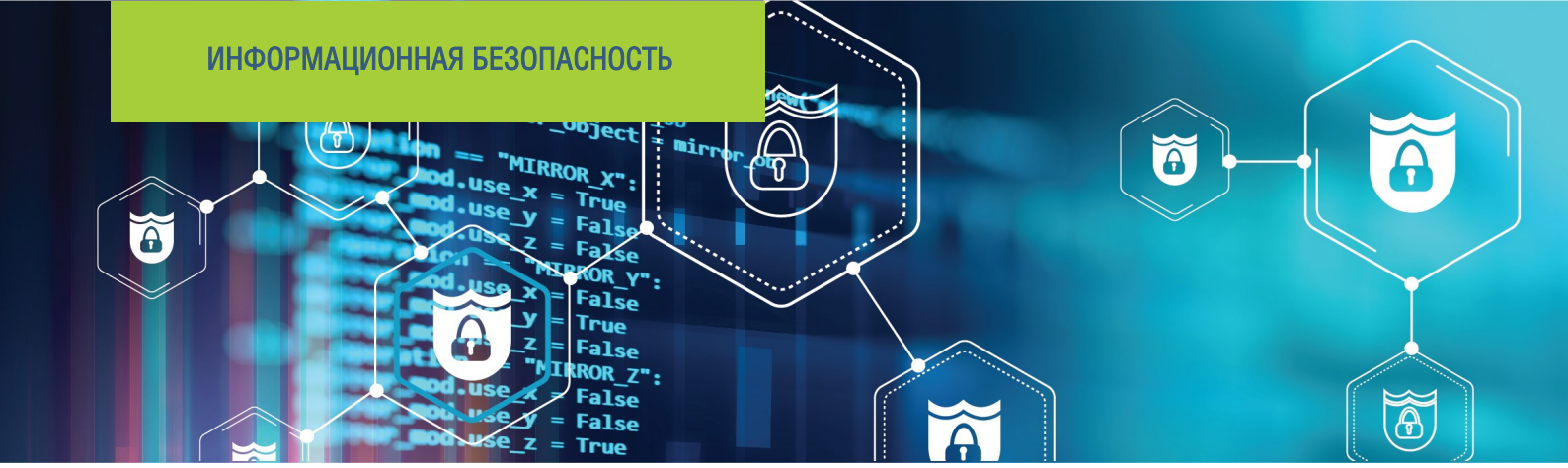

Нейтрализация угроз безопасности информации БДУ ФСТЭК с использованием решений InfoDiode

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.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Условные обозначения

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

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

ДС I◄ НС — InfoDiode направлен из менее доверенного сегмента в более доверенный сегмент, передача данных из более доверенного сегмента в менее доверенный физически невозможна.

ДС I◄►I 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.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

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 ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.006 Угроза внедрения кода или данных УБИ.170 Угроза неправомерного шифрования информации УБИ.188 Угроза подмены программного обеспечения 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 удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.171 Угроза скрытного включения вычислительного устройства в состав бот-сети	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. Для нейтрализации угрозы необходимо использование СЗИ, не допускающего передачу вредоносного кода в информационную систему. InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов удаленного управления гарантирует невозможность использования информационной системы в качестве одного из узлов ботнета.	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы
УБИ.172 Угроза распространения «почтовых червей»	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. Для нейтрализации угрозы необходимо использование СЗИ, не допускающего передачу вредоносного кода в информационную систему. InfoDiode позволяет гарантированно отделить защищаемый сетевой сегмент от других сегментов и обеспечить невозможность распространения «почтовых червей» внутрь защищаемого сетевого сегмента.	Нейтрализация угрозы	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.175 Угроза «фишинга»	«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. Для нейтрализации угрозы необходимо использование СЗИ, не допускающего возможности перехода на «фишинговые» ресурсы. InfoDiode за счет однонаправленности передачи данных и разрыва двусторонних протоколов гарантирует невозможность перехода на «фишинговые» ресурсы.	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
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 УБИ.151 Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Сбор информации о системах и сетях является важным этапом при планировании атаки на организацию. Злоумышленники стремятся получить любую техническую информацию, которая может оказаться полезной для реализации атаки. Одним из этапов сбора информации является автоматизированное сканирование сети организации, которое позволяет получить сведения о топологии сети, её узлах, открытых портах и сетевых службах и т.д. Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль и ограничение используемых сетевых протоколов и передаваемых пакетов. InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность получения злоумышленником какой-либо информации о защищенном сетевом сегменте и информационных системах, размещенных в нем: топологии сегмента, адресации информационных систем, аппаратном и программном обеспечении, открытых портах, сетевых службах, уязвимостях и т.д., то есть полностью нейтрализует класс угроз, связанный со сбором информации путем сканирования сетевого сегмента.	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы
УБИ.103 Угроза определения типов объектов защиты УБИ.132 Угроза получения предварительной информации об объекте защиты УБИ.218 Угроза раскрытия информации о модели машинного обучения	Сбор информации о системах и сетях является важным этапом при планировании атаки на организацию. Злоумышленники стремятся получить любую техническую информацию, которая может оказаться полезной для реализации атаки. Одним из возможных векторов сбора информации является перехват исходящих из информационной системы или сетевого сегмента данных и их анализ с целью получения сведений о системах, используемом аппаратном и программном обеспечении, алгоритмах обработки данных и т.д. Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль и ограничение используемых сетевых протоколов и передаваемых пакетов. InfoDiode позволяет гарантированно отделить сетевой сегмент с информационной системой от всех других сегментов и обеспечить невозможность получения каких-либо данных информационной системы за границами этого сегмента.	Не относится к функции безопасности	Нейтрализация удаленного вектора	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.009 Угроза восстановления предыдущей уязвимой версии BIOS УБИ.013 Угроза деструктивного использования декларированного функционала BIOS УБИ.024 Угроза изменения режимов работы аппаратных элементов компьютера УБИ.045 Угроза нарушения изоляции среды исполнения BIOS УБИ.144 Угроза программного сброса пароля 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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее ограничить удаленный доступ к BIOS/UEFI. 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.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.123 Угроза подбора пароля 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. Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе. 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 угрозы	Нейтрализация угрозы	Нейтрализация угрозы

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
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 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	Получение несанкционированного удаленного доступа к различным узлам инфраструктуры является первичной целью злоумышленника при атаке на организацию. Это необходимо, чтобы впоследствии использовать данный узел инфраструктуры организации как плацдарм для закрепления в инфраструктуре и дальнейших действий по достижению конечной цели. В качестве целей для несанкционированного доступа могут выступать информационные системы, сетевое оборудование, гипервизоры или виртуальные машины, хранилища данных, средства защиты информации и т.д. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить контроль и ограничение удаленного подключения к элементам инфраструктуры организации. InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность удаленного несанкционированного доступа к инфраструктуре организации.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
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 УБИ.219 Угроза хищения обучающих данных	Одной из конечных целей злоумышленника может являться получение доступа к защищаемой информации организации. Это могут быть персональные данные клиентов или сотрудников, коммерческая или иные виды тайн, установленных законодательством, критичные финансовые сведения, информация о контрагентах и т.д. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить ограничение передачи данных за пределы контура безопасности. InfoDiode за счет однонаправленности передачи данных гарантирует невозможность хищения данных из контура безопасности, в том числе при использовании методов шифрования или стеганографии при их передаче.	Не относится к функции безопасности	Нейтрализация удаленного вектора	Не относится к функции безопасности
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 УБИ.222 Угроза подмены модели машинного обучения	Одной из конечных целей злоумышленника может являться получение доступа к защищаемой информации организации и её модификация или уничтожение. Это могут быть персональные данные клиентов или сотрудников, номера счетов клиентов, сотрудников или контрагентов, технологические и интеллектуальные разработки организации и т.д. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи данных или команд на их изменение в системы хранения и обработки таких данных. InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной передачи данных или команд на их изменение в защищаемый сетевой сегмент.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.107 Угроза отключения контрольных датчиков УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд в информационные системы. InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной передачи команд в защищаемый сетевой сегмент, защищая информационные системы от внешнего влияния.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.212 Угроза перехвата управления информационной системой	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированного доступа и направления команд в информационную систему. 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 удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.007 Угроза воздействия на программы с высокими привилегиями УБИ.087 Угроза несанкционированного использования привилегированных функций BIOS	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд в информационные системы. InfoDiode за счет однонаправленности передачи данных гарантирует невозможность несанкционированной передачи команд в защищаемый сетевой сегмент, защищая информационные системы от внешнего влияния.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.122 Угроза повышения привилегий	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированного доступа к информационной системе. InfoDiode за счет однонаправленности передачи данных и разрыва двунаправленных протоколов гарантирует невозможность удаленного несанкционированного доступа к инфраструктуре организации, защищая компоненты информационные системы от эксплуатации их уязвимостей.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация угрозы при условии нескомпрометированного СЗИ

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов УБИ.155 Угроза утраты вычислительных ресурсов	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее ограничивать нагрузку, а также возможности по эксплуатации уязвимостей системы. 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».	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.109 Угроза перебора всех настроек и параметров приложения	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. Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе, а также передачу конфигурационных файлов. 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.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными	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. Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль, ограничение и защиту используемых сетевых протоколов и передаваемых пакетов. 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.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация угрозы при условии нескомпрометированного СЗИ
УБИ.178 Угроза несанкционированного использования системных и сетевых утилит	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. Для нейтрализации таких угроз необходимо использование СЗИ, позволяющего обеспечить контроль и ограничение используемых сетевых протоколов и передаваемых пакетов. 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.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.124 Угроза подделки записей журнала регистрации событий	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. Для нейтрализации угрозы необходимо использование СЗИ, позволяющего обеспечить невозможность удаленного доступа к хранилищу. 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.	Неприменимо	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.033 Угроза использования слабостей кодирования входных данных	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». Для нейтрализации угрозы необходимо использование СЗИ, позволяющего ограничивать несанкционированные запросы к информационной системе. 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.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.012 Угроза деструктивного изменения конфигурации/ среды окружения программ	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. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее обеспечить невозможность несанкционированной передачи команд и потенциально опасного программного обеспечения в информационные системы. 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.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации	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. 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.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием однонаправленного шлюза InfoDiode

УБИ	Интерпретация УБИ и подход к нейтрализации	Infodiode ДС ►I НС	Infodiode ДС I◄ НС	Infodiode ДС I◄►I НС
УБИ.030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию	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. Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированные подключения к информационной системе. 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.	Нейтрализация удаленного вектора	Не относится к функции безопасности	Не относится к функции безопасности
УБИ.197 Угроза хищения аутентификационной информации из временных файлов cookie	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. Основной способ их похищения — вредоносные программы, которые передают cookie злоумышленникам через открытый RDP-порт. Для нейтрализации угрозы необходимо использование СЗИ, позволяющего контролировать несанкционированную передачу данных по RDP-порту информационной системы. 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.	Нейтрализация угрозы	Нейтрализация угрозы	Нейтрализация угрозы

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

МДР InfoDiode расширяет возможности шлюза однонаправленной передачи данных **InfoDiode** в части контроля и своевременной приостановки передачи данных при нарушении заданных политик безопасности и обмена данными между сетевыми сегментами (доменами) с разным уровнем критичности обрабатываемой информации. Применение **МДР InfoDiode** полностью сохраняет функции безопасности однонаправленных шлюзов **InfoDiode** (нейтрализацию угроз - см. предыдущий раздел брошюры) и дополнительно расширяет перечень нейтрализуемых угроз. Расширение перечня обеспечивается за счет нейтрализации тех угроз, которых не нейтрализуются **InfoDiode** при указанном ранее размещении, а также за счет новых угроз, нейтрализуемых именно МДР **InfoDiode** (такие новые выделены **жирным** в таблицах настоящего раздела). В настоящем разделе приведены угрозы, нейтрализуемые **МДР InfoDiode PRO,** которое реализовано на базе АПК InfoDiode PRO, **и МДР InfoDiode SMART**, реализованное на АПК InfoDiode SMART.

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.006 Угроза внедрения кода или данных УБИ.170 Угроза неправомерного шифрования информации УБИ.208 Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	МДР InfoDiode PRO расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозы удаленного внедрения и исполнения вредоносного программного обеспечения в информационной системе при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode PRO при получении файла (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) передает его в интегрированные с ним антивирусные системы или песочницу, и дальнейшая передача в целевую систему осуществляется только при условии успешной проверки сторонним СЗИ. Такой подход позволяет ограничивать передачу любых зараженных файлов в информационные системы защищаемого сегмента.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора при совместном использовании с антивирусом или песочницей	Нейтрализация удаленного вектора при совместном использовании с антивирусом или песочницей
УБИ.172 Угроза распространения «почтовых червей»	МДР InfoDiode PRO расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу распространения «почтовых червей» при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode PRO при получении почтового сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) передает его в интегрированные с ним антивирусные системы или песочницу, и дальнейшая передача в целевую систему осуществляется только при условии успешной проверки сторонним СЗИ. Такой подход позволяет ограничивать передачу любых зараженных почтовых сообщений в информационные системы защищаемого сегмента.	Нейтрализация угрозы	Нейтрализация угрозы при совместном использовании с антивирусом или песочницей	Нейтрализация угрозы при совместном использовании с антивирусом или песочницей

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.188 Угроза подмены программного обеспечения **УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения** **УБИ.217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения**	Одним из распространённых векторов атак на организации является компрометация поставщиков программного обеспечения, подрядчиков организации или других участников цепочки поставок программного обеспечения. Внесение в дистрибутивы программного обеспечения вредоносного кода или различных «бэкдоров» значительно облегчает для злоумышленников дальнейшую атаку на организацию. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющего обеспечить проверку всех поставляемых в организацию дистрибутивов на наличие вирусного кода или недекларированной функциональности. МДР InfoDiode PRO при получении дистрибутива программного обеспечения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) передает его в интегрированную с ним песочницу, и дальнейшая передача в целевую систему осуществляется только при условии успешной проверке сторонним СЗИ. Такой подход позволяет ограничивать передачу дистрибутивов в защищаемый сегмент, если они не прошли проверки статического, динамического и поведенческого анализа в песочнице, что обеспечивает надежную защиту от компрометации дистрибутивов или поставщиков/подрядчиков организации.	Неприменимо	Нейтрализация удаленного вектора при совместном использовании с песочницей	Нейтрализация удаленного вектора при совместном использовании с песочницей
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 УБИ.219 Угроза хищения обучающих данных	МДР InfoDiode PRO расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозы утечек защищаемой информации из информационной системы при использовании InfoDiode, направленного из более доверенного сегмента в менее доверенные. МДР InfoDiode PRO при получении файла (как на сервер, находящийся в более доверенном сегменте, так и на находящийся в менее доверенном) передает его в интегрированные с ним системы предотвращения утечек (DLP), и дальнейшая передача в целевую систему осуществляется только при условии успешной проверке сторонним СЗИ. Такой подход позволяет ограничивать передачу файлов, содержащих защищаемую информацию, из доверенного сетевого сегмента, что обеспечивает надежную защиту от утечек данных.	Нейтрализация удаленного вектора при совместном использовании с DLP	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора при совместном использовании с DLP

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.038 Угроза исчерпания вычислительных ресурсов хранилища больших данных	Одним из направлений атак на организацию может быть приведение информационных систем и ресурсов организации в состояние «отказ в обслуживании». Такие атаки на системы хранения данных основываются на исчерпании возможностей системы из-за превышения допустимой нагрузки на нее. Для нейтрализации таких угроз необходимо использовать СЗИ, позволяющее ограничивать нагрузку на систему хранения данных. МДР InfoDiode PRO контролирует поток передаваемых данных в систему хранения данных (как на сервере, находящимся в менее доверенном сегменте, так и на находящимся в более доверенном) на соответствие преднастроенным политикам интенсивности передачи данных, и их передача осуществляется только при условии соответствия политикам. Такой подход позволяет ограничивать поток передаваемых в систему хранения данных, что обеспечивает её надежную защиту от превышения допустимой нагрузки и состояния «отказ в обслуживании».	Неприменимо	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.063 Угроза некорректного использования функционала программного и аппаратного обеспечения УБИ.107 Угроза отключения контрольных датчиков **УБИ.112 Угроза передачи запрещённых команд на оборудование с числовым программным управлением** УБИ.113 Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу удаленного направления деструктивных команд в информационные системы при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленную передачу в информационную систему деструктивных и запрещенных команд, которые могут привести к нарушению режима работы системы, ее перезагрузке или отключению, состоянию «отказ в обслуживании» и т.д., что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.183 Угроза перехвата управления автоматизированной системой управления технологическими процессами УБИ.212 Угроза перехвата управления информационной системой	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу удаленного перехвата управления информационными системами при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленную передачу команд, позволяющих перехватить управление информационными системами и автоматизированными системами управления технологическими процессами, что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.012 Угроза деструктивного изменения конфигурации/ среды окружения программ	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу удаленного деструктивного изменения конфигурации или среды окружения при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении конфигурации (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) в структурированном формате (JSON, в перспективе XML) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет контролировать и ограничивать передачу конфигураций в информационные системы и автоматизированные системы управления технологическими процессами, что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.050 Угроза неверного определения формата входных данных, поступающих в хранилище больших данных **УБИ.177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью**	Если в информационной системе, имеющей внешние интерфейсы, не осуществляется контроль за входящими данными, злоумышленник может удаленно направлять различные данные, содержащие опасные паттерны кода, служебные символы и т.д. или легитимные команды, содержащие недопустимые значения параметров, на вход системы с целью вывести систему из штатного состояния, эксплуатации уязвимостей или «отказа в обслуживании». Для нейтрализации угрозы необходимо использование СЗИ, позволяющего ограничивать несанкционированные запросы к информационной системе. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленную передачу в информационную систему деструктивных и запрещенных сообщений, что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Неприменимо	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.033 Угроза использования слабостей кодирования входных данных	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу эксплуатации слабостей кодирования входных данных при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленную передачу в информационную систему некорректных сообщений, которые могут привести к нарушению режима работы системы, что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация угроз с использованием междоменного решения InfoDiode (МДР InfoDiode)

УБИ	Интерпретация УБИ и подход к нейтрализации	МДР InfoDiode ДС ►I НС	МДР InfoDiode ДС I◄ НС	МДР InfoDiode ДС I◄►I НС
УБИ.109 Угроза перебора всех настроек и параметров приложения	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозу удаленного перебора настроек и параметров информационной системы при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленное несанкционированное изменение параметров и настроек информационной системы для подбора наиболее уязвимой конфигурации, которая позволит ему в развитии атаки, или же приведет систему в состояние «отказ в обслуживании», что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора
УБИ.007 Угроза воздействия на программы с высокими привилегиями УБИ.122 Угроза повышения привилегий	МДР InfoDiode SMART расширяет сферу применения однонаправленных шлюзов InfoDiode и позволяет нейтрализовать угрозы удаленного повышения привилегий и использования программ, обладающих высокими привилегиями, при использовании InfoDiode, направленного в более доверенный сегмент. МДР InfoDiode SMART при получении сообщения (как на сервер, находящийся в менее доверенном сегменте, так и на находящийся в более доверенном) проводит анализ полей сообщения на соответствие преднастроенным политикам передачи команд, и дальнейшая передача в целевую систему осуществляется только при условии соответствия им. Такой подход позволяет ограничивать удаленное направление команд, использующих привилегированные функции или программы, что обеспечивает надежную защиту информационных систем от несанкционированного внешнего воздействия.	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора	Нейтрализация удаленного вектора

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация иных сетевых угроз с использованием комплементарных СЗИ

Решения **InfoDiode** нейтрализуют множество угроз, связанных с сетевым взаимодействием информационных систем и пользователей, но в ряде случаев возникает необходимость использования других комплементарных СЗИ. Это актуально в ситуациях, когда существует необходимость полноценного двустороннего сетевого взаимодействия между системами, при сопряжении сегментов с сетью Интернет, а также если нейтрализация конкретного типа угроз не является функцией безопасности решений **InfoDiode**. В качестве комплементарных СЗИ могут выступать межсетевые экраны, многофункциональные межсетевые экраны уровня сети (NGFW), криптографические шлюзы и другие. В настоящем разделе приведены угрозы, для нейтрализации которых невозможно или недостаточно использования решений линейки **InfoDiode** и необходимо использование комплементарных СЗИ. Указанные УБИ и их интерпретация приведены справочно, экспертно. Интерпретация направлена на то, чтобы предоставить конечным пользователям более полный взгляд на построение защиты сетевого периметра при внедрении решений **InfoDiode** и иных средств защиты.

УБИ	Интерпретация УБИ и подход к нейтрализации
УБИ.041 Угроза межсайтового скриптинга УБИ.042 Угроза межсайтовой подделки запроса УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов УБИ.186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет УБИ.174 Угроза «фарминга»	Самым слабым звеном системы обеспечения информационной безопасности любой организации остается человек, и именно на работников организации направлено значимое число атак. Наличие у информационной системы или устройства работника доступа в сеть Интернет открывает злоумышленникам ряд возможностей по их компрометации. Для этого могут быть использованы различные сценарии: внедрение вредоносного кода на Интернет-сайты, направление вредоносных ссылок работникам с применением методов социальной инженерии, чтобы вынудить работников перейти по ней, скрытая установка вредоносного программного обеспечения, «фишинговые сайты», эксплуатация возможностей перенаправления на сторонний ресурс за счет такой возможности протокола HTTP и многие другие. В такой ситуации решения InfoDiode неприменимы, так как работа в сети Интернет требует полноценного двунаправленного сетевого соединения между устройством работника и серверами, на которых развернуты Интернет-сайты, однонаправленность передачи данных нарушит существующие рабочие процессы. Для нейтрализации угроз таких типов необходимо использовать СЗИ, которые осуществляют контроль за благонадежностью посещаемых работниками сайтов, фильтрацию ссылок и перенаправления на сторонние сайты, проверку на вредоносный код всех входящих данных. При этом при компрометации Интернет-сегмента InfoDiode позволяет локализовать атаку исключительно в пределах одного сегмента, в случае если InfoDiode (или пара разнонаправленных InfoDiode) размещен между Интернет-сегментом и иными корпоративными сегментами, за счет однонаправленности передачи данных и разрыва двунаправленных протоколов.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация иных сетевых угроз с использованием комплементарных СЗИ

УБИ	Интерпретация УБИ и подход к нейтрализации
УБИ.069 Угроза неправомерных действий в каналах связи УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети УБИ.130 Угроза подмены содержимого сетевых ресурсов УБИ.017 Угроза доступа/перехвата/ изменения HTTP cookies	Одним из векторов атаки на организации является компрометация канала передачи данных и дальнейший перехват или модификация сообщений, различных данных, аутентификационной информации, сетевых пакетов и т.д. Получив такую информацию, злоумышленник может её использовать для получения несанкционированного доступа с помощью учетных записей пользователей или же применять для воздействия на работников путем ввода их в заблуждение методами социальной инженерии. В случае модификации сообщений злоумышленник может изменить реквизиты платежной транзакции или же изменить настройки промышленной системы, что приведет к тяжелому ущербу для организации. Нейтрализация таких угроз не относится к функциям безопасности InfoDiode, рекомендуется использовать СЗИ, обеспечивающие целостность и конфиденциальность канала передачи данных, а также аутентификацию всех участников сетевого взаимодействия.
УБИ.128 Угроза подмены доверенного пользователя УБИ.131 Угроза подмены субъекта сетевого доступа	Подмена одного из участников сетевого взаимодействия является одним из возможных сценариев для получения несанкционированного доступа к информационным системам. Злоумышленник может выдавать себя за легитимного пользователя или же осуществить скрытую подмену сетевого ресурса, к которому обращается пользователь, выполнять приём/передачу данных от имени пользователя или ресурса, используя это для дальнейшего развития атаки на организацию. Нейтрализация таких угроз не относится к функциям безопасности InfoDiode, рекомендуется использовать СЗИ, обеспечивающие аутентификацию всех участников сетевого взаимодействия.
УБИ.001 Угроза автоматического распространения вредоносного кода в грид-системе УБИ.002 Угроза агрегирования данных, передаваемых в грид-системе УБИ.047 Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Системы распределенных вычислений состоят из множества узлов с единым централизованным управлением. Такая архитектура системы сама по себе несет некоторые угрозы безопасности всей системы: получение несанкционированного доступа к узлу и дальнейшее распространение вредоносного кода по всей системе или нарушение её работоспособности, возможность перехвата результатов вычислений в каналах связи, а также ряд других угроз. Решения InfoDiode неприменимы для обеспечения безопасности грид-систем, так как для взаимодействия между узлами грид-системы требуется полноценное двунаправленное сетевое соединение, однонаправленность передачи данных нарушит необходимое взаимодействие. Для нейтрализации угроз таких типов необходимо использовать СЗИ, которые осуществляют фильтрацию сетевого трафика, а также обеспечивают конфиденциальность и целостность канала передачи данных.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Нейтрализация иных сетевых угроз с использованием комплементарных СЗИ

УБИ	Интерпретация УБИ и подход к нейтрализации
УБИ.062 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Перенаправление сетевого трафика работника или информационной системы на сервера злоумышленников с использованием прозрачного прокси-сервера может быть результатом предыдущих шагов атаки на организацию. При успешной реализации такой угрозы злоумышленник может осуществлять перехват или модификацию сообщений, различных данных, аутентификационной информации, сетевых пакетов и т.д., и использовать полученные данные для дальнейшего развития атаки. Нейтрализация таких угроз не относится к функциям безопасности InfoDiode, рекомендуется использовать СЗИ, обеспечивающие целостность и конфиденциальность канала передачи данных, а также аутентификацию всех участников сетевого взаимодействия.
УБИ.068 Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением	Одним из широко используемых способов взаимодействия между информационными системами являются прикладные программные интерфейсы (API). Несмотря на свою простоту и удобство, их наличие порождает ряд угроз, которыми могут воспользоваться злоумышленники для осуществления деструктивного воздействия на API в целях реализации функций, изначально не предусмотренных информационной системой. Для обеспечения безопасности API решения InfoDiode неприменимы, так как для их корректной работы требуется полноценное двунаправленное сетевое соединение, однонаправленность передачи данных нарушает корректное взаимодействие между системами. Для нейтрализации такой угрозы необходимо использовать СЗИ, которые осуществляют фильтрацию сетевого трафика, обеспечивают конфиденциальность и целостность канала передачи данных, а также аутентификацию всех участников сетевого взаимодействия.
УБИ.075 Угроза несанкционированного доступа к виртуальным каналам передачи	Широкое использование различных систем виртуализации заставляет злоумышленников находить новые способы атаки на такие системы. Одной из потенциальных угроз является компрометация виртуального канала передачи данных и дальнейший перехват или модификация сетевых пакетов. Реализация такой угрозы может привести к нарушению работы всей инфраструктуры виртуализации организации. Решения InfoDiode представляют собой аппаратно-программный комплекс, в связи с чем их использование для обеспечения безопасности виртуальных каналов передачи затруднительно. Для нейтрализации такой угрозы необходимо использовать СЗИ, которые осуществляют фильтрацию сетевого трафика, обеспечивают конфиденциальность и целостность канала передачи данных, а также аутентификацию всех участников сетевого взаимодействия.
УБИ.173 Угроза «спама» веб-сервера	Атаки на организации с использованием спам-сообщений являются одними из наиболее распространенных из-за свой простоты автоматизации и низкой стоимости. Спам-сообщения могут содержать ссылки на фишинговые или мошеннические ресурсы или зараженные файлы, использование которых приводит к компрометации информационной системы и дальнейшему развитию атаки. Нейтрализация такой угрозы не относится к функциям безопасности InfoDiode, рекомендуется использовать СЗИ, обеспечивающие фильтрацию и контентный анализ сетевого трафика.

AMT GROUP

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

www.amt.ru
www.infodiode.ru