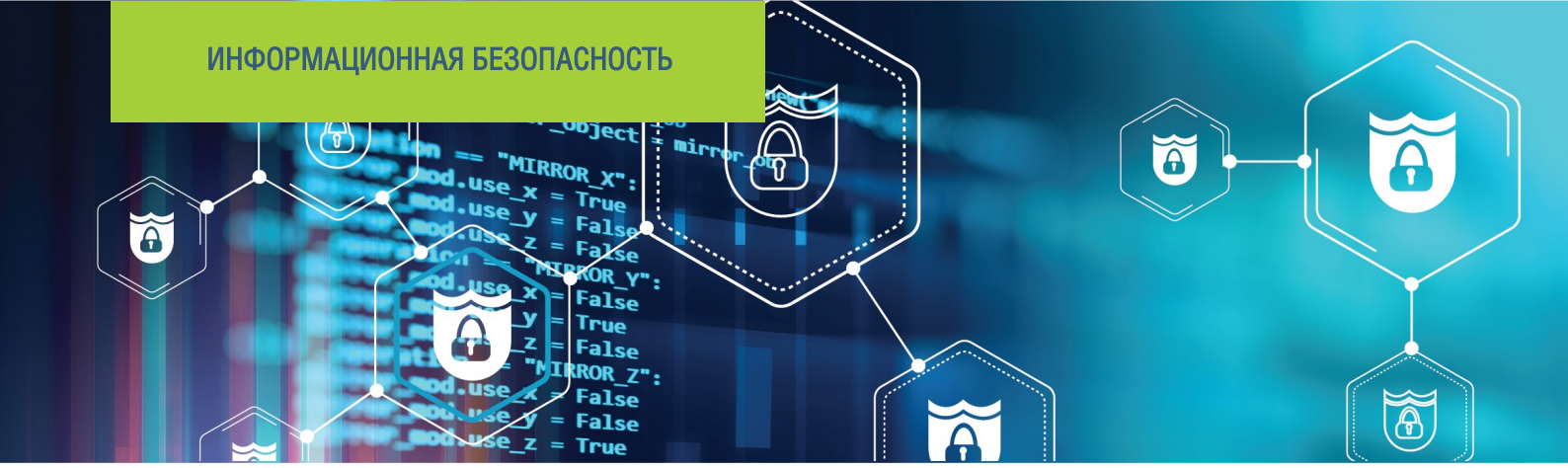

Однонаправленные шлюзы InfoDiode - реализуемые меры ФЗ и приказов ФСТЭК

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 № 21), и в отношении защиты данных в государственных информационных системах (приказ ФСТЭК № 117), и в отношении решений применяемых на объектах критической информационной инфраструктуры и системах АСУ ТП (приказы ФСТЭК N 117 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

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм 187-ФЗ от 26 июля 2017 г.

187-ФЗ от 26 июля 2017 г.	Обеспечение
Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры. Принципами обеспечения безопасности критической информационной инфраструктуры являются: 1)законность; 2)непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры; 3)приоритет предотвращения компьютерных атак.	1) Решения InfoDiode являются сертифицированными решениями ФСТЭК УД (4), что позволяет применять их для защиты КИИ вплоть до 1 категории; 2) Продукты InfoDiode представляют собой комплексные решения, поставляемые производителем, который имеет полную линейку устройств класса «диод». Устройства и решения поставляются на рынок более 10-и лет. В том числе совершенствуются уже внедренные линейки в части производительности, функциональности, надежности, обновления ПО. Обеспечивается полный цикл поддержки уже внедренных комплексов; 3) InfoDiode обеспечивает предотвращение удаленных сетевых атак во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты.
Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры. 2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются: 1)предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации; 2)недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры; ...	1) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью неправомерный доступ к информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты; 2) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта. Защита обеспечивается во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты;

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

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 239 от 14 марта 2014 г.

Приказ ФСТЭК N 239 от 14 марта 2014 г.	Обеспечение
III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов. 16. Задачами обеспечения безопасности значимого объекта являются: а) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации; б) недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта; в) обеспечение функционирования значимого объекта в проектных режимах его работы в условиях воздействия угроз безопасности информации; г) обеспечение возможности восстановления функционирования значимого объекта критической информационной инфраструктуры. …	а) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью неправомерный доступ к информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты; б) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта. Защита обеспечивается во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты; в) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта в том числе в проектных режимах. Защита обеспечивается во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты; г) Решения InfoDiode позволяют создать закрытый контур хранения резервных копий, доступ к которому по двунаправленному каналу в целях модифицирования информации невозможен. Наличие такого контура обеспечивает хранение эталонных неизменяемых копий, позволяющих восстановить инфраструктуру объекта критической информационной инфраструктуры в случае реализованного инцидента ИБ.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 21 от 18 февраля 2013 г.

Приказ ФСТЭК N 21 от 13 февраля 2013 г.	Обеспечение
II. Состав и содержание мер по обеспечению безопасности персональных данных 8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.	InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью неправомерный доступ к информации (в том числе персональным данным), ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации. Защита обеспечивается во всех случаях, когда такая атака осуществляется. В том числе защита обеспечивается при реализации атак, возникающих в ходе взаимодействия с иными информационными системами и информационно-телекоммуникационными сетями. Функция безопасности обеспечивается физической изоляцией объекта защиты. Дополнительно, применение InfoDiode позволяет формировать и передавать обезличенные реплики персональных данных в иные сети и сегменты, исключая доступ к эталонным персональным данным в защищаемых сетевых сегментах.

Интерпретация некоторых норм Приказа ФСТЭК N 31 от 14 марта 2014 г.

Приказ ФСТЭК N 31 от 14 марта 2014 г.	Обеспечение
Внедрение системы защиты автоматизированной системы управления и ввод ее в действие. 15.4. Установка и настройка средств защиты информации осуществляется в случаях, если такие средства необходимы для блокирования (нейтрализации) угроз безопасности информации, которые невозможно исключить настройкой (заданием параметров) программного обеспечения автоматизированной системы управления и (или) реализацией организационных мер защиты информации.	InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта. Защита обеспечивается во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты. Комплексы InfoDiode реализуют в своем составе функции безопасности (физическая однонаправленность), которые НЕ могут быть исключены или отключены настройкой (заданием параметров) программного обеспечения автоматизированной системы управления, самого СЗИ InfoDiode или иными

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 117 от 11 апреля 2025 г.

Приказ ФСТЭК N 117 от 11 апреля 2025 г.	Обеспечение
10. Оператор (обладатель информации) должен обеспечивать защиту информации, обрабатываемой в информационных системах, в целях: а) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее - нарушение безопасности информации); б) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.	Применение InfoDiode в инфраструктуре организации за счет надежной изоляции ключевых сетевых сегментов и нейтрализации удаленных сетевых атак снижает возможность наступления негативных последствий от нарушения конфиденциальности, целостности, доступности информации, а также от нарушения функционирования информационных систем. Функция безопасности, реализованная на физическом (аппаратном) уровне, гарантирует необходимый уровень защиты информации, обрабатываемой в информационных системах.
34. Для достижения целей защиты информации оператором (обладателем информации) должны проводиться следующие мероприятия: д) обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа; р) обеспечение защиты информации при взаимодействии с подрядными организациями; с) обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании	Решения InfoDiode могут использоваться для защиты информации ограниченного доступа при её обработке, хранении и обращении за счет физической однонаправленности передачи данных и разрыва двунаправленных сетевых протоколов, что ограничивает возможности по получению несанкционированного доступа к информации ограниченного доступа. Также функции междоменного решения InfoDiode позволяют обеспечить контроль за передаваемой информацией и позволяют исключить утечки информации ограниченного доступа и иной конфиденциальной информации из информационной системы.
39. Мероприятия по управлению обновлениями должны включать проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестировании обновлений до их применения в контурах промышленной эксплуатации информационных систем, выдаче разрешения подразделениям (работникам) оператора (обладателя информации) на применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации информационных систем с использованием безопасных настроек и конфигураций, установленных во внутренних стандартах по защите информации. Бесконтрольная установка обновлений программных, программно-аппаратных средств не допускается.	Функции междоменного решения InfoDiode позволяют обеспечить контроль за передаваемыми дистрибутивами и обновлениями программных, программно-аппаратных средств, в том числе обеспечить блокирование зараженных файлов за счет интеграции с антивирусными системами или «песочницами», а также проверять целостность и подлинность обновлений за счет интеграции с криптопровайдером.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 117 от 11 апреля 2025 г.

Приказ ФСТЭК N 117 от 11 апреля 2025 г.	Обеспечение
30. Проводимые мероприятия и принимаемые меры по защите информации должны быть направлены на блокирование (нейтрализацию) актуальных для информационной системы угроз безопасности информации (далее - актуальные угрозы) в соответствии с целями защиты информации, определенными в политике защиты информации. В зависимости от целей защиты информации, мероприятия и меры по защите информации должны быть направлены на: а) исключение утечки информации ограниченного доступа и иной конфиденциальной информации; б) предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них; в) предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них; г) предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них; д) предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них; з) исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем; и) недопущение распространения с использованием информационных систем противоправной информации; л) обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.	Решения InfoDiode могут использоваться в качестве мер по защите информации и позволяют эффективно блокировать (нейтрализовать) актуальные для информационной системы угрозы безопасности информации за счет своих функций безопасности: — Физическая однонаправленность передачи данных через InfoDiode и разрыв двунаправленных сетевых протоколов гарантируют невозможность получения удаленного несанкционированного доступа к информационной системе, что позволяет предотвратить несанкционированную модификацию, подмену, уничтожение информации, содержащейся в системе, а также минимизирует риски нарушения её функционирования из-за удаленного воздействия или распространения противоправной информации с использованием информационной системы; — Функции междоменного решения InfoDiode, которые позволяют обеспечить контроль за передаваемой информацией, позволяют исключить утечки информации ограниченного доступа и иной конфиденциальной информации из информационной системы. Также использование решения InfoDiode возможно для построения надежного хранилища резервных копий, которое будет недоступно для злоумышленников даже при компрометации всей инфраструктуры организации (хранилище «черного дня»). Оно позволяет обеспечить возможность восстановление данных организации в случае их модификации или уничтожения вследствие реализации угроз безопасности информации.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 117 от 11 апреля 2025 г.

Приказ ФСТЭК N 117 от 11 апреля 2025 г.	Обеспечение
40. Мероприятия по защите информации при обработке, хранении и обращении с информацией ограниченного доступа должны исключать: неправомерное распространение информации ограниченного доступа вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети "Интернет"; доступ к информации ограниченного доступа лиц, для которых информация не предназначена и (или) для которых такой доступ запрещен.	Функции междоменного решения InfoDiode позволяют обеспечить контроль за передаваемой информацией, в том числе за счет интеграции с системами предотвращения утечек (DLP) обеспечить блокировку информации ограниченного доступа, передаваемой через InfoDiode.
41. Мероприятия по обеспечению защиты информации при применении конечных устройств информационных систем должны исключать возможность несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью "Интернет" и (или) доступные из сети "Интернет".	InfoDiode за счет разрыва двунаправленных сетевых протоколов обеспечивает нейтрализацию удаленных сетевых атак, имеющих целью получение несанкционированного доступа к информационным системам, на взаимодействующие с сетью "Интернет" интерфейсы и порты.
49. Мероприятия по осуществлению мониторинга информационной безопасности должны предусматривать сбор данных о событиях безопасности, их обработке и анализе, а также выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации. Мероприятия по осуществлению мониторинга информационной безопасности должны проводиться в отношении всех информационных систем, за исключением локальных и изолированных информационных систем, в которых должен обеспечиваться контроль журналов регистрации событий безопасности.	Использование решения InfoDiode при построении ситуационного центра информационной безопасности (SOC) позволяет обеспечить сбор данных с агентов и сетевых сенсоров, размещенных на критических системах организации, и при этом за счет однонаправленного потока данных гарантировать невозможность проникновения злоумышленника в ключевые сетевые сегменты даже в случае компрометации инфраструктуры SOC.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 117 от 11 апреля 2025 г.

Приказ ФСТЭК N 117 от 11 апреля 2025 г.	Обеспечение
52. Посредством проведения мероприятий по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций должна быть обеспечена возможность восстановления выполнения функций (процессов, видов работ) информационных систем, для которых оператором (обладателем информации) установлены требования к непрерывному режиму функционирования (далее - значимые функции), в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.	Использование решения InfoDiode возможно для построении надежного хранилища резервных копий, которое будет недоступно для злоумышленников даже при компрометации всей инфраструктуры организации (хранилище «черного дня»). Оно позволяет обеспечить возможность восстановление данных организации в случае их модификации или уничтожения вследствие реализации угроз безопасности информации.
58. Посредством проведения мероприятий по защите информации при взаимодействии оператора (обладателя информации) с подрядными организациями должна быть исключена возможность несанкционированного доступа или воздействий на информационные системы и содержащуюся в них информацию через взаимодействующие с информационными системами программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы, используемые для доступа подрядных организаций к информационным системам.	Использование решения InfoDiode при организации взаимодействия с подрядными организациями позволяет изолировать сетевые сегменты с необходимыми системами или репликами систем или баз данных с необходимым уровнем обезличивания, что гарантирует невозможность несанкционированного доступа или воздействий на информационные системы и содержащуюся в них информацию через взаимодействующие с информационными системами программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы
61. При взаимодействии пользователей в целях выполнения ими своих обязанностей (функций) с сервисами на основе искусственного интеллекта посредством направления запроса и получения ответа должны быть: а) при взаимодействии в формате строго заданных шаблонов запросов и ответов: определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам; определены шаблоны ответов искусственного интеллекта и обеспечен контроль соответствия ответов установленным оператором (обладателем информации) шаблонам.	В случаях, когда взаимодействие с сервисами искусственного интеллекта должно проводиться в формате строго заданных шаблонов запросов и ответов, функции междоменного решения InfoDiode позволяют обеспечить контроль за передаваемой информацией между сервисами на основе искусственного интеллекта и пользователями за счет возможности сверки передаваемых запросов и ответов с заданными шаблонами.

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

Реализация мероприятий методических документов ФСТЭК путем применения СЗИ InfoDiode

Интерпретация некоторых мероприятий Методического документа ФСТЭК от 12 апреля 2026 г.

Методический документ ФСТЭК от 12 апреля 2026 г.	Обеспечение
2.9. Основными принципами создания информационных систем в защищенном исполнении являются: … минимизация интерфейсов информационных систем, доступных для субъектов доступа, в соответствии с функциями информационной системы; сегментация (микросегментация) информационных систем с учетом уровней значимости защищаемых информационных ресурсов (разбиение на сегменты безопасности) и контроль доступа в выделенные сегменты на основе уровня доступа субъектов доступа; …	Применение InfoDiode в инфраструктуре организации позволяет обеспечить надежную изоляцию ключевых сетевых сегментов и информационных систем, а также ограничить доступ к интерфейсам информационной системы из других сегментов. Это достигается за счет функций безопасности InfoDiode — физической (аппаратной) однонаправленной передачи данных и разрыва двунаправленных сетевых соединений.
2.11. Рост числа сервисов, предоставляемых информационными системами, неразрывно связан с увеличением количества требуемых для их функционирования интерфейсов, что ведет к расширению поверхности компьютерных атак на информационные системы. Уменьшение поверхности компьютерных атак является одной из важнейших задач по защите информационных систем и содержащейся в них информации. Решению данной задачи способствуют унификация применяемых программных, программно-аппаратных средств и контроль их использования. Контроль интерфейсов информационных систем, прежде всего доступных из сети «Интернет», и недопущение их несанкционированного ввода в действие и эксплуатации обеспечивают снижение возможности нарушителей по реализации угроз безопасности информации.	Применение InfoDiode в инфраструктуре организации за счет надежной изоляции ключевых сетевых сегментов и информационных систем снижает поверхность атаки, гарантированно нейтрализуя удаленный вектор реализации угроз, направленный внутрь защищаемого сегмента. Это достигается за счет функций безопасности InfoDiode — физической (аппаратной) однонаправленной передачи данных и разрыва двунаправленных сетевых соединений.

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

Реализация мероприятий методических документов ФСТЭК путем применения СЗИ InfoDiode

Интерпретация некоторых мероприятий Методического документа ФСТЭК от 12 апреля 2026 г.

Методический документ ФСТЭК от 12 апреля 2026 г.	Обеспечение
3.4. Управление обновлениями (КО) … получение обновлений программных, программно-аппаратных средств из источников, содержащих механизмы проверки подлинности и целостности обновлений; проверку подлинности и целостности обновлений программных, программно-аппаратных средств; …	Применение InfoDiode совместно с профильными СЗИ (антивирусом, «песочницей», криптопровайдером) в инфраструктуре организации позволяет обеспечить контроль за передаваемыми файлами обновлений информационных систем. Передаваемые файлы, помимо проверки на соблюдение внутренних политик InfoDiode, направляются на проверку на заражение, а также на проверку ЭП, и будут переданы в целевую систему только если они будут признаны безопасными на всех этапах контроля.
3.5. Обеспечение ЗИ при обработке, хранении и обращении с информацией ограниченного доступа (ОД) … контроль передачи, распространения информации ограниченного доступа в информационной системе, в том числе контроль вывода информации ограниченного доступа из информационной системы; … 6) обеспечение контроля перемещения используемых в информационной системе съемных внешних средств хранения информации за пределы контролируемой зоны; 7) применение средств защиты от неправомерной передачи информации из информационной системы (в том числе DLP-систем и средств однонаправленной передачи информации); …	Применение InfoDiode совместно с профильными СЗИ (системой предотвращения утечек) в инфраструктуре организации позволяет обеспечить контроль за передаваемыми между сегментами файлами. Передаваемые файлы, помимо проверки на соблюдение внутренних политик InfoDiode, направляются на контентный анализ, и будут переданы в целевую систему, только если файлы будут признаны безопасными на всех этапах контроля.
3.11. Обеспечение мониторинга информационной безопасности (МБ) … 3) должны применяться технические средства однонаправленного ответвления сетевого трафика; 4) должны применяться пассивные (энергонезависимые) технические средства однонаправленного ответвления сетевого трафика.	Применение InfoDiode позволяет надежно отделить инфраструктуру технологической сети или иных ключевых сегментов от сегмента ситуационного центра информационной безопасности, обеспечив нейтрализацию удаленных сетевых атак на информационные системы технологической сети в случае компрометации ситуационного центра. При этом InfoDiode сохраняет возможность передачи SPAN-трафика и данных SIEM агентов в ситуационный центр для дальнейшего его анализа.

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

Реализация мероприятий методических документов ФСТЭК путем применения СЗИ InfoDiode

Интерпретация некоторых мероприятий Методического документа ФСТЭК от 12 апреля 2026 г.

Методический документ ФСТЭК от 12 апреля 2026 г.	Обеспечение
3.14. Обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций (НФ) … Должно быть обеспечено резервное копирование информации, содержащейся в информационных системах, необходимой для обеспечения выполнения значимых функций, а также ее хранение в местах, исключающих несанкционированный доступ к ее копиям. …	Применение InfoDiode позволяет построить надежное хранилище резервных копий — хранилище «черного дня». За счет разрыва двунаправленных сетевых протоколов InfoDiode нейтрализует вектор атаки, связанный с удаленным НСД. Также за счет контроля за передаваемыми файлами резервных копий, проверяемыми на соответствие политикам безопасности передачи данных как InfoDiode, так и профильными СЗИ (антивирусом, «песочницей»), обеспечивается передача в хранилище только безопасных резервных копий.
3.16. Обеспечение защиты информации при взаимодействии с подрядными организациями (ЗП) … В случае если в результате предоставленного доступа в информационных системах подрядных организаций осуществляется обработка и хранение полученной информации, в них должны быть приняты меры по защите информации в соответствии с настоящим методическим документом. … 3) должен быть обеспечен контроль загружаемых подрядными организациями в информационные системы файлов на наличие в них вредоносного программного обеспечения, а также контроль выгружаемых подрядными организациями файлов.	Применение InfoDiode позволяет изолировать сети организации от прямого воздействия со стороны подрядчиков за счет разрыва двунаправленных протоколов. А за счет контроля за передаваемыми подрядчиками файлами, проверяемых на соответствие политикам безопасности передачи данных как с помощью InfoDiode, так и профильными СЗИ (антивирусом, «песочницей»), обеспечивается передача во внутренние сегменты только безопасных файлов.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Реализация мероприятий методических документов ФСТЭК путем применения СЗИ InfoDiode

Интерпретация некоторых мероприятий Методического документа ФСТЭК от 12 апреля 2026 г.

Методический документ ФСТЭК от 12 апреля 2026 г.	Обеспечение
3.17. Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании (ОО) ... использование программных, программно-аппаратных средств, обеспечивающих анализ и фильтрацию входящего трафика в соответствии с матрицей коммуникаций информационных систем с сетью «Интернет», и возможность блокирования входящего трафика, обладающего признаками компьютерных атак, направленных на отказ в обслуживании, от сетевого до прикладного уровня информационных систем; …	Применение InfoDiode на периметре ключевых сетевых сегментов позволяет изолировать информационные системы организации от внешнего воздействия, направленного на отказ в обслуживании. Это достигается за счет функций безопасности InfoDiode — физической (аппаратной) однонаправленной передачи данных и разрыва двунаправленных сетевых соединений.
3.18. Обеспечение защиты информации при использовании искусственного интеллекта (ИИ) … выделение информационной инфраструктуры разработки системы искусственного интеллекта от иной инфраструктуры разработчика, не связанной с разработкой данной системы, в отдельный изолированный сегмент; … обеспечению изоляции системы искусственного интеллекта; … 1) должно быть обеспечено выделение информационной инфраструктуры разработки от иной инфраструктуры разработчика, не связанной с разработкой данной системы, в отдельный физически изолированный сегмент; … 5) должно быть обеспечено выделение системы искусственного интеллекта в информационной системе в отдельный изолированный сегмент информационной системы; …	Применение InfoDiode позволяет обеспечить надежную изоляцию информационной инфраструктуры разработки системы искусственного интеллекта от иной инфраструктуры разработчика, обеспечив нейтрализацию удаленных сетевых атак на информационные системы разработки искусственного интеллекта в случае компрометации иной инфраструктуры разработки организации. Это достигается за счет функций безопасности InfoDiode — физической (аппаратной) однонаправленной передачи данных и разрыва двунаправленных сетевых соединений.

AMT GROUP

119121, Россия, Москва, Ружейный переулок, 6с1.
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.

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

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

www.amt.ru
www.infodiode.ru

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

* Рекомендованная (необязательная) мера приказов

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
ЗКУ.1	Управление доступом к конечным устройствам ... 4) в составе конечного устройства, предназначенного для подключения к нескольким информационным системам информационной инфраструктуры оператора, должны применяться компоненты, обеспечивающие гарантированное (физическое) разделение информационных систем (сегментов, контуров) и невозможность сохранения созданных данных в энергонезависимую память; … **Интерпретация:** СЗИ класса "диод" - InfoDiode - позволяет гарантированно разделить информационные системы (сегменты, контуры) на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь из любых внешних сегментов. **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.
ЗКУ.5	Контроль и фильтрация трафика на конечном устройстве ... 4) в составе конечного устройства должны применяться аппаратные средства гарантированной блокировки линий обмена данными по команде и (или) по расписанию. … **Интерпретация:** СЗИ класса "реле" - InfoRelay - позволяет гарантированно раскоммутировать сетевые сегменты на физическом уровне по нажатию на кнопку на устройстве или по истечению заданного временного таймера, исключая возможность направить какой-либо физический сигнал по такому каналу связи. **Реализация в InfoRelay** Реализуется физическим принципом работы аппаратной компоненты InfoRelay — нажатие на кнопку на устройстве приводит к переключению аппаратного реле и физическому «разрыву» соединения между сетями.

Мера	Описание
ЗКУ.6	Анализ и реагирование на события безопасности ... 4) должны обеспечиваться блокирование и (или) изоляция конечного устройства, на котором выявлены компьютерные инциденты. … **Интерпретация:** СЗИ класса "реле" - InfoRelay - позволяет гарантированно раскоммутировать сетевые сегменты на физическом уровне при выявлении компьютерного инцидента по нажатию на кнопку на устройстве или по истечению заданного временного таймера, исключая возможность направить какой-либо физический сигнал по такому каналу связи. **Реализация в InfoRelay:** Реализуется физическим принципом работы аппаратной компоненты InfoRelay — нажатие на кнопку на устройстве приводит к переключению аппаратного реле и физическому «разрыву» соединения между сетями.
ЗИВ.2	Управление доступом к устройствам «интернета вещей» … 9) устройства «интернета вещей» и вычислительной сети устройств «интернета вещей» в целом, используемые в информационных системах в целях выполнения ими своих функций, должны быть изолированы от сетей связи, предназначенных для доступа к сети «Интернет» и (или) иной общедоступной сети связи. **Интерпретация:** СЗИ класса "диод" - InfoDiode - позволяет гарантированно отделить устройства «интернета вещей» на физическом уровне от сетей связи, предназначенных для доступа к сети «Интернет» и (или) иной общедоступной сети связи, исключая возможность направить какой-либо физический сигнал по каналу свя- **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
119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.amt.ru
www.infodiode.ru

Мера	Описание
ЗИВ.2	Защита данных … выделение сетей устройств «интернета вещей» в отдельные сегменты информационной системы; **Интерпретация:** СЗИ класса "диод" - InfoDiode - позволяет гарантированно отделить устройства «интернета вещей» на физическом уровне от иных информационных систем и сетевых сегментов, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь сегмента «интернета вещей». **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.
АВЗ.3	Антивирусная проверка сетевого трафика Реализация антивирусной защиты сетевого трафика должна предусматривать: антивирусную проверку файлов, извлекаемых из сетевого трафика; … реагирование по результатам антивирусной проверки файлов, извлекаемых из сетевого трафика, в соответствии с порядком, установленным в эксплуатационной документации. **Интерпретация:** Совместное использование СЗИ класса "диод" - InfoDiode со средствами антивирусной защиты позволяет обеспечить контроль за потоками передачи файлов между сетевыми сегментами и информационными системами, исключая возможность передачи файла без проведения его проверки на антивирусном средстве. Если файл был признан средством антивирусной защиты потенциально опасным, то InfoDiode блокирует передачу такого файла. **Реализация в InfoDiode:** Реализуется за счет политик безопасности передачи данных InfoDiode — передача из публичного сегмента в защищаемый возможна только при условии подтверждения соблюдения всех политик безопасности передачи, включая обязательную проверку на внешнем средстве антивирусной защиты и получения от него вердикта о возможности дальнейшей передаче файла.
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы ... 1) должно обеспечиваться блокирование сетевого трафика или изоляция сегмента, в котором обнаружены компьютерные атаки; **Интерпретация:** СЗИ класса "реле" - InfoRelay - позволяет гарантированно раскоммутировать сетевые сегменты на физическом уровне при выявлении компьютерной атаки по нажатию на кнопку на устройстве или по истечению заданного временного таймера, исключая возможность направить какой-либо физический сигнал по такому каналу связи. **Реализация в InfoRelay:** Реализуется физическим принципом работы аппаратной компоненты InfoRelay — нажатие на кнопку на устройстве приводит к переключению аппаратного реле и физическому «разрыву» со-

Мера	Описание
МСЭ.1	Сегментация сети В информационной системе должна быть реализована сегментация информационной системы. ... При сегментации информационной системы должны обеспечиваться контроль и фильтрация сетевого трафика на границах сегментов. ... Указанные меры защиты информации реализуются за счет применения в информационной системе межсетевых экранов и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также (при необходимости) за счет физической изоляции отдельных сегментов информационной системы, определяемых оператором. **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 серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). В том числе обеспечивается сегментирование информационной (автоматизированной) 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
МСЭ.2	Организация демилитаризованной зоны … Демилитаризованная зона должна быть изолирована от внутренних сегментов информационной системы, обрабатывающих информацию ограниченного доступа, с применением межсетевых экранов и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации. ... **Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной (автоматизированной) системы на физическом уровне, в том числе от демилитаризованной зоны, 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

Мера	Описание
МСЭ.3	Контроль сетевого доступа и фильтрация трафика … Контроль должен осуществляться с применением правил фильтрации трафика, разработанных с учетом актуальных угроз, и (или) с применением средств однонаправленной передачи информации. … **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 серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). При этом InfoDiode позволяет осуществлять передачу данных из доверенного в недоверенные сегменты по строго предопределенному в конфигурации устройства списку сетевых протоколов. **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
МСЭ.4	Маскирование системы Затруднение проведения анализа информационной системы и получения сведений о ее конфигурации и особенностях функционирования внешними нарушителями безопасности информации. … **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

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

Мера	Описание
ЗКС.1	Защита данных при передаче по каналам связи ... В информационной системе должна быть обеспечена защита каналов передачи данных, выходящих за пределы контролируемой зоны, которая включает: контроль всех сетевых взаимодействий на портах и интерфейсах приложений и сетевых сервисов, доступных из сети «Интернет»; формирование и поддержание в актуальном состоянии правил межсетевого экранирования с учетом меры защиты информации МСЭ.3; ограничение доступа пользователей, приложений и сетевых сервисов к неиспользуемым портам, сетевым службам и сервисам; отключение небезопасных версий протоколов и сетевых служб. Реализация указанной меры защиты информации обеспечивается за счет применения межсетевых экранов и (или) многофункциональных межсетевых экранов уровня сети, и (или) средств однонаправленной передачи информации, а также с использованием шифровальных (криптографических) средств защиты информации в соответствии с законодательством Российской Федерации. **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 серверным компонентам, среде виртуализации, коммутационному оборудованию и т.п) из любых внешних сегментов (открытых/недоверенных). При этом InfoDiode позволяет осуществлять передачу данных из доверенного в недоверенные сегменты по строго предопределенному в конфигурации устройства списку сетевых протоколов. **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

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

www.amt.ru
www.infodiode.ru