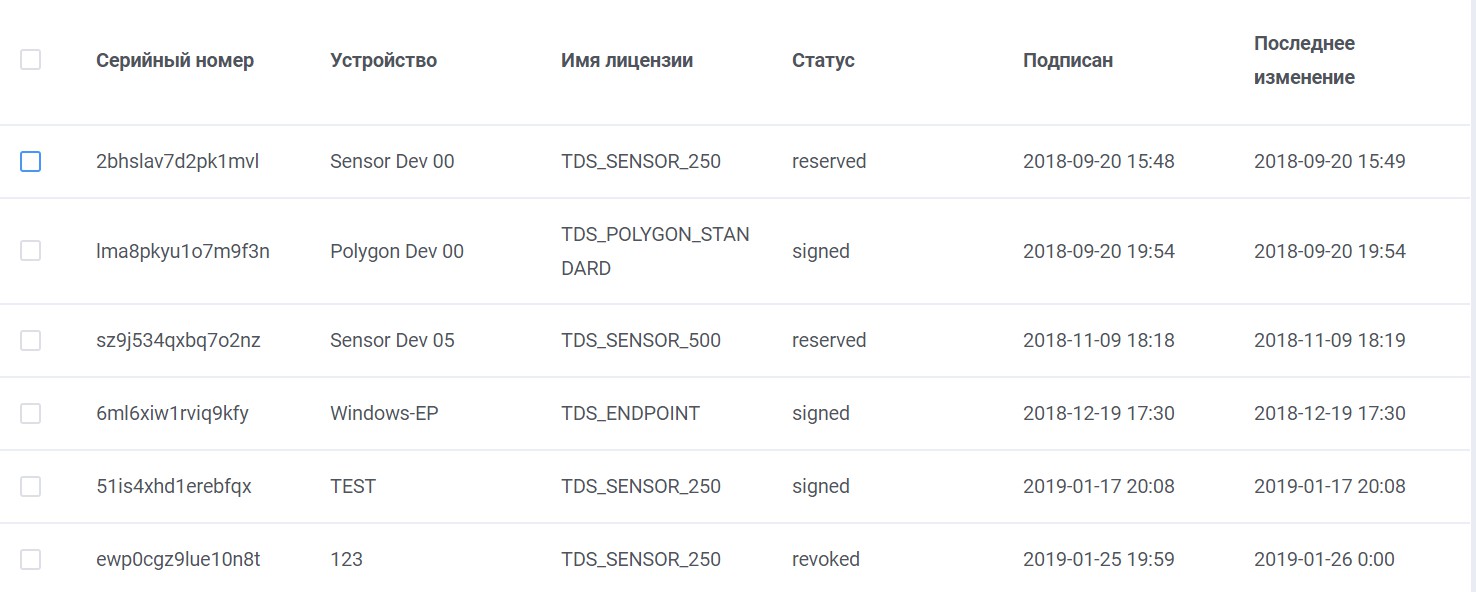
Активирует на сенсоре протокол mDNS и позволяет осуществлять мультикаст DNS запросы для разрешения адресов в доменные/сетевые имена.

**Использование Netbios**

Активирует на сенсоре использование протокола Netbios для определения сетевых имён хостов.

## 6.4.4. PKI

В данном меню предоставляется список всех UUID (сертификатов) созданных с момента активации TDS HuntBox.



### 6.4.4.1. Данные по сертификатам

По каждому сертификату доступна следующая информация:

* **Серийный номер**

UUID сертификата. Используется для регистрации и синхронизации новых компонент TDS c HuntBox

* **Устройство**

Имя, выданное при создании и генерации сертификата для нового устройства.

* **Имя лицензии**

Тип лицензии. Зависит от типа устройства.

* **Статус**
  + Reserved - сертификат создан, подписан. По нему зарегистрирован компонент TDS. Сертификат используется в работе
  + Signed - сертификат создан (подписан), но ещё не используется. По нему возможно зарегистрировать новый компонент TDS на HuntBox
  + Revoked - сертификат отозван. Связанное с ним устройство отсоединено от TDS HuntBox без возможности дальнейшей работы
  + Requested - запрос на отзыв сертификат со стороны подключенных компонент TDS. Компонента TDS будет работать до те пор пока сертификат не будет отозван - перейдёт в статус revoked
* **Подписан**

Дата выпуска сертификата на TDS HuntBox

* **Последнее изменение**

Дата последнего изменения статуса сертификата.

### 6.4.4.2. Изменение сертификатов

При выборе одного или нескольких сертификатов появляется возможность изменить статус сертификата:

* **Подписать**

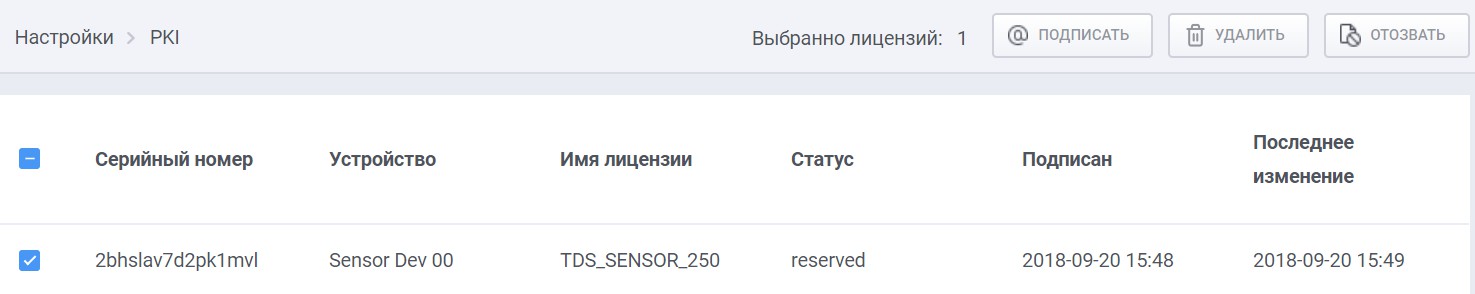
Подписать зарезервированный сертификат

* **Отозвать**

Отозвать подписанный сертификат. Компонент TDS зарегистрированный на HuntBox по данному сертификату будет отсоединён.

* **Удалить**

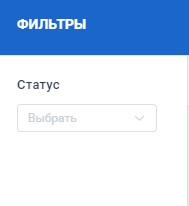
Удалить сертификат.



Изменение сертификата

### 6.4.4.3. Фильтры

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтр PKI

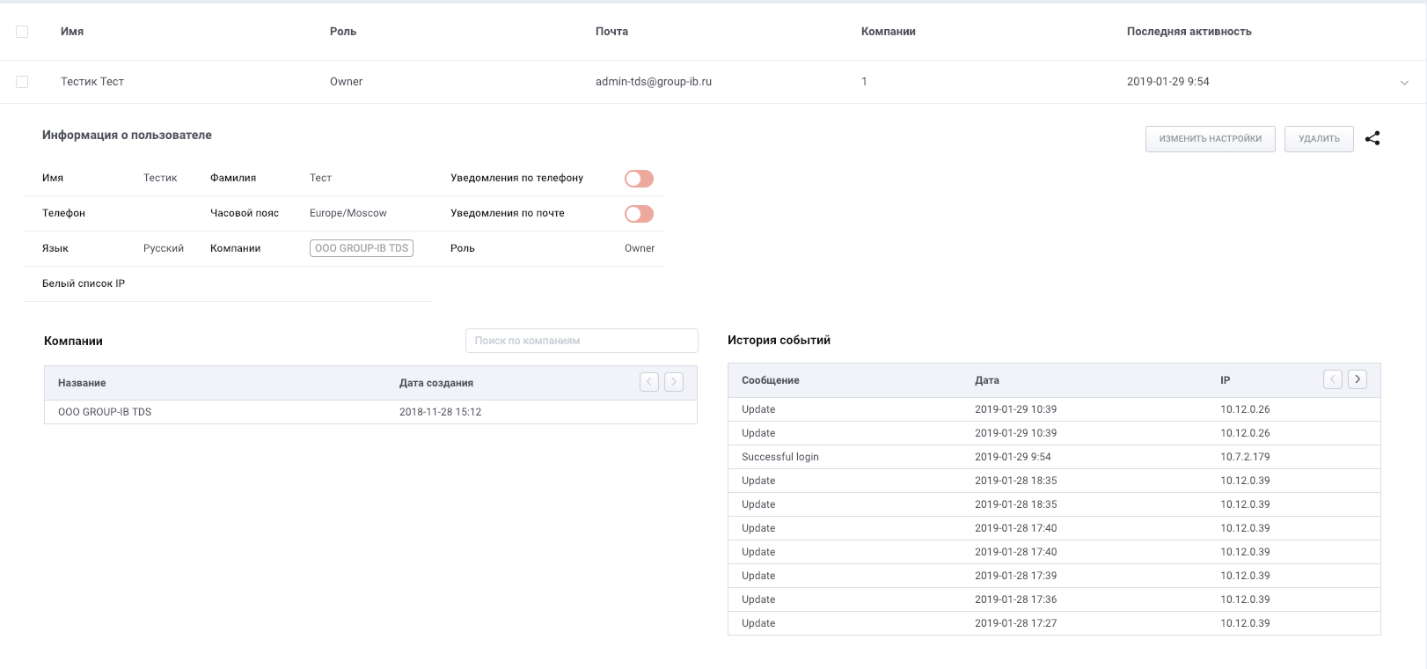
Доступные фильтры:

* Статус
  + Requested
  + Signed
  + Reserved
  + Revoked

## 6.4.5. Пользователи

Данная страница содержит информацию о пользователях, зарегистрированных в системе TDS, а также позволяет добавлять/удалять пользователей и вносить изменения в профили. В списке пользователей представлена общая информация по каждой записи. По каждому пользователю доступна полная информация (см. разделы ниже)

### 6.4.5.1. Полная информация по пользователю



Полная информация пользователя

**Информация о пользователе**

* Имя - Имя и Фамилия пользователя.
* Роли - функция для определения прав доступа к ресурсам и управления этим доступом.
  + Owner - создатель проекта. Пользователь имеет права на выполнение любых действий.
  + Admin - привилегированный пользователь, имеющий права, включающие изменение прав доступа к продукту TDS для других пользователей, регистрация и удаление пользователей, изменение ролей пользователей. В одной организации может быть несколько администраторов.
  + Analyst - аналитик по реагированию и мониторингу на инциденты.
  + User - пользователь системы TDS обладающий правами доступа стандартного пользователя. Ему доступны: Dashboard, Алерты, Расследование.
  + Manager - имеет минимальные права доступа: Dashboard, Алерты.
* Почта - email-адрес пользователя. Используется как логин при аутентификации. Данный адрес будет использоваться для оповещений от SOC Group-IB по инцидентам при наличии поддержки 24/7. А так же будет использоваться HuntBox-ом для автоматической рассылкой сообщений о статусах алертов.
* Последняя активность - представлены крайние записи активности из пункта История событий.
* Белый список IP - В качестве более высокого уровня безопасности учетной записи, рекомендуется добавление белого списка IP адресов. Данный список позволит обеспечить доступ к учетной записи только по представленным IP адресам, для этого необходимо указать один IP адрес или его диапазон.
* Уведомления - используется два типа уведомлений:
  + Почта - оповещение пользователя о созданном тикете в системе TDS. Используется почта из соответствующего раздела
  + Телефон - при происшествии критических инцидентов специалисты SOC Group-IB дополнительно оповестят пользователя телефонным звонком.

**Компании**

Наименование организации к которой относится пользователь. Компания определяет область видимости информации для аккаунта. Дополнительная информация содержится в разделе Компании.

**История событий**

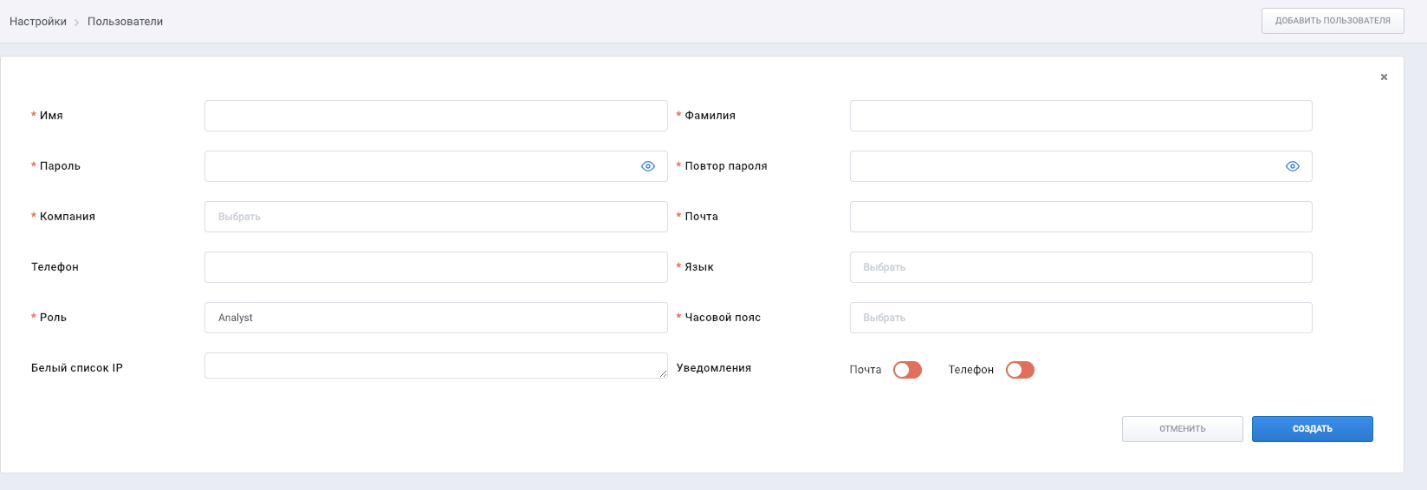
Данный модуль позволяет вести логирование действий пользователя.



Полная информация пользователя

### 6.4.5.2. Добавить пользователя

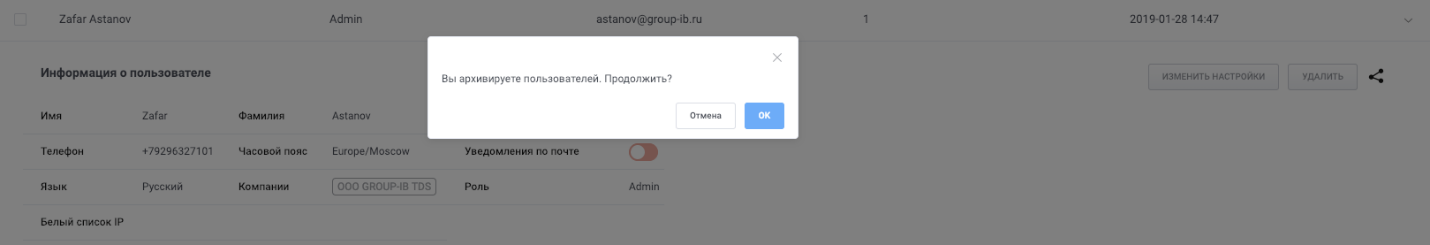
Для добавления нового пользователя в систему TDS необходимо провести регистрацию. Пользователю с ролью admin или owner требуется зайти на страницу "Настройки" и нажать на "Добавить пользователя". Следующие поля обязательны к заполнению: Имя, Фамилия, Пароль, Повтор пароля, Компания, Почта, Язык интерфейса, Часовой пояс и Роль. Поля необязательные к заполнению: Телефон, Белый список IP и Уведомления.



Создание пользователя

### 6.4.5.3. Удаление пользователя

Для обеспечения более высокого уровня безопасности архитектуры клиента, при удалении пользователя учетная запись архивируется. Тем самым все внесенные записи, настройки сохраняются. Для удаления пользователя необходимо выбрать учетную запись и нажать "Удалить".



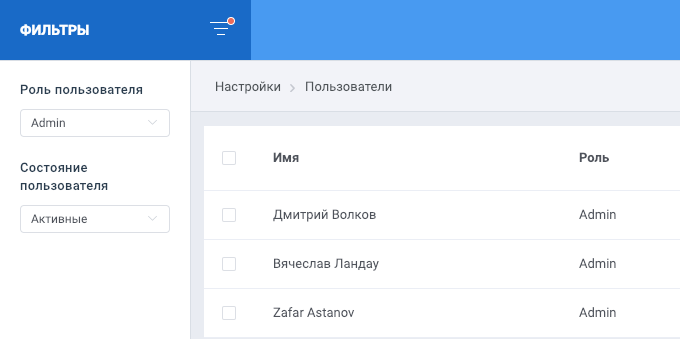
Удаление пользователя

### 6.4.5.4. Фильтры

Для фильтрации данных на странице "Пользователи" существует два фильтра:

* Роль пользователя - позволяет сортировать информацию о пользователях исходя из выбранной роли.
* Состояние пользователя - сортирование информации об активных или удаленных пользователях.

Например, данный фильтр позволяет выбрать только активных пользователей с ролью Администратора.



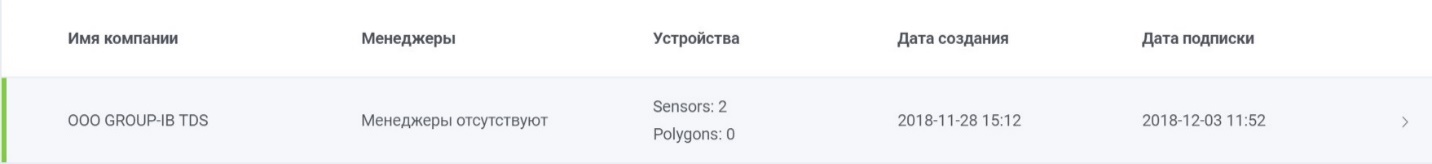
Фильтрация пользователей

## 6.4.6. Компании

TDS Huntbox даёт возможность создавать несколько компаний в разрезе одной инсталляции, что позволяет разграничивать доступные данные среди пользователей, а также реализовывать более сложные иерархические структурные разграничения прав доступа. Все подключаемые модули (sensor, polygon, endpoint) соотносятся с сущностью Компания из числа созданных в настоящем разделе. Таким образом, все события, формируемые данными модулями, будут разграничены по доступу в соответствии с принадлежностью модуля к Компании.

### 6.4.6.1. Общий список компаний

Предоставляет список компаний с описанием общих данных по ним.



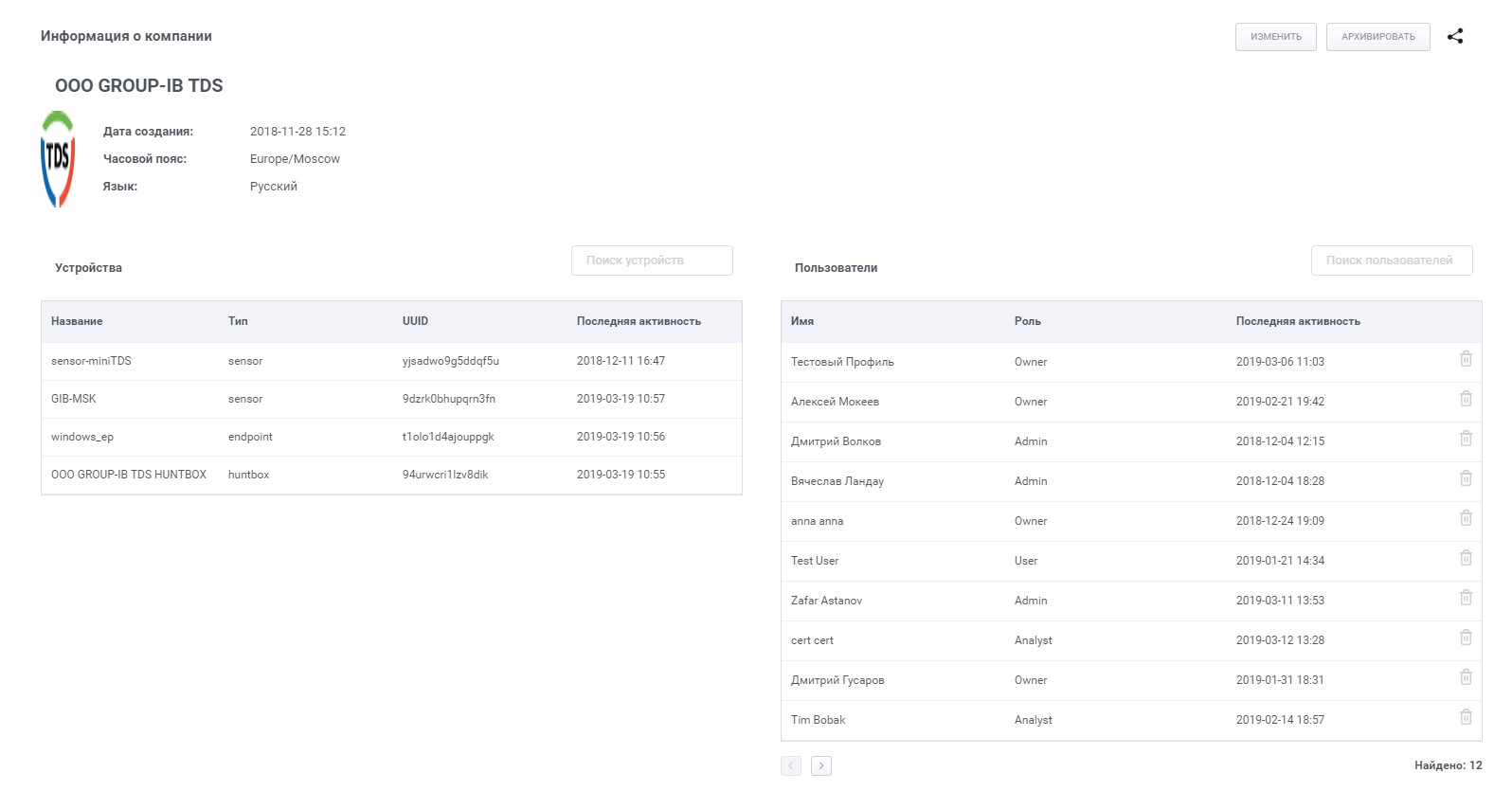
Список компаний

Доступны следующие данные:

* Имя компании
* Менеджеры - список пользователей с ролью менеджер
* Устройства - количество прикрепленного к данной компании оборудования с разделением по типам
* Дата создания - дата создания компании
* Дата подписки - дата начала подписки

### 6.4.6.2. Информация о компании

При выборе компании доступной в списке открывается полная информация о компании. В левом верхнем углу будет отображаться заданный при создании компании логотип. Общие данные можно отредактировать по кнопке **Изименить** в правом верхнем углу.



Информация о компании

**Устройства**

Предоставляет список устройств, привязанных к выбранной компании. Краткая информация:

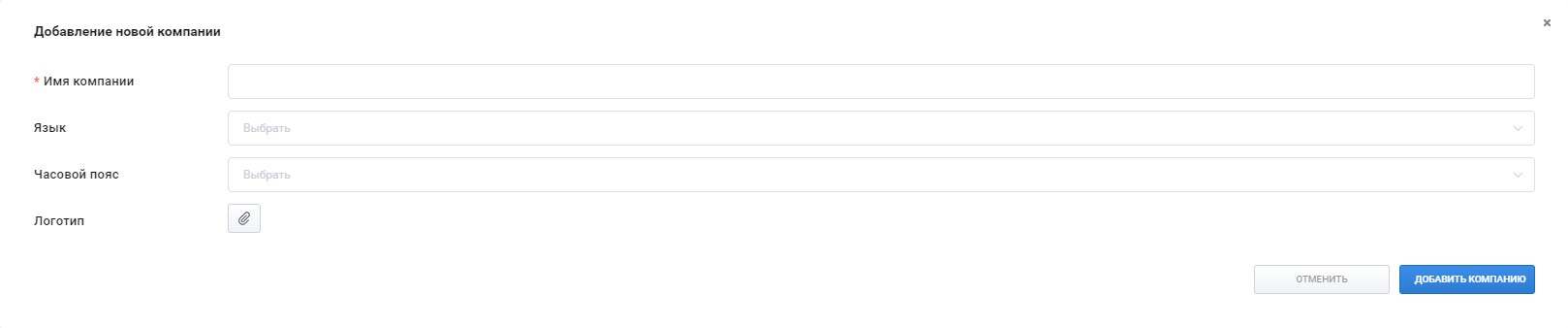
* Название - имя устройства
* Тип - тип компоненты системы (sensor, polygon, endpoint)
* UUID - идентификатор ключа активации
* Последняя активность - крайняя дата активности системы

**Пользователи**

Список пользователей, привязанных к компании. Предоставляется следующая информация по пользователям:

* Имя - имя пользователя в системе
* Роль - присвоенная пользователю роль
* Последняя активность - крайняя дата активности пользователя

### 6.4.6.3. Добавление новой компании



Для добавления новой компании нажмите на кнопку **Добавить компанию** и заполните следующие поля:

* Имя компании - уникальное название компании в рамках HuntBox (поле обязательное к заполнению)
* Язык - выберете язык интерфейса по умолчанию
* Часовой пояс - задайте часовой пояс по умолчанию
* Логотип - имеется возможность задать нестандартный логотип компании (Будет отображаться в правом верхнем углу)

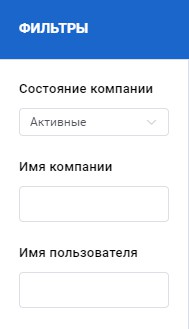
### 6.4.6.4. Архивирование компании

При архивировании компании ... Для архивирования компании выберите её в списке компаний, раскройте полное описание и нажмите кнопку **Архивировать**.

### 6.4.6.5. Фильтры

**Фильтры типов**

По кнопке фильтров в левом верхнем углу веб-интерфейса открывается меню фильтрации.



Фильтры компании

Доступные фильтры компании:

* Состояние компании - выбор компаний в состоянии:
  + Активные - отображать только активные
  + Архивные - отображать только архивные
  + Пусто - отображать полный список компании
* Имя компании
* Имя пользователя