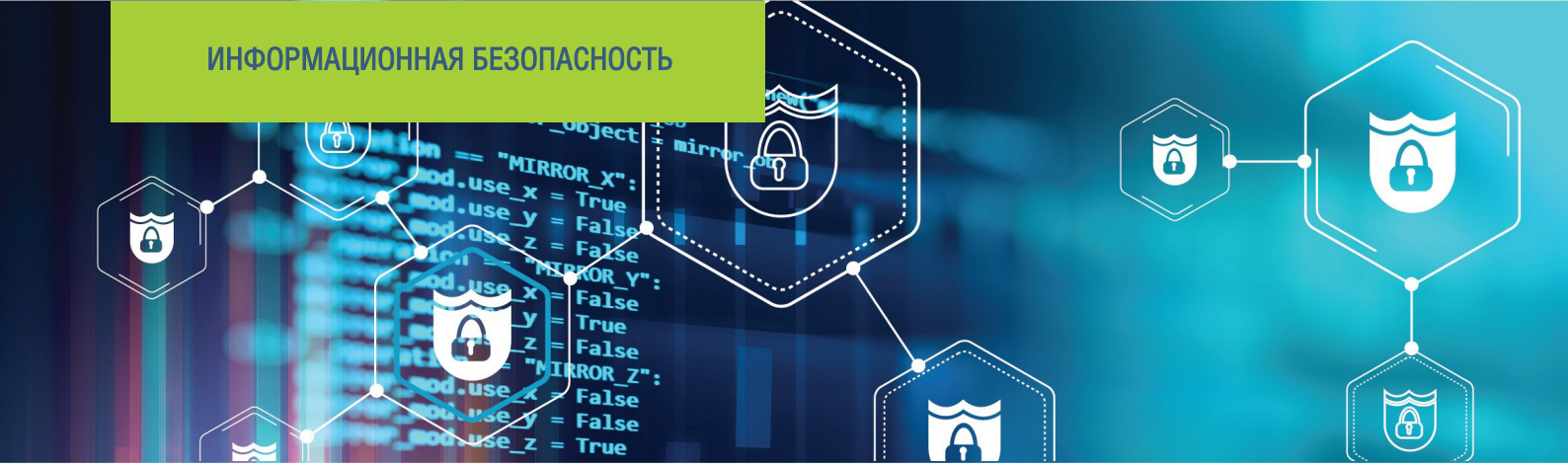


Применение KICS for Networks и KICS for Nodes с InfoDiode

По мере того, как промышленные предприятия становятся все более «цифровыми», инвестируют в интеллектуальные технологии и новые системы автоматизации, им приходится пересматривать подходы к защите промышленного сегмента. Воздушный зазор между технологической сетью и корпоративной ИТ-инфраструктурой становится препятствием развития цифровизации предприятия, но и полный отказ от него создает значительные риски для всей критической инфраструктуры. Особенности оборудования и протоколов в технологических сетях требуют применения отдельного класса решений по обеспечению кибербезопасности, который отличается от традиционных «офисных» средств защиты. Для своевременного обнаружения вредоносной активности в технологической сети предприятия необходимо проводить непрерывный мониторинг трафика по специфическим протоколам. В решении этой задачи предприятиям помогают специализированные продукты — средства обнаружения вторжений (СОВ, Intrusion Detection Systems, IDS), например, Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) и Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes). Однако, трафик для анализа должен передаваться в условиях гарантированной изоляции защищаемого сетевого сегмента, чтобы исключить воздействие на защищаемый сегмент злоумышленника.

Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) – специализированное средство пассивного мониторинга промышленной сети, направленное на защиту автоматизированных систем управления и исполнительных механизмов на сетевом уровне.

Kaspersky Industrial CyberSecurity for Nodes – средство комплексной защиты серверов и рабочих станций в промышленных системах управления от информационных угроз.

InfoDiode - продукт, построенный на принципах однонаправленной передачи данных и позволяющий обеспечивать эффективную защиту доверенного сегмента. Технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

InfoDiode, KICS for Networks и KICS for Nodes разработаны специально для промышленных предприятий и объектов критической инфраструктуры.

Результаты комплексного тестирования подтвердили эффективное совместное использование продуктов для обнаружения аномальной активности и несанкционированных действий в технологической сети на уровне программируемых логических контроллеров (ПЛК) и действий пользователя. Таким образом обеспечивается защита технологического процесса и промышленного оборудования как от ошибок персонала, так и от целенаправленных действий злоумышленников.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

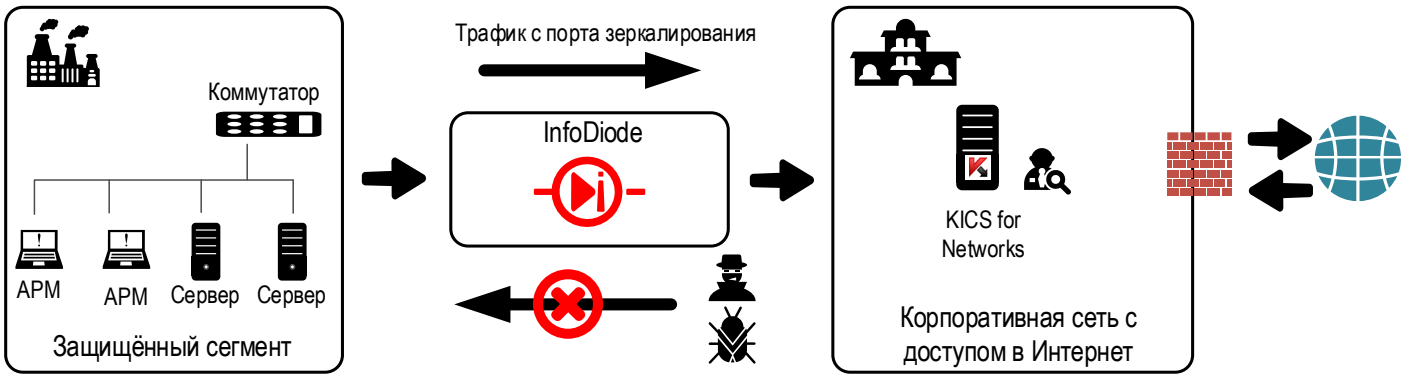
28.08.2024

Сценарий передачи зеркалированного трафика на сенсор KICS for Networks

Анализаторы трафика KICS могут размещаться как централизованно, так и в варианте «облачного сервиса». В таких условиях очевидно, что сегменты промышленных сетей должны поддерживать высокий уровень изоляции, предотвращающий любые внешние воздействия на объекты этих сетевых сегментов со стороны сетей, в которых размещены анализаторы трафика. Данный сценарий демонстрирует решение этой задачи при помощи совместного использования KICS for Networks и **InfoDiode**.

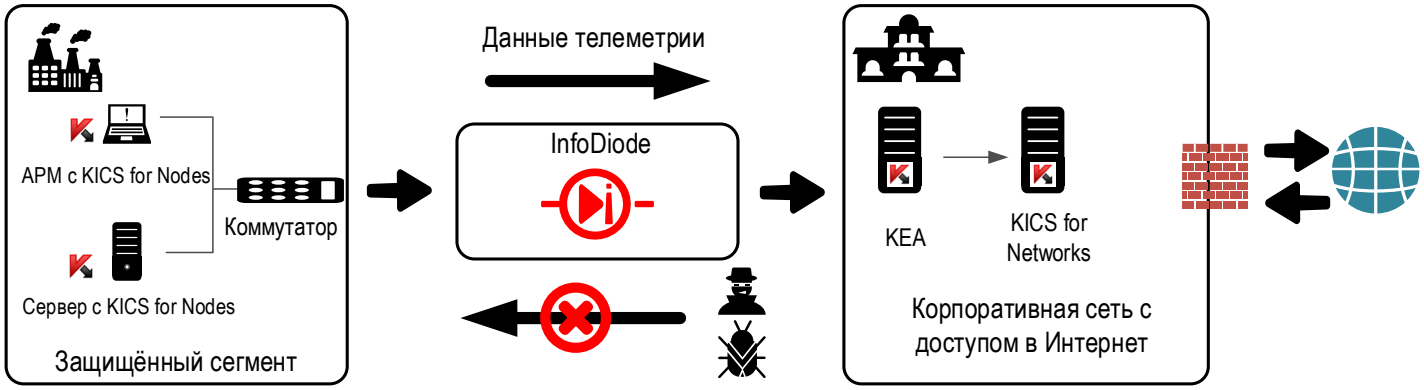
InfoDiode в совместном решении выступает в качестве системы однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем, сохраняя канал для обеспечения передачи трафика на сенсор KICS for Networks.

Архитектура использования KICS for Networks и **InfoDiode** предполагает применение аппаратных комплексов **InfoDiode** (AK InfoDiode RACK module, AK InfoDiode MINI) между источником анализируемого трафика и сенсором KICS for Networks в сетях передачи данных промышленных объектов. В частности, трафик с устройств защищённого сегмента сети передаётся через коммутатор с настроенным SPAN портом в односторонний канал связи **InfoDiode**. Зеркалированный трафик из защищённого сегмента поступает на сенсор KICS for Networks для проведения анализа, а любое воздействие через этот же канал связи на защищённый сегмент сети полностью исключается.



Сценарий передачи телеметрии и событий с KICS for Nodes на сенсор KICS for Networks

В данном сценарии в закрытом сегменте устанавливается программное решение для защиты конечных узлов Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes), с которого при помощи агента интеграции Kaspersky Endpoint Agent (KEA) данные телеметрии (информация об узлах, событиях безопасности, сессиях) передаются через InfoDiode в менее доверенный сегмент для агрегирования и обработки средствами Kaspersky Industrial CyberSecurity for Networks (KICS for Networks), что исключает воздействие на защищаемый сегмент по тому же каналу со стороны злоумышленника.



AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

28.08.2024

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программными продуктами

Kaspersky Industrial CyberSecurity for Networks

продукция компании

АО «Лаборатория Касперского»

Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2

в дальнейшем именуемыми «**KICS for Networks**» и «**Лаборатория Касперского**» соответственно

и

Аппаратным комплексом

«AMT InfoDiode» однонаправленной передачи данных

продукция компании

АО «АМТ-ГРУП»

Россия, 115162, г. Москва, ул. Шаболовка, д. 31, корп. Б, под. 3

в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**» соответственно

AMT GROUP -Diode info

kaspersky

Аппаратный комплекс **InfoDiode** является системой однонаправленной передачи данных, обеспечивающий высочайший уровень изоляции критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами.

KICS for Networks является специализированным средством пассивного мониторинга промышленной сети, входящим в состав решения Kaspersky Industrial CyberSecurity, и направленным на удовлетворение требований к мерам защиты информации в автоматизированной системе управления.

АМТ-ГРУП и «**Лаборатория Касперского**» настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

АМТ-ГРУП и «**Лаборатория Касперского**» провели всесторонние тесты продукта **KICS for Networks** при совместном использовании с моделями аппаратных комплексов **InfoDiode** (АК InfoDiode rack module, АК InfoDiode Mini) в сетях передачи данных промышленных объектов с разграничением доступа на базе **InfoDiode**, используемого между источником анализируемого трафика и сенсором **KICS for Networks**. В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно. Тесты подтвердили полную совместимость продуктов в заявленном сценарии использования.

АО «Лаборатория Касперского»

Дата:

01 декабря 2020 года

Должность:

Управляющий директор в России, странах СНГ и Балтии

Подпись _____

(М.Ю. Прибочий)

АО «АМТ-ГРУП»

Дата:

01 декабря 2020 года

Должность:

Технический директор

Подпись _____

(В.В. Леонов)

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программными продуктами

Kaspersky Industrial CyberSecurity for Networks

продукция компании

АО «Лаборатория Касперского»

Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.3

в дальнейшем именуемыми «**KICS for Networks**» и «**Лаборатория Касперского**» соответственно

и

Комплексом

InfoDiode SMART однонаправленной передачи данных

продукция компании

АО «АМТ-ГРУП»

Россия, 115162, г. Москва, ул. Шаболовка, д. 31, корп. Б, под. 3

в дальнейшем именуемыми «**InfoDiode SMART**» и «**АМТ-ГРУП**» соответственно

AMT GROUP -Diode kaspersky

Комплекс **InfoDiode SMART** является системой однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами.

KICS for Networks является специализированным продуктом промышленного класса, предназначенным для инвентаризации, мониторинга, выявления рисков и угроз промышленных инфраструктур. Являясь частью решения Kaspersky Industrial CyberSecurity, продукт предоставляет возможность выявления угроз кибербезопасности и аномалий пассивным образом на основе анализа копии сетевого трафика, и (опционально) данных телеметрии с устройств, защищенных продуктом KICS for Nodes. Решение предоставляет инструменты для расследования и ручного реагирования на угрозы на уровне защищаемых устройств и сетевой инфраструктуры.

АМТ-ГРУП и «**Лаборатория Касперского**» настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

АМТ-ГРУП и «**Лаборатория Касперского**» провели всесторонние тесты продукта **KICS for Networks** при совместном использовании с комплексом **InfoDiode SMART** в сетях передачи данных промышленных объектов с разграничением доступа на базе InfoDiode SMART, используемого для передачи телеметрии между конечными узлами защищенного сегмента и сервером интеграции KICS for Networks. В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно. Тесты подтвердили полную совместимость продуктов в заявленном сценарии использования.

АО «АМТ-ГРУП»

Дата:

17 июня 2024 года

Должность:

Технический директор

Подпись _____

(Б.В. Молчанов)

АО «Лаборатория Касперского»

Дата:

17 июня 2024 года

Должность:

Управляющий директор в России, странах СНГ

Подпись _____

(А.В. Кулашова)

AMT GROUP -DiodeInfo

kaspersky