



Однонаправленная
передача данных

Защита
объектов КИИ

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

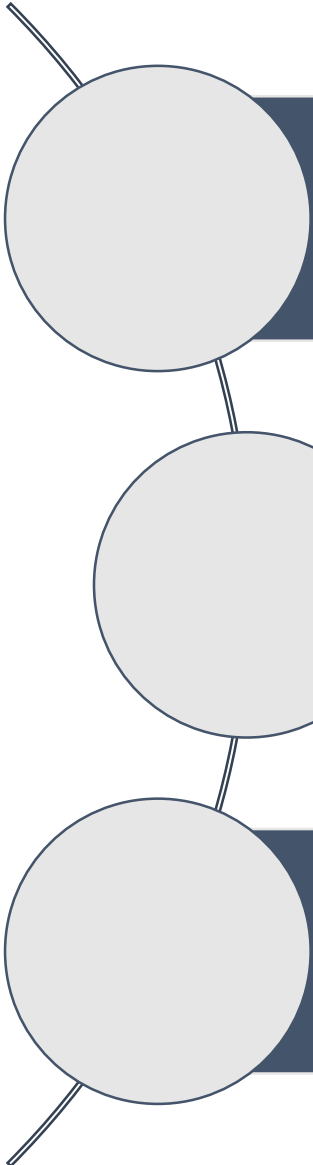
Info
-Diode



IT

05.10.2023

Продукты InfoDiode - как часть комплексных решений по защите доменов с разными уровнем доверия.



InfoDiode – решения для сегментации сети на физическом уровне

Задачи и вызовы междоменного взаимодействия

Направления развития InfoDiode в части Междоменных решений

5 опорных факторов, влияющих на выбор решений по обмену данными

1. Информационная изоляция объекта – ведет к потере конкурентоспособности
Обмен данными является одним из ключевых конкурентных факторов развития предприятий
2. Использование решений в АСУ ТП ограничено (Siemens, GE, Honeywell, Bentley Nevada и др.), но протоколы обмена остались. Промышленность, энергетика, транспорт работают со своими стандартными промышленными протоколами
Промышленные данные нужны за пределами технологического сегмента в формате пригодном для обработки
3. 166 Указ Президента
Сроки выполнения близятся
4. Решения должны быть комплексными
Защита объекта не сводится только к защите данных, периметра или рабочих мест
5. Угрозы и злоумышленники никуда не делись.
Риски для КИИ только растут



Инфраструктура СЗИ по некоторым направлениям строится фактически с нуля

В указанных условиях логичным решением является защитить периметр предприятия, сохранив передачу данных

- **Однонаправленный шлюз** – устройство, обеспечивающее передачу файловой и потоковой информации в одном направлении и не позволяющее передачу в обратном
 - Однонаправленность передачи гарантируется аппаратными решениями
 - Применяется для соединения разных сегментов сети



АМТ-ГРУП предоставляет полную линейку решений класса «диод» для защиты КИИ и АСУ ТП и ИТ инфраструктуры

- 1. АК InfoDiode** - базовое, сертифицированное ФСТЭК УД (4), аппаратное решение, гарантирующее защиту на аппаратном уровне и эффективно решающее задачу по передаче UDP, Syslog, SPAN трафика
- 2. АПК InfoDiode PRO** – сертифицированное ФСТЭК УД (4) решение для передачи значимых файловых потоков, дистрибутивов, реплик ВМ и баз данных, электронной почты, бэкапов и т.п.
- 3. АПК InfoDiode SMART** – новое решение для передачи за пределы периметра КИИ промышленных и специфических протоколов, в том числе видео, для интеграции SCADA систем, организации удаленных ситуационных центров за границей периметра, в условиях гарантированной изоляции КИИ



Продукты InfoDiode совместимы со многими решениями СЗИ, АСУТП, ИТ



ICS4, RU



Сегментация сети – локализуем данные, передаем часть данных



Сегментация сети – локализуем управление, передаем данные





Аппаратные «диоды»

Плюсы

- Недорого
- Решают базовые задачи изоляции
- Plug&Play, не требуют сопровождения службы эксплуатации

Минусы

- Не имеют IP, MAC адреса, требуют коммутации «порт-порт»
- Передать даже асинхронный TCP/IP трафик не получится

Аппаратно- программные «диоды»

Плюсы

- Решают задачу передачи протоколов прикладного уровня, в том числе промышленных протоколов, передают несколько видов трафика одновременно
- Доп функции СЗИ (NAT, white list/порты, контроль изменений конфигурации, контроль доступа, ввод в домен)
- Возможности по контролю за функционированием: SNMP, Syslog, NTP...

Минусы

- Могут занимать 3 или более RU
- Требуют специалиста в эксплуатации с базовыми навыками
- Требуют периодического (хотя и редкого) обновления ПО
- Имеют ограниченную функциональность контроля за передачей

Междоменные решения

Плюсы

- Регламентируют обмен
- Дополняют «традиционные диоды» функциями и решениями по контролю трафика
- Более комплексный подход к защите периметра организации

Минусы

- Предполагают более активное участие ИБ специалистов в контроле за передачей
- Как правило требуют проектных решений, включающих несколько СЗИ
- Часто строятся на двух разнонаправленных аппаратно-программных «диодах»

В основе обмена
лежит принцип
физической
однаправленности
физический сигнал
только в одну сторону

Задачи и вызовы междоменного взаимодействия



Домен – логически объединенная совокупность организационно-технических активов и ресурсов, подчиняющихся единой политике безопасности

Домен содержит данные, информационные системы и сети определенных классов, категорий безопасности, которые сегментированы, в том числе, в зависимости от возможностей передачи информации. Для некоторых доменов требуется установление большей степени доверия, тогда как для других меньшее доверие



- Доверенная сеть (в ряде случаев сеть/система-источник)** - область, формирующая наибольшие риски в отношении утраты, компрометации, нарушения характеристик обрабатываемой информации, систем, сегментов, данных, процессов
- Менее доверенная сеть (недоверенная сеть, в ряде случаев сеть/система-приемник)** - область, формирующая наибольшие риски в части вероятности организации атак из нее на иные сегменты и сети
- Периметр** - граница доверенной сети, на которой выполняется аутентификация запросов, регулируются информационные потоки, применяются организационно-технические меры для снижения рисков в отношении информации, сетей, данных, процессов

Отношения между доменами описываются в организационно-распорядительных документах **(политиках безопасности)**

1. **Увеличение интенсивности обмена** в рамках производственных циклов, обмена данными с контрагентами и органами власти
2. **Возможность утечки данных по тем же каналам**, которые используются для сопряжения доменов, систем
3. **Рост атак на ранее редко атакуемые типы устройств:** ПЛК, IP камеры, VoIP, UPS, NAS, СРК
4. Появление в составе вредоносного кода **специализированных фрагментов «под АСУ ТП»** (часто конкретного сектора, предприятия)
5. Атаки не всегда ведут к «убыткам». У части киберпреступников мотивом является **длительное присутствие**
6. **Компрометация вендоров** (в том числе СЗИ) для организации атаки, использование обновлений ПО, патчей в качестве инструмента атаки
7. **Рост количества атак на ИТ-ресурсы топ-менеджеров, руководство**, в том числе в целях использования в качестве «плацдарма» для развития атаки



❑ **Безопасность.** Средства обмена (в т.ч. носители данных) не представляют угрозы отправителям и приемникам данных. В случае обнаружения угроз, они должны быть своевременно локализованы или нивелированы



❑ **Конфиденциальность.** Средства обмена учитывают уровень доверия между субъектами и предотвращают возможности по нарушению конфиденциальности передаваемой информации при ее передаче



❑ **Скорость.** Средства обмена предоставляют достаточную скорость доступа к необходимой информации с соблюдением всех организационных и организационно-технических мер ("протоколов безопасности")



❑ **Достоверность.** Наличие гарантий, что полученная информация и ее источник не были скомпрометированы, а сама информация может быть использована для принятия решений



❑ **Надежность.** Решения по обмену данными обладают высокой степенью надежности и отказоустойчивости, возможностями по резервированию



- Контроль состояния узлов доступа и доступа к сети
- Преобразование и нормализация данных
- «Разрыв протоколов»
- Снижение вероятности использования уязвимостей «нулевого дня»
- Фильтрация и карантин
- Контроль сетевых потоков и антивирусная защита
- Защита от утечек данных
- Подтверждение происхождения данных и маркировка данных
- Решение по криптографии
- Исключение стеганографии

**Направление
усложнения
междоменных
решений**

- Реализация мер по соблюдению политики в области безопасности данных участниками обмена

Продукты InfoDiode развиваются как часть Междоменных решений



- Комплексные однонаправленные решения
 - Разрыв протоколов
 - Контроль состояния узлов доступа как в части состояния средства обмена, так и в части целостности ПО
 - Увеличение скорости передачи данных до 10G
 - Обмен данными с SIEM
 - Интеграция с DLP
 - Защита от утечек данных
 - Подтверждение происхождения данных

- Комплексные двунаправленные решения
 - Передача SIP трафика
 - Передача QUIC трафика
 - Передача NTP
 - Поддержка IPSec
 - ...



- Адрес: 115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б, подъезд 3, этаж 2, вход с Конного переулка
- Телефон/Факс: +7 (495) 725-7660, +7 (495) 646-7560
- Факс: +7 (495) 725-7663
- E-mail: InfoDiode@amt.ru
- Сайт: InfoDiode.ru
- Техническая поддержка: <https://support.amt.ru>



СПАСИБО ЗА ВНИМАНИЕ!