Инв. № подл.	Подп. и дата	Взам. инв. N	Инв. N дубл.	Подп. и дата

Программное обеспечение

«Специальное программное обеспечение взаимодействия с Kaspersky Anti Targeted Attack Platform»

Руководство пользователя

RU.ЦБМК. 00124-01 92 01

2022

Содержание

Введение

Настоящее руководство пользователя содержит описание эксплуатации программного обеспечения «Специальное программное обеспечение взаимодействия с Kaspersky Anti Targeted Attack Platform» (далее – СПО KATA) и включает:

- перечень сертификатов внешних систем;
- порядок регистрации внешних систем в средстве защиты от целевых атак Kaspersky Anti Targeted Attack Platform (далее – СЗЦА KATA);
- описание полей встроенной базы данных для статистики;
- действий после сбоев и ошибок эксплуатации ПО.

1. Область применения

Специальное программное обеспечение взаимодействия с Kaspersky Anti Targeted Attack Platform предназначено для обеспечения потребностей Заказчиков информационных систем, не имеющих подключений к сетям связи общего доступа, в обеспечении контролируемой отправки на проверку в СЗЦА КАТА файлов из выделенной папки.

СПО КАТА обеспечивает, посредством установления временных периодов и размера очередей, контролируемую отправку файлов и управление загрузкой обрабатываемого модуля. Также СПО реализует повторную отправку файла в случае переполнения очереди или ошибки сети, контроль и очистку сведений по результатам успешной проверки журнала СЗЦА КАТА, что позволяет сохранять только информацию о выявленных угрозах.

2. Формирование сертификатов внешних систем

Каждая система, от имени которой отправляются файлы на проверку в СЗЦА КАТА, считается внешней системой по отношению к СЗЦА КАТА. Для регистрации новой внешней системы в СЗЦА КАТА необходимо сформировать сертификат, который будет отправляться в запросе к СЗЦА КАТА вместе с проверяемым файлом, идентифицируя тем самым принадлежность этого файла к внешней системе.

Для корректной работы СПО необходимо сформировать сертификат в формате .pem, закрытый ключ в формате .key и конвертировать сертификат в формат .pfx для каждой внешней системы, от имени которой будут отправляться на проверку файлы. Файлы сертификатов должны быть размещены на сервере, где производилась установка и запуск СПО КАТА.

Например, процедура генерации сертификата может быть следующая:

1. Создается приватный ключ:

```
openssl genrsa -des3 -out <имя ключа>.key 2048
```

2. Генерируется запрос на сертификат:

```
openssl req -new -key <имя ключа>.key -out <имя запроса>.csr
```

3. Генерируется сертификат сроком на 3048 дней:

```
openssl x509 -req -days 3048 -in<имя запроса>.csr -signkey <имя ключа>.key -out <имя сертификата>.pem
```

4. Сертификат PEM конвертируется в формат PFX.

3. Регистрация внешних систем

Для начала работы с API СЗЦА КАТА необходимо выполнить регистрацию в СЗЦА КАТА каждой внешней системы, от имени которой будут отправляться файлы на проверку. Такие системы считаются внешними системами по отношению к СЗЦА КАТА. Внешняя система должна пройти авторизацию на сервере СЗЦА КАТА. Подробная документация доступна на официальном сайте производителя СЗЦА КАТА.

Чтобы выполнить интеграцию внешней системы с СЗЦА КАТА, необходимо выполнить следующие действия:

1. Генерация уникального идентификатора внешней системы для обращения к API.
2. Генерация сертификата сервера внешней системы.
3. Создание произвольного запроса от имени внешней системы в СЗЦА КАТА, содержащий идентификатор **sensorId**.
4. Подтвердить запрос на авторизацию от внешней системы в веб-интерфейсе СЗЦА КАТА.

Чтобы обработать запрос на интеграцию от внешней системы, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Внешние системы**.
2. В таблице **Список серверов** отобразятся уже подключенные внешние системы, а также запросы на интеграцию с СЗЦА КАТА от внешних систем.
3. В строке с запросом на интеграцию выполните одно из следующих действий:

– если вы хотите настроить интеграцию с внешней системой, нажмите на кнопку **Принять**.

– если вы не хотите настраивать интеграцию с внешней системой, нажмите на кнопку **Отклонить**.

4. В окне подтверждения нажмите на кнопку **Да**.

Запрос на интеграцию от внешней системы будет обработан.

4. Описание базы данных статистики

База данных StatisticOperationFile.db содержит таблицу OperationFiles, в которой хранится статистическая информация, описание полей которой представлено в таблице ниже:

Наименование параметра	Описание
Id	Идентификатор (ключевое поле)
DateTimeLoadFile	Дата и время загрузки файла
DateTimeSendForCheckFile	Дата и время отправки на проверку файла
DateTimeGetResult	Дата и время получения ответа от СПО КАТА КАТА
DateTimeDeleteFile	Дата и время удаления обработанного файла
SystemId	Идентификатор внешней системы
FileInitialPath	Директория скачиваемого файла
FileWorkPath	Директория файла, отправляемого на проверку
FileName	Наименование файла
ScanId	Сгенерированный идентификатор для файла, необходимы при отправке файла на проверку
Status	Статус обработки файла
Message	Информация по статусам проверки и служебным сообщениям

5. Начало работы в СПО KATA

Начало работы с СПО осуществляется запуском соответствующей службы в оснастке «Службы» операционной системы Windows (Рисунок 1).

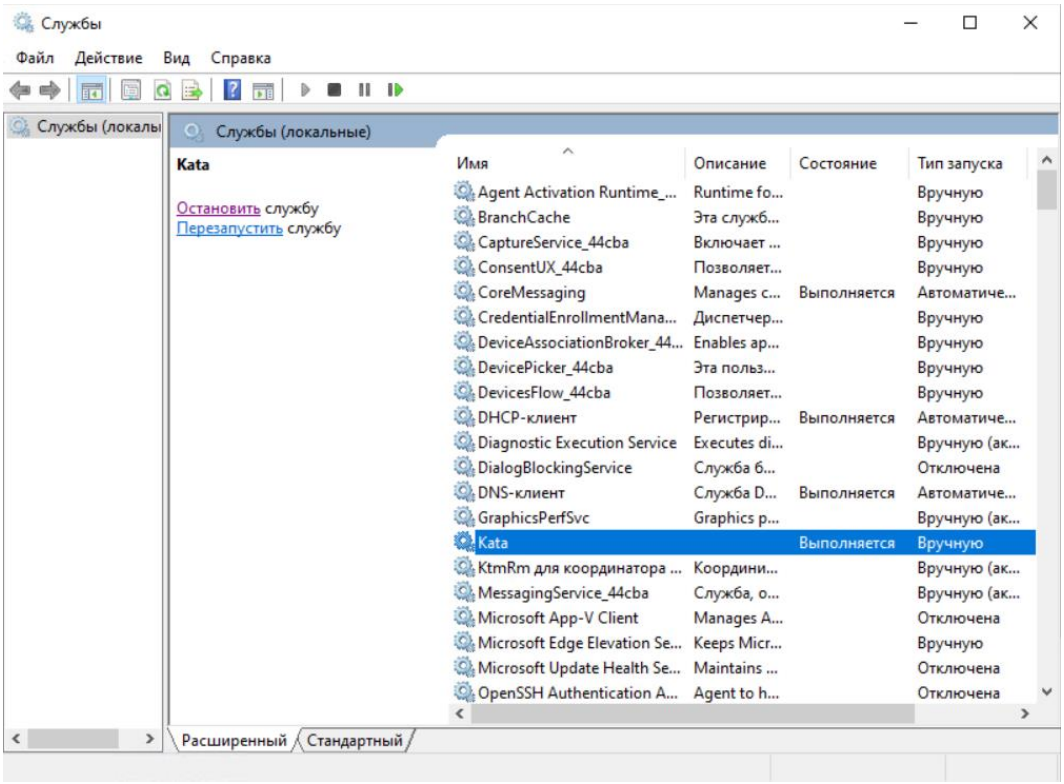

Рисунок 1

6. Действия пользователей в случае возникновения ошибок и сбоев

ВАЖНО! Любые действия пользователей в СПО КАТА по устранению возникших ошибок или сбоев должны выполняться по указанию администратора.

В случае возникновения ошибок или сбоев пользователь в кратчайшие сроки с использованием электронной почты, телефона или непосредственно должен оповестить об этом администратора. В своем сообщении пользователь должен указать:

- время возникновения ошибки;
- краткое описание ошибки;
- приложить файл с LogServiseKata.txt из корневой папки СПО КАТА;
- приложить файлы FileWatcher.log и MainLogFile.log из папки Logs;
- в случае появления сообщения об ошибке необходимо указать код ошибки, описание текста этого сообщения (при отправке администратору сообщения по электронной почте, по возможности, приложить скриншот экрана с данным сообщением);
- описать выполненные действия в СПО, которые пользователь выполнял до появления ошибки и которые, по мнению пользователя, привели или могли привести к появлению данной ошибки.

После этого пользователь должен выполнить полученные от администратора рекомендации.