



## Нейтрализация угроз безопасности информации БДУ ФСТЭК с использованием решений линейки InfoDiode



В сложившейся на сегодняшний день ситуации, когда ежедневно осуществляются сотни атак на российские (и не только российские) организации различных секторов экономики, задача обеспечения безопасности собственной инфраструктуры остаётся одной из наиболее сложных и важных. Современные атаки на организации имеют целенаправленный и многоступенчатый характер, и в случае их успеха приводят к критическим последствиям: остановке деятельности организации, утечке конфиденциальных данных, значительным финансовым потерям, а в ряде случаев и к техногенным катастрофам.

Поэтому при проектировании информационных систем одним из важнейших этапов является моделирование актуальных угроз, которым подвержена разрабатываемая система. Целью моделирования угроз является определение угроз безопасности, на основании которых осуществляется внедрение мер защиты информации для информационных систем. Модель угроз дает возможность осознанно подойти к построению системы обеспечения информационной безопасности организации и обоснованно выбрать СЗИ, которые позволяют минимизировать вероятность реализации угроз.

В настоящем документе представлен анализ угроз безопасности, приведенных в Банке данных угроз безопасности информации ФСТЭК России, для нейтрализации которых могут эффективно применяться решения на основе однонаправленных шлюзов **InfoDiode**.

**InfoDiode** - продукт для однонаправленной передачи данных, позволяющий обеспечивать эффективную защиту критичных сегментов сети. Технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого («воздушный зазор»), обеспечивают возможность передачи данных между сегментами разной критичности и исключают возможность организации обратного (в том числе двунаправленного) соединения на физическом уровне. Такой подход позволяет нейтрализовать ряд наиболее часто эксплуатируемых угроз безопасности, связанных с сетевым взаимодействием, и ограничить возможности злоумышленника при планировании внешних информационных атак.

## Условные обозначения

В таблицах ниже используются следующие обозначения размещения InfoDiode в инфраструктуре организации:

**ДС ► | НС** — InfoDiode направлен из более доверенного сегмента в менее доверенный сегмент, передача данных из менее доверенного сегмента в более доверенный физически невозможна.

**ДС | ◀ НС** — InfoDiode направлен из менее доверенного сегмента в более доверенный сегмент, передача данных из более доверенного сегмента в менее доверенный физически невозможна.

**ДС | ◀ ► | НС** — Использование двух разнонаправленных InfoDiode — из менее доверенного в более доверенный и из более доверенного в менее доверенный, возможна двунаправленная передача данных.

Также используется следующая статусная модель, обозначающая возможность нейтрализации угроз безопасности информации при условии размещения InfoDiode в инфраструктуре организации указанным способом:

**Нейтрализация угрозы** — угроза полностью нейтрализуется.

**Нейтрализация удаленного вектора** — InfoDiode полностью нейтрализует удаленный (дистанционный) вектор реализации данной угрозы. Обозначение используется в том случае, когда при формулировании угрозы явно указан также локальный вектор атаки.

**Нейтрализация угрозы при совместном использовании с СЗИ** — InfoDiode нейтрализует данную угрозу при условии его работы в связке с другими СЗИ (антивирус, DLP или другим).

**Нейтрализация угрозы при условии нескомпрометированного СЗИ** — InfoDiode нейтрализует данную угрозу при условии, что компоненты InfoDiode, размещаемые в менее доверенном сегменте, не будут скомпрометированы злоумышленником.

**Не относится к функции безопасности** — Нейтрализация данной угрозы безопасности не является функцией безопасности InfoDiode.

**Неприменимо** — Использование InfoDiode нецелесообразно в связи с необходимостью поддержки двунаправленного канала связи или по иным причинам.



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

В настоящем разделе приведены угрозы, нейтрализуемые однонаправленными шлюзами линейки **InfoDiode**: **АПК InfoDiode PRO**, предназначенным для передачи файловых потоков, и **АПК InfoDiode SMART**, предназначенным для передачи промышленных протоколов и реплик SCADA систем. Указанные модели **InfoDiode** приведены в качестве примера, для большей наглядности особенностей нейтрализации угрозы, однако нейтрализация угроз аналогичным образом выполняется и решениями **АК InfoDiode**.

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►   НС	Infodiode ДС   ◀ НС	Infodiode ДС   ◀ ►   НС
УБИ.006	Угроза внедрения кода или данных			
УБИ.170	Угроза неправомерного шифрования информации			
УБИ.188	Угроза подмены программного обеспечения	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники			

Одним из этапов атак на организации является внедрение и исполнение вредоносного программного обеспечения в информационную систему. В качестве вредоносного программного обеспечения обычно выступают различные инструменты, необходимые злоумышленнику для дальнейших действий: программы для удаленного управления системой, для эксплуатации уязвимостей системы, для шифрования данных, для майнинга криптовалюты и т.д.

Внедрение вредоносного кода может быть реализовано как локально, так и дистанционно путем направления вредоносного кода по сети и его удаленный запуск в системе. Также при реализации данной угрозы может быть использована социальная инженерия, благодаря которой легитимный сотрудник, введенный в заблуждение, может осуществить запуск вредоносного кода.

Для нейтрализации таких угроз необходимо использование СЗИ, не допускающего передачу вредоносного кода в информационную систему.

InfoDiode позволяет гарантированно отделить защищаемый сетевой сегмент от других сегментов и обеспечить невозможность передачи вредоносного программного обеспечения в информационную систему.



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.171 Угроза скрытого включения вычислительного устройства в состав бот-сети	<p>Одним из возможных вариантов внедряемого вредоносного кода является программное обеспечение, обеспечивающее включение информационной системы в ботнет и дальнейшее его использование для атак типа «отказ в обслуживании» или источника других вредоносных рассылок.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, не допускающего передачу вредоносного кода в информационную систему.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов удаленного управления гарантирует невозможность использования информационной системы в качестве одного из узлов ботнета.</p>	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы
УБИ.172 Угроза распространения «почтовых червей»	<p>Опасность «почтовых червей» заключается в их скрытном распространении при получении пользователями электронных писем, содержащих вредоносный код. И каждый скомпрометированный узел становится новым центром рассылки зараженных писем.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, не допускающего передачу вредоносного кода в информационную систему.</p> <p>InfoDiode позволяет гарантированно отделить защищаемый сетевой сегмент от других сегментов и обеспечить невозможность распространения «почтовых червей» внутрь защищаемого сетевого сегмента.</p>	Нейтрализация угрозы	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.175 Угроза «фишинга»	<p>«Фишинговые» рассылки являются одним из самых распространенных векторов атаки на организации. Недостаточный уровень осведомленности сотрудников, которые подвергаются социальной инженерии, позволяет злоумышленнику заставить их перейти по вредоносной ссылке и скачать вредоносное программное обеспечение или ввести свои учетные данные.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, не допускающего возможности перехода на «фишинговые» ресурсы.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двусторонних протоколов гарантирует невозможность перехода на «фишинговые» ресурсы.</p>	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб			
УБИ.099	Угроза обнаружения хостов			
УБИ.104	Угроза определения топологии вычислительной сети	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL			
УБИ.103	Угроза определения типов объектов защиты			
УБИ.132	Угроза получения предварительной информации об объекте защиты	Не относится к функции безопасности	Нейтрализация удаленного вектора	Не относится к функции безопасности
УБИ.218	Угроза раскрытия информации о модели машинного обучения			

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.009 Угроза восстановления предыдущей уязвимой версии BIOS	Несанкционированное использование функциональности BIOS/UEFI может быть реализовано как локально, так и удаленно с использованием протоколов iKVM или IPMI. Это позволяет злоумышленнику, не имея физического доступа к информационной системе, осуществлять различные несанкционированные манипуляции с BIOS/UEFI: использование стандартного функционала для нарушения работы информационной системы; восстановление уязвимой версии для её эксплуатации и развития атаки; сброс и замена пароля к BIOS/UEFI и т.д.			
УБИ.013 Угроза деструктивного использования декларированного функционала BIOS	Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее ограничить удаленный доступ к BIOS/UEFI.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.024 Угроза изменения режимов работы аппаратных элементов компьютера	InfoDiode позволяет гарантированно отделить сетевой сегмент с информационной системой от всех других сегментов и обеспечить невозможность воздействия на BIOS/UEFI с использованием протоколов iKVM или IPMI.			
УБИ.045 Угроза нарушения изоляции среды исполнения BIOS	Несанкционированное использование функциональности BIOS/UEFI может быть реализовано как локально, так и удаленно с использованием протоколов iKVM или IPMI. Это позволяет злоумышленнику, не имея физического доступа к информационной системе, осуществлять атаки перебором «грубой силой» пароля BIOS/UEFI для получения НСД к информационной системе и дальнейшего развития атаки.			
УБИ.144 Угроза программного сброса пароля BIOS	Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе.	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы
УБИ.123 Угроза подбора пароля BIOS	InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность перебора паролей информационной системы, в том числе при работе с BIOS/UEFI по протоколам iKVM или IPMI.			



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети			
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети			
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети			
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети			
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам			
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации			

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.088	Угроза несанкционированного копирования защищаемой информации			
УБИ.111	Угроза передачи данных по скрытым каналам			
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Не относится к функции безопасности	Нейтрализация удаленного вектора	Не относится к функции безопасности
УБИ.219	Угроза хищения обучающих данных			
УБИ.091	Угроза несанкционированного удаления защищаемой информации			
УБИ.179	Угроза несанкционированной модификации защищаемой информации			
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.222	Угроза подмены модели машинного обучения			



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения	Получение злоумышленником возможности удаленно передавать несанкционированные команды в информационную систему может привести к тяжелым последствиям для организации: команда, изменяющая режим работы оборудования на производстве, может привести к порче выпускаемой продукции или самого оборудования, а перезагрузка или отключение контрольных датчиков, например, на энергостанции — к техногенной катастрофе.			
УБИ.107 Угроза отключения контрольных датчиков	Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд в информационные системы.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной передачи команд в защищаемый сетевой сегмент, защищая информационные системы от внешнего влияния.			
УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами	Удаленный перехват управления информационной системой или автоматизированной системой управления технологическими процессами возможен в случае компрометации злоумышленником самой системы или же системы централизованного управления объектом. Это возможно как путем получения несанкционированного доступа, так и путем направления или модификации команд, направляемых в информационную систему.			
УБИ.212 Угроза перехвата управления информационной системой	Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированного доступа и направления команд в информационную систему.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
	InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированного доступа и направления команд в информационную систему, что защищает информационные системы или автоматизированные системы управления технологическими процессами от перехвата управления злоумышленником.			

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.007 Угроза воздействия на программы с высокими привилегиями	<p>После получения первоначального доступа к инфраструктуре организации злоумышленникам необходимо обеспечить возможность выполнения различных команд для дальнейшего развития атаки. При этом для выполнения многих команд им необходимо получить полномочия учетной записи администратора системы. Одним из способов их выполнения может быть использование программ, обладающих высокими привилегиями, или же функциями BIOS/UEFI.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.087 Угроза несанкционированного использования привилегированных функций BIOS	<p>Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд в информационные системы.</p> <p>InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной передачи команд в защищаемый сетевой сегмент, защищая информационные системы от внешнего влияния.</p>			
УБИ.122 Угроза повышения привилегий	<p>После получения первоначального доступа к инфраструктуре организации злоумышленникам необходимо обеспечить возможность выполнения различных команд для дальнейшего развития атаки. При этом для выполнения многих команд им необходимо получить полномочия учетной записи администратора системы. Одним из способов их выполнения может быть эксплуатация уязвимостей системы или программного обеспечения, чтобы получить возможность выполнения команд с полномочиями администратора.</p> <p>Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированного доступа к информационной системе.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность удаленного несанкционированного доступа к инфраструктуре организации, защищая компоненты информационных системы от эксплуатации их уязвимостей.</p>	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация угрозы при условии нескомпрометированного СЗИ

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.143	<p>Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации</p> <p>Одним из направлений атак на организацию может быть приведение информационных систем и ресурсов организации в состояние «отказ в обслуживании». Классические атаки типа «отказ в обслуживании» основываются на одном из двух принципов: либо на исчерпании возможностей системы из-за превышения допустимой нагрузки на нее, либо путем эксплуатации уязвимостей, направленных на исчерпание системных ресурсов.</p>			
УБИ.153	<p>Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов</p> <p>Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее ограничивать нагрузку, а также возможности по эксплуатации уязвимостей системы.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.155	<p>Угроза утраты вычислительных ресурсов</p> <p>InfoDiode за счет однонаправленности передачи данных гарантирует невозможность передачи сетевых запросов к информационной системе, а также обеспечивает защиту от удаленной эксплуатации уязвимостей, которые могут привести систему в состояние «отказ в обслуживании».</p>			
УБИ.109	<p>Угроза перебора всех настроек и параметров приложения</p> <p>Злоумышленник может организовать перебор всех возможных настроек и параметров информационной системы, чтобы подобрать наиболее уязвимую конфигурацию, которая позволит ему в развитии атаки, или же приведет систему в состояние «отказ в обслуживании». Такая атака может строиться как путем прямого несанкционированного доступа к системе, так и путем направления конфигурационных файлов для их применения в системе.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе, а также передачу конфигурационных файлов.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность перебора настроек и параметров системы как путем несанкционированного доступа, так и путем направления измененной конфигурации в информационную систему.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными	<p>Протоколы сетевого обмена, так же как любая информационная система, имеют слабости и уязвимости. Злоумышленники часто используют такие слабости для получения несанкционированного доступа к системам организации или данным, передаваемым по этим протоколам.</p> <p>Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль, ограничение и защиту используемых сетевых протоколов и передаваемых пакетов.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов позволяет гарантированно отделить сетевой сегмент с информационной системой от всех других сегментов и обеспечить невозможность использования слабостей сетевых протоколов злоумышленником для целей получения несанкционированного доступа к системам, находящимся в защищаемом сегменте.</p>	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация угрозы при условии нескомпрометированного СЗИ
УБИ.178 Угроза несанкционированного использования системных и сетевых утилит	<p>Современные информационные системы имеют большое количество различных системных и сетевых утилит, которые необходимы для поддержания их работы. Такие утилиты часто могут использоваться злоумышленниками для получения несанкционированного доступа к системам организации или дальнейшего развития атаки.</p> <p>Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль и ограничение используемых сетевых протоколов и передаваемых пакетов.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов позволяет гарантированно отделить сетевой сегмент с информационной системой от всех других сегментов и обеспечить невозможность использования злоумышленником системных и сетевых утилит для целей получения несанкционированного доступа к системам, находящимся в защищаемом сегменте.</p>	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.124 подделки журнала событий	<p>Угроза записей регистрации</p> <p>На этапе сокрытия следов своей деятельности злоумышленнику необходимо уничтожить или изменить журналы событий, чтобы затруднить дальнейшее расследование инцидента. Одним из способов обеспечения безопасности журналов событий является их репликация в единое защищенное хранилище. При этом злоумышленник также может получить доступ к такому хранилищу и модифицировать журналы событий.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, позволяющего обеспечить невозможность удаленного доступа к хранилищу.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов позволяет гарантированно отделить сетевой сегмент с хранилищем журналов событий от всех других сегментов и обеспечить невозможность модификации или уничтожения злоумышленником содержимого хранилища.</p>	Неприменимо	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.033 использования входных данных	<p>Угроза слабостей кодирования</p> <p>Если в информационной системе, имеющей внешние интерфейсы, не осуществляется контроль за входящими данными, злоумышленник может направлять различные данные, содержащие опасные паттерны кода, служебные символы и т.д., на вход системы с целью вывести систему из штатного состояния, эксплуатации уязвимостей или «отказа в обслуживании».</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, позволяющего ограничивать несанкционированные запросы к информационной системе.</p> <p>InfoDiode за счет однонаправленности передачи данных гарантирует невозможность направления запросов к информационной системе из-за пределов защищаемого сегмента, благодаря чему нейтрализует вектор атаки на информационную систему, связанный со слабым контролем входных данных.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.012 Угроза деструктивного изменения конфигурации/ среды окружения программ	<p>Получение злоумышленником возможности изменять конфигурацию информационных систем может привести к некорректной работе или полной приостановке технологических процессов организации. Изменение конфигурации системы может быть реализовано как локально, так и дистанционно путем направления несанкционированных команд в систему или внедрению вредоносного кода.</p> <p>Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд и потенциально опасного программного обеспечения в информационные системы.</p> <p>InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной удаленной передачи команд и потенциально опасного программного обеспечения в сетевой сегмент, защищая находящиеся в нем информационные системы от внешнего влияния.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации	<p>Получение злоумышленником возможности изменять конфигурацию средств защиты информации ставит под угрозу безопасность всей организации, и позволяет злоумышленнику свободно перемещаться между информационными системами, компрометируя их и продвигаясь к своей конечной цели.</p> <p>InfoDiode за счет физической однонаправленности передачи данных даже в случае компрометации сервера, принимающего данные, гарантирует выполнение своей функции безопасности и не позволяет злоумышленнику получить доступ к защищаемому сегменту.</p>	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора



## Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ► I HC	Infodiode ДС I ◀ HC	Infodiode ДС I ◀► I HC
УБИ.030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию	<p>Одной из частых ошибок конфигурации информационных систем является использование учётных записей «по умолчанию», предназначенных для первичного входа в систему. Информация о таких учетных записях размещена в сети Интернет, что облегчает злоумышленникам проведение атаки на организацию.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность проведения аутентификации в информационной системе, что защищает организацию от удаленного ввода учетных данных «по умолчанию» и перебора логинов и паролей.</p>	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.197 Угроза хищения аутентификационной информации из временных файлов cookie	<p>Хищение временных файлов cookie является одним из способов получения несанкционированного доступа к информационным системам за счет перехвата сессии или получения из них авторизационных данных или токенов доступа. Основным способ их похищения — вредоносные программы, которые передают cookie злоумышленникам через открытый RDP-порт.</p> <p>Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированную передачу данных по RDP-порту информационной системы.</p> <p>InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность соединения по протоколу RDP, что обеспечивает защиту временных файлов cookie от хищения и передачи злоумышленнику.</p>	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы