**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«TDS Polygon»**

**Версия 1.0**

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

**СОДЕРЖАНИЕ**

[1. Аннотация 3](#_Toc531867849)

[2. Настройки доступа и учетных записей 3](#_Toc531867850)

[2.1. Разграничение прав доступа 3](#_Toc531867851)

[2.2. Настройки учетной записи 3](#_Toc531867852)

[3. Раздел анализ файлов 4](#_Toc531867853)

[4. Раздел сигнатуры 5](#_Toc531867854)

[4.1. Описание угрозы 5](#_Toc531867855)

# Аннотация

Настоящий документ содержит руководство пользователя по использованию программного обеспечения «TDS Polygon» версии 1.0 (далее – ПО).

# Настройки доступа и учетных записей

Доступ к системе предоставляется через Веб. Доступ к Веб-интерфейсу доступен авторизованным клиентам системы.

# Разграничение прав доступа

**Разграничение прав на сетевом уровне**

Доступ к системе через Веб может быть разрешен только по белому списку IP-адресов. Все IP-адреса, указанные в анкете для подключения, добавляются в список разрешенных и их можно посмотреть в настройках учетной записи.

Если вы пытаетесь получить доступ с IP-адреса, который не добавлен в список разрешенных, то вы получите сообщение об ошибке с кодом 403.

**Разграничение прав на уровне пользователей**

Количество пользователей в системе не ограничивается и определяется желаниями клиента. Каждому пользователю могут назначаться отдельные права.

# Настройки учетной записи

Для перехода в раздел настройки учетной записи необходимо в правом верхнем углу нажать на имя своего профиля и выбрать «Настройки профиля».

Страница состоит из следующих блоков: информация по пользователей.

**Информация о пользователе**

Первый блок этого раздела показывает настройки вашего пользователя и права доступа. Значение часового пояса используется для отображения сведений о времени обнаружения угроз в вашей временной зоне. В этом же блоке вы можете изменить пароль для своей учетной записи, для чего необходимо нажать на кнопку «Изменить пароль».

# Раздел анализ файлов

Предоставляет функционал поведенческого анализа файлов и подробную статистику.

При нажатии на кнопку 

Предоставляется возможность загрузить необходимые данные для анализа. Возможно загрузить как отдельный объект, так и несколько предварительно заархивированных файлов.

Загруженное ПО и/или файлы будут проанализированы относительно операционной системы, релевантной загружаемому объекту. После отправки данных на анализ в списке «Анализ файлов» появится новая строка со статусом проводимой задачи. После того как анализ будет завершён, выбрав имя анализируемого файла в отдельной вкладке откроется страница с результатом.

По результатам анализа могут быть представлены следующие данные:

1. Информация по файлу(ам):
* Оценка вредоносности – классификатор с использованием алгоритмов машинного обучения определяет вероятность вредоносности по выявленным поведенческим маркерам. Вредоносным считается вероятность 50% и выше.
* Время анализа с датой
* Известные имена – известные альтернативные имена файлов данного вредоносного ПО
* Размер файла – в том числе ссылка на сам вредоносный файл. Файлы не признанные вредоносными не будут храниться в Системе
* Хеш-сумма MD5 / SHA1 / SHA256
* Связанные события – события ИБ, связанные с данным файлом
1. Поведенческие маркеры:
* Вредоносные – предоставляют результаты изучения поведения, анализируемого ПО и/или файлов и могут включать различные показатели (действия с процессами, действия с прикладным операционным ПО, действия с файловой системой, действия и т.п.) – полный перечень маркеров является интеллектуальной собственностью компании Group-IB и не будет раскрыт.
* Прочие – маркеры не являющиеся вредоносными, но представляющие дополнительные данные для аналитиков и расследований.
1. Сетевая активность – копия трафика, генерируемого анализируемым ПО – если есть. Файл в формате PCAP
2. Дерево процессов – полное дерево процессов, затрагиваемых при работе анализируемого файла. По каждому процессу предоставляются затронутые элементы системы (ключи реестров, файлы, новые процессы, мьютексы и т.п.)
3. Файловая структура –древовидная структура файлов, загруженных для анализа
4. Видео – представляет запись рабочего стола виртуального контейнера, в котором отображается графическая активность анализируемого ПО – если имеется

Поиск по разделу осуществляется в строке «Поиск»



Доступны следующие критерии поиска:

* File\_name – по имени файлов
* md5 / sha1 / sha256 – по значению хеш-суммы
* user\_name – по имени пользователя системы

# Раздел сигнатуры

В разделе представлены сигнатуры с аналитической информацией. Сигнатуры могут быть связаны с разделом угроз и разделом ботнетов. Сигнатуры могут быть отфильтрованы по Активности, Классу Угроз, уровню опасности.

Каждая сигнатура предоставляет аналитические данные по срабатыванию за определенный период:

* Имя
* Класс угроз к которому принадлежит сигнатура
* Время первого срабатывания
* Время последнего срабатывания
* Число событий
* Отношение ложных к общему числу событий
* Угроза к которой принадлежит сигнатура из раздела «Угрозы» - может быть пустой
* График событий, связанных с данной сигнатурой
* Уровень опасности события, связанного со срабатыванием данной сигнатуры
* Время добавления сигнатуры

Изнутри описания сигнатуры(в классе угроз), можно перейти в описпание угрозы, тоносящейся к данной сигнатуре.

# Описание угрозы

По каждой угрозе доступно краткое описание с полями:

* Имя
* Класс угрозы
* Атакуемое ПО
* Описание
* Количество сигнатур
* Дата добавления

По каждой угрозе так же доступно полное описание предоставляющее:

* Общее описание, в том числе целевое применение данной грозы
* Функциональность и модули (если применимо)
* Индикаторы компрометации (если применимо)
* Связанные сигнатуры