Применение CL DATAPK с однонаправленным шлюзом InfoDiode

В результате несанкционированных воздействий на АСУ ТП по каналам связи могут возникнуть чрезвычайные ситуации и/или нарушения выполняемых системой функций управления. При этом сетевой трафик является наиболее доступной информацией, позволяющей определить текущее состояние автоматизированной системы. Поэтому, чтобы выявить предпосылки реализации угроз ИБ и не допустить возникновение инцидентов ИБ в АСУ ТП, необходим непрерывный анализ и мониторинг состояния информационной безопасности, основанный на применении программно -аппаратных комплексов оперативного мониторинга и контроля защищенности АСУ ТП. Одним из таких комплексов является решение CyberLympha DATAPK.

CyberLympha DATAPK (CL DATAPK) – разработка компании Сайберлимфа, являющаяся развитием концепции мониторинга и анализа состояния ИБ для АСУ ТП, в том числе, интернета вещей (IoT) и промышленного интернета вещей (IIoT). Эффективность CL DATAPK подтверждена многочисленными инсталляциями DATAPK на предприятиях различных областей промышленности.

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 и нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

Совместное использование решений **InfoDiode** и патентованных методов анализа трафика от CL DATAPK позволяет выстроить комплексную и надежно функционирующую систему мониторинга трафика промышленного сегмента. Применение **InfoDiode** в составе системы мониторинга позволяет реализовать физическую изоляцию компонентов АСУ ТП и гарантировать отсутствие влияния подсистемы мониторинга ИБ на функции АСУ ТП. Таким образом обеспечивается полноценное выполнение требований по обеспечению ИБ промышленных систем автоматизации. **InfoDiode** и CL DATAPK 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. Их использование обеспечивает дополнительную защиту технологического процесса и промышленного оборудования как от ошибок персонала, так и от целенаправленных атак злоумышленников.

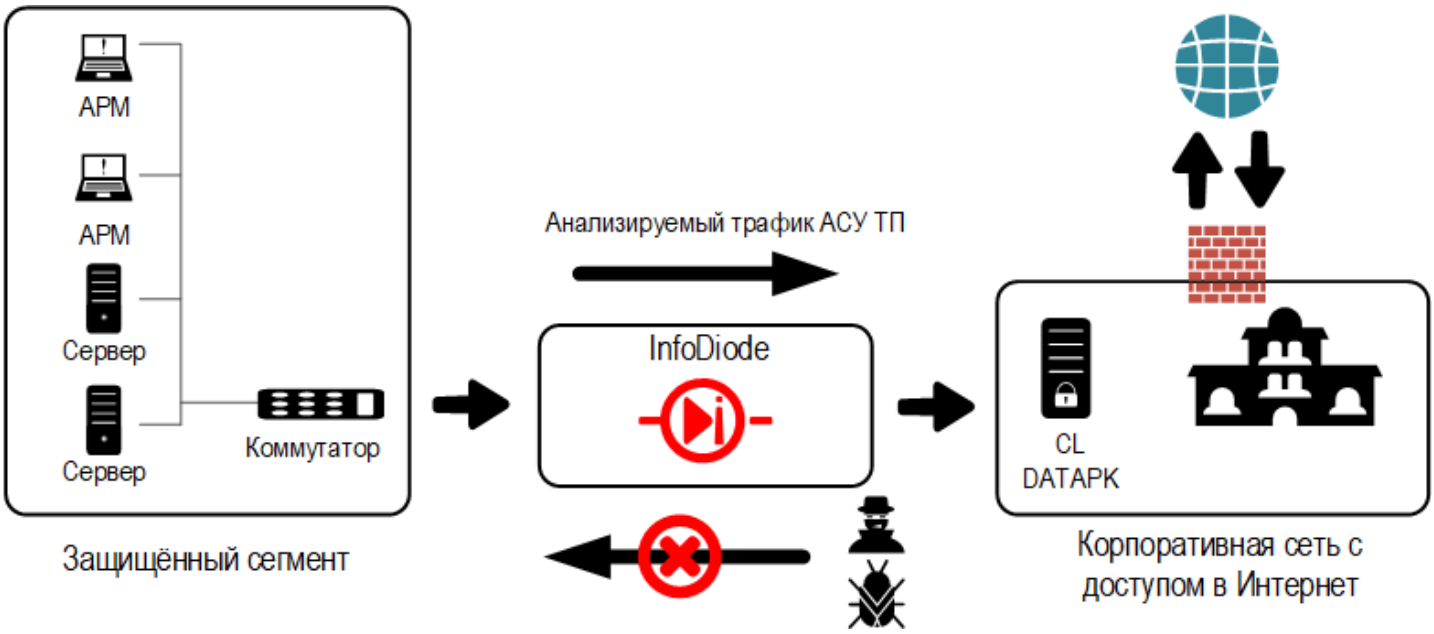
119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий передачи трафика закрытого сегмента на интерфейс CL DATAPK

С целью оперативного мониторинга и контроля состояния защищенности АСУ ТП объектов критической информационной инфраструктуры анализаторы трафика CL DATAPK могут размещаться в IT-сегменте сети, имеющем более низкие требования к безопасности нежели сегмент АСУ ТП, например в сегменте Интернет. В таких условиях очевидно, что сегменты промышленных сетей должны поддерживать высокий уровень изоляции. Применяемый уровень изоляции должен быть достаточным, чтоб предотвращать любые внешние воздействия на объекты этих сетевых сегментов со стороны сетей, в которых размещена анализаторы трафика. Представленный ниже сценарий демонстрирует решение этой задачи при помощи совместного использования CL DATAPK и **InfoDiode**.

Архитектура совместного использования CL DATAPK с моделями аппаратных комплексов **InfoDiode** (АК InfoDiode RACK, АК InfoDiode MINI) в сетях передачи данных промышленных объектов предполагает разграничение доступа путём размещения **InfoDiode** между источником анализируемого трафика и CL DATAPK. При этом возможен как сценарий передачи копии трафика через SPAN-порт коммутатора на слушающий интерфейс CL DATAPK для пассивного мониторинга АСУ ТП, так и сценарий отправки событий узлов АСУ ТП по UDP (Syslog, SNMP-trap) на активный сетевой интерфейс DATAPK. Оба сценария полностью исключают любое воздействие через этот же канал связи на защищённый сегмент сети.

В результате проведенных тестирований была подтверждена возможность полнофункционального совместного использования решений.



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

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программными продуктами

CL DATAPK

продукция компании

ООО «СайберЛимфа»

Россия, 121205, г. Москва, ИЦ Сколково, ул. Нобеля, 7

в дальнейшем именуемыми «**CL DATAPK**» и «**СайберЛимфа**»

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.

CL DATAPK – программный комплекс, созданный для оперативного мониторинга и контроля состояния защищенности систем автоматизации, в том числе, АСУ ТП критически важных объектов и объектов критической информационной инфраструктуры.

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

АМТ-ГРУП и **СайберЛимфа** провели всесторонние тесты продукта **CL DATAPK** 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 **CL DATAPK**. 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.

ООО «СайберЛимфа»

Дата:

15 апреля 2021 года

Должность:

Директор

Подпись_____

(А.А. Шанин)

АО «АМТ-ГРУП»

Дата:

15 апреля 2021 года

Должность:

Технический директор

Подпись_____

(В.В. Леонов)