**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
TDS Atmosphere**

**ГТДС.00013-01**

**ОПИСАНИЕ РЕАЛИЗАЦИИ**

**СОДЕРЖАНИЕ**

[Аннотация 2](#_Toc48846420)

[1. Назначение ПО 2](#_Toc48846421)

[2. Программно-аппаратные среды функционирования ПО 2](#_Toc48846422)

[3. Общие принципы функционирования ПО 2](#_Toc48846423)

[4. Реализация ПО 5](#_Toc48846424)

[4.1 Модуль предоставления возможности загрузки ПО в Систему 5](#_Toc48846425)

[4.2 Модуль предоставления результатов анализа 5](#_Toc48846425)

[4.3 Модуль защиты удаленного доступа и контроля изменений 5](#_Toc48846425)

# Аннотация

Настоящий документ содержит описание реализации программного обеспечения TDS Atmosphere ГТДС.00013-01 (далее – ПО).

# Назначение ПО

TDS Atmosphere – Программное обеспечение для поведенческого анализа, обеспечивающее выявление ранее неизвестного вредоносного кода с использованием передовых алгоритмов машинного обучения. Решение позволяет эффективно выявлять ранее неизвестные угрозы, осуществляя анализ файлов в изолированной среде. Он позволяет предотвратить заражения в результате фишинговых рассылок, либо загрузки/получения вредоносных файлов, осуществляющих заражения с использованием ранее неизвестных вредоносных программ и инструментов.

Использование модуля TDS Atmosphere обеспечивает обнаружение ранее неизвестного вредоносного ПО и сложных целевых атак.

Основными целями создания Системы являются:

* Предоставление интерфейса с отображением результатов проведения поведенческого анализа объектов;
* Повышение качества и количества раскрываемых преступлений;
* Предоставление прозрачной статистической и аналитической информации.

# Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

* Windows Internet Explorer версии 8.0 и выше;
* Google Chrome версии 4.0 и выше;
* Mozilla Firefox версии 3.5 и выше;
* Apple Safari версии 4.0 и выше;
* Opera версии 10.5 и выше;
* iOS Safari версии 3.2 и выше;
* Opera Mobile версии 11.0 и выше;
* Google Chrome for Android версии 11.0 и выше;
* Mozilla Firefox for Android версии 26.0 и выше;
* Windows Internet Explorer Mobile версии 10.0 и выше.

# Общие принципы функционирования ПО

Внутри Системы используется набор виртуальных машин с различными операционными системами. Анализируемый объект в автоматизированном режиме запускается на виртуальной машине. После запуска происходит запись следов работы внутри операционной системы в результате запуска объекта, исходя из показателей компрометации. Показатели компрометации могут обновляться в соответствии с понимаем современного ландшафта киберпреступлений. По итогам анализа доступен подробный отчет со следующими информационными блоками:

* Развернутая информация о файле;
* Поведенческие маркеры;
* Сведения о сетевая активности;
* Дерево процессов;
* Видео.

На рисунке 1 изображены общие принципы функционирования ПО TDS Atmosphere
ГТДС.00013-01 с остальными модулями TDS.



 Рисунок 1. Общие принципы функционирования ПО

Основные технические требования отображены в таблице ниже.

Таблица 1 – Технические требования для TDS Atmosphere

|  |  |  |
| --- | --- | --- |
| **TDS Atmosphere** | **Standard** | **Enterprise** |
| **CPU** | 2.1 GHz, 20 C (2 threads per core), 27.5 MB | 2.1 GHz, 40 C (2 threads per core), 27.5 MB |
| **RAM, GB** | 128 GB, RDIMM | 256 GB, RDIMM |
| **SSD, GB\*\*** | 2 х 480 | 2 х 480 |
| **Mgmt Ethernet** | 1 Ethernet | 1 Ethernet |

# Реализация ПО

Системы состоит из следующих модулей:

* Модуль предоставления возможности загрузки ПО в Систему;
* Модуль предоставления результатов анализа;
* Модуль защиты удаленного доступа и контроля изменений.

В рамках предоставляемого интерфейса операторы системы имеют возможность загружать ПО и файлы в Систему и получать данные по результатам анализа.

**4.1 Модуль предоставления возможности загрузки ПО в Систему**

В разделе «Управление -> Анализ файлов» представлена возможность загрузить ПО и/или набор файлов для проведения поведенческого анализа.

**4.2 Модуль предоставления результатов анализа**

В разделе «Управление -> Анализ файлов» предоставляется список работ по анализу ПО и/или файлов. Каждая строка отражает задачу анализа. По задаче анализа предоставляется детализированная информация:

* Развернутая информация о файле;
* Поведенческие маркеры;
* Сведения о сетевая активности;
* Дерево процессов;
* Видео.

# Модуль защиты удаленного доступа и контроля изменений

Модуль защита удалённого доступа обеспечивает:

* сохранение конфиденциальности и целостности передаваемой информации;
* возможность ограничения доступа к системе для всех адресов кроме указанного в настройках;
* неотключаемый протокол внесения изменений в Систему и выгрузки данных из системы:
	+ загрузка новых данных;
	+ изменение параметров пользователей Системы;
	+ выгрузка данных в отдельный файл со скачиванием через клиентский браузер;
	+ создание новых пользователей Системы;
	+ выдача пользователю дополнительных прав.