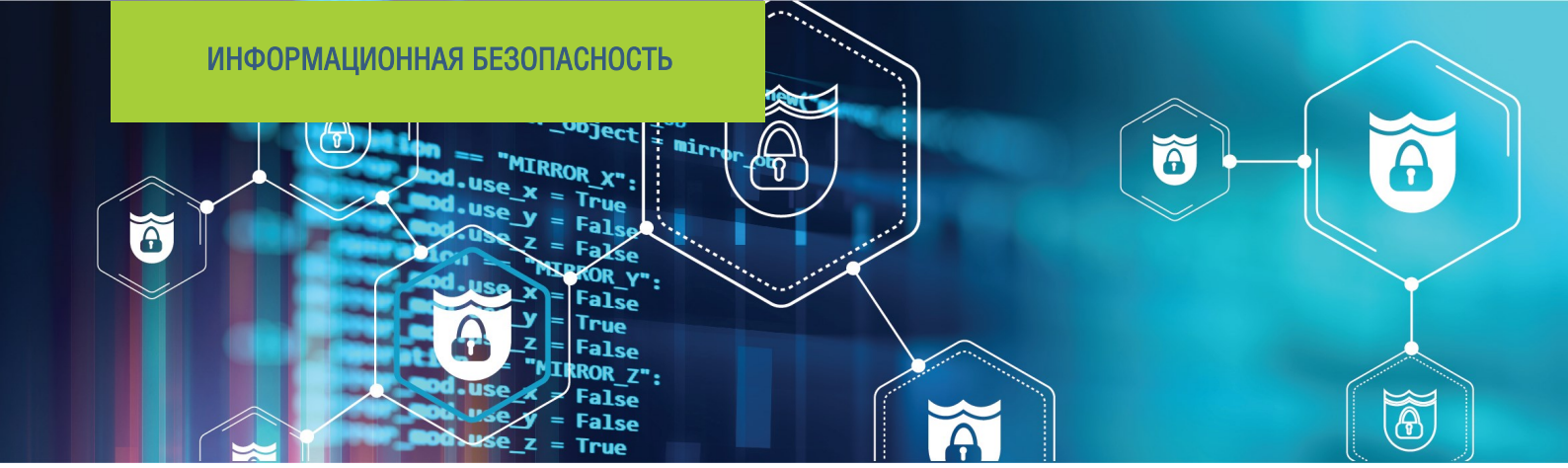

Однонаправленные шлюзы InfoDiode - реализуемые меры приказов ФСТЭК

Приказ ФСТЭК от 25 декабря 2017 г. N 239 устанавливает требования и состав мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры. В частности, предусматриваются меры по защите информационной (автоматизированной) системы и ее компонентов (ЗИС), включая защиту периметра информационной (автоматизированной) системы, сегментирование системы, защиту от угроз отказа в обслуживании (DOS, DDOS-атак), исключение доступа через общие ресурсы, реализацию электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек и другие.

В терминологии сетей связи практически любое сетевое подключение к защищаемому сегменту/объекту трактуется как «двунаправленное» и, чаще всего, таким и является. Двунаправленное взаимодействие несет в себе риски потери управления критическим объектом управляющими службами/диспетчерскими подразделениями/службами поддержки. Это становится возможным из-за высокой вероятности реализации атаки по двунаправленному каналу. Речь идет о классе управляемых атак, для организации которых необходимое условие - наличие оперативной обратной связи, то есть обмена вида «запрос-ответ». Такой обмен обеспечивается преимущественно в рамках стека протокола TCP/IP. Примеры известных реализуемых угроз, в основе которых лежит двунаправленный характер информационного обмена — WannaCry, Petya, EternalRocks и другие.

Отдельным значимым риском для КИИ является направление/загрузка чего-либо в критический сегмент: вредоносного кода, шпионского ПО и т.п. для целей мониторинга, сбора информации, нанесения отложенного ущерба.

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, обеспечивают возможность передачи данных и нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

Организация управляемых атак в случае размещения однонаправленного шлюза **InfoDiode** по направлению «из некритического сегмента» в критический становится практически невозможной. Организация управляемых атак, в том числе таких, как DDOS, равно как и передача каких-либо данных в критический сегмент в случае размещения однонаправленного шлюза **InfoDiode** по направлению «из критического сегмента в некритический» становятся полностью невозможными.

Комплексные решения с использованием продукта **InfoDiode** могут быть успешно применены как элемент защиты периметра объекта КИИ. **InfoDiode** позволяет сохранить канал передачи информации и обеспечить при этом выполнение требований приказа ФСТЭК от 25 декабря 2017 г. N 239 в части применяемых мер защиты.

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

Перечень мер приказов ФСТЭК России, реализуемых применением InfoDiode

Приказ ФСТЭК N 239 от 25 декабря 2017 г. и N 31 от 14 марта 2014 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.4	Сегментирование информационной (автоматизированной) системы
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию
ЗИС.31	Защита от скрытых каналов передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
ЗИС.35	Управление сетевыми соединениями

Приказ ФСТЭК N 17 от 11 февраля 2013 г. и N 21 от 18.02.2013 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

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