# БЕЗОПАСНОСТЬ ОБЪЕКТОВ ТЭК И ПРОМЫШЛЕННОСТИ

## Применение однонаправленных шлюзов INFODIODE

С течением времени киберугрозы, с которыми мы сталкиваемся, становятся все более изощренными. Как следствие, и применяемые средства защиты должны продолжать развиваться в соответствии с современными требованиями и тенденциями. Традиционные архитектуры систем безопасности в значительной степени построены на межсетевых экранах самых разных типов и производителей, программных системах обнаружения компьютерных атак. Однако даже самые продвинутые программные решения «пропускают» целые классы атак, которые могут приходить со стороны открытой или неконтролируемой части сети. При этом объем доли обнаруженных атак напрямую зависит от актуальности и скорости обновления базы сигнатур и угроз самой системы обнаружения.

В большинстве случаев исправление последствий компьютерных инцидентов обходится организациям исключительно дорого. Часто злоумышленники полностью достигают своих целей, которые в условиях объектов ТЭК и промышленности все чаще не ограничиваются кибершпионажем, а переходят в плоскость киберсаботажа, повреждения оборудования объектов, остановке и нарушению их технологических процессов. Такой подход к обеспечению информационной безопасности и построению систем безопасности нельзя считать приемлемым и достаточным.

### Существующие системы безопасности недостаточны для объектов ТЭК и промышленности

В течение многих лет принцип построения систем защиты на базе специализированного ПО считался стандартом. В настоящий момент это понимание изменилось. Отдельные исследования и экспертные организации фактически признают, что построение систем безопасности критических объектов только на базе межсетевых экранов и программных решений не отвечает потребностям комплексной защиты и не обеспечивает должный уровень безопасности.

# Предприятия ТЭК и промышленности – целевые объекты для осуществления наиболее критических компьютерных атак

Как правило, значимые объекты топливно-энергетического комплекса и промышленности являются одной из ключевых целей для специальных служб иностранных государств, террористов, хактивистов и других групп. Компьютерные атаки со стороны указанных групп могут приводить к повреждению оборудования, нарушению технологических процессов, гибели персонала и граждан; могут наносить значимый, в том числе непоправимый, ущерб окружающей среде и экологии.
Системы управления и промышленной автоматики критических объектов обеспечивают контроль за функционированием сложных и опасных физических процессов. Утрата такого контроля может иметь катастрофические последствия. Интуитивно понятно, что станок, турбина, генератор, холодильный агрегат, конвейер и т.п. не могут быть «восстановлены из резервной копии». Обнаружение фактов вторжений и компьютерных атак, реагирование и исправление ситуации требуют огромного количества времени и средств даже для того, чтобы просто восстановить базовое и безопасное функционирование сложного технического комплекса.

## Угрозы предприятиям ТЭК и промышленности

Многие современные сетевые атаки начинаются с того, что часть вредоносного ПО тем или иным образом оказывается в открытом сегменте сети объекта или сети, имеющей более низкий уровень безопасности/доверия. Дальнейшие шаги развития атаки заключаются в том, чтобы проникнуть в технологическую, то есть более закрытую и критическую сеть. Часто для этого могут использоваться и методы социальной инженерии (например, манипулирование сотрудниками с целью загрузки ими файлов, вложений из писем и т.п.). После попадания в технологический сегмент значимым аспектом функционирования вредоносного кода является возможность установки удаленного соединения с центром/сервером своего управления. После установки соединения злоумышленник может использовать удаленное подключение для развития компьютерной атаки внутри технологической сети и/или сбора информации.

Как только вредоносный код достаточно проникает в отдельные участки технологической сети, запускается атака, наносящая критический ущерб, который может касаться кражи информации, приводить к повреждению оборудования и прекращению функционирования объектов ТЭК и промышленности.

На практике наиболее часто встречаются следующие категории компьютерных атак:

- фишинг (отправка специальным образом сформированных электронных писем, манипулирование сотрудниками с целью получения их учетных данных, загрузки вредоносного ПО);
- взлом веб-приложений (эксплуатация уязвимостей с целью получения несанкционированного доступа в периметр защищаемых сетей);
- компрометация домен-контроллера (атака на ключевые узлы ИТ-инфраструктуры, создание фиктивных учетных записей с привилегированным доступом);
- атака через клиенты ПО (компрометация на уровне клиентского промышленного ПО, в том числе установленного у подрядчиков, поставщиков и производителей, с целью получения несанкционированного доступа к узлам технологических сетей).

Современные и хорошо спланированные компьютерные атаки относительно беспроблемно преодолевают все средства защиты в виде программного обеспечения и программно-аппаратных комплексов, в том числе межсетевые экраны, системы криптографической защиты, системы обнаружения вторжений, антивирусы, и др.

## Традиционная архитектура систем сетевой безопасности

Традиционно выстроенная архитектура сетевой безопасности, основанная на программных решениях и межсетевых экранах, базируется на заранее принятом допущении, что такие средства защиты являются высокоэффективными лишь условно, а все ПО априори имеет уязвимости, даже если о них неизвестно на данный момент. Такой подход поощряет построение системы безопасности, исходя из потребностей обнаружения компьютерных атак, поиска субъектов и объектов этих атак, их идентификации и изоляции, последующего восстановления данных из резервной копии. То есть архитектура такой системы безопасности строится на основе пассивной стратегии защиты, что в условиях функционирования объектов ТЭК и промышленности недостаточно из-за потенциально высокого масштаба ущерба. Именно поэтому в последнее время наблюдается экспертный консенсус – межсетевых экранов и программных продуктов недостаточно для защиты критических объектов от современных угроз, которые все чаще приобретают характер киберсаботажа и диверсии в отношении всего объекта ТЭК, промышленности или его значимых частей. Любая вредоносная удаленно выполненная операция в отношении оборудования критического объекта представляет собой неприемлемый риск для всего объекта.

Современный взгляд на проблему говорит о том, что важную роль в предотвращении компьютерных атак играет изменение принципа построения архитектуры системы защиты. На смену пассивной стратегии защиты приходит превентивная, предполагающая гарантированное предотвращение вторжений.

# Современные атаки требуют современных средств защиты

Наиболее важным принципом, который позволяет построить предотвращающую компьютерные атаки архитектуру, является принцип сегментации сетей. Он предполагает отделение технологической сети от сети с меньшим уровнем доверия и безопасности, например, от корпоративной сети или сети Интернет, и последующую защиту периметра технологической сети. Реализовать этот принцип позволяет использование однонаправленных шлюзов. Однонаправленные шлюзы, установленные на периметре критической инфраструктуры, не поддерживают двунаправленной связи для организации внешнего маршрутизируемого подключения, что исключает доступ через общие ресурсы и обеспечивает надежную защиту периметра информационной (автоматизированной) системы за счет сегментирования сети/информационных систем.

Однонаправленные шлюзы InfoDiode позволяют обеспечить безопасную интеграцию технологической и корпоративной сетей, а также непрерывный мониторинг функционирования технологической сети из других сегментов, в том числе возможность реагирования на инциденты со стороны служб SOC. Замена по крайней мере одного уровня межсетевых экранов однонаправленными шлюзами позволяет построить гарантированную защиту системы управления критическим объектом от компьютерных атак, исходящих из внешних сетей. При этом обеспечивается возможность мониторинга состояния и функционирования оборудования со стороны внутренних и внешних служб, в том числе, при необходимости, производителей оборудования.

Однонаправленные шлюзы обеспечивают репликацию промышленных серверов/данных, предоставляют промышленные данные для внешних корпоративных сетей. В результате применение однонаправленных шлюзов становится практически бесшовным. При этом исключаются уязвимости, которые, как правило, сопровождают построение архитектуры на основе межсетевых экранов и программных средств защиты.

## Архитектура системы защиты с использованием InfoDiode

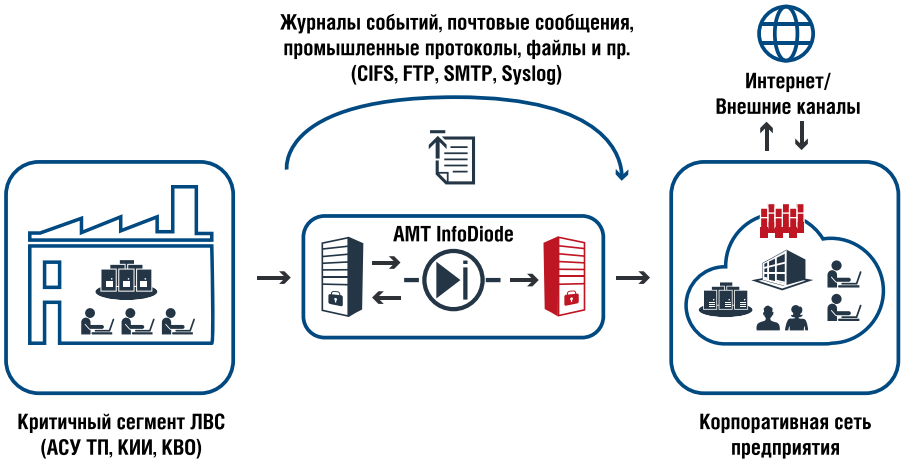
Однонаправленные шлюзы InfoDiode являются основой для построения комплексной системы защиты и обеспечения безопасности объектов ТЭК и промышленности. Шлюзы обеспечивают аппаратную защиту сетей промышленных объектов и энергетики. В однонаправленном исполнении эталонная архитектура представляет собой комплекс решений, в котором интеграция технологической и корпоративной сети реализуется только через однонаправленные шлюзы, а не через межсетевые экраны. Такая архитектура позволяет полностью исключить возможность удаленного доступа к критическому объекту.

Однонаправленные шлюзы InfoDiode представляют собой комплекс аппаратного и программного обеспечения, обеспечивающего передачу информации только в одном направлении, чаще всего из технологической сети во внешнюю/корпоративную сеть. Внешние пользователи и приложения взаимодействуют с репликами таких данных фактически в реальном времени.

За счет организации такого обмена, в том числе, минимизируются риски нарушения персоналом требований ИБ. Такие риски возникают при использовании персоналом съемных носителей, а также в случае применения относительно примитивных решений с «воздушным зазором» между технологической и корпоративной сетями вместо однонаправленного шлюза.

Предприятия ТЭК и промышленности, по-прежнему, могут выполнять сегментацию своих технологических сетей с использованием межсетевых экранов, обеспечивая их применение в сетях одного уровня доверия и критичности. При этом точки сопряжения между сетью Интернет, открытыми сетями, корпоративными и технологическими сетями защищаются однонаправленными шлюзами.

Таким образом, получая эшелонированную защиту технологической сети, предприятия ТЭК и промышленности существенно повышают свою безопасность, минимизируя возможность компьютерных атак и распространения вирусной активности из открытых сетей и сети Интернет.



# Варианты применения InfoDiode

## 1. Интеграция технологической и корпоративной сети

Наиболее распространенным способом применения однонаправленных шлюзов на объектах ТЭК и промышленности является обеспечение безопасной и эффективной интеграции технологической и корпоративной сетей. В таких случаях продукт InfoDiode, как правило, заменяет межсетевые экраны и приложения на пограничных точках между технологической и корпоративной сетями.

### Репликация баз данных и передача исторических данных

Однонаправленные шлюзы InfoDiode часто применяются для репликации различных источников данных из технологической сети предприятий в корпоративную сеть. Репликация исторических данных, доставка файлов могут быть использованы в сценариях предоставления отчетности, обмена сырыми данными и файлами, обеспечивающими сопровождение процессов отладки и мониторинга.

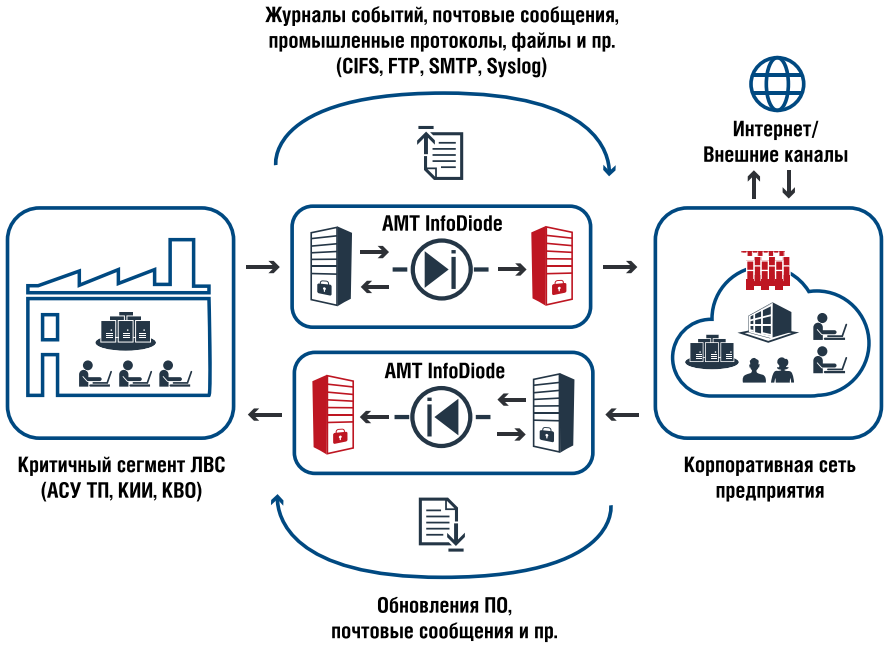
В том случае, когда в технологическом сегменте сети накапливаются данные, которые необходимо предоставлять для анализа пользователями корпоративной сети, установка однонаправленного шлюза InfoDiode обеспечивает передачу таких данных в корпоративную сеть, где соответствующие пользователи и приложения могут обращаться к ним без какой-либо угрозы для технологической сети и оборудования критической инфраструктуры.

### Получение обновлений

В том случае, когда требуется периодическое обновление антивирусных баз, программного обеспечения и получение иных обновлений и сигнатурных баз, важных для обеспечения безопасности технологической сети объекта ТЭК и промышленности, InfoDiode, установленный для передачи данных из выделенного стороннего сегмента сети в технологический (то есть в обратную сторону), обеспечивает эффективное решение этой задачи. Такое архитектурное решение снижает риски, которые возникают при использовании межсетевых экранов.

### Интеграция с программными решениями

Еще одним сценарием передачи данных через InfoDiode является передача Syslog трафика на специализированные серверы/системы безопасности. Такая передача выполняется в целях фиксации событий в SIEM системах, специализированных системах обнаружения вторжений и изменения сетевой топологии, функционирующих в рамках корпоративных SOC, NOC центров. В тех случаях, когда структура предприятия имеет филиальную структуру, решение InfoDiode может использоваться для сбора/передачи данных в головные SIEM системы и центры компетенций.

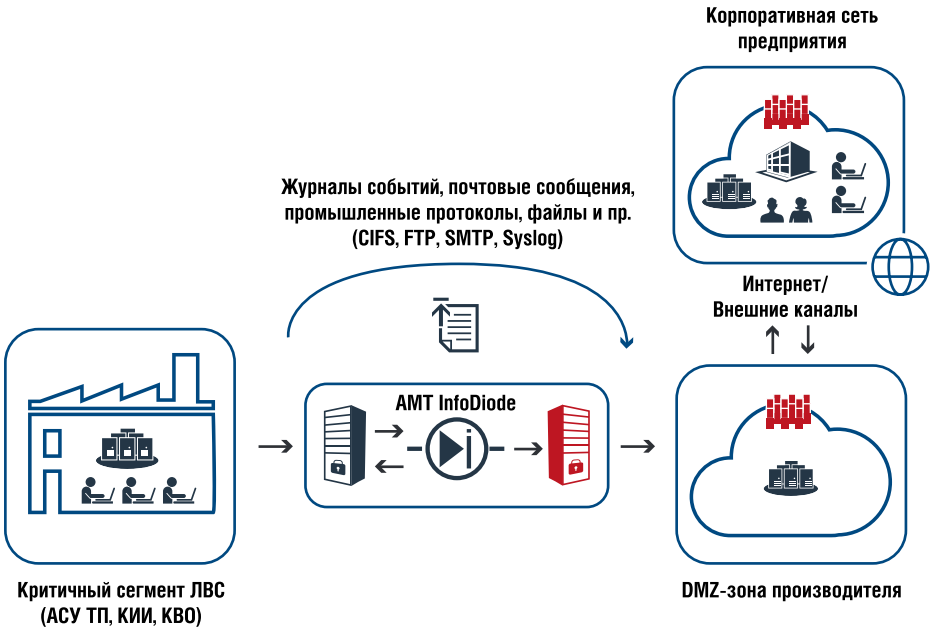



InfoDiode позволяет реализовать безопасную интеграцию технологической и корпоративной сети за счет создания полнофункциональной реплики данных в корпоративной сети, в то время как установка второго экземпляра InfoDiode в обратную сторону (внутрь технологического сегмента) обеспечивает доставку плановых обновлений антивирусных баз и программных продуктов, а также иных обновлений и баз сигнатур.

## 2. Мониторинг и контроль функционирования оборудования объекта защиты со стороны поставщиков и производителей

На значительном количестве предприятий объектов ТЭК и промышленности существует потребность в поддержке функционирующего оборудования со стороны поставщиков и производителей. Для этого, в том числе, могут использоваться специализированные средства мониторинга и диагностики, производимые самим производителем/поставщиком

Применение однонаправленных шлюзов InfoDiode решает эту задачу путем развертывания решения, которое может реплицировать серверы управления и данные из критически важного сегмента сети в сеть DMZ поставщика/производителя. DMZ подключается к центральной системе управления поставщика; чаще всего через VPN. Реплики, передаваемые в DMZ, могут являться точными копиями систем завода и обеспечивать поставщику/производителю полную прозрачность состояния оборудования.




InfoDiode позволяет поставщикам/производителям в режиме реального времени контролировать функционирование поставленного ими оборудования, проактивно принимать меры реагирования. При этом обеспечивается гарантированная защита от компьютерных атак, которые могут быть организованы из сети поставщика/производителя.

# Соответствие требованиям регуляторов

Приказ ФСТЭК от 25 декабря 2017 г. N 239 предусматривает применение мер безопасности объектов критической информационной инфраструктуры и исключение факторов, способствующих повышению уязвимости объектов КИИ. В частности, в рамках мер обеспечения безопасности значимых объектов КИИ предусматриваются меры по защите информационной (автоматизированной) системы и ее компонентов (ЗИС), включая защиту периметра информационной (автоматизированной) системы, сегментирование системы, защиту от угроз отказа в обслуживании (DOS, DDOS-атак), исключение доступа через общие ресурсы, реализацию электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек и другие.

## Двунаправленные соединения - риски для объектов КИИ

В современной терминологии сетей связи практически любое сетевое подключение к защищаемому сегменту/объекту трактуется как «двунаправленное» и чаще всего таким и является. Промежуточные звенья сети, средства защиты, дополнительное оборудование не оказывают какого-либо влияния на принципиальный, «двунаправленный», характер такого взаимодействия, вне зависимости от типа средств защиты (межсетевые экраны, маршрутизаторы, программное обеспечение и т.п.).

При этом важным аспектом двунаправленного взаимодействия остается тот факт, что оно априори несет в себе риски потери управления критическим объектом со стороны авторизованных управляющих служб/диспетчерских подразделений/служб поддержки. Это становится возможным из-за относительно высокой вероятности реализации атаки по двунаправленному каналу. Речь идет о классе управляемых атак, для эффективной организации которых необходимым условием является наличие оперативной обратной связи – обмена вида «запрос-ответ», обеспечиваемого преимущественно в рамках стека протокола TCP/IP. Помимо «стандартных» угроз прямого получения злоумышленником доступа к критическому объекту и последующего нанесения ущерба, примерами известных реализуемых угроз, в основе которых лежит двунаправленный характер информационного обмена, являются WannaCry, Petya, EternalRocks и другие.

Отдельным значимым риском для КИИ является возможность направления/загрузки чего-либо в критический сегмент: загрузка вредоносного кода, загрузка шпионского ПО и т.п. для целей мониторинга, сбора информации, нанесения отложенного ущерба.

## InfoDiode как средство решения задачи

Организация управляемых атак в случае размещения однонаправленного шлюза InfoDiode, установленного для передачи данных из некритического сегмента в критический в условиях отсутствия обратной связи, становится практически невозможной. Организация управляемых атак, в том числе таких, как DDOS, равно как и передача каких-либо данных в критический сегмент в случае размещения однонаправленного шлюза InfoDiode, установленного для передачи данных из критического сегмента в некритический, становятся полностью невозможными.

Полученные в результате использования продукта InfoDiode комплексные решения могут быть успешно применены как элемент защиты периметра объекта КИИ. При этом выгоды, достигаемые за счет соответствия требованиям регуляторов и за счет минимизации рисков, реализуемых управляемыми атаками на инфраструктуру объектов КИИ, могут достигать десятков миллионов рублей в год. Важным аспектом комплексных решений на базе InfoDiode является сохранение канала связи и сетевой связности ИТ-инфраструктуры в целом, что позволяет решать задачи передачи информации между изолируемыми сегментами сети, а также обеспечить ежедневное и эффективное функционирование бизнеса.

# Как улучшить средства и системы безопасности

Несколько лет назад межсетевые экраны были фактически единственной доступной технологией, способной защитить наиболее критические объекты сети и отделить их от корпоративной сети, сетей сторонних обслуживающих организаций и сети Интернет.

Когда на практике требовалось получить информацию с защищаемого объекта в реальном времени, единственным решением было обеспечить прямую сетевую связность, использовать межсетевые экраны и аналогичные средства защиты и верить в надежность принятых мер. Однако современные компьютерные атаки демонстрируют способность планомерно и эффективно обходить все программные средства обеспечения безопасности, в том числе межсетевые экраны.

## Решение от АМТ-ГРУП

АМТ-ГРУП предлагает однонаправленные шлюзы InfoDiode, которые обеспечивают замену межсетевым экранам и аналогичным решениям, гарантируя надежную и безопасную интеграцию технологической и корпоративной сетей. Сегодня однонаправленные шлюзы являются распространенным средством защиты, которое широко используется во всем мире. Фактически эти решения являются передовой практикой, которую рекомендуют к внедрению ведущие эксперты по информационной безопасности, регуляторы и экспертные организации. В современном мире мы, имея эффективное решение в области безопасности, доступное и на российском рынке, должны задать себе вопрос «какие из наших критических объектов должны быть настолько доступны для окружающего мира, что мы можем позволить себе защищать их только с помощью межсетевого экрана»?

Преимущества развертывания однонаправленных шлюзов для снижения рисков очевидны. Надежность и безопасность функционирования объектов ТЭК и промышленности, их оборудования подвергаются серьезному риску при реализации современных компьютерных атак.

Для реализации атак на критические объекты, защищенные однонаправленными шлюзами, хактивисты, организованные преступные группы и специальные службы иностранных государств не имеют другого выбора, кроме как пытаться преодолеть физический (и, как следствие, более контролируемый) периметр объекта. Существенная и постоянно увеличивающаяся сложность организации таких атак в сравнении с получаемыми преимуществами является причиной того, что однонаправленные шлюзы столь часто становятся рекомендуемым средством защиты, а их применение считается передовой практикой защиты периметра КИИ.