?????? ? kesl-control ? avp.com

KESL-CONTROL – KES Linux

Для возможности локального управления KESL в него встроена утилита kesl-control. Она позволяет просматривать различные параметры состояния, создавать и запускать задачи. Для ознакомления с полным списком возможностей утилиты выполните в терминале команду `kesl-control`

Для просмотра общей информации о kesl выполните команду :

```
kesl-control --app-info
```

`kesl-control --get-app-settings` — вывод списка параметров приложения вывод списка параметров приложения

Далее приведены команды, которые могут быть вам полезны в использовании kesl

> Важно! Ко всем командам kesl-control можно добавить флаг --json. Он позволяет делать вывод команды или запись в файл в json-формате

Работа с лицензиями

`kesl-control -L --query` – получить информацию об используемой лицензии

`kesl-control --add-active-key <код активации или путь до файла ключа>` - добавить активную лицензию.

`kesl-control --add-reserve-key <код активации или путь до файла ключа>` - добавить резервную лицензию.

`kesl-control --remove-active-key` - удалить активный ключ лицензии.

`kesl-control --remove-reserve-key` - удалить резервный ключ лицензии.

`kesl-control --load-mdr-blob /tmp/mdr_blob.p7` - загрузить файл MDR BLOB для активации интеграции с Managed Detection and Responce

Работа с задачами

`kesl-control --get-task-list` - вывести список всех доступных задач. Здесь вы сможете узнать имя и номер задачи для их дальнейшего использования

`kesl-control --get-settings <Имя задачи или её номер>` - получить параметры задачи.

`kesl-control --get-task-state <Имя задачи или её номер>` - получить состояние задачи

`kesl-control --start-task <Имя задачи или её номер>` - запустить указанную задачу

`kesl-control --stop-task <Имя задачи или её номер>` - остановить указанную задачу

`kesl-control --suspend-task <Имя задачи или её номер>- приостановить задачу.`

`kesl-control --resume-task <Имя задачи или её номер>` - возобновить выполнение задачи.

`kesl-control --get-schedule <Имя задачи или её номер>` - получить расписание задачи

`kesl-control --get-schedule <Имя задачи или её номер> --file /tmp/schedule.txt` - сохранить расписание задачи в файл.

`kesl-control --set-schedule <Имя задачи или её номер> --file /tmp/schedule.txt` - применить расписание задачи из файла.

Сканирование

`kesl-control --scan-file <путь к папке или файлу> -- action DisinfectDeleteIfNotPossible` - проверить указанный файл или каталог на угрозы при обнаружении попытаться вылечить файл и удалить, если это невозможно

Для флага –action можно использовать DisinfectInformIfNotPossible (лечить или информировать, если лечение невозможно), Inform (информировать)

`kesl-control --scan-container <идентификатор/имя[:тег]>` - проверить образ контейнера

`kesl-control --scan-ioc --path <путь к ioc-файлам> --excludes /var/log /tmp` - выполнить поиск IOC с исключением указанных путей из области поиска.

`kesl-control --scan-ioc --path path <путь к ioc-файлам> --scope /home` - ограничить область поиска по IOC.

Получение статистики

`kesl-control --get-statistic --files` - показать статистику по наиболее проверяемым файлам

`kesl-control --get-statistic –processes` - показать статистику проверки по наиболее чатозапускаемым процессам

`kesl-control --get-statistic –mountpoints` - показать список точек монтирования

`kesl-control --export-settings --file /tmp/kesl-settings.txt` - экспортировать все параметры приложения в файл.

Работа с карантином и резервным храниищем

`kesl-control --put /tmp/suspicious.file – вручную поместить указанный файл в карантин`

`kesl-control -Q --query -n 30` - получить информацию о файлах в карантине, показать последние 30 элементов.

`kesl-control -Q --mass-remove --query` - удалить файлы из карантина .

`kesl-control -B --query -n 30` - получить информацию о файлах в резервном хранилище, показать последние 30 элементов.

`kesl-control -B --restore <идентификатор_объекта> --file /tmp/restored.file` - восстановить файл из резервного хранилища в указанный путь.

`kesl-control -B --mass-remove --query` - удалить файлы из резервного хранилища по заданному фильтру.

События работы KESL

`kesl-control -E --query  -n 100 --reverse` - получить последние 100 событий работы приложения по показать их в обратном порядке (с конца)

`kesl-control -W` - включить «живой» вывод событий приложения в консоль

Контроль устройств

`kesl-control --get-device-list` - получить список подключённых устройств.

`kesl-control --get-device-list --export <имя файла>` - экспортировать список устройств в файл.

`kesl-control --trusted-devices --list` - показать список доверенных устройств.

`kesl-control --trusted-devices --add <идентификатор>` - добавить устройство в доверенные.

`kesl-control --trusted-devices --delete <идентификатор>` - удалить устройство из доверенных.

`kesl-control --request-temporary-device-access --device-id <идентификатор> --access-duration <длительность в часах> --path <путь к файлу для сохранения запроса о временном доступе>` - создать запрос временного доступа.

`kesl-control --upload-temporary-device-access-key --path /tmp/access.key` - загрузить ключ временного доступа.

Работа с Firewall

`kesl-control -F --query` - получить состояние задачи управления сетевым экраном

`kesl-control --add-rule --name AllowSSH --action allow --protocol tcp --direction in --local any:22 --remote any — добавление правила разрешить входящие SSH-подключения`

`kesl-control --add-rule --name BlockHTTP --action block --protocol tcp --direction out --remote any:80` - заблокировать исходящий HTTP трафик

`kesl-control --add-rule --name AllowDNS --action allow --protocol udp --direction out --remote any:53` - разрешить исходящие DNS запросы

`kesl-control --move-rule --name AllowSSH --at 1` - изменить приоритет правила, переместив его на позицию 1.

`kesl-control --del-rule --name AllowSSH` - удалить правило по имени

`kesl-control --del-rule --index 3` - удалить правило по индексу.

`kesl-control --add-zone Trusted --address 192.168.1.0/24` - добавить сеть в доверенную зону.

Флаг --add-zone поддерживает 3 значения: Trusted, Local или Public

`kesl-control --del-zone Trusted --address 192.168.1.0/24` - удалить сеть из доверенной зоны

`kesl-control --get-blocked-hosts` - получить список заблокированных устройств (компонентом сетевой защиты)

`kesl-control --allow-hosts <идентификатор>` - разблокировать устройство.

Работа с исключениями

`kesl-control --set-settings < идентификатор/имя задачи > -- add-exclusion /opt/app` - добавить путь в исключения задачи проверки

`kesl-control --set-settings < идентификатор/имя задачи > -- del-exclusion /opt/app` - удалить путь из исключений задачи проверки

`kesl-control -N --query auto` - показать автоматически созданные исключения из проверки зашифрованных соединений.

`kesl-control -N --query kl` - показать исключения из проверки зашифрованных соединений, заданные «Лабораторией Касперского».

`kesl-control -N --query user` - показать пользовательские исключения из проверки зашифрованных соединений.

`kesl-control --clear-web-auto-excluded` - очистить список SSL-исключений, автоматически исключённых из проверки

`kesl-control --list-bypass-endpoints` - показать список настроенных исключений из перехвата трафика.

`kesl-control --add-bypass-endpoints --direction out --remote-ip 10.10.10.5 --dst-port 443` - добавить исключение из перехвата для исходящего трафика к указанному IP и порту.

`kesl-control --add-bypass-endpoints --direction in --remote-ip 192.168.1.100 --dst-port 8443` - добавить исключение из перехвата для входящего трафика от указанного IP и порта.

`kesl-control --remove-bypass-endpoints --direction out --remote-ip 10.10.10.5 --dst-port 443` - удалить исключение из перехвата трафика.

`kesl-control --list-certificates` - просмотреть список доверенных корневых сертификатов

`kesl-control --add-certificate <путь к сертификату pem или der>` - добавить сертификатв список доверенных корневых сертификатов

`kesl-control --remove-certificate <субъект сертификата>` - удалить сертификат из списка доверенных корневых сертификатов

`kesl-control --list-bypass-endpoints` - получить список исключений из перехвата трафика

`kesl-control --add-bypass-endpoints --direction out --remote-ip 10.10.10.5 --dst-port 443` - добавить исключение для исходящего HTTPS трафика к IP.

`kesl-control --add-bypass-endpoints --direction in --remote-ip 192.168.1.100 --dst-port 8443` - добавить исключение для входящего трафика.

`kesl-control --remove-bypass-endpoints --direction out --remote-ip 10.10.10.5 --dst-port 443` - - удалить исключение из перехвата трафика

`kesl-control --set-settings < идентификатор/имя задачи > -- add-path /opt/` - добавить путь в область задачи проверки

`kesl-control --set-settings < идентификатор/имя задачи > -- del-path /opt/` - удалить путь из области задачи проверки

`kesl-control --set-settings < идентификатор/имя задачи >` - применить значения по умолчанию для параметров задачи

Интеграция с KATA и KEDR

`kesl-control --add-kataedr-server-certificate <путь до сертификата>` - добавить сертификат сервера KATA/OSMP.

`kesl-control --remove-kataedr-server-certificate` - удалить сертификат сервера KATA/OSMP.

`kesl-control --query-kataedr-server-certificate` - показать сертификат сервера KATA/OSMP.

Для выбора интеграции с EDR Expert (OSMP) необходимо дополнительно использовать флаг --server-type <response|telemetry>. Т.к. сертификаты для сбора событий и реагирования используются разные сертификаты. Таким образом команды будут составляться по следующей логике:

`kesl-control --add-kataedr-server-certificate <путь до сертификата> --server-type telemetry` - добавить сертификат сервера телеметрии

`kesl-control --add-kataedr-server-certificate <путь до сертификата> --server-type response` - добавить сертификат сервера реагирования

`kesl-control --add-kataedr-client-certificate <путь до сертификата>` - добавить клиентский сертификат KATA/OSMP.

`kesl-control --remove-kataedr-client-certificate` - удалить клиентский сертификат KATA/OSMP.

`kesl-control --query-kataedr-client-certificate` - показать клиентский сертификат KATA/OSMP.

Для выбора интеграции с EDR Expert (OSMP) необходимо также дополнительно использовать флаг --server-type <response|telemetry> как указано в предыдущем блоке команд.

Интеграция с NDR

`kesl-control --add-katandr-server-certificate <путь до сертификата>` - добавить сертификат сервера NDR.

`kesl-control --remove-katandr-server-certificate` - удалить сертификат сервера NDR.

`kesl-control --query-katandr-server-certificate` - показать сертификат сервера NDR.

`kesl-control --add-katandr-client-certificate <путь до сертификата>- добавить сертификат клиента NDR.`

`kesl-control --remove-katandr-client-certificate` - удалить сертификат клиента NDR.

`kesl-control --query-katandr-client-certificate` - показать сертификат клиента NDR.

Интеграция с Sandbox

`kesl-control --add-sandbox-server-certificate <путь до сертификата>` - добавить сертификат сервера Sandbox.

`kesl-control --remove-sandbox-server-certificate` - удалить сертификат сервера Sandbox.

`kesl-control --query-sandbox-server-certificate` - показать сертификат сервера Sandbox.

`kesl-control --add-sandbox-client-certificate <путь до сертификата>` - добавить клиентский сертификат Sandbox.

`kesl-control --remove-sandbox-client-certificate` - удалить клиентский сертификат Sandbox.

`kesl-control --query-sandbox-client-certificate` - показать клиентский сертификат Sandbox.

`kesl-control --sandbox <путь до файла или директории>` - отправить файл/директорию на проверку в Sandbox.

Интеграция KUMA

`kesl-control --add-kuma-server-certificate <путь до сертификата>` - добавить сертификат сервера KUMA.

`kesl-control --remove-kuma-server-certificate` - удалить сертификат сервера KUMA.

`kesl-control --query-kuma-server-certificate` - показать сертификат сервера KUMA.

`kesl-control --add-kuma-client-certificate <путь до сертификата>` - добавить клиентский сертификат KUMA.

`kesl-control --remove-kuma-client-certificate` - удалить клиентский сертификат KUMA.

`kesl-control --query-kuma-client-certificate` - показать клиентский сертификат KUMA.

Интеграция MDR

`kesl-control --load-mdr-blob <путь до blob-файла>` - загрузить файл MDR BLOB.

`kesl-control --remove-mdr-blob` - удалить файл MDR BLOB.

При использовании KESL в режиме Лёгкого агента

`kesl-control --svm-info` - информация о подключении к SVM.

`kesl-control --viis-info` - информация о подключении к Серверу интеграции.

`kesl-control --ksvla-info` – общая информация о состоянии Лёгкого агента

AVP.COM – KES Windows

Для возможности локального управления KES Windows через командную строку можно использовать утилиту avp.com. Утилита доступна по пути C:\Program Files (x86)\Kaspersky Lab\KES.<версия>. Она позволяет просматривать различные параметры состояния, создавать и запускать задачи. Для ознакомления с полным списком возможностей утилиты выполните в командной строке по указанному ранее пути команду:

```
avp.com –help
```

ADDKEY, LICENSE, MDRLICENSE — работа с лицензиями

`avp.com ADDKEY <путь к license.key>` - добавить ключ лицензии (код не поддерживается)

`avp.com LICENSE /CHECK` - вывести информацию о всех лицензиях

`avp.com LICENSE /CHECK <Идентификатор лицензии | Серийный номер ключа>` - вывести информацию о конкретной лицензии.

`avp.com MDRLICENSE /ADD <путь к mdr_blob.p7>` - добавить blob-файл для активации MDR.

`avp.com MDRLICENSE /DEL` - удалить MDR blob-файл.

STATUS, STATISTICS, START, STOP — запуск задач и компонентов

`avp.com STATUS – вывести полный список и показать статус всех задач и компонентов.`

`avp.com STATUS <имя задачи или компонента>` - статус конкретной задачи/компонента.

`avp.com STATISTICS <имя задачи или компонента>` - просмотр статистики работы конкретной задачи/компонента.

`avp.com START <имя задачи или компонента>` - запуск конкретной задачи/компонента. /S – в асинхронном режиме

`avp.com START <имя задачи или компонента> /R:<путь к файлу>` - записать критические события.

`avp.com START <имя задачи или компонента>/RA:<путь к файлу>` - записать все события.

`avp.com STOP <имя задачи или компонента>` - остановка конкретной задачи/компонента

SCAN — сканирование

`avp.com SCAN C:\` - проверить указанный каталог.

`avp.com SCAN C:\` - проверить указанный каталог.

`avp.com SCAN /ALL` - проверить весь компьютер.

`avp.com SCAN /MEMORY` - проверить оперативную память.

`avp.com SCAN /STARTUP` - проверить объекты автозагрузки.

`avp.com SCAN /REMDRIVES` - проверить съемные носители.

`avp.com SCAN /FIXDRIVES` - проверить локальные диски.

`avp.com SCAN /NETDRIVES` - проверить сетевые диски.

`avp.com SCAN C:\ /i0` - только отчёт без лечения.

`avp.com SCAN C:\ /i3` - лечить, при невозможности удалить (по умолчанию).

`avp.com SCAN C:\ /i4` - удалить заражённые файлы.

`avp.com SCAN C:\ -e:a` - исключить архивы из проверки.

`avp.com SCAN C:\ -e:b` - исключить почтовые базы.

`avp.com SCAN C:\ -e:*.iso` - исключить файлы по маске.

`avp.com SCAN C:\ /R:scan.log` - записать критические события в отчёт.

`avp.com SCAN C:\ /RA:scan.log` - записать все события.

`avp.com SCAN C:\ /S` - запустить асинхронно.

IOCSCAN — поиск индикаторов компрометации

`avp.com HELP IOCSCAN` - полный перечень возможных функций сканирования по IOC

`avp.com IOCSCAN <путь к IOC>` - выполнить IOC-сканирование по файлу.

`avp.com IOCSCAN /PATH=<путь к папке с IOC-файлами>` - выполнить сканирование по набору IOC из папки

`avp.com IOCSCAN <путь к IOC> /FILES=on /DRIVES=ALL` - проверка файлов на всех дисках

`avp.com IOCSCAN <путь к IOC> /EXCLUDES=c:\temp;c:\backup` - исключить пути.

`avp.com IOCSCAN <путь к IOC> /SCOPE=c:\windows;c:\users` - ограничить область поиска.

YARA — сканирование по правилам YARA

`avp.com YARA <путь к правилу>` - выполнить сканирование по одному правилу.

`avp.com YARA <путь к правилу> <путь к правилу>` - использовать несколько правил.

`avp.com YARA /PATH=<путь к каталогу с правилами>` - использовать каталог с правилами

`avp.com YARA <путь к правилу> /SCANFOLDERS=<путь к папке> /RECURSIVE=on` - сканировать указанную папку рекурсивно.

`avp.com YARA <путь к правилу> /SCANMEMORY=on` - сканировать память процессов.

`avp.com YARA <путь к правилу> /FASTSCAN=on` - включить сканирование в быстром режиме

`avp.com YARA <путь к правилу> /SCANFOLDERS=<путь к папке> /EXCLUDES=<путь к папке>` - исключить каталог

`avp.com YARA <путь к правилу> /LOGFOLDER=<путь к файлу>` - сохранить результат сканирования в отчёт.

UPDATE — обновление баз

`avp.com UPDATE` - обновить базы.

`avp.com UPDATE /local` - выполнить локальную задачу обновления.

`avp.com UPDATE " URL или путь к папке"` - обновить с указанного источника.

`avp.com UPDATE /R:<путь к файлу>` - записать критические события.

`avp.com UPDATE /RA:<путь к файлу>` - записать все события.

`avp.com UPDATE /S — запустить задачу обновления асинхронно.`

ROLLBACK — откат обновления баз

`avp.com ROLLBACK` - откатить базы к предыдущей версии.

`avp.com ROLLBACK /R:<путь к файлу>` - записать критические события.

`avp.com ROLLBACK /RA:<путь к файлу>` - записать все события.

`avp.com ROLLBACK /S` - запустить асинхронно.

TRACES — работа с трассировками

`avp.com TRACES on` - включить трассировку.

`avp.com TRACES off` - отключить трассировку.

`avp.com TRACES on 500` - включить трассировку уровень 500 (по умолчанию).

Доступны уровни 100, 200, 300, 400, 500, 600.

`avp.com TRACES on 500 file` - писать трассировку в один файл.

`avp.com TRACES on 500 rot /rotcount=5 /rotsize=50` - запись трассировки в ограниченное количество файлов rotcount ограниченного размера rotsize (Мб) с последующей перезаписью.

`avp.com TRACES compress /<on|off>` - включить/выключить сжатие трассировок.

RESTORE — восстановление из файлов из карантина и резервного хранилища

`avp.com RESTORE /QUARANTINE eicar.com` - восстановить файл из карантина.

`avp.com RESTORE /BACKUP eicar.com` - восстановить файл из резервного хранилища.

`avp.com RESTORE /REPLACE C:\eicar.com – восстановить из карантина с заменой существующего файла.`

EXPORT, IMPORT — экспорт и импорт настроек

`avp.com STATUS – вывести список всех задач и компонентов`

`avp.com EXPORT <имя задачи или компонента> <путь к файлу .txt или .dat>` - экспорт настроек задачи или компонента в файл

`avp.com IMPORT <путь к файлу .dat>` - импорт настроек задачи или компонента из файла (поддерживаются только бинарные .dat файлы)

EDRKATA — интеграция с Kaspersky Anti Targeted Attack

`avp.com EDRKATA /SHOW` - показать настройки подключения KATA

`avp.com EDRKATA /SET /servers=<адрес:порт> /server-certificate=<сертификат сервера> /client-certificate=<клиентский сертификат> /client-certificate-password=<пароль клиентского сертификата> /timeout=<таймаут подключения в секундах> /sync-period=<период синхронизации в минутах>` - настроить подключение к серверу KATA.

`avp.com HELP EDRKATA` - получить полный список параметров подключения к KATA

EDREXPERTONPREM — интеграция с EDR Expert On-Premise

`avp.com EDREXPERTONPREM /SHOW` - показать настройки EDR Expert

`avp.com EDREXPERTONPREM /SET /mode=EDRKATA /servers=<адрес:порт>/server-certificate=<сертификат сервера>` - режим интеграции с EDR KATA

`avp.com EDREXPERTONPREM /SET /mode=EDRExpertOnPrem /servers==<адрес:порт> /server-certificate==<сертификат сервера>` - режим интеграции с EDR (OSMP)

`avp.com EDREXPERTONPREM /SET /mode=< EDRKATA | EDRExpertOnPrem> /servers==<адрес:порт> /server-certificate==<сертификат сервера> /client-certificate=<клиентский сертификат> /client-certificate-password=<пароль клиентского сертификата> /timeout=<таймаут подключения в секундах> /sync-period=<период синхронизации в минутах>` - режим интеграции с дополнительными параметрами

`avp.com HELP EDREXPERTONPREM` - получить полный список параметров подключения к EDR On-Premise

NDR — интеграция с Network Detection and Response

`avp.com NDR /SHOW` - показать настройки NDR

`avp.com NDR /SET /servers=<адрес:порт> /server-certificate=<сертификат сервера> /client-certificate=<клиентский сертификат> /client-certificate-password=<пароль клиентского сертификата> /timeout=<таймаут подключения в секундах> /sync-period=<период синхронизации в минутах>` - настроить подключение к серверу KUMA.

`avp.com HELP NDR` - получить полный список параметров подключения к KUMA

SANDBOX — интеграция с Sandbox

`avp.com SANDBOX /SHOW` - показать настройки Sandbox.

`avp.com SANDBOX /SET --servers=<адрес:порт Sandbox> --pinned-certificate=<путь к сертификату сервера> --client-certificate=< путь к клиентскому сертификату> --client-certificate-password=<пароль клиентского сертификата> --timeout=<таймаут в мс, по умолчанию 5000> --mode=<KSB| KATAManual | KATAAuto | KATAFull> – установить параметры Sandbox.`

KSB – автоматическая отправка в песочницу KSB KATAManual – ручная отправка в песочницу KATA KATAAuto – автоматическая отправка в песочницу KATA KATAFull – Как ручная, так и автоматическая отправка данных в песочницу KATA

KUMA — интеграция с Kaspersky Unified Monitoring and Analysis

`avp.com KUMA /SHOW` - показать настройки подключения KUMA

`avp.com KUMA /SET /servers=<протокол://адрес:порт> /server-certificate=<сертификат сервера> /client-certificate=<клиентский сертификат> /client-certificate-password=<пароль клиентского сертификата> /timeout=<таймаут подключения в секундах>` - настроить подключение к серверу KUMA.

`avp.com HELP KUMA` - получить полный список параметров подключения к KUMA

TELEMETRYFILTERS — настройка фильтрации телеметрии

`avp.com TELEMETRYFILTERS /EXPORT <путь к файлу>` - экспорт фильтрации телеметрии в файл

`avp.com TELEMETRYFILTERS /IMPORT <путь к файлу>` - импорт фильтрации телеметрии из файла.

KSN — управление Kaspersky Security Network

`avp.com KSN /GLOBAL` - включить стандартный KSN.

`avp.com KSN /PRIVATE <путь к файлу .pkcs7>` - включить KPSN с файлом настроек.

ISOLATION — сетевая изоляция хоста

`avp.com ISOLATION /STAT` - показать статус сетевой изоляции.

`avp.com ISOLATION /OFF` - отключить изоляцию.

PREVENTION — управление запретом запуска объектов

`avp.com PREVENTION /SHOW` - показать состояние всех задач Prevention.

`avp.com PREVENTION /SHOW EDR` - показать настройки Prevention для EDR.

`avp.com PREVENTION /SHOW KATA` - показать настройки Prevention для KATA.

`avp.com PREVENTION /SHOW KICS` - показать настройки Prevention для KICS.

`avp.com PREVENTION /DISABLE` - отключить все задачи Prevention.

`avp.com PREVENTION /DISABLE EDR` - отключить Prevention для EDR.

SVMINFO, VIISINFO, KSVLAINFO – Работа с KES в режиме Лёгкого агента

`avp.com SVMINFO` - показать информацию о подключении к SVM

`avp.com VIISINFO` - показать информацию о подключении к серверу интеграции.

`avp.com KSVLAINFO` - показать информацию о работе приложения в режиме Лёгкого агента.

Дополнительные команды

`avp.com EXIT` - завершить работу KES

`avp.com EXITPOLICY — отключить применяемую с KSC политику`

`avp.com STARTPOLICY` - включить применяемую с KSC политику

`avp.com RESETMDRMACHINEID` - сбросить идентификатор MDR

`avp.com SERVERBINDINGDISABLE` - отключить защиту подключения к серверу администрирования

`avp.com PBATESTRESET` - удалить информацию о несовместимости системного диска и агента аутентификации. Может быть необходимо Перед запуском полнодискового шифрования. Подробнее см. в справке

Revision #5
Created 2 April 2026 12:07:26 by Сергей
Updated 3 April 2026 13:33:58 by Сергей