Troubleshooting

В данном разделе описывается процесс сбора информации для обращения в техническую поддержку

- Решение наиболее частых проблем с KICS for Networks
- Получение информации с KICS for Networks для обращения в техническую поддержку
- Правило оформления запроса в техническую поддержку
- Получение информации с KICS for Nodes для обращения в техническую поддержку
  - Kaspersky Industrial CyberSecurity for Windows Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
- Руководство по сбору логов с устройства при возникновении проблем с установкой KICS for nodes (windows)

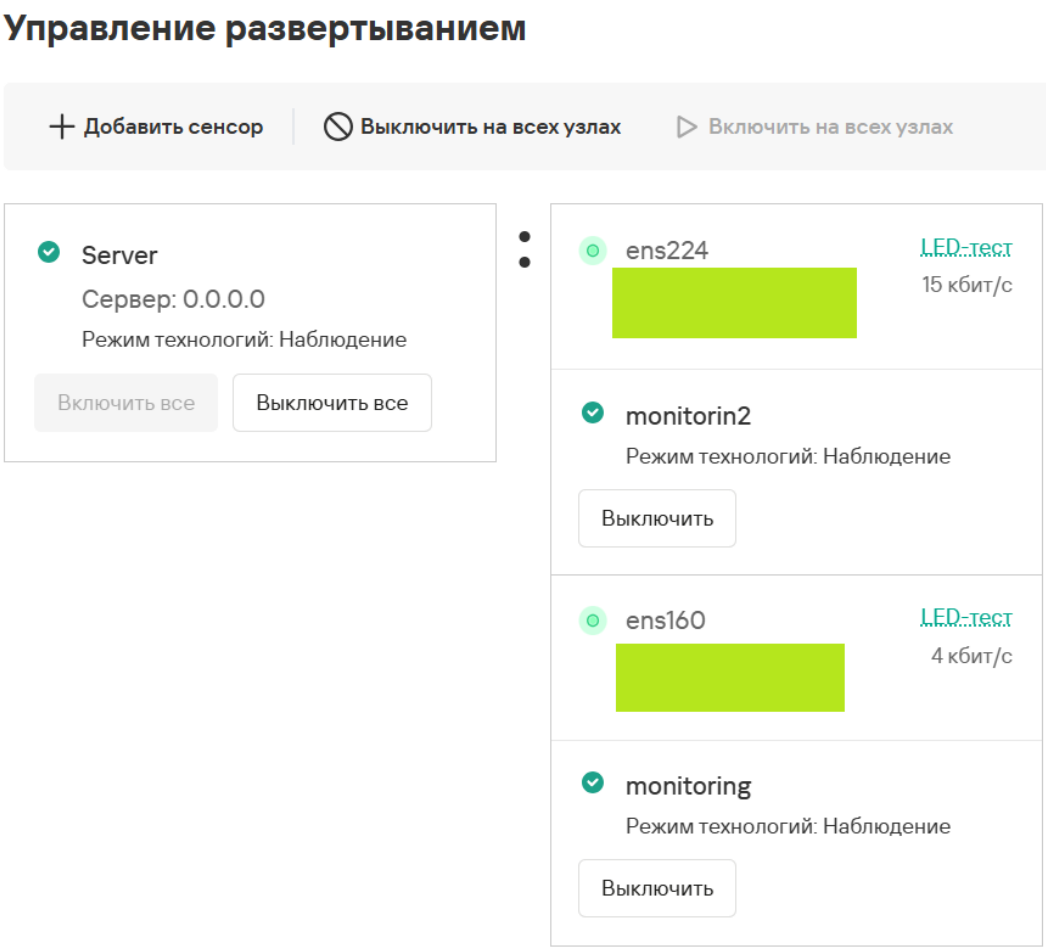
??????? ???????? ?????? ??????? ? KICS for Networks

?? ????????? ?????? ?? ????? ???????????, ? ??? ????? ???? ???????? ? ??? ??????????

1. ???????? ????????? ????? ???????????

Программа зарегистрировала событие, описание которого содержит следующий текст: `Отсутствует трафик на точке мониторинга`. В описании события указана длительность отсутствия трафика, имя точки мониторинга и сетевой интерфейс, на который не поступает трафик. Работоспособность точки мониторинга можно проверить в веб-интерфейсе KICS for Networks в разделе **"Параметры → Развертывание".** Первым делом, нужно убедиться, что точка мониторинга включена и её статус отображается как "OK". Также обратите внимание на значение скорости трафика, это значение должно отличаться от нуля.

Также в настройках ОС посмотрите, что сетевой интерфейс **правильно настроен**. Проверьте настройки IP-адреса, маски подсети и шлюза.



2. ???????? ??????????? ???????????

Первым делом нужно убедитесь, что **сетевой кабель** подключен к соответствующему Ethernet-порту сетевого интерфейса точки мониторинга и проверьте, что **сетевой кабель** исправен и надежно подключен.

3. ???????? ????????? SPAN

При подключении точки мониторинга к **сетевому коммутатору** промышленной сети, нужно убедитесь, что на коммутаторе правильно настроено **зеркалирование трафика (SPAN)**. Убедитесь, что трафик перенаправляется на порт, к которому подключена точка мониторинга. Для этого посмотрите состояние SPAN-сессии с помощью следующей команды:

```
#show monitor session <номер сессии>
```

В выводе нужно убедиться, сессия активна (Session Status : Active), и проверить, правильно ли указаны порты или VLAN-ы источника (Source Ports) и порт назначения (Destination Ports).

Для того, чтобы убедиться, что передача трафика реализована корректно, нужно воспользоваться ПО для анализа трафика , например, Wireshark, чтобы записать PCAP-файл. При анализе PCAP-файл вы должны убедиться, что:

- Конфигурации коммутатора выполнены корректно.
- В захваченном трафике должны присутствовать обычные одноадресные пакеты (например, ping или HTTP-запросы). Если вы видите в основном только широковещательные ARP-запросы, это признак неверной настройки SPAN.
- Трафик, проходящий через коммутатор, относится к области мониторинга.
- Присутствуют в трафике OT-протоколы.

image.png

Если по итогу анализа трафика все условия выполняются корректно, но траффик так и не поступает на точку мониторинга KICS for Networks обратитесь в службу технической поддержки через Kaspersky CompanyAccount.

????? ????????? ????? ??????????? ??? ????????? ? ????????? ???????

В списке уведомлений о проблемах в работе программы появляется сообщение о нарушении работы из-за обнаруженных проблем на точке мониторинга.

Как правило, состояние *Ошибка* на **точке мониторинга** может быть связана прежде всего с неподдерживаемым операционным состоянием (operational state), в котором находится сетевой интерфейс. Чтобы точка мониторинга корректно функционировала сетевой интерфейс должен находиться в операционном состоянии *UP.* Если сетевой интерфейс находится, например, в состоянии *UNKNOWN,* то данное состояние переводят точку мониторинга в состояние Ошибка из-за возможных проблем при получении или обработке сетевых пакетов.

Проверить состояние сетевого интерфейса можно с помощью команд `ip link`. На проблемном сетевом интерфейсе наиболее вероятны следующие операционные состояния:

- *DOWN*. В этом случае вы можете перевести интерфейс в операционное состояние *UP* с помощью команды:
  `sudo ip link set <имя интерфейса> up`
- *UNKNOWN*. Такое операционное состояние может быть связано с неправильным добавлением интерфейса. Например, в состоянии *UNKNOWN* могут работать сетевые интерфейсы, добавляемые по умолчанию на виртуальной машине VMware. В этом случае рекомендуется заново добавить (создать) сетевой интерфейс с правильными параметрами, используя соответствующие средства для работы с сетевыми интерфейсами.

После того, как мы перевели сетевой интерфейс в состояние *UP,* нужно перейти в раздел разделе **"Параметры → Развертывание"** и посмотреть состояние точки мониторинга.

?? ?????????? ?????????? ????????????? ? ????????????? ????? ?? ??? ??, ??? ?? ????????? ???????? ????? ?????? ? ??????????? ????????

Перед проведение профилактических и пусконаладочных работ нужно выбрать один из следующих вариантов решения проблемы:

- Оставить включенными все точки мониторинга на Сервере и на сенсорах программы. В этом случае при просмотре сведений о событиях и взаимодействиях устройств учитывайте время и перечень проводимых профилактических и пусконаладочных работ.
- Выключить точки мониторинга, на которые поступает трафик из сегментов промышленной сети, где проводятся профилактические и пусконаладочные работы. Например, если работы проводятся в одном цехе, вы можете выключить точку мониторинга, на которую поступает трафик из этого цеха, и оставить включенными все остальные точки мониторинга.
- Выключить все точки мониторинга на всех узлах с установленными компонентами программы. Вы можете выбрать этот вариант, если профилактические и пусконаладочные работы проводятся во всей промышленной сети.

Если вы выбрали вариант выключить точки мониторинга, сразу же после окончания работ не забудьте их включить.

> Обратите внимание, что злоумышленники могут попытаться получить несанкционированный доступ к сети именно в период профилактических и пусконаладочных работ на АСУ ТП. Для принятия решения о выключении точек мониторинга руководствуйтесь регламентами и процедурами для обеспечения безопасности, принятыми на вашем предприятии.

В случае, если изменились в процессе работ состав или параметры сетевого оборудования промышленной сети (например, MAC-адреса или IP-адреса), внесите соответствующие изменения для контроля процесса, контроля взаимодействий и контроля активов.

??? ??????, ???? ?? ??????? ????? ???????, ?? ??????? ?????????? ?????? ??? ?????? KICS for Networks, ??????????? ????????? ?????????????

Прежде всего нужно убедиться, что сервер удовлетворяет аппаратным и программным требованиям. Для корректной работы KICS for Networks нужно:

1. Освободить на жестком диске компьютера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства, а именно: на сервере объем свободного пространства на жестком диске: 750 ГБ и дополнительно по 250 ГБ для каждой точки мониторинга на этом компьютере. На сенсоре - объем свободного пространства на жестком диске: 50 ГБ и по 250 ГБ для каждой точки мониторинга на этом компьютере.
2. Перезапустить сервисы, обеспечивающие работу компонентов KICS for Networks (При перезагрузке компьютера, который выполняет функции Сервера или сенсора,

происходит автоматический запуск компонентов KICS for Networks).

??? ??? ??????????? ? ???-?????????? KICS for Networks ?????? ????? ????????????? ? ??????????? ??????????? ?? ????????????? ????????? ?? ???????? ???????????

Данное предупреждение о сертификате безопасности возникает в следствии того, что на веб-сервере используется самоподписанный сертификат. Для того, чтобы получить и использовать доверенный сертификат нужно обратиться к системному администратору вашей организации. Следующим шагом будет добавление для веб-сервера доверенного сертификата, для этого нужно перейти в раздел **Параметры → Серверы подключений**.

??? ??????, ???? ? SPAN ???????, ???????????? ? KICS for Networks ???????? ??????????, ?? ??????????? ? ??????? ????????????

Если SPAN-трафик организован через порты, то первым делом нужно посмотреть куда идут физически порты и убедиться в корректности подключения. Если SPAN-трафик организован через VLAN, то нужно посмотреть какие порты подключены к VLAN корпоративного сегмента и какие порты подключены к VLAN промышленного сегмента.

Далее нужно проверить конфигурацию текущих настроек коммутатора с помощью следующей команды:

```
#show monitor session all
```

В выводе убедитесь, что в списке исходных портов или VLAN нет лишних.

В некоторых коммутаторах можно настроить фильтрацию по VLAN. Например, вам нужно мониторить трафик только в определенной VLAN, не зеркалируя весь транк. Для этого, например, на коммутаторах cisco есть команда:

```
#filter vlan [номер_VLAN]
```

Для того, чтобы убедиться, что передача трафика реализована корректно, воспользуйтесь ПО для анализа трафика , например, Wireshark, чтобы записать PCAP-файл. При анализе PCAP-файл вы должны убедиться, что:

- Конфигурации коммутатора выполнены корректно.
- Трафик, проходящий через коммутатор, относится к области мониторинга.
- Присутствуют в трафике OT-протоколы, используемые в области мониторинга..

Для этого скачиваем ПО Wireshark и устанавливаем его. После чего проделываем следующие шаги:

1. Запустите программу и нажмите Кнопка Опции захвата в WireShark.

image.png

2. Выберите один или несколько сетевых интерфейсов, с которых нужно собрать логи, и нажмите **Старт.** Чтобы выбрать несколько сетевых интерфейсов, зажмите Ctrl на клавиатуре и последовательно выбирайте необходимые интерфейсы из списка, нажимая на них левой клавишей мыши.

При выборе сетевого интерфейса ориентируйтесь на график активности, либо предварительно выполните команду ipconfig /all и посмотрите, какому интерфейсу соответствует основной IP-адрес компьютера.

image.png

4. Воспроизведите проблему.

5. Нажмите Кнопка Остановить захват пакетов в Wireshark.

image.png

6. Нажите **Файл → Сохранить как** и сохраните логи в формате по умолчанию. Далее проанализируйте логи самостоятельно, либо обратитесь в службу технической поддержки через Kaspersky CompanyAccount.

????????? ??????????? ? KICS for Networks ??? ????????? ? ???????????? ?????????

> Специалисты Службы технической поддержки "Лаборатории Касперского" могут запросить у вас журналы Kaspersky Industrial CyberSecurity for Networks и другие данные системы.
>
> Журналы располагаются на компьютерах с установленными компонентами Kaspersky Industrial CyberSecurity for Networks. Сведения о директориях для хранения журналов представлены в статье Директории для хранения данных программы.
>
> Для доступа к журналам нужно иметь root-права в операционной системе.

> Перед тем как собрать логи для техподдержки, необходимо поменять уровень ведения журналов работы процессов на «Отладка».

Чтобы изменить уровни ведения журналов для процессов Kaspersky Industrial CyberSecurity for Networks, выполните следующие шаги:

1. Подключитесь к Серверу Kaspersky Industrial CyberSecurity for Networks через веб-интерфейс под учетной записью Администратора.
2. Выберите раздел **Параметры → Ведение журналов**.
3. Измените уровень ведения журналов на **"Отладка"**
4. Дождитесь применения изменений (до применения изменений отображается индикатор выполнения).
5. Повторите процесс, при котором возникает проблема

> Также специалисты Службы технической поддержки "Лаборатории Касперского" могут запросить дополнительные данные о компонентах программы. Эти данные можно получить с помощью скрипта централизованной установки компонентов программы kics4net-deploy-<номер версии программы>.bundle.sh или с помощью скрипта для локального запуска kics4net-gather-artefacts.sh, который находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

>

Чтобы получить данные о компонентах программы с помощью скрипта kics4net-deploy-<номер версии программы>.bundle.sh выполните следующие шаги

1. На компьютере, с которого выполнялась централизованная установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории kics4net-release_<номер версии программы>/linux-astra.
2. Введите команду:

   ```
   bash kics4net-deploy-<номер версии программы>.bundle.sh --gather-artefacts -<параметр> <имя директории>
   ```

   где:
   - `<параметр>` – определяет режим получения данных.
     Предусмотрены следующие параметры:
     - `a` – для получения всех данных;
     - `c` – для получения данных о сертификатах;
     - `i` – для получения данных о конфигурации обнаружения вторжений;
     - `t` – для получения файлов дампа трафика.
   - `<имя директории>` – имя директории для копирования архивных файлов с данными.
3. В приглашениях `SSH password` и `BECOME password` введите пароль учетной записи пользователя, от имени которого выполнялась установка компонентов программы.

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh. При успешном завершении файлы будут созданы в указанной директории.

Чтобы получить данные об установленном на компьютере компоненте программы с помощью скрипта kics4net-gather-artefacts.sh выполните следующие шаги

1. Выполните вход в систему с учетными данными пользователя с root-правами.
2. Перейдите в директорию /opt/kaspersky/kics4net/sbin/ и введите команду запуска скрипта для получения данных о компоненте программы:

   ```
   bash kics4net-gather-artefacts.sh -<параметр> <имя директории>
   ```

   где:
   - `<параметр>` – определяет режим получения данных.
     Предусмотрены следующие параметры:
     - `a` – для получения всех данных;
     - `c` – для получения данных о сертификатах;
     - `i` – для получения данных о конфигурации обнаружения вторжений;
     - `t` – для получения файлов дампа трафика.

- `<имя директории>` – имя директории для копирования архивных файлов с данными.

Дождитесь завершения работы скрипта kics4net-gather-artefacts.sh. При успешном завершении файлы будут созданы в указанной директории.

??????? ??????????? ??????? ? ??????????? ?????????

> Чтобы предоставить полную информацию технической поддержке о вашей проблеме, используйте описанный ниже шаблон.

==========

Environment/Pre-Conditions:

<Версия продукта(ов)>

<Версия ОС>

==========

Steps to Reproduce:

<Подробно опишите шаги воспроизведения проблемы>

==========

Actual Result:

<Описание результата воспроизведения проблемы>

==========

Expected Result:

<Описание ожидаемого результата>

==========

Steps taken to troubleshoot:

<Описание шагов, предпринятых к устранению проблемы>

==========
==========

Detailed issue description:

<Подробное описание возникшей проблемы>

==========
==========

????????? ????????? ? KICS for Nodes ??? ????????? ? ???????????? ?????????

Kaspersky Industrial CyberSecurity for Windows Nodes

> Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

> Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

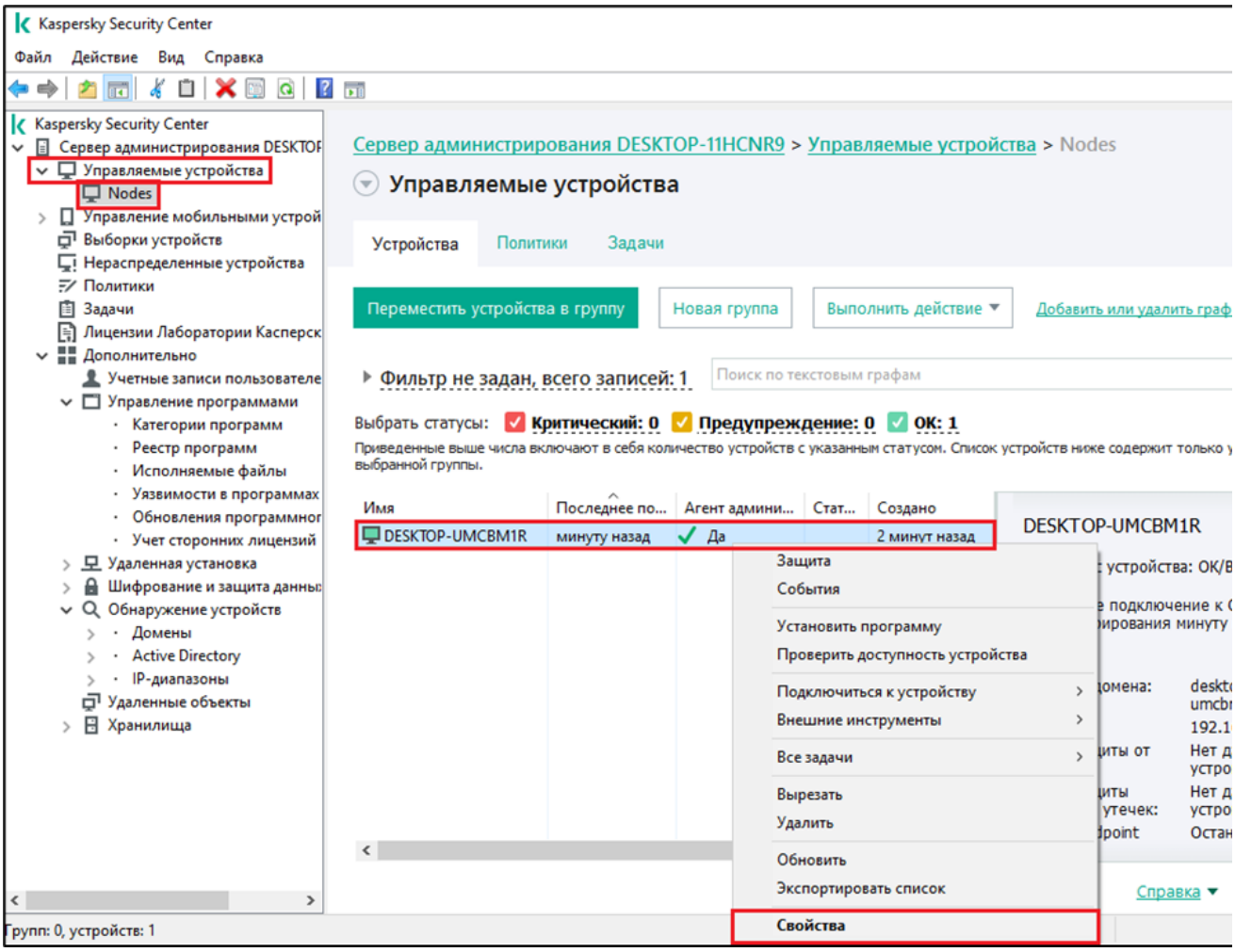
> Поддержка программы предоставляется в течение ее жизненного цикла (см. страницу жизненного цикла программ).

> Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

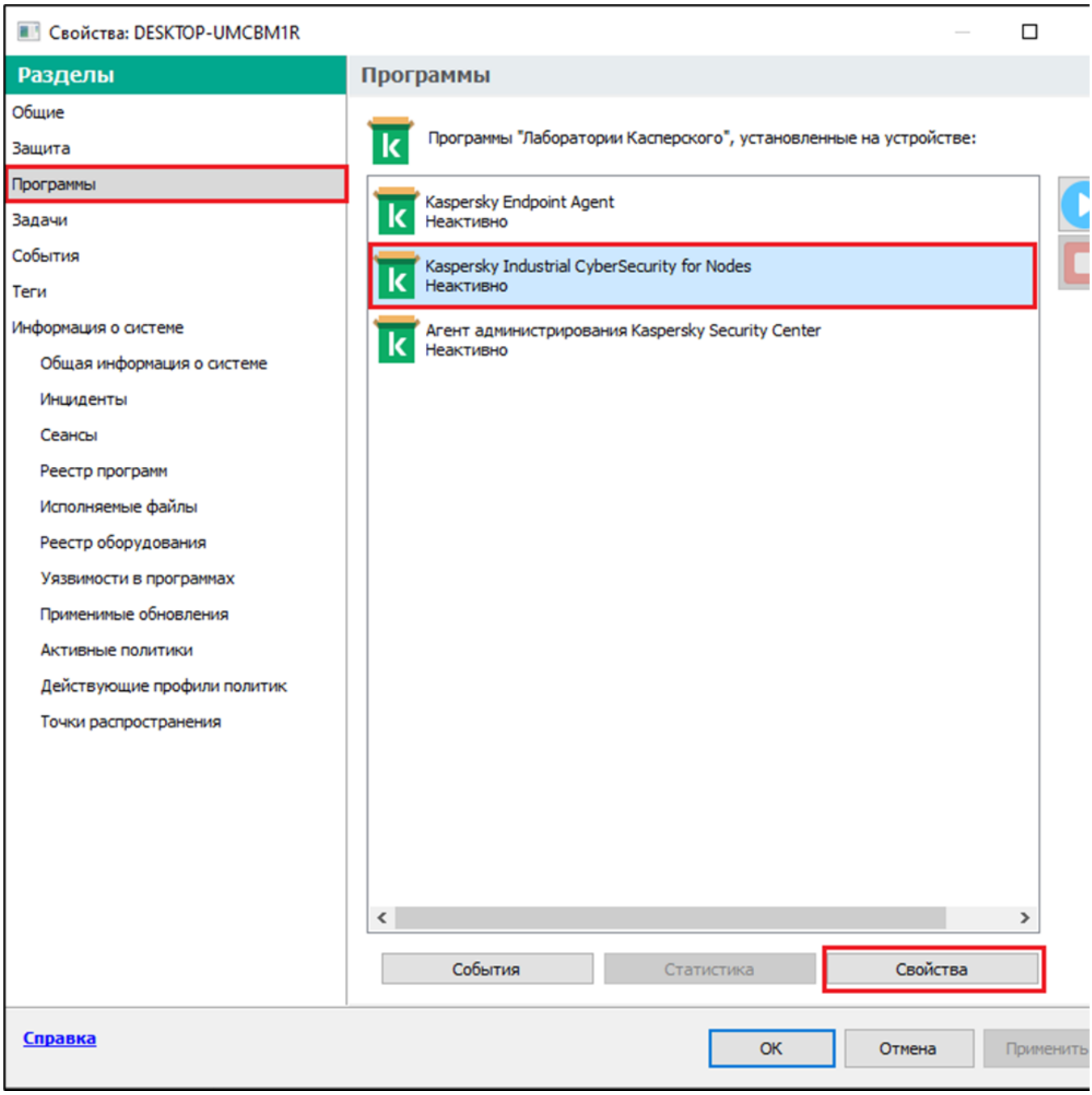
Для отправки обращения в Службу технической поддержки используйте шаблон, описанный в статье "Правило оформления запроса в техническую поддержку"

Для сбора диагностической информации с KICS for Windows Nodes выполните следующие шаги:

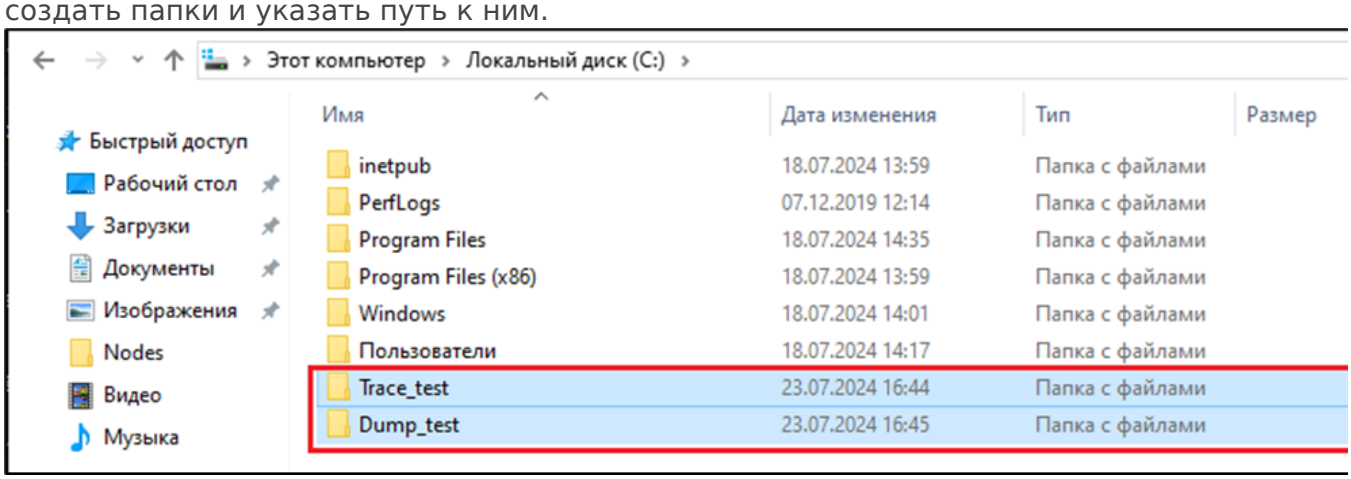
1. Перейдите в MMC-консоль Kaspersky Security Center
2. В папке «Управляемые устройства» дерева Консоли администрирования откройте папку с названием группы администрирования, в состав которой входит нужное вам устройство.
   1. В рабочей области выберите вкладку "Устройства"
   2. В контекстном меню устройства выберите пункт "Свойства"



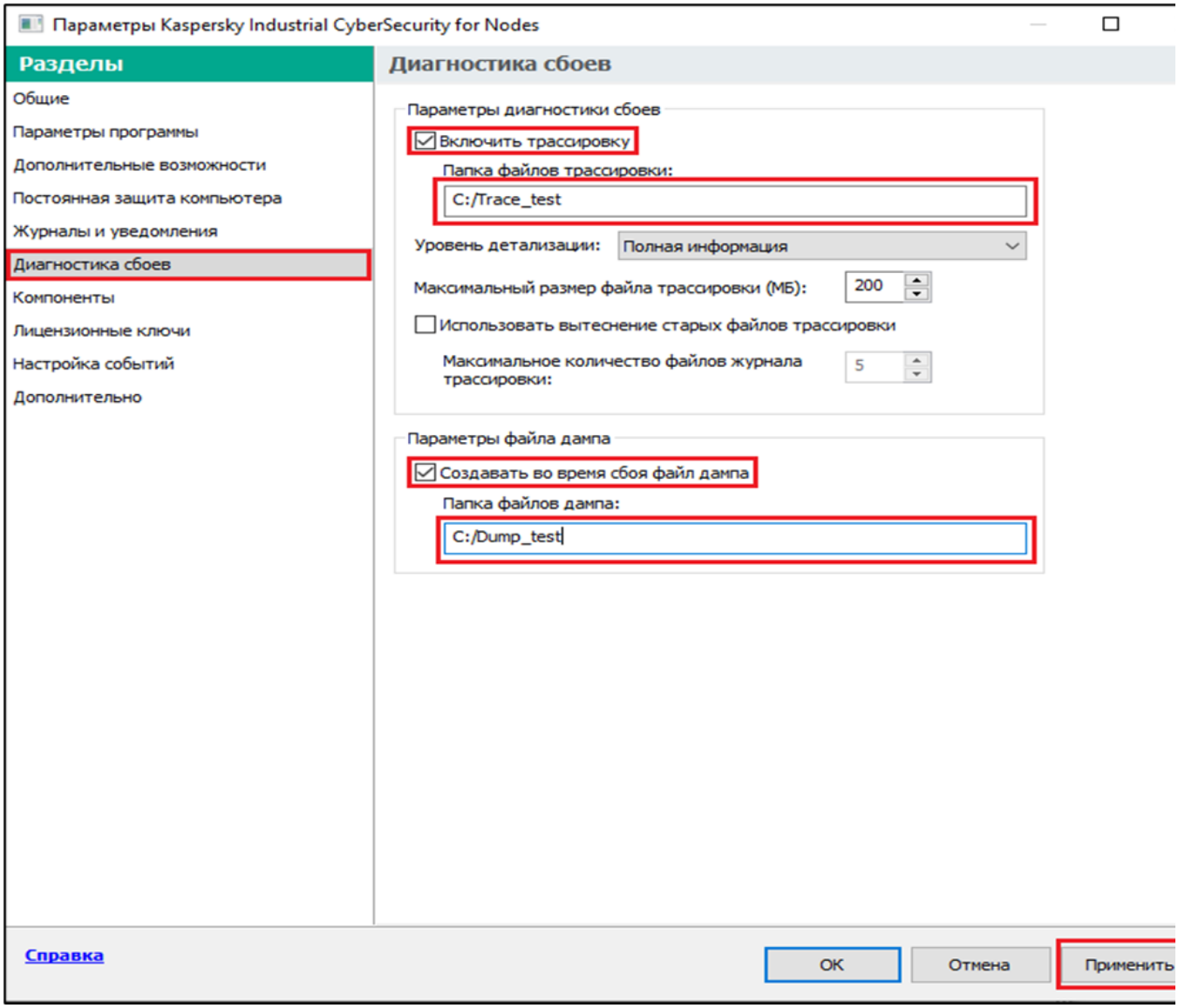
3. Выберите раздел "Программы". В рабочей области окна отобразится список программ "Лаборатории Касперского", установленных на устройстве. Нажмите на Kaspersky Industrial CyberSecurity for Nodes, затем нажмите на кнопку "Свойства"



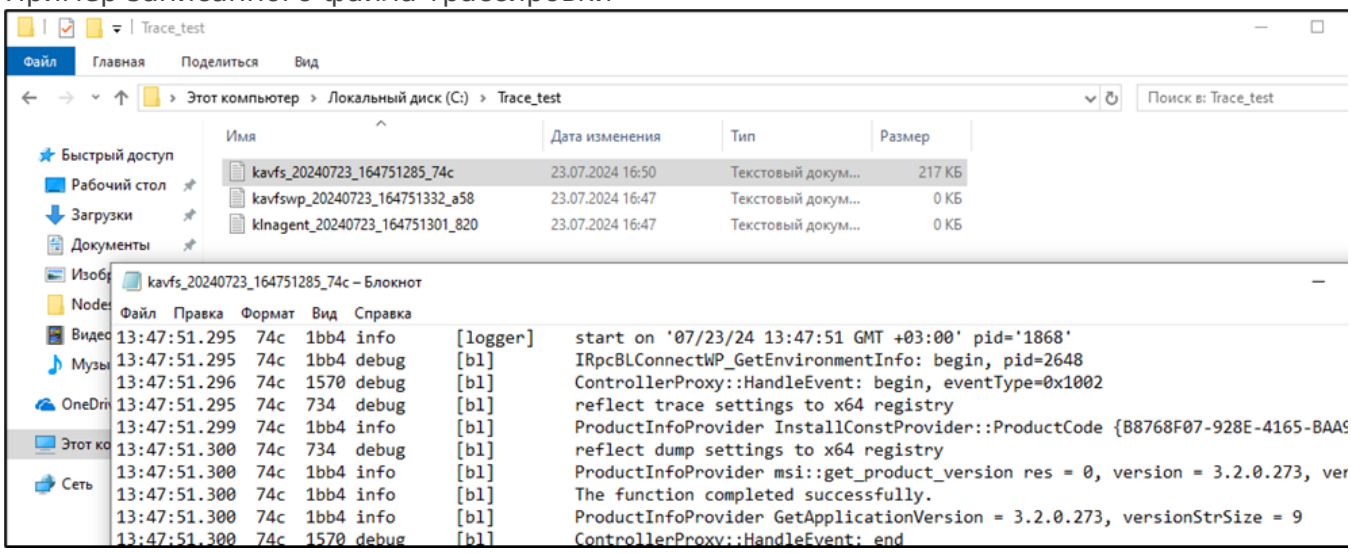
4. Kaspersky Industrial CyberSecurity for Nodes не создает папку для сохранения файлов трассировки или файлов дампа на устройстве автоматически. Необходимо заранее создать папки и указать путь к ним.



5. Установите флажки и укажите путь к папкам.



6. Пример записанного файла трассировки



Kaspersky Industrial CyberSecurity for Linux Nodes

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

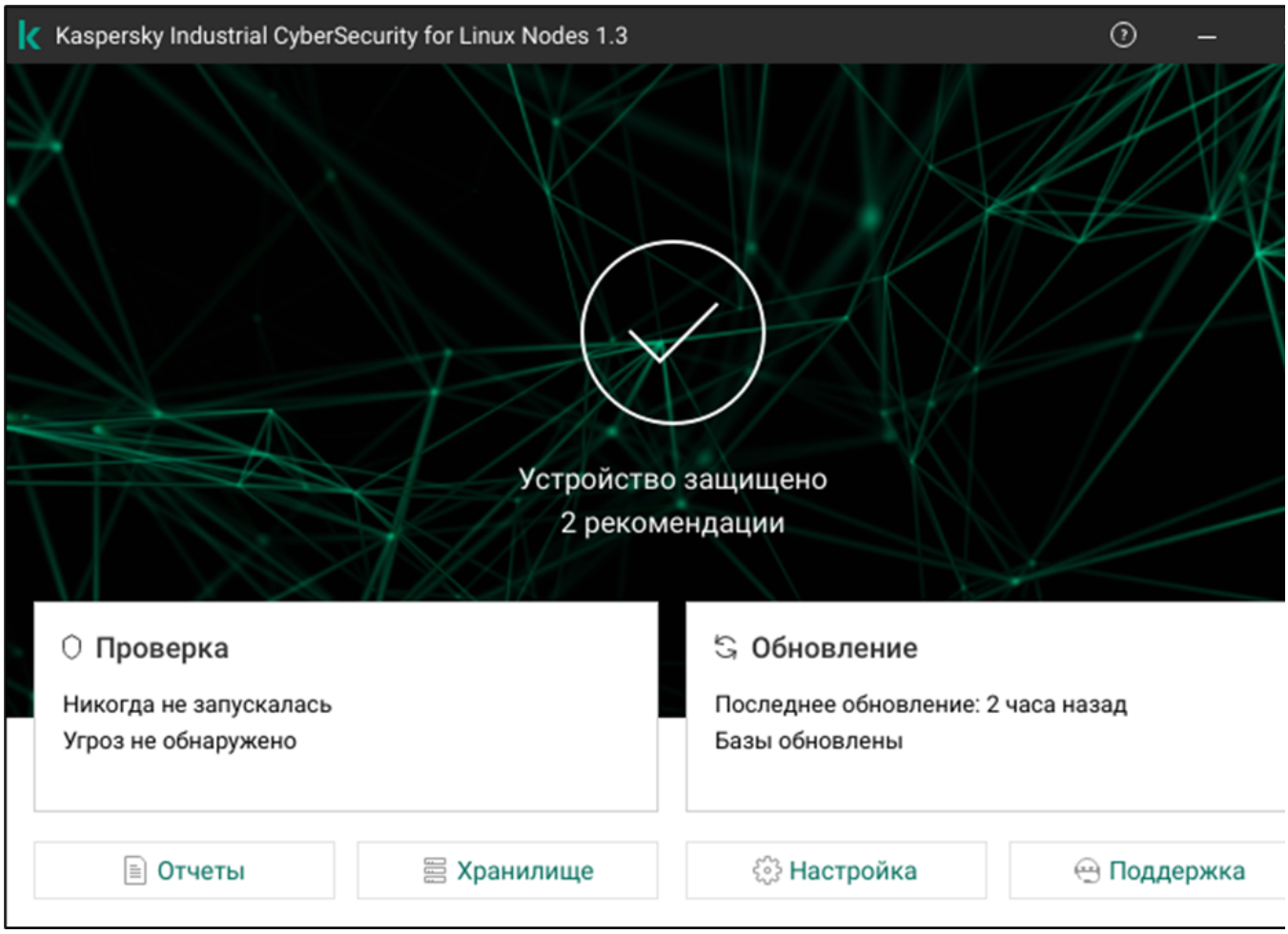
Поддержка программы предоставляется в течение ее жизненного цикла (см. страницу жизненного цикла программ).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

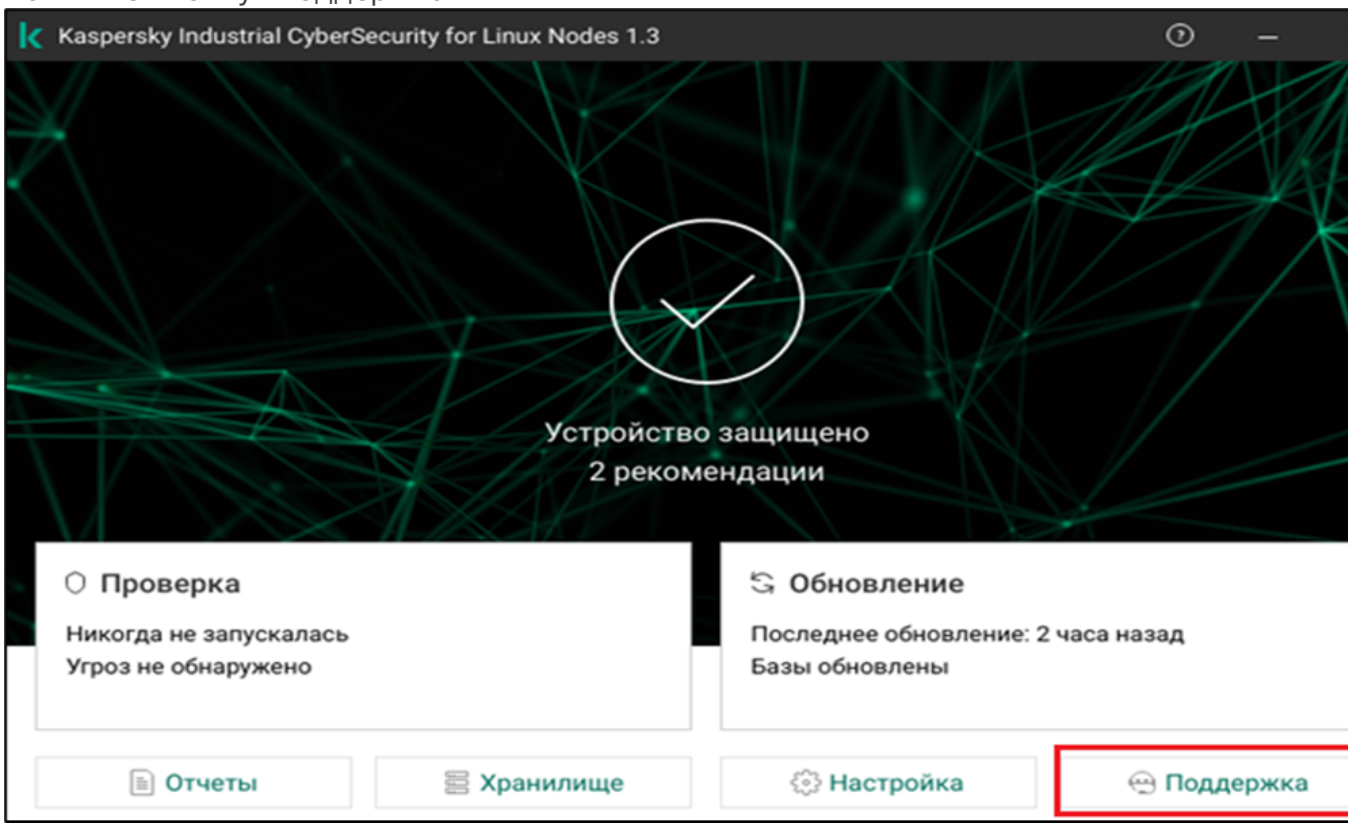
Для отправки обращения в Службу технической поддержки используйте шаблон, описанный в статье "Правило оформления запроса в техническую поддержку"

Для сбора диагностической информации с KICS for Windows Nodes выполните следующие шаги:

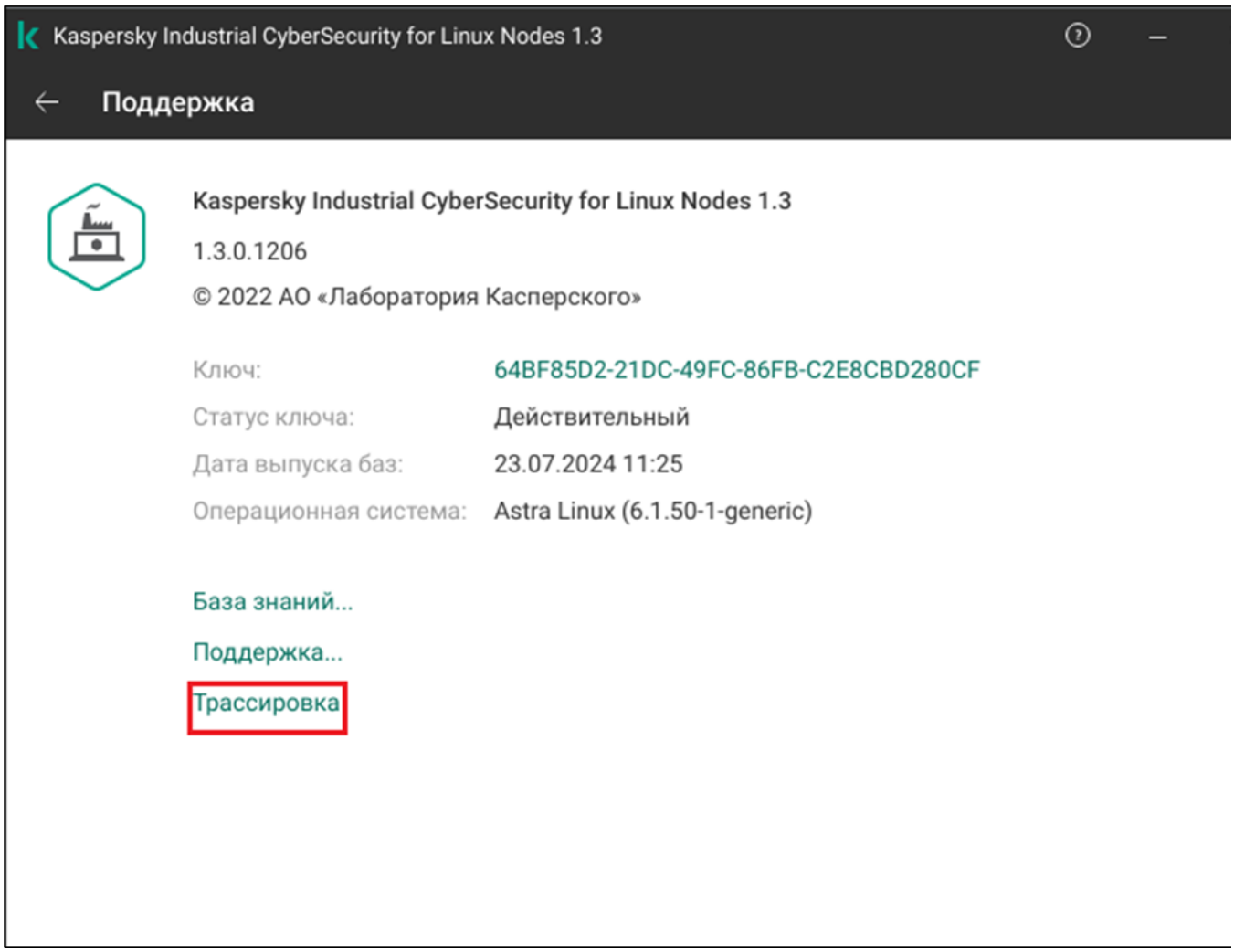
1. Откройте главное окно приложения.



2. Нажмите кнопку "Поддержка".



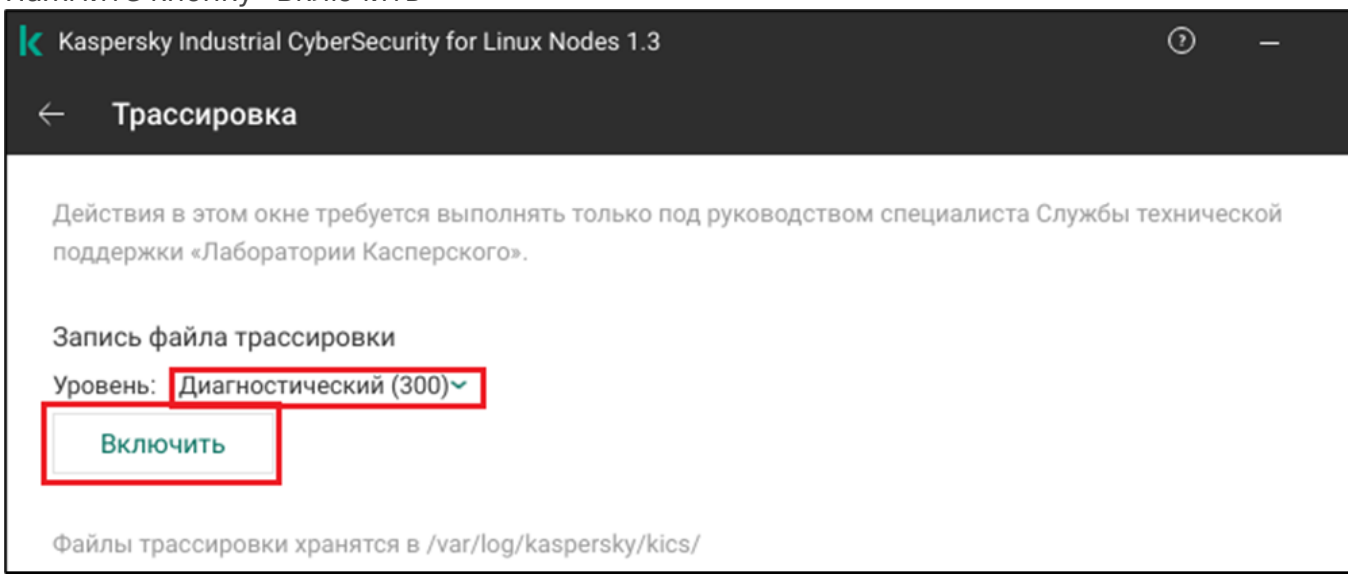
3. Нажмите кнопку "Трассировка".



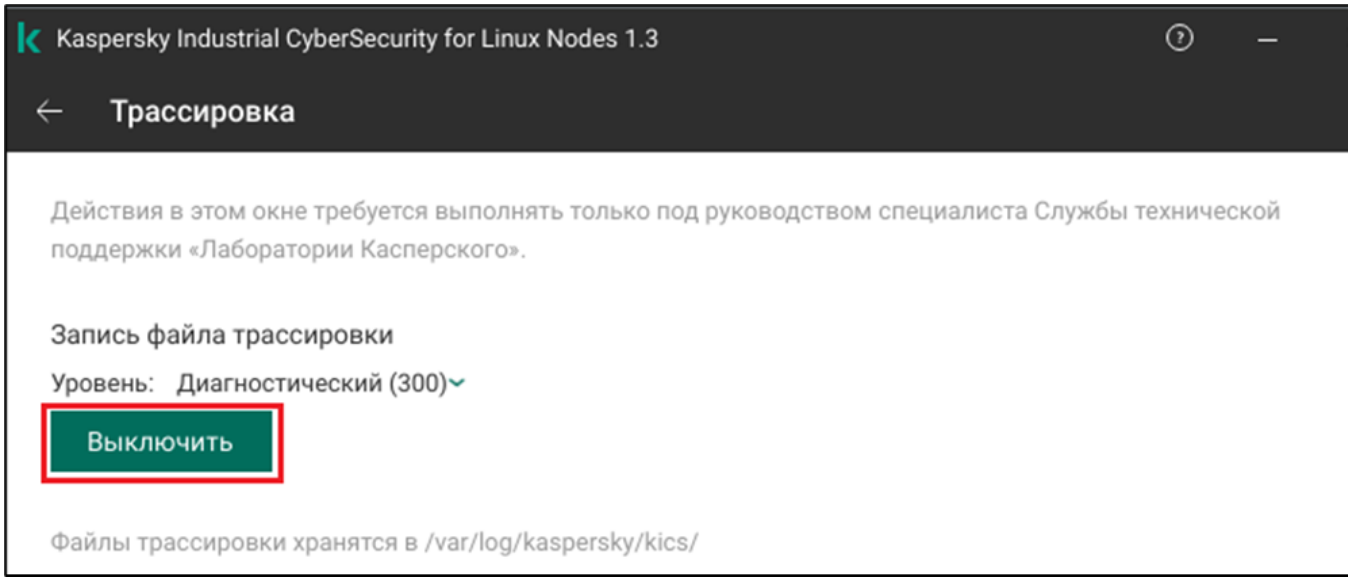
4. В раскрывающемся списке "Уровень" выберите уровень детализации файла трассировки.

   > Рекомендуется уточнить требуемый уровень детализации у специалиста из Службы технической поддержки "Лаборатории Касперского". По умолчанию установлено значение "Диагностический (300)".

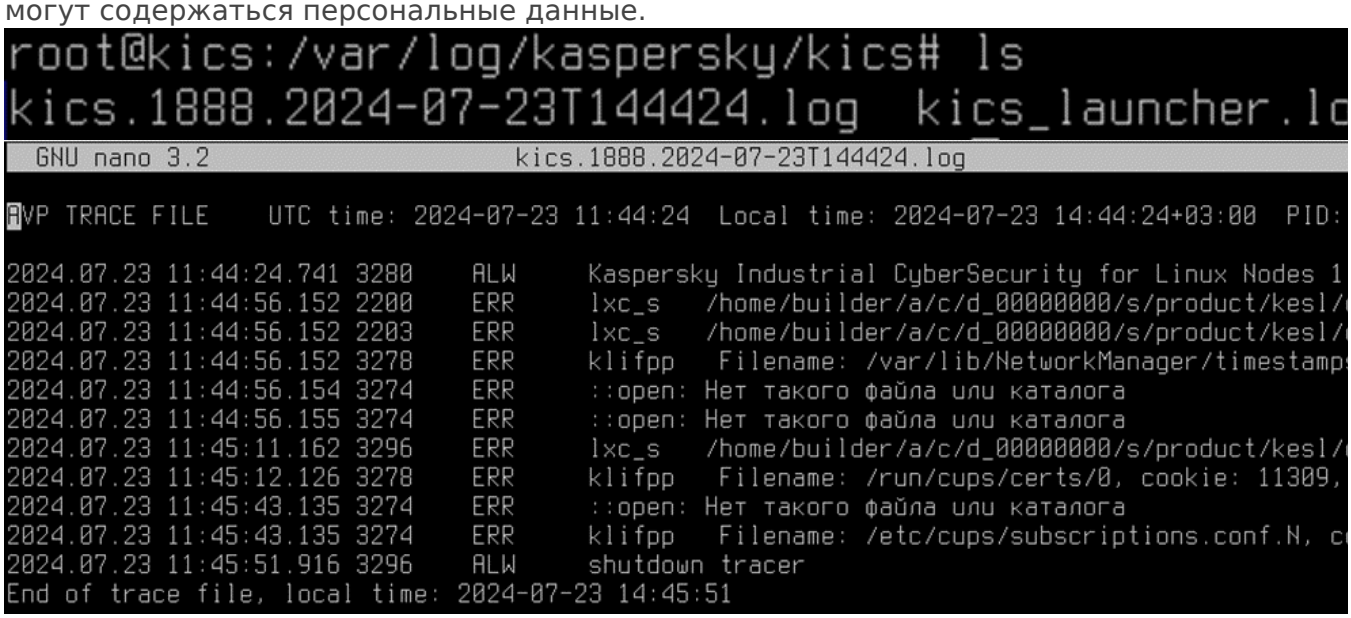
   Нажмите кнопку "Включить"



5. Воспроизведите ситуацию, при которой возникает проблема. Нажмите на кнопку "Выключить", чтобы остановить процесс трассировки.



6. Созданные файлы трассировки хранятся в директории **/var/log/kaspersky/kics/**. В файлах трассировки содержится информация об операционной системе, а также могут содержаться персональные данные.



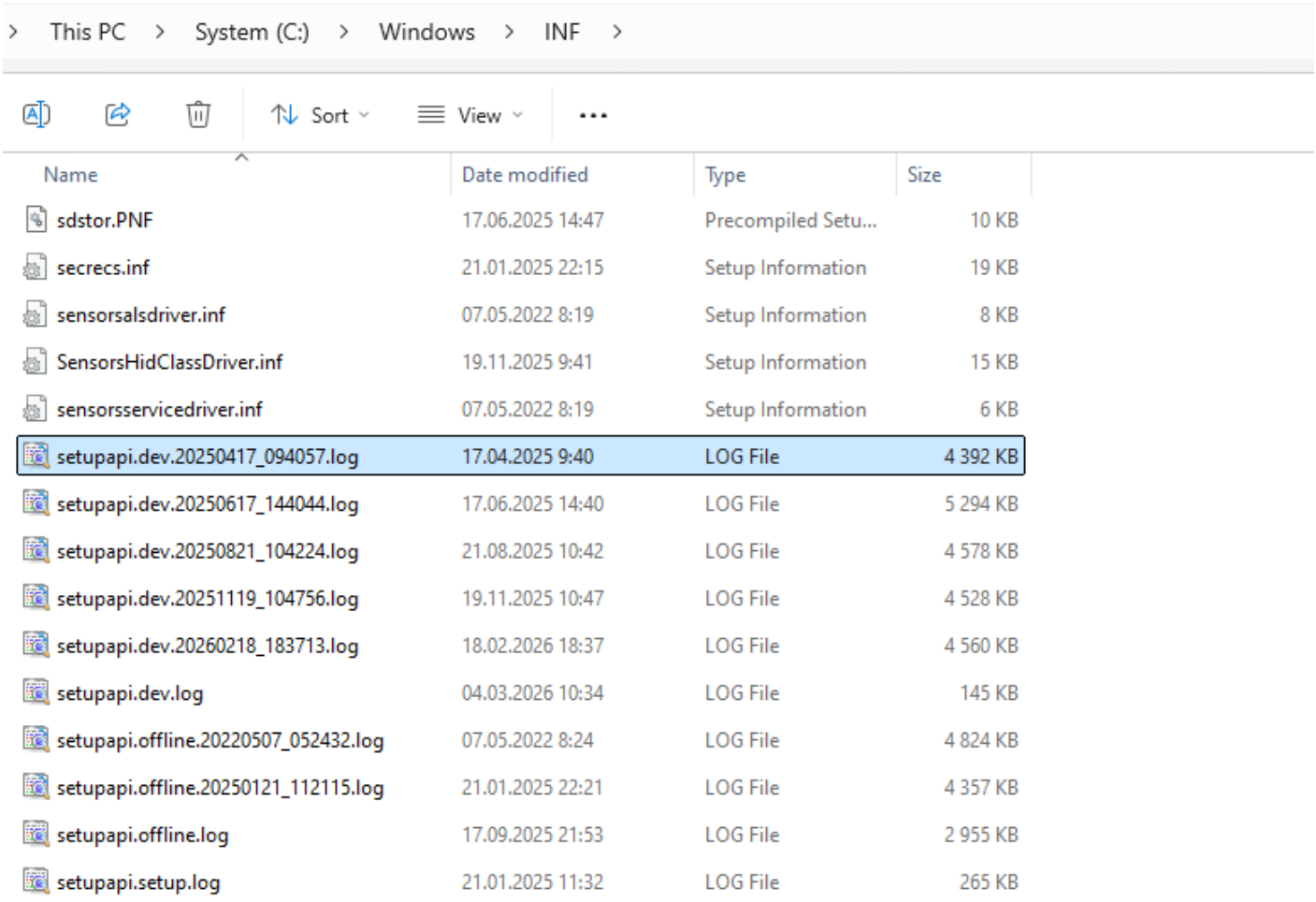
?????????? ?? ????? ????? ? ?????????? ??? ????????????? ??????? ? ?????????? KICS for nodes (windows)

При возникновении ошибок во время установки KICS for Nodes для анализа проблемы технической поддержкой необходимо собрать диагностическую информацию.

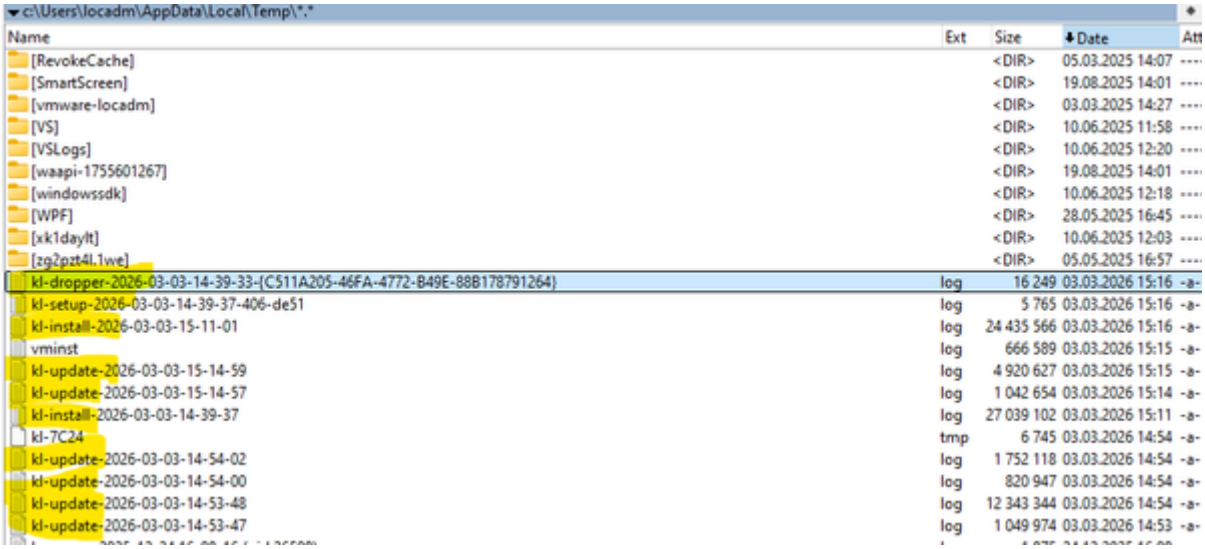
Существует несколько способов сбора диагностической информации:

1. Нужно скачать утилиту Kaspersky Get System Info (GSI), которая представляет собой утилиту для сбора информации об операционной системе. Данная утилита соберет все необходимые данные для анализа. Более подробна информация представлена по ссылке: получение отчета утилиты Kaspersky Get System Info.
2. В случае, когда не предоставляется возможность установить утилиту для сбора информации об операционной системе, все диагностические данные нужно собрать вручную.

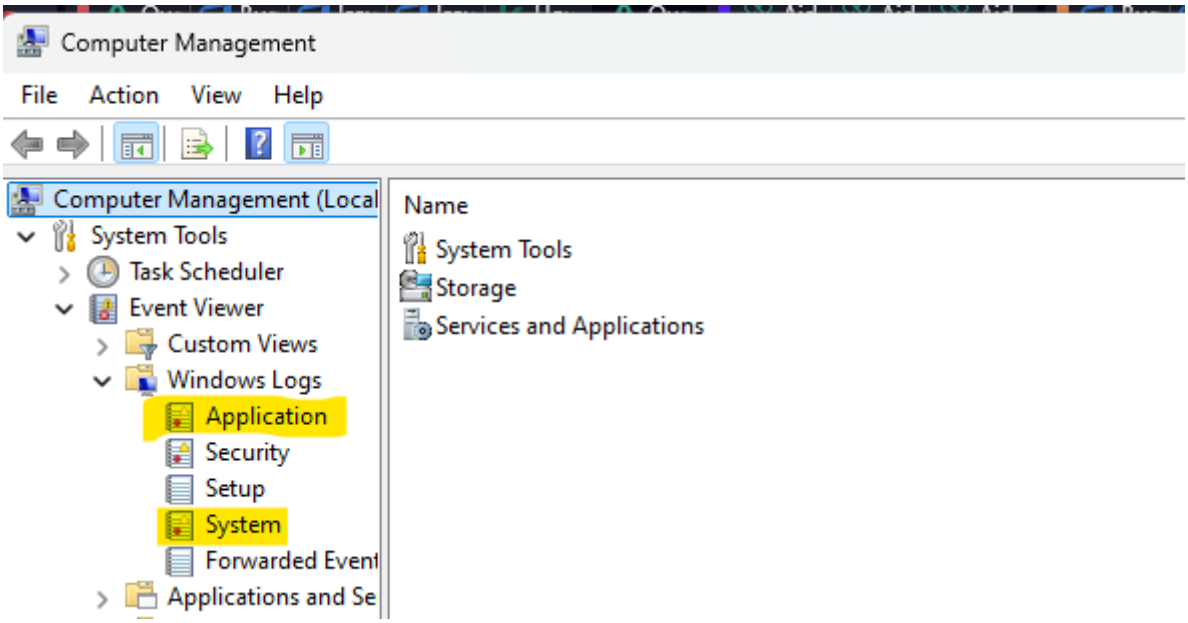
Переходим в директорию C:\windows\infinf, ??? ??? ????? ????? ?? ????? setupapi*:



????????? ????? ????? ??????? ?? ????????? ??????? ???????? ???????????? ???????????? ???????, ?? ???????? ????????????? ????????? (??????? %temp%). ????????????? ????: C:|Users\locadm\AppData\Local\Temp\.



?? ????????????? ???? ????????? ? ?????? ????????? ???????? ? ????????? ?????? ?? ????????? ????????:


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Name
System Tools
Storage
Services and Applications

??? ?????????? ?????? ?????????? ? ??????????? ?????????.