

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

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

- [Схема установки KICS for Networks all-in-one](#)
- [Схема установки сервера KICS for Networks с внешними сенсорами](#)
- [Подключение Kaspersky Industrial CyberSecurity for Networks к промышленной сети через диод данных](#)
- [Получение трафика промышленных сетей от компонентов решения Kaspersky SD-WAN](#)

????? ?????????? KICS for Networks all-in-one

В данном разделе находится информация о схеме развертывания решения KICS for Networks без использования внешних серверов.

При установке Сервера без внешних сенсоров все данные для обработки и анализа поступают только на компьютер, выполняющий функции Сервера. Вы можете применить этот способ установки, если компьютер имеет достаточное количество сетевых интерфейсов для получения данных из различных источников.

Подробнее про данный тип развертывания решения можно ознакомиться [здесь](#)

На рисунке ниже показан пример схемы развертывания Сервера без сенсоров. Сетевые интерфейсы компьютера, выполняющего функции Сервера, подключаются к SPAN-портам сетевых коммутаторов (SPAN-порты и соединения обозначены желтым цветом) и получают копию трафика из трех сегментов промышленной сети. Выделенная сеть Kaspersky Industrial CyberSecurity обозначена линиями зеленого цвета.

[image.png](#)

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

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

???????????

В данном разделе находится информация о схеме развертывания решения KICS for Networks с использованием внешних сенсоров.

Способ установки Сервера и внешних сенсоров предполагает использование нескольких компьютеров для установки компонентов программы. На одном из компьютеров устанавливается Сервер. На остальных компьютерах устанавливаются сенсоры, которые будут получать данные из вычислительных сетей. В программе может использоваться до 50 сенсоров.

Подробнее про данный тип развертывания решения можно ознакомиться [здесь](#)

На рисунке ниже показан пример схемы развертывания Сервера и трех сенсоров. Сетевые интерфейсы компьютеров, выполняющих функции сенсоров, подключаются к SPAN-портам сетевых коммутаторов (SPAN-порты и соединения обозначены желтым цветом) и получают копию трафика из соответствующих сегментов промышленной сети. Выделенная сеть Kaspersky Industrial CyberSecurity обозначена линиями зеленого цвета.

[image.png](#)

???????????? Kaspersky Industrial CyberSecurity for Networks ? ?????????????????? ????? ?????? ????? ????????

В данном разделе находится информация о подключении KICS for Networks к промышленной сети через диод данных.

Для подключения Kaspersky Industrial CyberSecurity for Networks к промышленной сети вы можете дополнительно использовать специальные устройства, обеспечивающие одностороннюю передачу данных из промышленной сети. Такие устройства называются *диодами данных*.

Подробнее про данную схему развертывания решения можно ознакомиться [здесь](#)

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

На рисунке ниже показана схема подключения коммутатора через диод данных к точке мониторинга на Сервере KICS for Networks. Через диод данных поступает зеркалированный трафик от SPAN-порта сетевого коммутатора в промышленной сети. В этой схеме применяется способ установки Сервера без внешних сенсоров.

[image.png](#)

На рисунке ниже показана схема подключения нескольких сенсоров Kaspersky Industrial CyberSecurity for Networks через диоды данных. Через диоды данных поступает трафик от SPAN-портов сетевых коммутаторов в промышленной сети. В этой схеме применяется способ установки Сервера и трех сенсоров.

[image.png](#)

Если вы хотите дополнительно разграничить сегменты промышленной сети, в которых установлены сенсоры, и сегмент выделенной сети Kaspersky Industrial CyberSecurity, в котором установлен Сервер, вы можете использовать межсетевой экран на линиях соединений сенсоров и Сервера.

????????? ?????? ?????????? ?????????????????? ????? ? ??????? ?
????????? ?????????????? ? EPP-????????????????? ?????? ??????
?????????

На рисунке ниже показана схема поступления трафика от SPAN-портов сетевых коммутаторов и получения данных телеметрии от EPP-приложения (KICS for Linux Nodes) из нескольких технологических площадок.

В данном сценарии через диод данных передается телеметрия собранная только с Kaspersky Industrial CyberSecurity for Linux Nodes. Телеметрию с Kaspersky Industrial CyberSecurity for Windows Nodes передать через диод данных не получится.

[BDkimage.png](#)

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

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

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

Kaspersky SD-WAN

В данном разделе находится информация о схеме получения трафика промышленных сети от компонентов решения Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity for Networks может работать в режиме интеграции с решением Kaspersky SD-WAN. При работе в этом режиме Kaspersky Industrial CyberSecurity for Networks получает зеркалированный трафик, который проходит через сетевые коммутаторы на удаленных технологических площадках, если на этих площадках установлен компонент решения Kaspersky SD-WAN устройство Customer Premise Equipment (далее "устройство CPE"). С помощью устройств CPE вы можете частично реализовать функции сенсоров Kaspersky Industrial CyberSecurity for Networks, обеспечив получение программой трафика промышленных сетей с географически разнесенных площадок. При этом данные передаются в программу по защищенным каналам.

Подробнее про данный тип развертывания решения можно ознакомиться [здесь](#)

На рисунке ниже показан пример схемы развертывания Kaspersky Industrial CyberSecurity for Networks и решения Kaspersky SD-WAN для случая, когда зеркалированный трафик из нескольких технологических площадок поступает на Сервер Kaspersky Industrial CyberSecurity for Networks через один шлюз SD-WAN. Компьютеры, подключенные к выделенной сети Kaspersky Industrial CyberSecurity, и компьютеры с центральными компонентами SD-WAN находятся в центральном офисе организации. Пунктирными линиями обозначен путь передачи зеркалированного трафика от сетевых коммутаторов на удаленных технологических площадках.

[image.png](#)