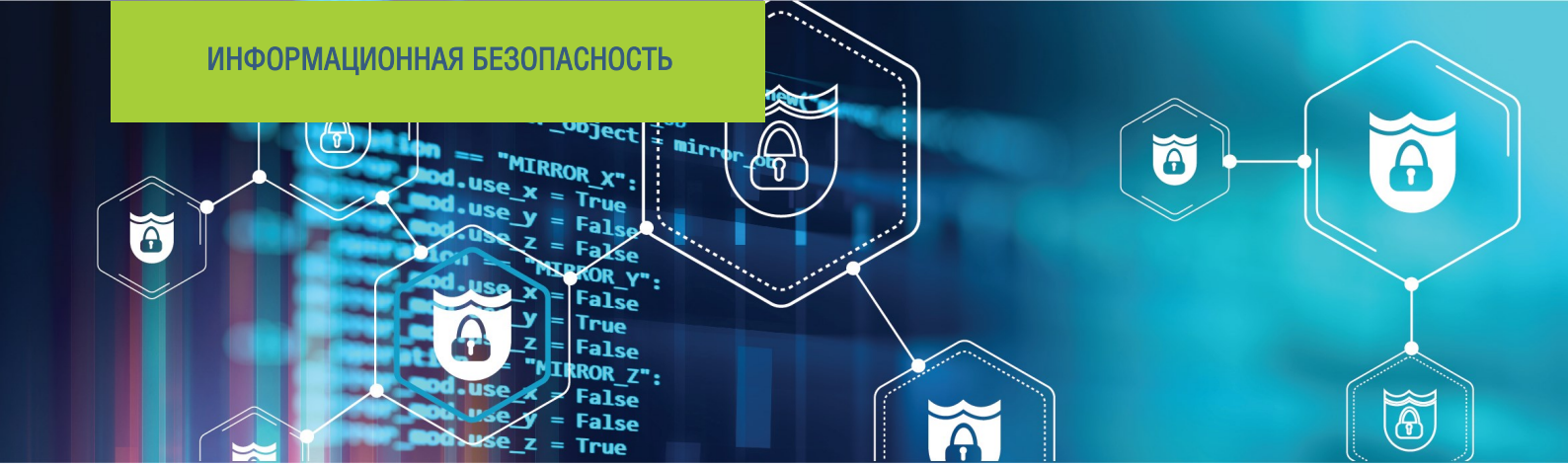

Однонаправленные шлюзы InfoDiode - реализуемые меры приказов ФСТЭК

Регулятор устанавливает требования и состав мер по обеспечению безопасности объектов защиты. Состав мер защиты варьируется, но содержит общие подходы и в отношении решений по обработке персональных данных (приказ ФСТЭК N 21) и в отношении защиты данных в государственных информационных системах (приказ ФСТЭК N 17) и в отношении решений применяемых на объектах критической информационной инфраструктуры и системах АСУ ТП (приказы ФСТЭК N 17 и N 239). В частности, регулятором 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 регулятора 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

22.05.2023

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.

Мера	Описание
ЗИС.2	**Расшифровка:** Защита периметра информационной (автоматизированной) системы **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной (автоматизированной) системы (изоляцию информационной системы на периметре) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных) **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети
ЗИС.3	**Расшифровка:** Эшелонированная защита информационной (автоматизированной) системы **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационно (автоматизированной) системы (изоляцию информационной системы на периметре) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). В том числе обеспечивается эшелонирование доступа к промежуточным репликам информационной (автоматизированной) системы. В частности, имея доступ к реплике данных, злоумышленник не может получить доступ к основной информационной (автоматизированной) системе. Частью эшелонирования является в том числе сегментирование ИС за счет реализации меры ЗИС.4 **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети
ЗИС.4	**Расшифровка:** Сегментирование информационной (автоматизированной) системы **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной (автоматизированной) системы (изоляцию информационной системы на периметре) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). В том числе обеспечивается сегментирование информационной (автоматизированной) системы. В частности, реализуется отделение контуров управления и контуров мониторинга, анализа, сбора данных. В качестве возможных направлений сегментации с полной физической изоляцией может быть обеспечено выделение Historian сервера, выделение копий и реплик баз данных информационной (автоматизированной) системы, передача данных функционирования (логов, событий безопасности, SPAN трафика) информационной (автоматизированной) системы в SOC, в SIEM систему, в IDS системы **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети

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

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

Мера	Описание
ЗИС.6	**Расшифровка:** Управление сетевыми потоками **Интерпретация:** СЗИ класса "диод" позволяет реализовать управление сетевыми потоками на уровне передачи данных прикладного уровня и исключить сетевые потоки, каналы, которые могут являться источником атаки. В частности, при применении решений InfoDiode может быть организован строго детерминированный, канал передачи информации из одного сетевого сегмента в другой, который позволит исключить какое-либо воздействие на защищаемый объект со стороны недоверенного сегмента (злоумышленника, нарушителя) **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику). Дополнительно реализуется организацией на InfoDiode строго регламентированных папок - endpoint для передачи данных
ЗИС.8	**Расшифровка:** Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы **Интерпретация:** СЗИ класса "диод" позволяет реализовать полное сокрытие топологии, архитектуры и конфигурации информационной (автоматизированной) системы. Это обеспечивается не только невозможностью передать какие-либо физические сигналы внутрь защищаемой сети/сегмента сети, но и за счет применения решений по NAT'ированию исходящего трафика, позволяющего скрыть адресацию сети отправителя и самого "диода" **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети, в том числе SPAN трафика
ЗИС.18	**Расшифровка:** Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию **Интерпретация:** СЗИ класса "диод" обеспечивает невозможность эксплуатации потенциальных уязвимостей средств межсетевого экранирования путем эксплуатации их известных уязвимостей и уязвимостей "нулевого дня" для целей организации несанкционированных каналов информации из недоверенных сегемнтов сети и ограничивает возможности подключения из доверенных сегментов сети к "диод", в том числе путем реализации мер аутентификации и авторизации и реализации доступа только с определённых IP адресов или подсетей. В том числе применение InfoDiode обеспечивает организацию строго детерминированного канала обмена данными с учетом принятой схемы адресации и доступа к IN и OUT серверам в составе InfoDiode. В том числе в составе InfoDiode предусмотрена возможность передачи копии, данных метаинформации о передаваемом трафике в отдельный источник DLP в целях фиксации фактов несанкционированной передачи информации **Реализация в InfoDiode:** Реализуется настройками доступа к сервисам строго из определенных подсетей. Реализуется самим физическим принципом работы аппаратной компоненты InfoDiode и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети, в том числе SPAN трафика

Мера	Описание
ЗИС.31	**Расшифровка:** Защита от скрытых каналов передачи информации **Интерпретация:** СЗИ класса "диод" обеспечивает невозможность эксплуатации потенциальных уязвимостей средств межсетевого экранирования путем эксплуатации их известных уязвимостей и уязвимостей "нулевого дня" для целей организации несанкционированных каналов информации из недоверенных сегемнтов сети и ограничивает возможности подключения из доверенных сегментов сети к "диод", в том числе путем реализации мер аутентификации и авторизации и реализации доступа только с определённых IP адресов или подсетей. В том числе применение InfoDiode обеспечивает организацию строго детерминированного канала обмена данными с учетом принятой схемы адресации и доступа к IN и OUT серверам в составе InfoDiode. В том числе в составе InfoDiode предусмотрена возможность передачи копии, данных метаинформации о передаваемом трафике в отдельный источник DLP в целях фиксации фактов несанкционированной передачи информации **Реализация в составе решения InfoDiode:** Реализуется настройками доступа к сервисам строго из определенных подсетей. Реализуется самим физическим принципом работы аппаратной компоненты InfoDiode и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети, в том числе SPAN трафика
ЗИС.34	**Расшифровка:** Защита от угроз отказа в обслуживании (DOS, DDOS-атак) Интерпретация: СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной (автоматизированной) системы на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверной компоненте, среде виртуализации, коммутационному оборудованию и т.п) из открытого/недоверенного сегмента. В том числе обеспечивается невозможность преодоления физической компоненты для организации DOS, DDOS атак на доверенный сегмент с информационной (автоматизированной) системой **Реализация в составе решения InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети
ЗИС.35	**Расшифровка:** Управление сетевыми соединениями **Интерпретация:** СЗИ класса "диод" обеспечивает организацию подключений из доверенного сегмента в IN части "диода" только по определенным IP адресам и портам, исключая возможность какого-либо прямого соединения с недоверенным сегментом, а также обхода каких-либо программно реализуемых правил межсетевого экранирования. СЗИ класса "диод" исключает возможность установления соединения с доверенным сегментом из недоверенного сегмента на физическом уровне **Реализация в составе решения InfoDiode:** Реализуется путем формирования правил подключения к InfoDiode только с определенных IP адресов и только с учетом пройденных процедур авторизации и аутентификации, а также с учетом определенных портов доступа. Наличие аппаратной компоненты полностью исключает возможность прямого подключения к внешним информационным ресурсам

Мера	Описание
ЗИС.16	**Расшифровка:** Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов **Интерпретация:** СЗИ класса "диод" обеспечивает невозможность эксплуатации потенциальных уязвимостей средств межсетевого экранирования путем эксплуатации их известных уязвимостей и уязвимостей "нулевого дня" для целей организации несанкционированных каналов информации из недоверенных сегемнтов сети и ограничивает возможности подключения из доверенных сегментов сети к "диод", в том числе путем реализации мер аутентификации и авторизации и реализации доступа только с опрелеленных ip-адресов или подсетей. В том числе применение InfoDiode обеспечивает организацию строго детерминированного канала обмена данными с учетом принятой схемы адресации и доступа к IN и OUT серверам в составе InfoDiode. В том числе в составе InfoDiode предусмотрена возможность передачи копии, данных метаинформации о передаваемом трафике в отдельный источник DLP в целях фиксации фактов несанкционированной передачи информации **Реализация в InfoDiode:** Реализуется настройками доступа к сервисам строго из определенных подсетей. Реализуется самим физическим принципом работы аппаратной компоненты InfoDiode и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети, в том числе SPAN трафика
ЗИС.17	**Расшифровка:** Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной системы (изоляцию информационной системы на периметре) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). В том числе обеспечивается сегментирование информационной (автоматизированной системы). В частности, реализуется отделение контуров управления и контуров мониторинга, анализа, сбора данных. В качестве возможных направлений сегментации с полной физической изоляцией может быть обеспечено выделение Historian сервера, выделение копий и реплик баз данных информационной (автоматизированной системы), передача данных функционирования (логов, событий безопасности, SPAN трафика) информационной (автоматизированной системы) в SOC, в SIEM систему, а также в IDS системы **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети

Мера	Описание
ЗИС.22	**Расшифровка:** Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной системы на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверной компоненте, среде виртуализации, коммутационному оборудованию и т.п) из открытого сегмента. Как следствие, реализуя защиту информационной системы от попыток нарушителей вызвать отказ в обслуживании. В том числе обеспечивается невозможность преодоления физической компоненты для организации DOS, DDOS атак на доверенный сегмент с информационной (автоматизированной) системой **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети
ЗИС.23	**Расшифровка:** Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной системы (изоляцию информационной системы на периметре) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных) **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети
УПД.3	**Расшифровка:** Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами **Интерпретация:** СЗИ класса "диод" позволяет реализовать управление сетевыми потоками на уровне передачи данных прикладного уровня и исключить сетевые потоки, каналы, которые могут являться источником атаки. В частности, при применении решений InfoDiode может быть организован строго определенный, детерминированный канал передачи информации из одного сетевого сегмента в другой, который позволит исключить какое-либо воздействие на защищаемый объект со стороны недоверенного сегмента (злоумышленника, нарушителя). СЗИ класса "диод" обеспечивает организацию подключений из доверенного сегмента в IN части "диода" только по определенным IP адресам и портам, исключая возможность какого-либо прямого соединения с недоверенным сегментом, а также обхода каких-либо программно реализуемых правил межсетевого экранирования. СЗИ класса "диод" исключает возможность установления соединения с доверенным сегментом из недоверенного сегмента на физическом уровне **Реализация в InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети