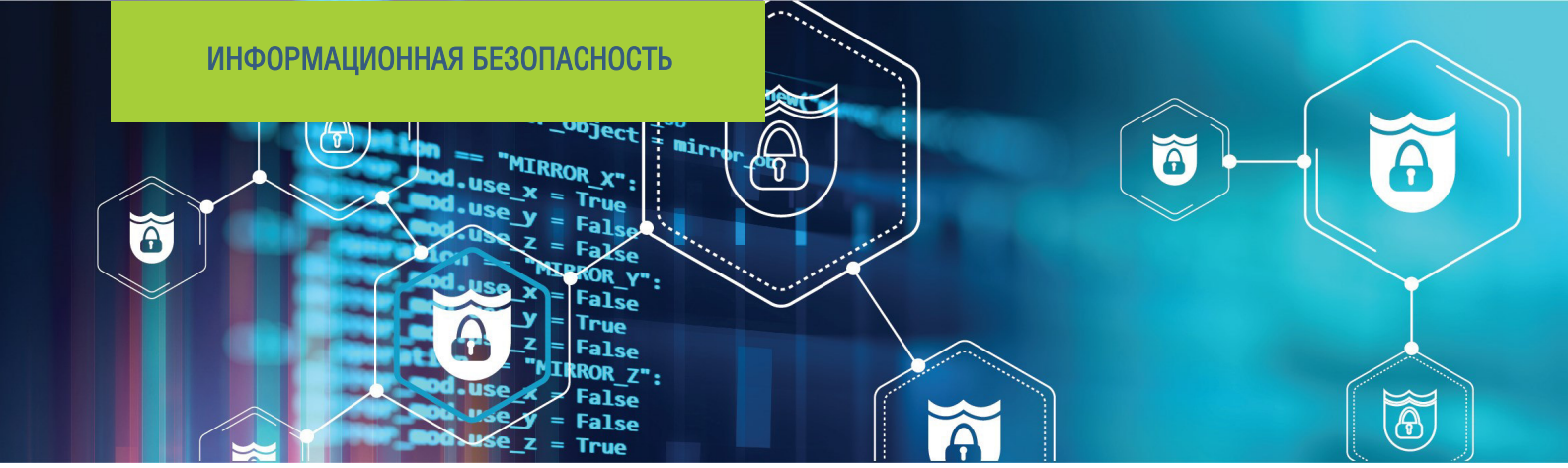


Применение PT Sandbox с однонаправленным шлюзом InfoDiode

Безопасная изолированная среда («песочница») - эффективный инструмент противодействия проникновению даже сложного вредоносного ПО в контур более доверенного сегмента из менее доверенных сегментов. Большое количество встроенных в «песочницу» механизмов позволяет обнаруживать скрытый вредоносный код в циркулирующем между сетевыми сегментами потоке данных и таким образом защитить конечную инфраструктуру более доверенного сегмента. Но для максимальной защиты наиболее критических сетевых сегментов необходимы решения, которые не только обнаруживают вредоносный код, но и предотвращают возможность удаленной эксплуатации вредоносного ПО, если оно каким-либо образом все-таки попало в защищаемый сегмент. Поэтому наибольший эффект применения «песочниц» для защиты критических сегментов достигается при их совместном применении с СЗИ для сегментации сети - физически однонаправленными шлюзами. Комплексное использование таких решений не позволяет злоумышленнику удаленно активировать вредоносный код, получить несанкционированный доступ к доверенному сегменту, закрепиться в нем, развивать атаку и одновременно дает специалистам ИБ мощные инструменты анализа входящего трафика.

Примерами комплексных решений «песочница» и однонаправленный шлюз являются междоменные решения на базе продукта **InfoDiode** и продвинутых средств детектирования PT Sandbox. Сопряжение сегментов, имеющих разный уровень доверия, однонаправленным каналом исключает возможность воздействия злоумышленника на защищаемый сегмент за счёт разрыва двунаправленных протоколов, а использование изолированной среды (песочницы) позволяет всесторонне и комплексно контролировать файловый поток, проводя статический, динамический и другие виды анализа, что обеспечивает комплексную защиту доверенного сегмента от целенаправленных атак и массовых угроз.

PT Sandbox («песочница») – это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности, позволяющий обнаруживать новые вирусы, эксплойты нулевого дня, программы-вымогатели и другое сложное вредоносное ПО.

InfoDiode – продукт, построенный на принципах однонаправленной передачи данных и позволяющий обеспечить эффективную защиту доверенного сегмента. Технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, обеспечивают возможность передачи данных в одном направлении и нивелируют риски эксплуатации злоумышленником двунаправленного канала для организации атаки.

Результаты комплексного тестирования подтвердили эффективное совместное применение комплекса **InfoDiode** и программного комплекса PT Sandbox в сценариях передачи данных из внешней сети в сеть доверенного сегмента. Таким образом, обеспечивается изоляция более доверенного сетевого сегмента с сохранением возможности импорта данных из внешних источников.

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

06.10.2025

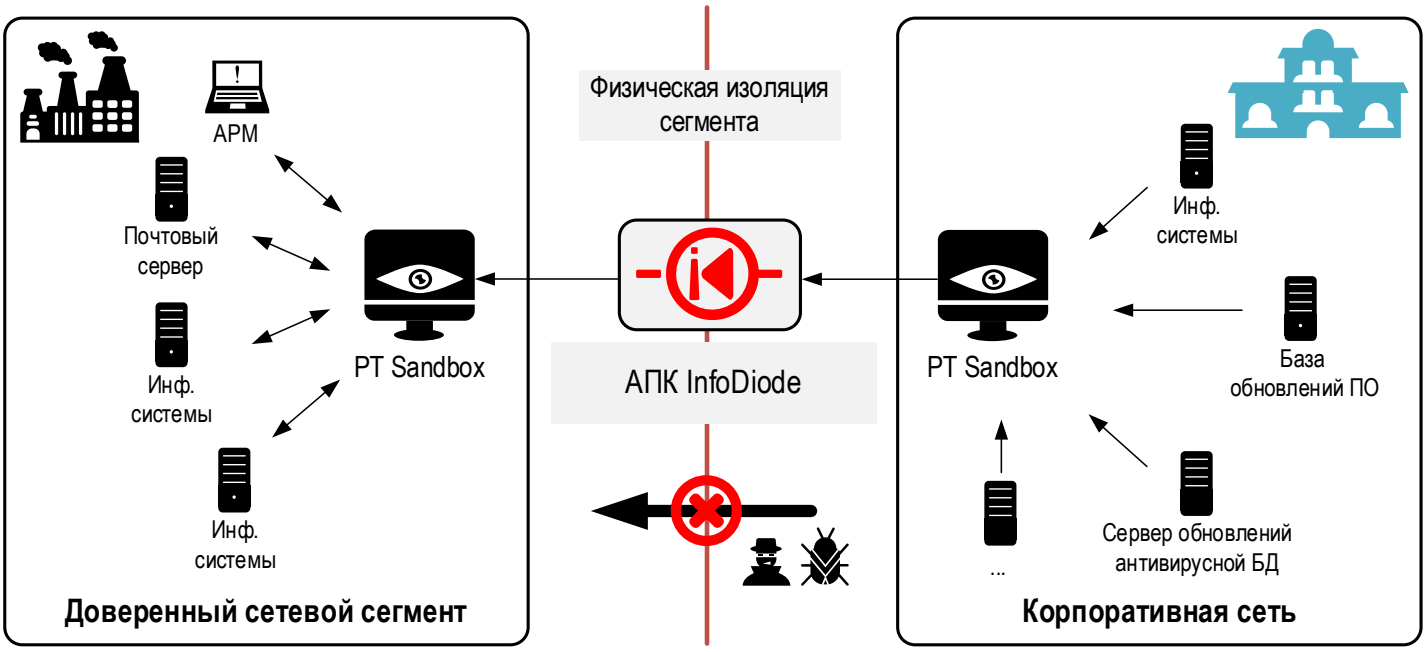
Сценарий передачи файлов в более доверенные сетевые сегменты

На практике использование комплекса однонаправленной передачи данных **InfoDiode** и программного комплекса PT Sandbox предполагает передачу файлового потока в более доверенный сегмент из менее доверенного сетевого сегмента в несколько этапов:

1. Сначала файлы направляются пользователями, поставщиками обновлений, системами на анализ в программный комплекс PT Sandbox, где они проходит статический, динамический анализ и иные исследования.
2. В случае отсутствия в направленных файлах вредоносного кода или других деструктивных признаков, файлы передаются на **InfoDiode,** где, в свою очередь, также проходит ряд проверок на соблюдение политик междоменной передачи.
3. После выполнения проверок на регламентное время передачи, допустимые ограничения на размер, тип файла и иные, установленные на IN стороне **InfoDiode**, данные передаются далее по однонаправленному каналу в более доверенный сетевой сегмент.
4. На выходе из **InfoDiode** файловый поток вновь подвергается проверкам на OUT стороне **InfoDiode** и только в случае их успешного прохождения передается далее.
5. В ряде случаев допускается размещение второй PT Sandbox в более доверенном сегменте, которая существенно повышает безопасность защищаемого сегмента за счет невозможности организации на нее удаленного вектора атаки и компрометации.

Совместное использование решений позволяет физически изолировать более доверенный сетевой сегмент и, таким образом, повысить его защищенность. При этом сохраняется контроль над процессом передачи файловых потоков (дистрибутивов, обновлений антивирусных баз и баз репутации, почтовых сообщений и пр.) из внешних источников.

Построение такой архитектуры серьёзно уменьшает вероятность попадания вредоносного ПО в защищаемый периметр, а в случае его проникновения, исключает возможность его эксплуатацию злоумышленником.



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

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

между системой статического и динамического анализа для выявления вредоносных объектов Positive Technologies Sandbox (далее – **«PT Sandbox»**),
разработчиком которой является
АО «Позитив Текнолоджиз»
(107061, город Москва, Преображенская пл, д. 8, помещ. 60),
в дальнейшем именуемое **«Positive Technologies»**,

и

комплексом однонаправленной передачи данных «AMT InfoDiode» (далее – **«InfoDiode»**),
правообладателем которой является
АО «АМТ-ГРУП»
(119121, Россия, Москва, Ружейный переулок, д. 6, стр. 1),
в дальнейшем именуемое «**АМТ-ГРУП**».

AMT GROUP InfoDiode positive technologies

Комплекс **InfoDiode** является системой однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется нужный уровень их функциональности для взаимодействия со смежными информационными системами.

PT Sandbox – это программный комплекс, предназначенный для проверки файлов и электронных писем на предмет угрозы информационной безопасности (песочница), позволяющий обнаруживать новые вирусы, эксплойты нулевого дня, программы-вымогатели и другое сложное вредоносное ПО. PT Sandbox не только детектирует угрозы, но и не допускает их проникновение в контур пользователя, обеспечивая комплексную защиту от целенаправленных атак и массовых угроз.

«АМТ-ГРУП» и **«Positive Technologies»** настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

«АМТ-ГРУП» и **«Positive Technologies»** провели всесторонние тесты **PT Sandbox (начиная с версии 5.23)** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

Файловый поток, передаваемый из менее доверенного сетевого сегмента, анализируется в **PT Sandbox** с помощью технологий машинного обучения статическим и динамическим методом, а также проходит проверку несколькими антивирусами, и в случае отсутствия в нём вредоносного кода или других деструктивных файлов передаётся на **InfoDiode** и далее через него по однонаправленному каналу в более доверенный сетевой сегмент.

Результат тестирования:

подтверждена полная совместимость продуктов в заявленном сценарии использования. Продукты могут использоваться совместно в указанном сценарии с учетом их индивидуальных системных требований.

АО «АМТ-ГРУП»

12 августа 2025 года

Технический директор

Подпись _____

(Е.В. Молчанов)

АО «Позитив Текнолоджиз»

12 августа 2025 года

Директор по продуктам

Подпись _____

(П.В. Мкртычян)