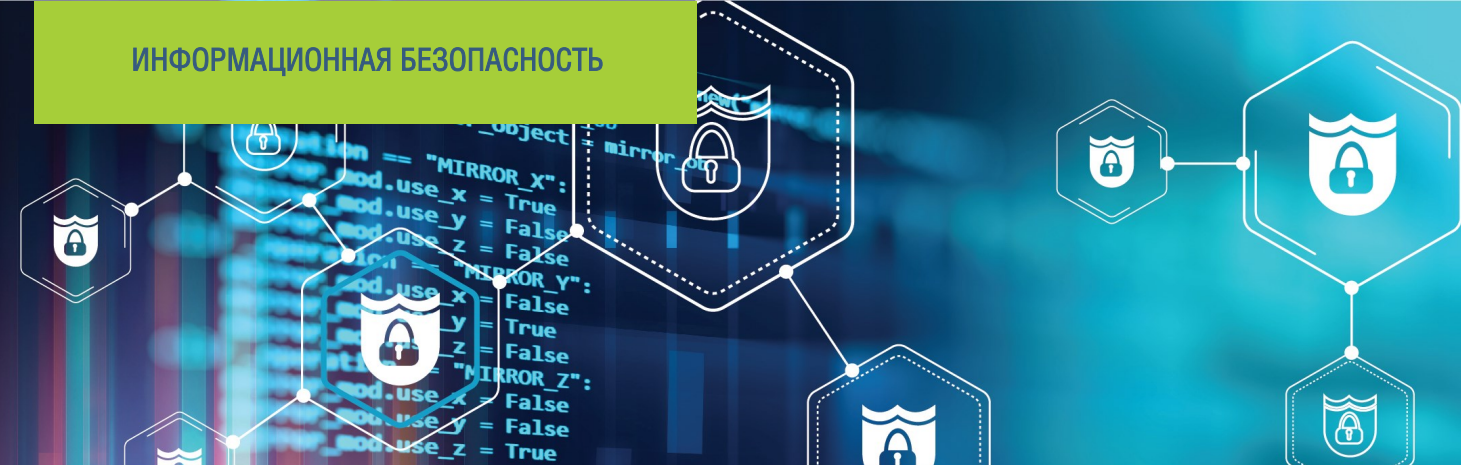




Однонаправленные шлюзы InfoDiode - реализуемые меры ФЗ и приказов ФСТЭК

-InfoDiode

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.

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;

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;	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) недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта;	б) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействие 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) обеспечение функционирования значимого объекта в проектных режимах его работы в условиях воздействия угроз безопасности информации;	в) InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействие 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) обеспечение возможности восстановления функционирования значимого объекта критической информационной инфраструктуры.	г) Решения InfoDiode позволяют создать закрытый контур хранения резервных копий, доступ к которому по двустороннему 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.
...	

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

Интерпретация некоторых норм Приказа ФСТЭК N 17 от 11 февраля 2013 г.

Приказ ФСТЭК N 17 от 11 февраля 2013 г.	Обеспечение
III. Требования к мерам защиты информации, содержащейся в информационной системе. 20.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.	InfoDiode обеспечивает предотвращение удаленных сетевых атак, имеющих целью информационное воздействие на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование информационной системы. В том числе атак, возникающих в ходе взаимодействия с иными информационными системами и информационно-телекоммуникационными сетями. Защита обеспечивается во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты.

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.

Выполнение норм и требований законодательства путем применения СЗИ InfoDiode

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 воздействие 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

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, обрабатываемую 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.

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 при построении надежного хранилища резервных копий, которое будет недоступно для злоумышленников даже при компрометации всей инфраструктуры организации (хранилище «черного дня»), позволяет обеспечить возможность восстановления данных организации в случае их модификации или уничтожения вследствие реализации угроз безопасности информации.

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
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 допускает-	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.

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 на взаимодействующие с сетью "Интернет" интерфейсы и порты, имеющих целью получение несанкционированного доступа к информационным системам.
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.

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 при построении надежного хранилища резервных копий, которое будет недоступно для злоумышленников даже при компрометации всей инфраструктуры организации (хранилище «черного дня»), позволяет обеспечить возможность восстановления 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.

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

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: Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы Интерпретация: СЗИ класса "диод" позволяет реализовать полное соккрытие 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 сегментов 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 сегментов 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 метаданных 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 "диола" 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 сегментов 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 определенных 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 метаданных 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 Histo-riap 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

* Рекомендованная (необязательная) мера приказов

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

Мера	Описание
ОЦЛ.3	Расшифровка: Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций Интерпретация: СЗИ класса "диод" - 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. 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
ОЦЛ4.	Расшифровка: Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) 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, в том числе передачу спам сообщений, документов, писем и т.п. 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