



## 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 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
<p>Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры.</p> <p>Принципами обеспечения безопасности критической информационной инфраструктуры являются:</p> <ol style="list-style-type: none"><li>1) законность;</li><li>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;</li><li>3) приоритет предотвращения компьютерных атак.</li></ol>	<ol style="list-style-type: none"><li>1) Решения InfoDiode являются сертифицированными решениями ФСТЭК УД (4), что позволяет применять их для защиты КИИ вплоть до 1 категории;</li><li>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;</li><li>3) InfoDiode обеспечивает предотвращение удаленных сетевых атак во всех случаях, когда такая атака осуществляется. Функция безопасности обеспечивается физической изоляцией объекта защиты.</li></ol>
<p>Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры.</p> <p>2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:</p> <ol style="list-style-type: none"><li>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;</li><li>2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;</li></ol> <p>...</p>	<ol style="list-style-type: none"><li>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;</li><li>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;</li></ol>

# 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.	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;
16. Задачами обеспечения безопасности значимого объекта являются:	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;
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;	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;
б) недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта;	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.
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.	
...	

## 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
<p>III. Требования к мерам защиты информации, содержащейся в информационной системе.</p> <p>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.</p>	<p>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.</p>

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

Приказ ФСТЭК N 21 от 13 февраля 2013 г.	Обеспечение
<p>II. Состав и содержание мер по обеспечению безопасности персональных данных</p> <p>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.</p>	<p>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.</p>



## 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
<p>Внедрение системы защиты автоматизированной системы управления и ввод ее в действие.</p> <p>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.</p>	<p>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 программными средствами.</p>

## 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	<p><b>Расшифровка:</b> Защита периметра информационной (автоматизированной) системы</p> <p><b>Интерпретация:</b> 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)</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.3	<p><b>Расшифровка:</b> Эшелонированная защита информационной (автоматизированной) системы</p> <p><b>Интерпретация:</b> 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.4	<p><b>Расшифровка:</b> Сегментирование информационной (автоматизированной) системы</p> <p><b>Интерпретация:</b> 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>

Мера	Описание
ЗИС.6	<p><b>Расшифровка:</b> Управление сетевыми потоками</p> <p><b>Интерпретация:</b> 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)</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.8	<p><b>Расшифровка:</b> Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы</p> <p><b>Интерпретация:</b> 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 "диоода"</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.18	<p><b>Расшифровка:</b> Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию*</p> <p><b>Интерпретация:</b> 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>

\* 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 метаинформации о передаваемом трафике в отдельный источник DLP в целях фиксации фактов несанкционированной передачи информации

**Реализация в составе решения InfoDiode:** Реализуется настройками доступа к сервисам строго из определенных подсетей. Реализуется самим физическим принципом работы аппаратной компоненты InfoDiode и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети, в том числе SPAN трафика

---

**ЗИС.34 Расшифровка:** Защита от угроз отказа в обслуживании (DOS, DDOS-атак)

**Интерпретация:** СЗИ класса "диод" - InfoDiode - обеспечивает полную изоляцию периметра информационной (автоматизированной) системы на физическом уровне, исключая возможность направить какой-либо физический сигнал по каналу связи внутрь (к серверной компоненте, среде виртуализации, коммутационному оборудованию и т.п) из открытого/недоверенного сегмента. В том числе обеспечивается невозможность преодоления физической компоненты для организации DOS, DDOS атак на доверенный сегмент с информационной (автоматизированной) системой

**Реализация в составе решения InfoDiode:** Реализуется физическим принципом работы аппаратной компоненты InfoDiode (физический сигнал - свет - направляется только в одну сторону - из источника к приемнику) и возможностью передачи строго определенных протоколов из доверенного в недоверенный сегмент сети

---

**ЗИС.35 Расшифровка:** Управление сетевыми соединениями

**Интерпретация:** СЗИ класса "диод" обеспечивает организацию подключений из доверенного сегмента в IN части "диода" только по определенным IP адресам и портам, исключая возможность какого-либо прямого соединения с недоверенным сегментом, а также обхода каких-либо программно реализуемых правил межсетевого экранирования. СЗИ класса "диод" исключает возможность установления соединения с доверенным сегментом из недоверенного сегмента на физическом уровне

**Реализация в составе решения InfoDiode:** Реализуется путем формирования правил подключения к InfoDiode только с определенных IP адресов и только с учетом пройденных процедур авторизации и аутентификации, а также с учетом определенных портов доступа. Наличие аппаратной компоненты полностью исключает возможность прямого подключения к внешним информационным ресурсам

Мера	Описание
ЗИС.16	<p><b>Расшифровка:</b> Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов*</p> <p><b>Интерпретация:</b> 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 метаинформации о передаваемом трафике в отдельный источник DLP в целях фиксации фактов несанкционированной передачи информации</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.17	<p><b>Расшифровка:</b> Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы</p> <p><b>Интерпретация:</b> 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-gram 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>

\* Рекомендованная (необязательная) мера приказов

Мера	Описание
ЗИС.22	<p><b>Расшифровка:</b> Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы</p> <p><b>Интерпретация:</b> 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ЗИС.23	<p><b>Расшифровка:</b> Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями</p> <p><b>Интерпретация:</b> 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)</p> <p><b>Реализация в InfoDiode:</b> 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</p>
УПД.3	<p><b>Расшифровка:</b> Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами</p> <p><b>Интерпретация:</b> 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</p> <p><b>Реализация в InfoDiode:</b> 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</p>

Мера	Описание
ОЦЛ.3	<p><b>Расшифровка:</b> Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций</p> <p><b>Интерпретация:</b> 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.</p> <p><b>Реализация в InfoDiode:</b> 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</p>
ОЦЛ4.	<p><b>Расшифровка:</b> 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)</p> <p><b>Интерпретация:</b> 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.</p> <p><b>Реализация в InfoDiode:</b> 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</p>