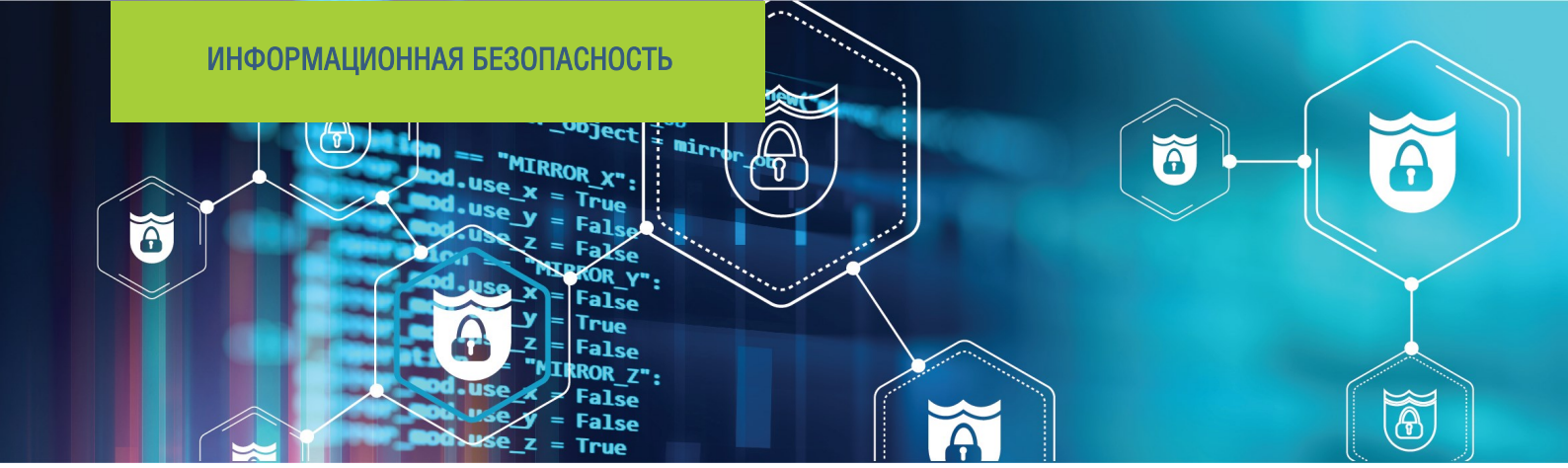

InfoDiode и требования нормативных актов и стандартов финансового сектора

Наиболее разрушительные современные атаки на компании и организации финансового сектора имеют целенаправленный и многоступенчатый характер. Начиная с проникновения в сетевую инфраструктуру организации через одну уязвимую точку на периметре сети организации, злоумышленники распространяют свой контроль на критически важные системы организации.

Значимой задачей при построении безопасной сети организации является проектирование потоков передачи данных между сегментами разной критичности так, чтобы минимизировать возможности нарушителей по проникновению в критически значимые сегменты и сети. Критически значимыми в организациях финансового сектора могут быть сегменты АРМ дистанционного банковского обслуживания с банками-корреспондентами, АРМ клиентов Банка России, продуктивных систем, хранилищ данных. В качестве менее доверенных сетевых сегментов обычно рассматриваются: интернет-сегмент, сегмент разработки и тестирования (в котором многие разработчики имеют административный доступ на свои АРМ), сегмент АРМ пользователей (наиболее уязвимы к воздействию методов социальной инженерии или несанкционированных действий работников организации), сегмент контакт-центра и другие.

Одним из решений, позволяющих обеспечить практическую защиту сети организации, являются однонаправленные шлюзы **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. То есть, обеспечивают гарантированную защиту сегмента от внешних информационных атак по сети.

Свой вклад в обеспечение безопасности финансовых организаций вносят регуляторы финансового сектора и некоммерческие организации, занимающиеся стандартизацией мер и методов защиты информации и ИТ-инфраструктуры. В настоящем документе представлены требования регуляторов (как российских, так и зарубежных), которые непосредственно определяют или рекомендуют применение устройств, аналогичных однонаправленным шлюзам **InfoDiode.**

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Реализация требований Банка России с помощью InfoDiode

Основным регулятором российского финансового сектора является Центральный банк Российской Федерации (Банк России), который в части обеспечения информационной безопасности финансовыми организациями отвечает за нормативное регулирование вопросов защиты информации, киберустойчивости и применения информационных технологий в финансовых организациях, а также обеспечивает контроль за соблюдением установленных требований.

Требования Банка России по защите информации для финансовых организаций распространяются на 3 технологических уровня: уровень инфраструктуры, уровень используемого прикладного программного обеспечения и приложений и уровень технологии обработки данных. При этом нормативные акты Банка России не содержат конкретного набора мер защиты уровня инфраструктуры. В качестве «каталога» мер защиты Банк России ссылается на Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», который охватывает различные аспекты безопасности финансовой организации, в том числе безопасности сети и сетевых взаимодействий. В таблице ниже приведен перечень нормативных актов Банка России, содержащих требования соответствия ГОСТ Р 57580.1-2017.

Субъект	Нормативный акт Банка России, содержащий ссылку на выполнение ГОСТ Р 57580.1-2017
Кредитные организации	п. 3.1 Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
Некредитные финансовые организации	п. 1.4 Положения Банка России от 20 апреля 2021 г. № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»
Субъекты Национальной платежной системы	п. 1.1, 3.5, 4.3, 6.5, 7.3 Положения Банка России от 17 августа 2023 г. № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
Субъекты, подключающиеся к платежной системе Банка России	п. 3, 4, 5, 6 Положения Банка России от 25 июля 2022 г. № 802-П «О требованиях к защите информации в платежной системе Банка России»
Субъекты, подключающиеся к платформе цифрового рубля	п. 4 Положения Банка России от 7 декабря 2023 г. № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Реализация требований ГОСТ Р 57580.1-2017 с помощью InfoDiode

ГОСТ Р 57580.1-2017 содержит отдельный раздел мер защиты, посвященный обеспечению защиты вычислительных сетей, их сегментации и межсетевому экранированию (глава 7.3.1). В соответствии с ГОСТ Р 57580.1-2017 применяемые финансовой организацией меры по сегментации и межсетевому экранированию вычислительных сетей должны обеспечивать: сегментацию и межсетевое экранирование внутренних вычислительных сетей, защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет, регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.

В таблице ниже описаны подходы к реализации таких мер защиты с использованием **InfoDiode**.

Мера защиты информации ГОСТ Р 57580.1-2017	Интерпретация
СМЭ.1 Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры каждого из контуров безопасности. СМЭ.2 Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, сегментов контуров безопасности и внутренних вычислительных сетей финансовой организации, не предназначенных для размещения информационной инфраструктуры, входящей в контуры безопасности.	InfoDiode обеспечивает надежную изоляцию одного сетевого сегмента (контура безопасности) от другого за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI: физический сигнал (свет) направляется только в одну сторону, от источника к приемнику, что обеспечивает гарантированную однонаправленность передачи данных, исключая возможность направить какой-либо сигнал по каналу связи в обратном направлении.
СМЭ.4 Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации в соответствии с установленными правилами и протоколами сетевого взаимодействия.	InfoDiode обеспечивает контроль в соответствии с правилами и протоколами сетевого взаимодействия по принципу белого списка: все взаимодействия, которые не разрешены конфигурацией InfoDiode, будут запрещены. Также за счет однонаправленной передачи сетевых пакетов на физическом уровне InfoDiode делает невозможным работу двунаправленных протоколов взаимодействия, что гарантирует невозможность их применения даже в случае компрометации СЗИ или ошибок при его конфигурации.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Реализация требований ГОСТ Р 57580.1-2017 с помощью InfoDiode (продолжение)

Мера защиты информации ГОСТ Р 57580.1-2017	Интерпретация
СМЭ.5 Реализация и контроль информационного взаимодействия с применением программных шлюзов между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации с целью обеспечения ограничения и контроля на передачу данных по инициативе субъектов логического доступа.	В отличие от программной реализации шлюзов в программно-аппаратном комплексе InfoDiode однонаправленная передача реализуется физическим принципом работы аппаратной компоненты InfoDiode: физический сигнал (свет) направляется только в одну сторону, из источника к приемнику, что обеспечивает гарантированное разграничение сетевых сегментов (контуров безопасности) даже в случае компрометации СЗИ или ошибок при его конфигурации.
СМЭ.6 Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации АС, в том числе тестирования ПО и объектов доступа. СМЭ.7 Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования (за исключением инфраструктурных сервисов, включая средства защиты информации, управляемые централизованно, клиентская составляющая которых размещена в сегменте разработки и тестирования, а средства управления - в иных внутренних вычислительных сетях финансовой организации).	InfoDiode может применяться для разграничения продуктивного сегмента и сегмента разработки и тестирования, в том числе для запрета сетевого взаимодействия по инициативе сегмента разработки и тестирования: • В случае если InfoDiode направлен из продуктивного сегмента в сегмент разработки и тестирования, за счет однонаправленной передачи данных исключается возможность направить какой-либо сигнал по каналу связи из сегмента разработки и тестирования; • В случае если InfoDiode направлен из сегмента разработки и тестирования в продуктивный сегмент, за счет однонаправленной передачи данных, и, как следствие, невозможности использования двунаправленных протоколов, исключается несанкционированное сетевое взаимодействие со стороны сегмента разработки и тестирования.

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

Реализация требований ГОСТ Р 57580.1-2017 с помощью InfoDiode (продолжение)

Мера защиты информации ГОСТ Р 57580.1-2017	Интерпретация
СМЭ.8 Выделение в составе сегментов контуров безопасности отдельных пользовательских сегментов, в которых располагаются только АРМ пользователей. СМЭ.9 Выделение в составе сегментов контуров безопасности отдельных сегментов управления, в которых располагаются только АРМ эксплуатационного персонала, используемые для выполнения задач администрирования информационной инфраструктуры. СМЭ.10 Выделение в составе сегментов контуров безопасности отдельных сегментов хранения и обработки данных, в которых располагаются ресурсы доступа, предназначенные для обработки и хранения данных, серверное оборудование и системы хранения данных.	InfoDiode может применяться для разграничения различных сетевых сегментов (контуров безопасности), таких как пользовательский сегмент, сегмент эксплуатационного персонала, сегмент хранилища данных, сегмент ситуационного центра безопасности и другие: во всех случаях InfoDiode позволяет надежно разделить сетевые сегменты за счет однонаправленной передачи данных.
СМЭ.13 Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет. СМЭ.14 Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет.	InfoDiode обеспечивает изоляцию сетевых сегментов (контура безопасности) от сети Интернет за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI: физический сигнал (свет) направляется только в одну сторону, от источника к приемнику, что обеспечивает гарантированную однонаправленность передачи данных.
СМЭ.17 Сокрытие топологии внутренних вычислительных сетей финансовой организации	InfoDiode за счет однонаправленной передачи сетевых пакетов на физическом уровне делает невозможным работу двунаправленных протоколов взаимодействия и, как следствие, сканирование сети организации для определения ее топологии.

AMT GROUP

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

www.amt.ru
www.infodiode.ru

Реализация требований ГОСТ Р 57580.1-2017 с помощью InfoDiode (продолжение)

Мера защиты информации ГОСТ Р 57580.1-2017	Интерпретация
СМЭ.20 Ограничение на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении взаимодействия с сетью Интернет СМЭ.21 Ограничение на перечень протоколов сетевого взаимодействия и сетевых портов, используемых при осуществлении почтового обмена электронными сообщениями с использованием сети Интернет	InfoDiode обеспечивает контроль в соответствии с правилами сетевых портов, как для общих протоколов, так и для почтовых, по принципу белого списка: использование сетевых портов, которые не нужны для реализации сетевых взаимодействий, разрешенных конфигурацией InfoDiode, будет ограничено.

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

Международный опыт стандартизации NIST и InfoDiode

Практика регулирования реализации мер информационной безопасности финансовых организаций в других странах достаточно схожа с требованиями Банка России. В США аналогичным регулятором является Министерство торговли США (U.S. Department of Commerce), а вопросами стандартизации информационной безопасности занимается подведомственный Национальный институт стандартов и технологий США (The National Institute of Standards and Technology, NIST).

Одним из базовых стандартов NIST является NIST Special Publication 800-53 Revision 5 «Security and Privacy Controls for Information Systems and Organizations». Данный стандарт содержит набор требований и рекомендаций по обеспечению комплексной безопасности организаций, в том числе включая управление доступами, аудит, управление конфигурациями, идентификацию и аутентификацию, безопасность инфраструктуры, сетей и приложений, целостность данных и систем и многие другие аспекты. Стоит отметить, что использование односторонних шлюзов рекомендовано NIST SP 800-53 как эффективное средство, позволяющее исключить утечку данных из критичного сегмента, не создавая помех для передачи данных в критичный сегмент.

Мера защиты информации NIST.SP 800-53	Интерпретация
AC-4 (7): Обеспечение односторонних потоков данных с использованием аппаратных механизмов контроля передачи данных.	InfoDiode в полной мере предоставляет возможности по реализации механизмов односторонней передачи данных за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI: физический сигнал (свет) направляется только в одну сторону, от источника к приемнику, что обеспечивает гарантированную однонаправленность передачи данных.
SC-7: Защита границ: • Мониторинг и управление сетевым взаимодействием на внешних и ключевых внутренних управляемых интерфейсах систем; • Выделение в подсети общедоступных компонентов систем, и их отделение от внутренней сети организации; • Подключение к внешним сетям или системам только через управляемые интерфейсы, включающие устройства защиты границ в соответствии с архитектурой безопасности и приватности.	InfoDiode обеспечивает надежную изоляцию одного сетевого сегмента (контура безопасности) от другого за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI: физический сигнал (свет) направляется только в одну сторону, от источника к приемнику, что обеспечивает гарантированную однонаправленность передачи данных, исключая возможность направить какой-либо сигнал по каналу связи в обратном направлении.
SC-49: Использование аппаратных средств для отделения сегментов и применения политик.	

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

Международный опыт стандартизации CIS Control и InfoDiode

Другим фреймворком по безопасности является CIS Critical Security Controls for Effective Cyber Defense, разработанный некоммерческой организацией Центр безопасности Интернета (Center for Internet Security). Аналогично NIST SP 800-53 фреймворк содержит рекомендации в виде набора значимых мер защиты, которые организации должны реализовать для блокирования или смягчения известных атак. Особенность подхода фреймворка CIS Control заключается в том, что в нем определены меры защиты с учетом их приоритета, в том числе сделан акцент на минимально необходимом количестве мер, которые значительно снижают риски кибербезопасности. Базовые меры защиты CIS Control, в том числе, включают в себя: инвентаризацию активов, защиту данных, безопасность конфигураций, управление учетными записями и доступами, выявление уязвимостей, аудит, антивирусную защиту, восстановление денных, управление, защиту и мониторинг сетевой инфраструктуры, безопасность приложений и многое другое.

В таблице ниже описаны подходы к реализации критических мер защиты CIS Controls с использованием **InfoDiode**.

Мера защиты информации CIS Controls	Интерпретация
3.12 Сегментирование обработки и хранения данных на основе уровня их конфиденциальности. Контроль за обработкой конфиденциальных данных в корпоративных сегментах с более низким уровнем конфиденциальности.	InfoDiode обеспечивает надежную изоляцию одного сетевого сегмента от другого с различными уровнями конфиденциальности за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI, таким образом исключая возможность передачи данных из сегмента с более высоким уровнем конфиденциальности в сегмент с низким уровнем конфиденциальности.
11.4 Создание и поддержка изолированной копии данных резервного копирования. Примеры реализаций включают в себя контроль версий резервных копий через автономные, облачные, внешние системы или сервисы.	InfoDiode может применяться для разграничения различных сетевых сегментов, в том числе для изоляции хранилища резервных копий: InfoDiode позволяет передавать резервные копии в хранилище по однонаправленному каналу и при этом ограничить иные сетевые взаимодействия.
12.2 Создание и поддержка безопасной сетевой архитектуры. Безопасная сетевая архитектура должна, как минимум, включать в себя сегментацию сети, минимальные привилегии и доступность.	InfoDiode обеспечивает надежную изоляцию одного сетевого сегмента от другого за счет однонаправленной передачи сетевых пакетов на физическом уровне модели OSI: физический сигнал (свет) направляется только в одну сторону, от источника к приемнику, что обеспечивает гарантированную однонаправленность передачи данных, исключая возможность направить какой-либо сигнал по каналу связи в обратном направлении.

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

Международный опыт регулирования, стандартизации CIS Control и InfoDiode (продолжение)

Мера защиты информации CIS Controls	Интерпретация
16.8 Разделение производственных и непроизводственных систем. Поддерживать отдельные среды (сетевые сегменты) для производственных (продуктивная среда) и непроизводственных (среда разработки и тестирования) систем.	InfoDiode может применяться для разграничения продуктивного сегмента и сегмента разработки и тестирования, в том числе для запрета сетевого взаимодействия по инициативе сегмента разработки и тестирования: • В случае, если InfoDiode направлен из продуктивного сегмента в сегмент разработки и тестирования, за счет однонаправленной передачи данных исключается возможность направить какой-либо сигнал по каналу связи из сегмента разработки и тестирования. • В случае, если InfoDiode направлен из сегмента разработки и тестирования в продуктивный сегмент, за счет однонаправленной передачи данных, и, как следствие, невозможности использования двунаправленных протоколов, исключается несанкционированное сетевое взаимодействие со стороны сегмента разработки и тестирования.

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