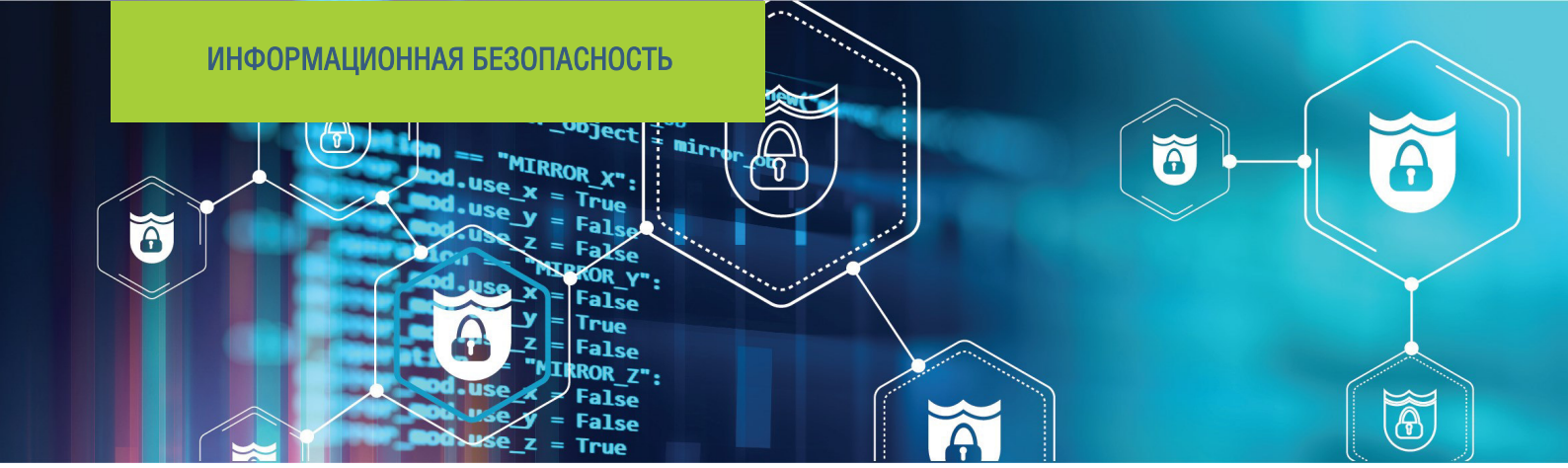


# Применение KICS for Networks с однонаправленным шлюзом InfoDiode

По мере того, как промышленные предприятия становятся все более «цифровыми»: активно инвестируют в интеллектуальные технологии и новые системы автоматизации и реализуют концепцию четвертой промышленной революции, им приходится пересматривать подходы к защите промышленного сегмента. Глухой «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. Кроме того, 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 промышленного 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).

Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) – специализированное средство пассивного мониторинга промышленной сети, входящее в семейство Kaspersky Industrial CyberSecurity и направленное на защиту автоматизированных систем управления и исполнительных механизмов на сетевом уровне. KICS for Networks является специализированным средством пассивного мониторинга промышленной сети, входящим в состав решения Kaspersky Industrial CyberSecurity.

**InfoDiode -** это 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, обеспечивают возможность передачи данных из одного сегмента в другой и нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

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

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

AMT GROUP

115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

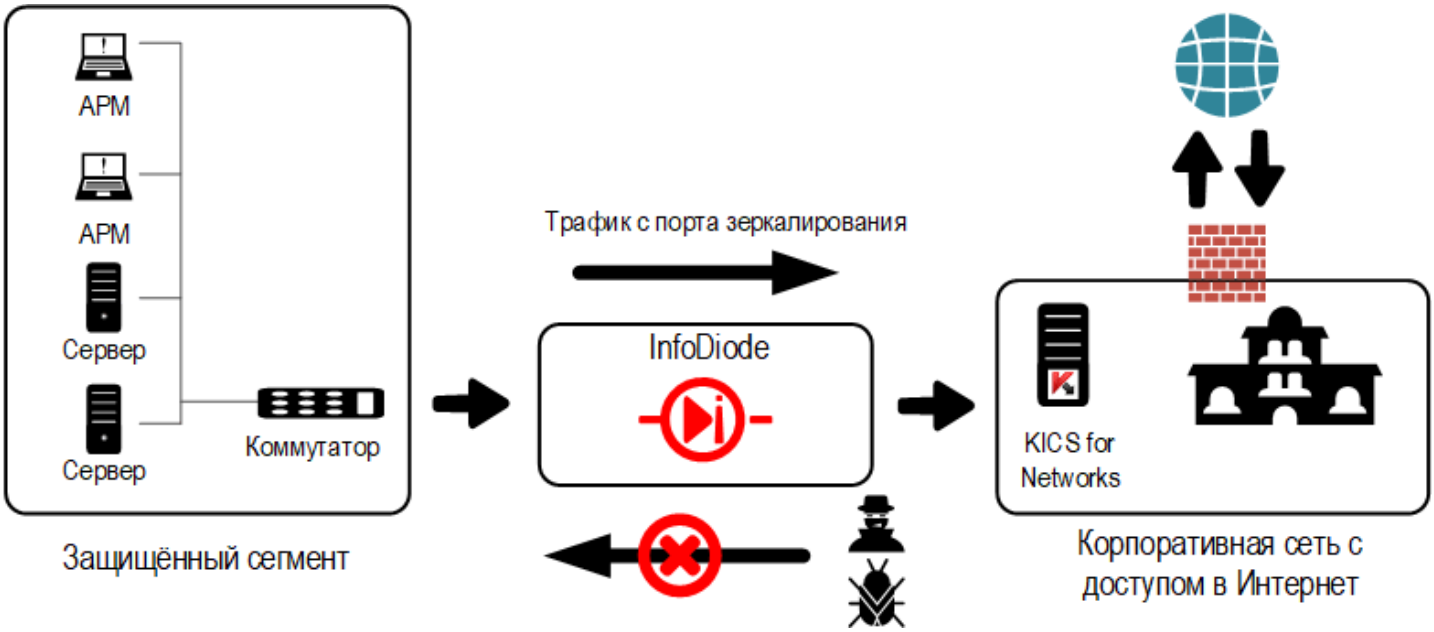
# Сценарий передачи трафика закрытого сегмента на сенсор KICS for Networks

Анализаторы трафика KICS могут как размещаться централизованно, так и могут предоставляться специалистам по безопасности как «облачный сервис». 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. При этом сохраняется канал для обеспечения передачи анализируемого трафика на сенсор KICS for Networks.

Архитектура совместного использования KICS for Networks и **InfoDiode** предполагает применение аппаратных комплексов **InfoDiode** (АК InfoDiode RACK module, АК 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**. Таким образом, 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.

Данный сценарий был протестирован совместно специалистами АМТ-ГРУП и Лаборатории Касперского. В результате была подтверждена возможность полнофункционального совместного использования решений.




115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.amt.ru
www.infodiode.ru

# 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

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)