InfoDiode как часть Междоменных решений

Значительный объем задач в области обеспечения безопасности - от противодействия угрозам национальной безопасности и террористическим атакам до противодействия несанкционированному воздействию на функционирование промышленных, энергетических, транспортных, медицинских, финансовых предприятий, органов государственного управления и власти, крупных коммерческих компаний - требует обеспечения безопасного обмена данными между организациями разных уровней. В некоторых случаях необходимость такого обмена закреплена законодательно.

В зависимости от стоящей задачи информация, создаваемая и обрабатываемая в более доверенных (закрытых) сегментах сети, может в отдельных случаях передаваться в общедоступные сегменты или сегменты с меньшим уровнем доверия и менее строгими политиками безопасности - для ее использования иным кругом лиц и потребителей. В других случаях характерна обратная ситуация - информация должна поступать из общедоступных или менее доверенных сетей в более доверенные в целях агрегации, обработки, анализа, систематизации. Передаваемые данные могут представлять собой отдельный документ, сигнал (набор сигналов), телеметрию или целые каталоги (архивы) файлов, содержащие изображения, карты, документы и базы данных.

Междоменные решения представляют собой интегрированный комплекс решений по обеспечению безопасности. Комплекс, как правило состоит из специализированного программного, и, в ряде случаев, аппаратного обеспечения, с интерфейсами для ручного или автоматического предоставления и/или ограничения доступа к информации разных категорий значимости, а также интерфейсы для организации передачи такой информации. Чаще всего междоменные решения представляют собой интегрированные программно-аппаратные комплексы, которые обеспечивают безопасный доступ к критичным данным и их передачу по сетям с различными уровнями доступа/доверия (включая ограничение такого обмена, если это противоречит существующим политикам безопасности).

Помимо технических решений внедрение междоменного взаимодействия предусматривает набор организационных мер, обеспечивающих корректность применения всех компонентов в составе комплекса междоменного решения. Таким образом, **междоменные решения представляют собой комплексную организационно-техническую интегрированную систему**.

AMT GROUP

Тел: +7 (777) 2142677 Email: info@infodiode.kz

www.infodiode.kz

www.amt-group.kz

Междоменные решения: термины и определения

Вопрос эффективности обмена между сетями как с одинаковым, так и с разным уровнем доверия является комплексным и непростым. Помимо сохранения конфиденциальности данных он касается иных, не менее значимых, факторов: скорости обмена, его достоверности, безопасности и надежности. В ряде случаев для обеспечения требований безопасности используются полностью изолированные сети. Однако полная изоляция сетей/сегментов, несмотря на серьезное повышение уровня безопасности, создает и очевидные проблемы. В контексте междоменных решений в условиях наличия сетей с различными уровнями доверия рассматриваются следующие компоненты:

- **Домен** - логически объединенная совокупность организационно-технических активов и ресурсов, подчиняющихся единой политике безопасности. Домен содержит данные, информационные системы и сети определенных классов, категорий безопасности, которые сегментированы, в том числе, в зависимости от возможностей передачи информации. Для некоторых доменов требуется установление большей степени доверия, тогда как для других требуется меньшее доверие.
- **Доверенная сеть** (в ряде случаев сеть/система-источник) - область, формирующая наибольшие риски в отношении утраты, компрометации, нарушения заданных характеристик обрабатываемой информации, систем, сегментов, данных, процессов;
- **Менее доверенная сеть** (недоверенная сеть, в ряде случаев сеть/система-приемник) - область, формирующая наибольшие риски в части вероятности организации атак из нее на иные сегменты и сети;
- **Периметр** - граница доверенной сети, на которой выполняется аутентификация запросов, регулируются информационные потоки, применяются организационно-технические меры для снижения рисков в отношении информации, сетей, данных, процессов.

Отношения между доменами описываются в организационно-распорядительных документах (**политиках безопасности**). Для каждого домена в политике определяется, какие требования к обеспечению безопасности, в частности, характеристики информации (целостность, конфиденциальность, доступность, неотказуемость и др.) должны быть выполнены.

Существуют разные типы междоменных решений:

1. **Междоменные решения по организации доступа** обеспечивают потребителям (системам, пользователям) возможность просматривать/читать и пользоваться информацией из доменов различных уровней доверия, снабженных соответствующими атрибутами/признаками/категориями. Решения по организации доступа размещаются между **системой или пользователем и различными доменами**. Примерами таких решений являются: изолированные рабочие станции, решения, основанные на регламентном/временном доступе с одной рабочей станции, решения класса KVM Switch, решения на основе системы виртуализации и др.
2. **Междоменные решения по организации передачи данных** обеспечивают возможность перемещения информации между доменами различных уровней доверия. Междоменные решения по организации передачи данных должны учитывать категорирование данных, отношения между доменами и применяемую для каждого домена политику. Решение по организации передачи данных размещается **между различными доменами**. Примерами таких решений являются: воздушный зазор, МСЭ, «диоды данных», однонаправленные комплексные решения, двунаправленные комплексные решения и др.

В настоящей брошюре более детально рассматриваются междоменные решения по организации передачи данных и их построение с использованием продуктов **InfoDiode.**

Функции междоменных решений по организации передачи данных

Несмотря на существование большого количества различных междоменных решений по организации передачи данных, в общем виде они могут быть описаны в терминах и функциях сетевых устройств или шлюзов безопасности. С точки зрения организации эшелонированной защиты, все указанные базовые функции сетевых устройств имеют важное значение для сетевой безопасности, однако их максимальная эффективность проявляется только в комплексе и только с учетом реализации дополнительно реализуемых **функций**:

1. **«Разрыв протоколов»** - реализация организационно-технических мер, направленных на замену прямого взаимодействия между доменами обменом через прокси компоненты, компенсация угроз, формируемых протоколами обмена, обеспечение дополнительных уровней терминирования и инспекции, а также реализация мер, направленных на исключение или минимизацию в применяемых решениях «уязвимостей нулевого дня».
2. **Преобразование и нормализация данных** - реализация организационно-технических решений в части форматов обмена, контроля за соблюдением форматов данных и форматов метаинформации.
3. **Контроль состояния узлов доступа и контроль доступа к сети** - реализация организационно-технических мер, обеспечивающих контроль доступа к домену на основании информации о пользователе, рабочей станции, ее состоянии и программном обеспечении на ней.
4. **Защита от утечек данных** - реализация организационно-технических решений, непосредственно предотвращающих утечки конфиденциальной информации.
5. **Контроль сетевых потоков, фильтрация данных и помещение их в карантин, антивирусная защита** - реализация организационно-технических мер, обеспечивающих контроль сетевых потоков и инспекцию (в том числе, санацию) трафика.
6. **Контроль происхождения данных и маркировка данных** - реализация организационно-технических решений, обеспечивающих наличие корректной информации, касающейся происхождения данных, в целях повышения достоверности получаемых данных.
7. **Решения по криптографии** - реализация организационно-технических решений, обеспечивающих хранение и передачу информации в зашифрованном виде для обеспечения конфиденциальности и безопасности, аутентификацию пользователей или устройств с использованием СКЗИ, а также выполнение соответствующих требований по использованию СКЗИ (например, порядка хранения ключей и т.п.).
8. **Исключение стеганографии** - реализация организационно-технических мер, исключающих стеганографию.

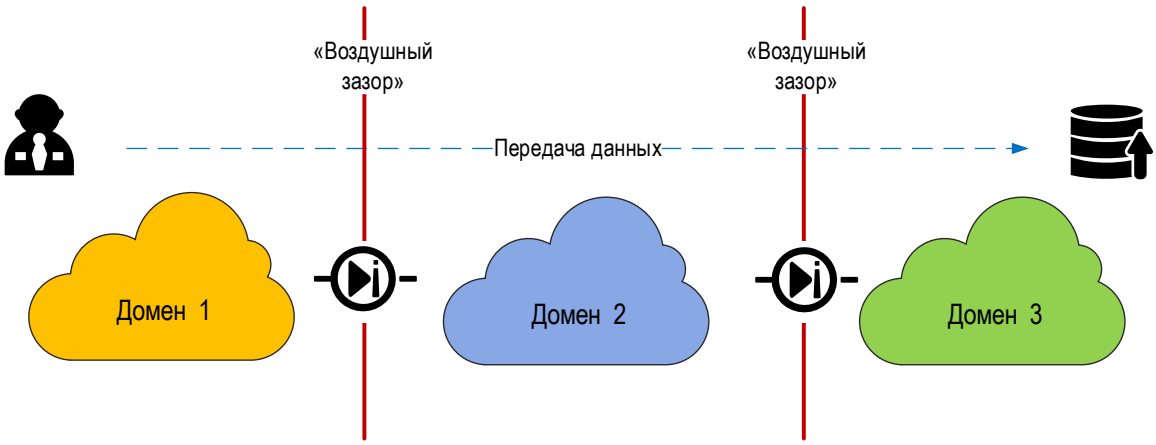
Применение сертифицированных решений при организации междоменного взаимодействия

В связи с тем, что междоменные решения часто сопрягают критическую инфраструктуру с менее доверенной и обеспечивают передачу данных различных уровней конфиденциальности, сертификация и аттестация комплекса междоменных решений и/или его составных компонентов может являться неотъемлемым условием, обеспечивающим эффективность и безопасность внедрения, применения, поддержки и сопровождения. Процедуры сертификации междоменных решений варьируются в зависимости от уровня требований к передаваемой междоменным решением информации и уровня критичности сопрягаемых систем, сетей и доменов. Как правило, минимальным уровнем сертификации междоменных решений является сертификация по УД4 в системе сертификации СТ РК ISO/IEC 15408-3-2017 .

Применение InfoDiode в составе междоменных решений

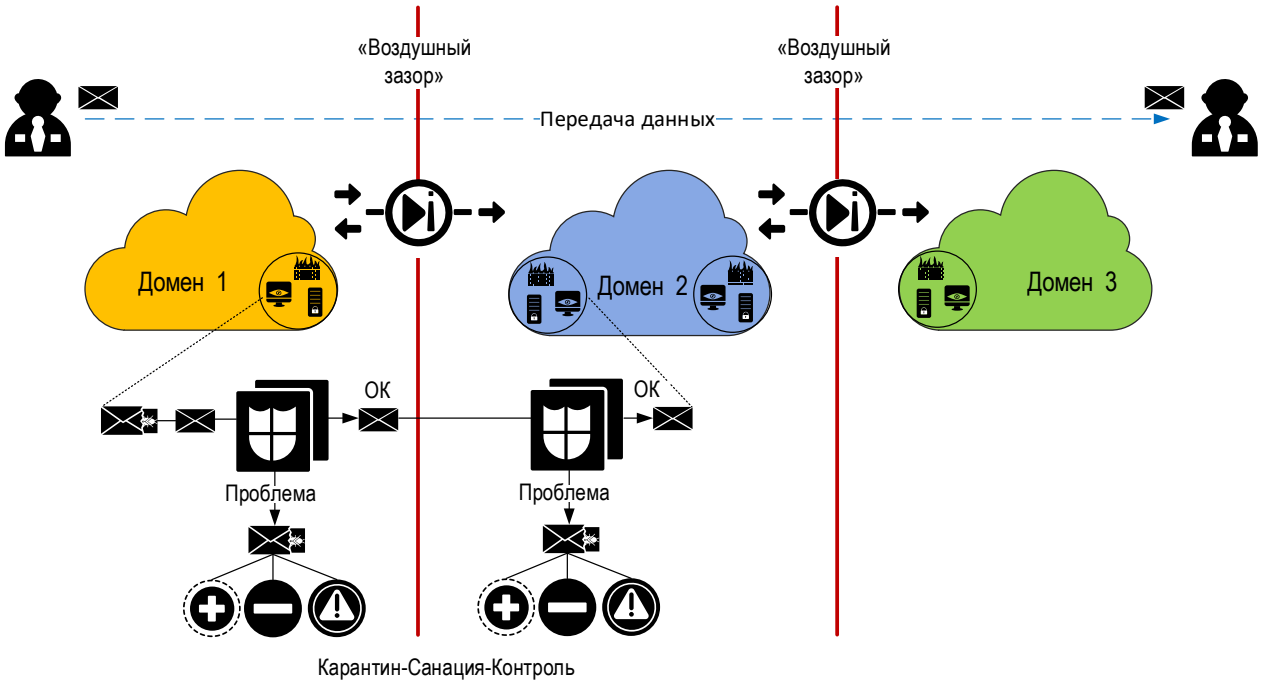
Организация однонаправленного взаимодействия с применением «диода данных» InfoDiode

Аппаратные решения **InfoDiode (АК InfoDiode)**, являясь основой однонаправленного взаимодействия между доменам, предоставляют базовые функции междоменных решений, такие как «разрыв протоколов» и исключение эксплуатации в самом аппаратном диоде уязвимостей «нулевого дня». В том числе аппаратные диоды могут использоваться в рамках построения комплексных систем обнаружения вторжений (СОВ) на базе решений смежных вендоров.



Однонаправленное взаимодействие с применением комплексных решений InfoDiode

Комплексные однонаправленные решения по организации передачи данных на базе **InfoDiode** представляют собой набор из нескольких решений, реализующих функции междоменного взаимодействия. Такие решения включают в свой состав функциональные возможности, как минимум, трех СЗИ (не ограничиваясь ими): МСЭ, «диод данных», решений по инспекции трафика (Антивирус, DPI, DLP). Их применение предполагает, в том числе, конкретную настройку комплексного решения на проверку содержимого информации, передаваемой между доменами.



AMT GROUP

Тел: +7 (777) 2142677 Email: info@infodiode.kz

www.infodiode.kz

www.amt-group.kz

Двунаправленное взаимодействие с применением комплексных решений InfoDiode

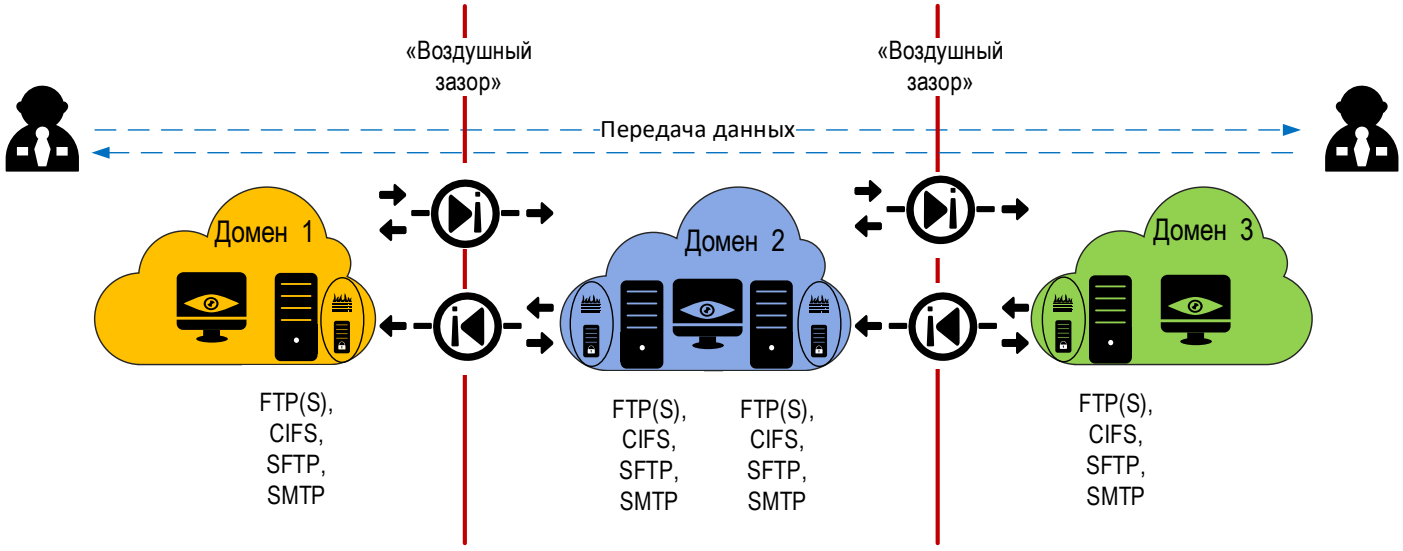
Двунаправленные комплексные решения на базе **InfoDiode**, по аналогии с однонаправленными, как правило, представляют собой комплекс из нескольких средств защиты, реализующих функции междоменного взаимодействия. В состав решений включаются два разнонаправленных комплекса решений, каждый из которых содержит, как минимум (но не ограничиваясь), следующие средства:

- МСЭ выполняет фильтрацию и организацию доступа на уровне стека TCP/IP к прокси решениям, выполняющим функции разрыва протокола (protocol break);
- Решения класса «диод данных» непосредственно реализуют изоляцию каждого из прокси решений и разрыв протокола (protocol break) со стороны взаимодействующего домена;
- Решения класса DLP, DPI, IDS и антивирусные решения выполняют проверку содержимого, в том числе, на факт наличия вложений, макросов, вредоносного кода.

Наличие двунаправленного обмена, в любом случае, повышает риски компрометации данных, нарушения целостности данных, а также риски информационной безопасности в целом. Однако, несмотря на сохранение рисков организации эффективных векторов атак на базе двунаправленного взаимодействия между доменами, данный класс решений в ряде случаев считается компромиссным как с точки зрения удобства обмена информацией, так и с точки зрения эффективности противодействия проникновения вредоносному коду при организации обмена между доменами с разными уровнями доверия.

Асинхронный обмен с применением InfoDiode

В ряде сценариев обмен через двунаправленные комплексные решения носит асинхронный, взаимно-изолированный характер, когда два контура междоменных решений передают через себя логически не связанный между собой асинхронный трафик (файлы, архивы, реплики баз данных и т.п.). В таком случае роль компонента, обеспечивающего функции DLP, DPI, IDS в междоменном решении, значительно возрастает. Функциональность «оркестратора» в таких решениях, часто выполняемая DLP и антивирусом, позволяет настраивать фильтры, обеспечивая выбор конкретного порядка действия для конкретного типа данных (передавать/не передавать, перенаправлять, санировать, удалять) и предоставляет дополнительные функции контроля передачи.



AMT GROUP

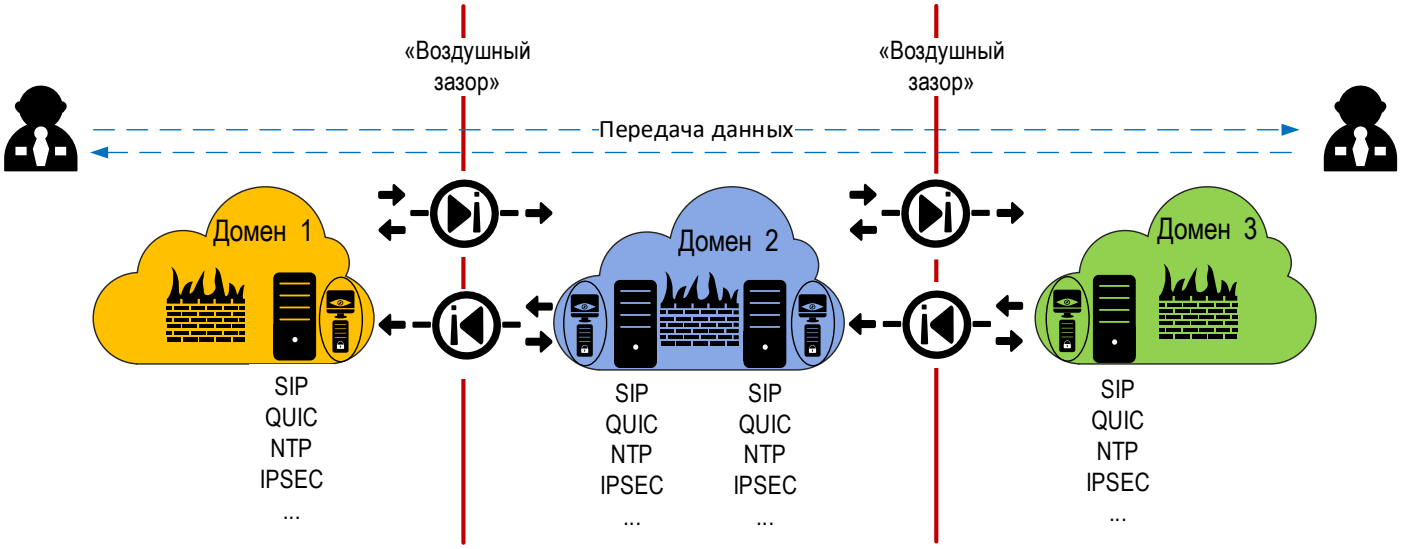
Тел: +7 (777) 2142677 Email: info@infodiode.kz

www.infodiode.kz

www.amt-group.kz

Синхронный обмен с применением InfoDiode

В других сценариях применения **InfoDiode** обмен данными носит синхронный характер для строго выделенного набора «двусторонних» протоколов обмена. В отличие от строго однонаправленного взаимодействия данный подход позволяет организовать между доменами, например, синхронизацию времени по протоколу NTP, защищенный криптографией VPN-канал на базе IPSEC, телефонию по протоколу SIP и другие виды взаимодействия, необходимые для обеспечения бизнес-процессов организации. Двунаправленный обмен в таких решениях все равно строится на базе однонаправленной компоненты, однако в таких сценариях роль компонента, обеспечивающего функции межсетевого экранирования, значительно возрастает.



InfoDiode - основа эффективного междоменного взаимодействия

Даже самая ценная информация становится бесполезной, если она не может быть оперативно получена и использована при принятии решений. Даже самая закрытая информация становится угрозой, если она недостаточно защищена от несанкционированного доступа или передается неконтролируемым образом.

Для эффективного доступа к информации и передачи информации между сетями одинакового и разного уровня доверия организациям всех уровней необходимы автоматизированные системы со встроенными «протоколами безопасности». Задача таких организационно-технических систем в общем виде может быть сформулирована как предоставление решения, которое позволяло бы **эффективно** обеспечивать доступ к данным и передавать данные между отдельными сетями/сегментами одинакового и разного уровня доверия только после прохождения ряда контролей и проверок. Фактическим решением данной задачи является организация защищенного «туннеля» между сетями/сегментами, конкретные потоки в котором формируются, одобряются и/или санируются в моменты передачи данных. В состав такого «туннеля» должны быть включены физические средства передачи, трансляторы протоколов, прикладные решения для файловой передачи (в т.ч. передачи эл. почты), сервисы интеграции, инструменты репликации баз данных и стриминга видео/рабочих столов, решения по контролю за передачей данных, решения по аудиту, оркестраторы.

Можно с уверенностью говорить, что решения **InfoDiode** выступают эффективной составной частью таких организационно–технических решений, выполняя часть функций в составе комплексных решений по междоменному обмену.

AMT GROUP

Тел: +7 (777) 2142677 Email: info@infodiode.kz

www.infodiode.kz

www.amt-group.kz