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 администратора

RU.ЦБМК. 00124-01 93 01

2022

Содержание

Список сокращений 3

1. Введение 4

2. Состав компонентов ПО и его среды функционирования 5

3. Порядок действий по приемке ПО 6

4. Порядок действий по безопасной установке и настройке 7

4.1. Установка служебных компонентов и среды выполнения 7

4.2. Установка СПО KATA 15

Список сокращений

БД	–	база данных
ОС	–	операционная система
ПО	–	программное обеспечение
СУБД	–	система управления базами данных

1. Введение

«Специальное программное обеспечение взаимодействия с Kaspersky Anti Targeted Attack Platform» (далее по тексту – «СПО KATA») обеспечивает потребности Заказчиков информационных систем, не имеющих подключений к сетям связи общего доступа, в обеспечении контролируемой отправки на проверку в Kaspersky Anti Targeted Attack Platform файлов из выделенной папки.

Настоящее руководство администратора содержит описание действий по приемке поставленного ПО и действий по его безопасной установке и настройке.

2. Состав компонентов ПО и его среды функционирования

В состав ПО входят следующие компоненты:

- служба мониторинга файлов и взаимодействия со средством защиты от целевых атак Kaspersky Anti Targeted Attack Platform (СЗЦА КАТА);
- встраиваемая СУБД SQLite для сбора и хранения статистики.

Среда функционирования ПО включает:

- операционную систему Microsoft Windows 10 и выше;
- программное обеспечение ASP.NET Core 3.1 Runtime - Windows Hosting Bundle и выше (среда выполнения ядра ASP.NET, позволяющая запускать существующие веб-приложения и серверные приложения);
- DB Browser for SQLite (клиент СУБД, обеспечивающий работу со встроенной СУБД SQLite).

3. Порядок действий по приемке ПО

При приемке ПО администратору необходимо проверить целостность упаковки и пломб, комплектность поставки в соответствии с таблицей 1.

Таблица 1 – Комплектность поставки ПО

Обозначение	Наименование (обозначение)	Кол-во	Примечание
RU.ЦБМК.00124-01 RU.ЦБМК.00124-01 92 01 RU.ЦБМК.00124-01 93 01	Комплект установки в составе: Дистрибутив ПО; Руководство пользователя; Руководство администратора.	1	Поставляется на компакт-диске

Комплект установки ПО поставляется на компакт-диске, содержащем:

- папку с дистрибутивом ПО;
- Руководство пользователя;
- Руководство администратора.

Папка Distr содержит файлы дистрибутива ПО и папку Config, содержащую конфигурационный файл с настройками приложения, такими как доступ к БД, настройка директорий для сертификатов и проверяемых файлов, настройки модуля взаимодействия с СЗЦА КАТА и авторизованных систем, временных интервалов и т.д.

4. Порядок действий по безопасной установке и настройке

СПО КАТА должно устанавливаться в операционной системе Microsoft Windows. Управление БД СПО КАТА должно выполняться в СУБД SQLite.

4.1. Установка служебных компонентов и среды выполнения

4.1.1. Установка компонента для работы с СУБД

Порядок установки:

1. Скачайте актуальный дистрибутив с официального сайта DB Browser for SQLite.
2. Запустите пакет установщика и последовательно выполните предложенные мастером по установке шаги (рисунок 1-5).

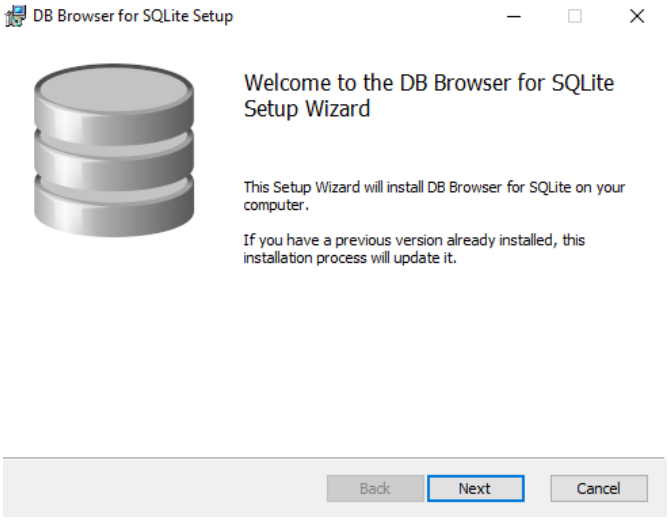


Рисунок 1

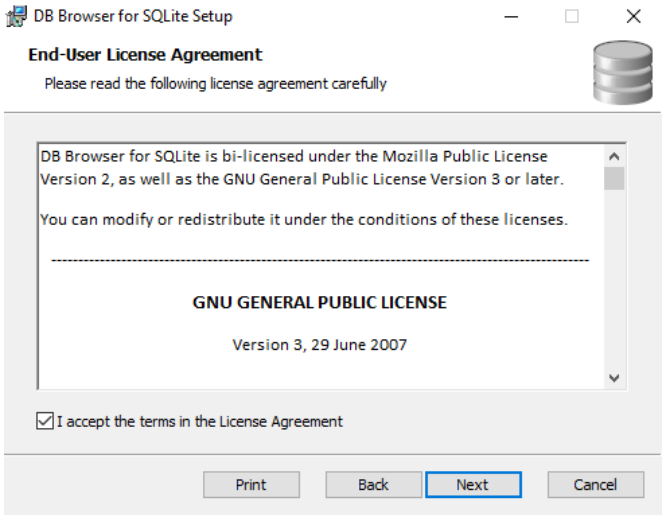


Рисунок 2

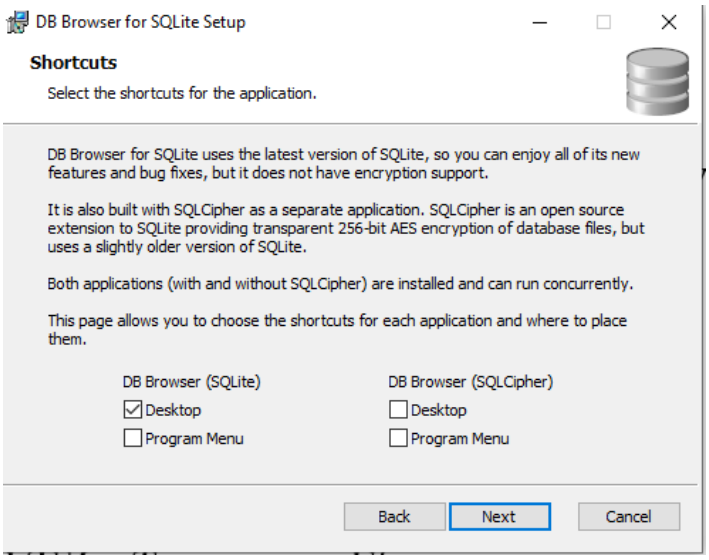


Рисунок 3

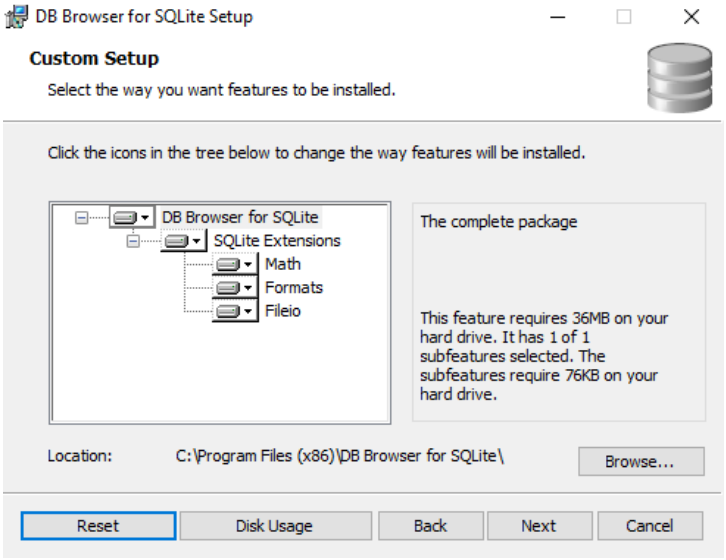


Рисунок 4

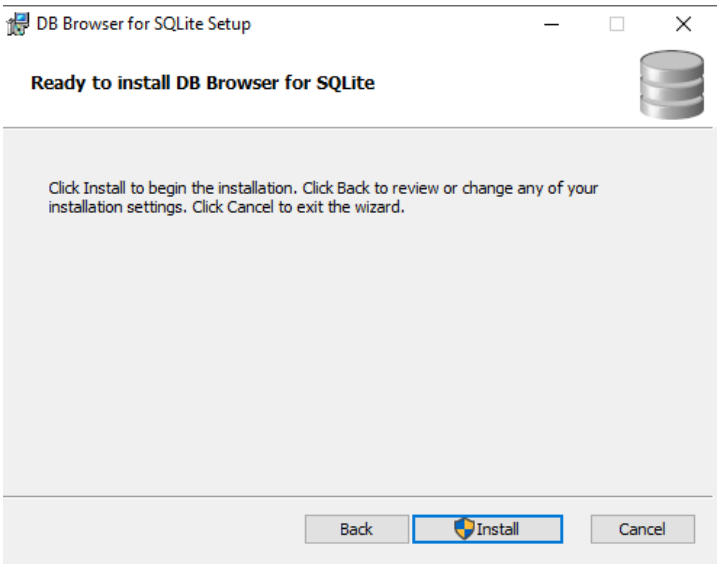


Рисунок 5

3. Установка завершена.

4.1.2. Порядок создания базы данных СПО КАТА

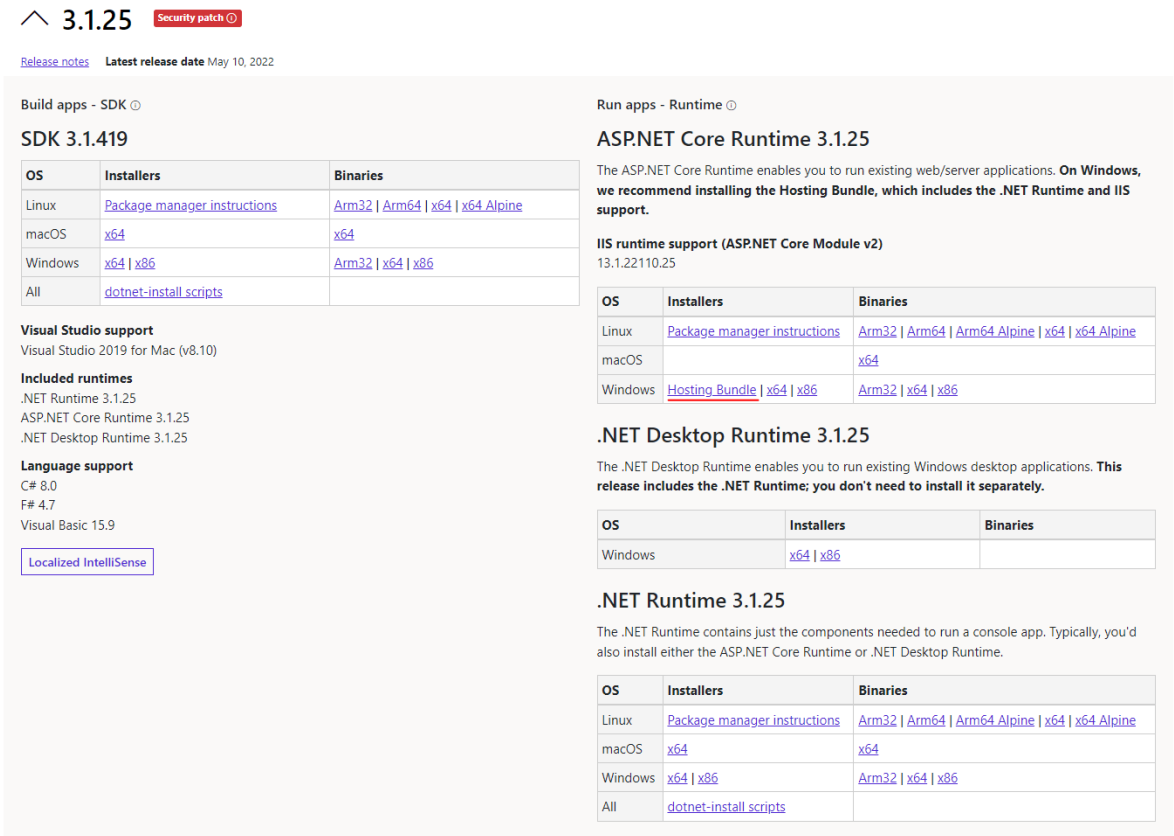
Проверка наличия БД StatisticOperationFile.db и ее создание выполняется автоматически при инициализации программы.

Важно: в случае возникновении ошибок во время работы с БД необходимо остановить работу ПО нажатием комбинации клавиш Ctrl+C и затем выполнить удаление файла БД StatisticOperationFile.db и повторно запустить ПО.

4.1.3. Установка среды выполнения ASP.NET Core 3.1 Runtime-Windows Hosting Bundle

Порядок установки:

1. Скачайте актуальный дистрибутив с официального сайта Microsoft.



3.1.25 Security patch

Release notes **Latest release date** May 10, 2022

Build apps - SDK

SDK 3.1.419

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm64 | x64 | x64 Alpine
macOS	x64	x64
Windows	x64 | x86	Arm32 | x64 | x86
All	dotnet-install scripts	

Visual Studio support
Visual Studio 2019 for Mac (v8.10)

Included runtimes
.NET Runtime 3.1.25
ASP.NET Core Runtime 3.1.25
.NET Desktop Runtime 3.1.25

Language support
C# 8.0
F# 4.7
Visual Basic 15.9

Localized IntelliSense

Run apps - Runtime

ASP.NET Core Runtime 3.1.25

The ASP.NET Core Runtime enables you to run existing web/server applications. **On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.**

IIS runtime support (ASP.NET Core Module v2)
13.1.22110.25

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS		x64
Windows	Hosting Bundle | x64 | x86	Arm32 | x64 | x86

.NET Desktop Runtime 3.1.25

The .NET Desktop Runtime enables you to run existing Windows desktop applications. **This release includes the .NET Runtime; you don't need to install it separately.**

OS	Installers	Binaries
Windows	x64 | x86	

.NET Runtime 3.1.25

The .NET Runtime contains just the components needed to run a console app. Typically, you'd also install either the ASP.NET Core Runtime or .NET Desktop Runtime.

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS	x64	x64
Windows	x64 | x86	Arm32 | x64 | x86
All	dotnet-install scripts	

Рисунок 6

2. Запустите пакет установщика и последовательно выполните предложенные мастером по установке шаги (рисунок 7-9).

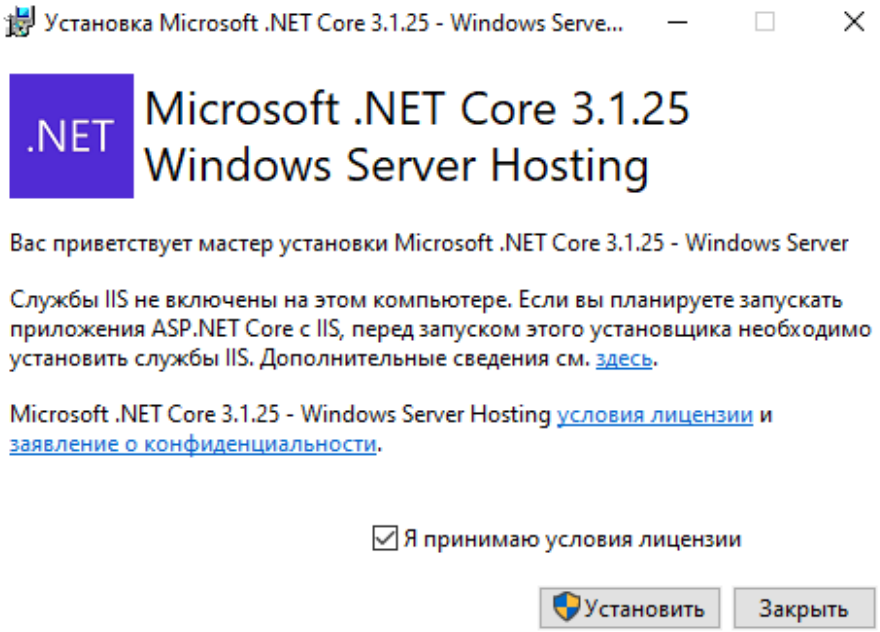


Рисунок 7

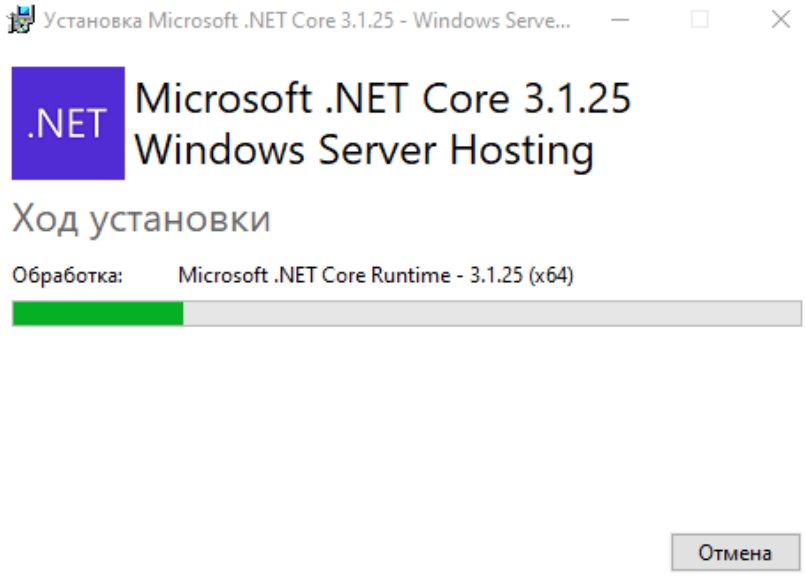


Рисунок 8

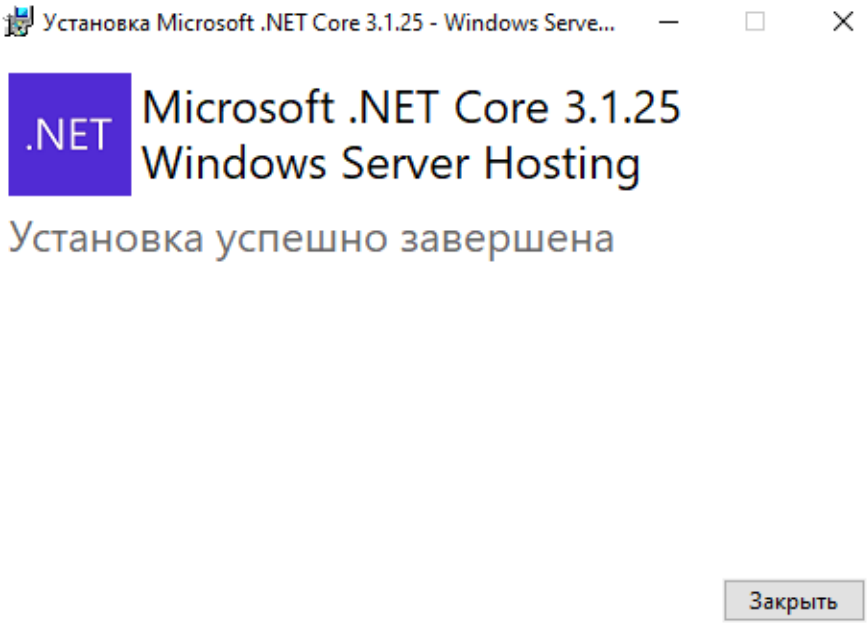


Рисунок 9

Установка среды выполнения ASP.NET Core 3.1 Runtime - Windows Hosting Bundle завершена.

4.1.4. Настройка параметров СПО КАТА

В конфигурационном файле \Distr\Config\ServerConfig.json необходимо установить значения для параметров приложения.

1. Настройка раздела CommonAppProperties с общими параметрами приложения:

Параметр	Описание	Пример
UrlCentralNodeKatap	Ip адрес СЗЦА КАТА	"UrlCentralNodeKatap": "https://192.168.52.100:443"
WorkPath	Рабочий каталог для работы с файлами	"WorkPath": "Files\\"
PathComplete	Каталог для обработанных файлов	"PathComplete": "Operating\\Complete\\"
PathError	Каталог для файлов, вызывающих ошибку при проверке	"PathError": "Operating\\Error\\"
TimeoutConnection	Интервал ожидания ответа от СЗЦА в минутах	"TimeoutConnection": 3
CountTryGetFile	Количество попыток ожидания доступности файла	"CountTryGetFile": 20

2. Настройка раздела MonitoringProperties с параметрами мониторинга:

Параметр	Описание	Пример
TimeoutSendFileForCheck	Период отправки файлов на проверку в СЗЦА в миллисекундах	"TimeoutSendFileForCheck": 1800000
CountFilesInQueueToSendForCheck	Количество файлов в очереди на отправку в СЗЦА	"CountFilesInQueueToSendForCheck": 20
TimeoutClearInfo	Период очистки информации о проверке в миллисекундах	"TimeoutClearInfo": 180000
CoutCycleForClearDB	Количество циклов проверки перед очисткой базы	"CoutCycleForClearDB": 3

3. Настройка раздела MonitoringProperties:ConfigFtpList с параметрами мониторинга файлов FTP источника:

Параметр	Описание	Пример
SystemId	Идентификатор внешней системы для СЗЦА KATA	"SystemId": "sensorFTP_CBI1"
NameFtpServer	Наименование внешней системы для СЗЦА KATA	"NameFtpServer": "CBI"
Url	Путь к целевой папке FTP	"Url": "ftp://192.168.3.2/Storage/TEST"
Login	Логин для авторизации на ресурсе FTP	"Login": "userLogin"
Password	Пароль для авторизации на ресурсе FTP	"Password": "userPassword"
Timeout	Период повторного обращения к FTP в миллисекундах	"Timeout": 60000
Pattern	Регулярное выражение для выборки информации о файлах на FTP	"Pattern": "(\\d+)\\s+(\\w+\\s+\\d{1,2})\\s+(\\d{2}:\\d{2})\\s+(.*\\..+)"
DateFormat	Формат даты на FTP	"DateFormat": "MMMd"
TimeFormat	Формат времени на FTP	"TimeFormat": "HH:mm"
UsePassive	Использование пассивного или активного режима на FTP	"UsePassive": true
FilterFile	Параметр в конфигурационном файле FTP фильтрует файлы по наличию в наименовании ключевых слов	

Параметр	Описание	Пример

	"FilterFile": {
	"ExceptFileName": [
	"update",
	"upd"
	],
	"IncludeFileName": [
	"file"
	]
	}	

Например, игнорирует файлы содержащие "update","upd", забирает только файлы включающие "file":
"FilterFile": {
"ExceptFileName": ["update","upd"],
"IncludeFileName": ["file"]
}
Например, игнорирует файлы содержащие "update","upd", забирает все другие файлы так как параметр не задан:
"FilterFile": {
"ExceptFileName": ["upd"],
"IncludeFileName": []
}		

4. Настройка раздела MonitoringProperties:ConfigFileWatcher с параметрами для директории мониторинга файлов с использованием библиотечного системного мониторинга:

Параметр	Описание	Пример
Url	Путь к папке для мониторинга файлов	"Url": "\\\\192.168.3.2\\Storage\\TESTWATCHER"
Login	Логин доля авторизации	"Login": "userLogin"
Password	Пароль для авторизации	"Password": "userPassword"
IsActive	Статус активации режима мониторинга	"IsActive": false
Примечание: параметр IsActive=true должен быть активен только у одного из параметров ConfigFileWatcher/ConfigMonitoringFolder		

5. Настройка раздела MonitoringProperties:ConfigMonitoringFolder с параметрами для директории мониторинга файлов с использованием самописного мониторинга:

Параметр	Описание	Пример
Url	Путь к папке для мониторинга файлов	"Url": "Z:\\"
Login	Логин доля авторизации	"Login": "userLogin"
Password	Пароль для авторизации	"Password": "userPassword"
Timeout	Параметр временной задержки в миллисекундах между циклами запроса информации о новых файлах	"Timeout": 15000
Owerwrite	Параметр, указывающий перезаписываются ли файлы в папке	"Owerwrite": true
IsActive	Статус активации режима мониторинга	"IsActive": true
Примечание: параметр IsActive=true должен быть активен только у одного из параметров ConfigFileWatcher/ConfigMonitoringFolder		

6. Настройка раздела MonitoringProperties:Systems с параметрами для сопоставления авторизованных в СЗЦА КАТА внешних систем с сертификатами на сервере:

Параметр	Описание	Пример
SystemId	Идентификатор внешней системы	"SystemId": "sensorFTP_CBI1"
SensorInstanceId	Идентификатор экземпляра сенсора для КАТА	"SensorInstanceId": "sensorGuid"
SensorId	Идентификатор сенсора для СЗЦА КАТА	"SensorId": "Guid"
SertPath	Путь к сертификату .pem	"SertPath": "D:\\cert\\System\\kata_sys2_cert.pem"
KeyPath	Путь к ключу .key	"KeyPath": "D:\\cert\\System\\kata_sys2_private.key"
PFXPath	Путь к сертификату .pfx	"PFXPath": "D:\\cert\\System\\server.pfx"
Password	Пароль, заданный при генерации сертификата	"Password": "sertPassword"
FilterFile	Для определения отношения файла к системе на основе регулярного выражения примененного к наименованию файла	"FilterFile": ".*sysName.*\\..*"

Настройка параметров ПО завершена.

4.2. Установка СПО КАТА

1. Перенести содержимое папки Distr в целевую папку на АРМ.

   Примечание: не рекомендуется выбирать системные диски для размещения элементов программы или в качестве рабочих каталогов.

2. Запуск командной строки с повышенными правами Администратора.
3. Установка сервиса осуществляется посредством выполнения команды:

```
sc create <Наименование службы> binPath=<Путь к исполняемому файлу .exe дистрибутива>
```

Результат успешного выполнения команды представлен ниже:

```
C:\Windows\system32>sc create Kata binPath=D:\TestKata\IntegrationKATA.exe
[SC] CreateService: успех
```

4. Скорректировать настройки в конфигурационном файле \Config\ServerConfig.json
5. Перенести в целевое расположение на АРМ сертификаты авторизованных внешних систем.
6. Далее, выполнив команду services.msc в оснастке «Службы» операционной системы Windows, найти созданную службу и запустить ее.

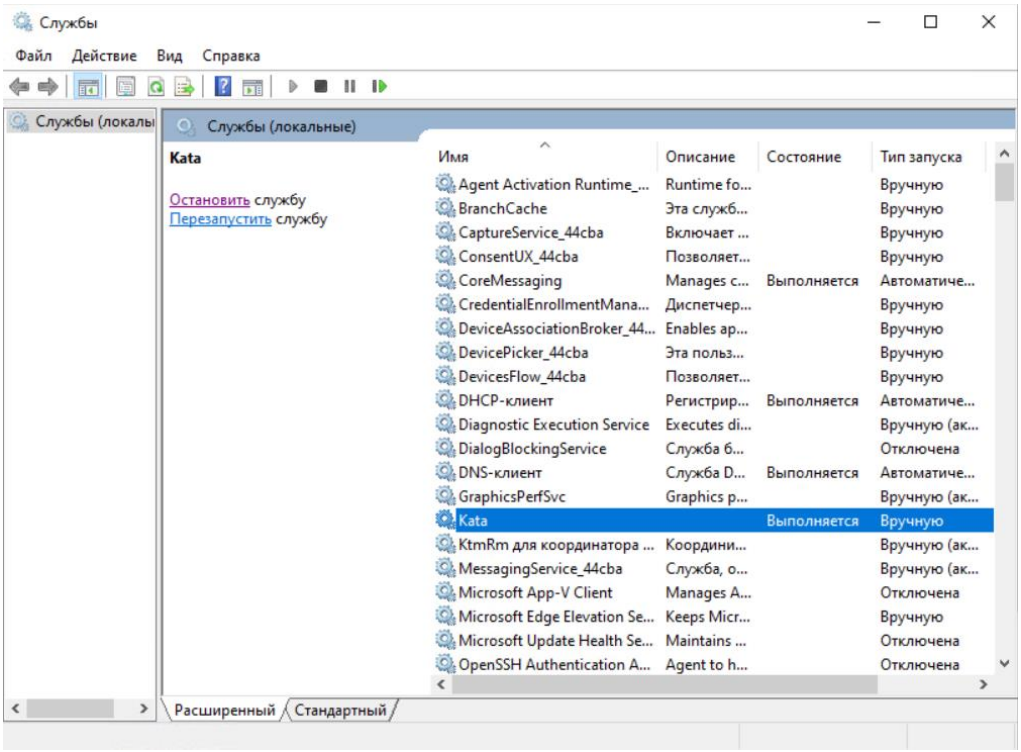


Рисунок 10

Установка ПО завершена.