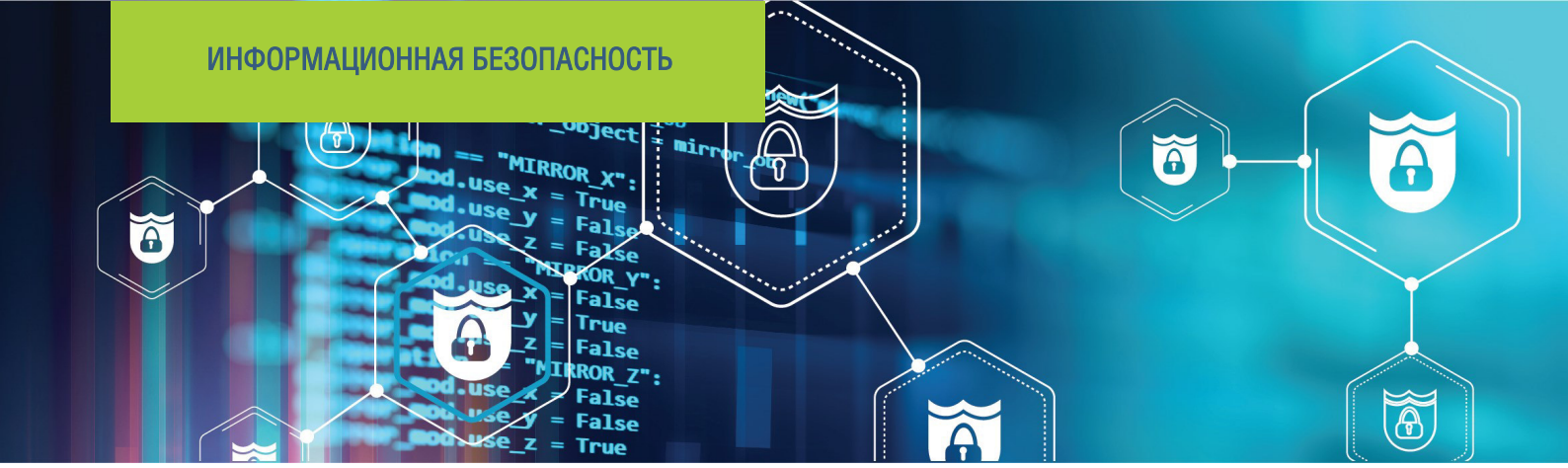


Применение AVSOFT ATHENA с однонаправленным шлюзом InfoDiode

Файловый поток, который циркулирует между сегментами с разным уровнем доверия, может представлять риски для критически важного сегмента. Одной из угроз такого обмена является возможность проникновения вредоносного кода в защищаемый сегмент вместе с файлами. Эффективным методом для определения, является ли файл вредоносным, без воздействия на реальную инфраструктуру является использование безопасных изолированных сред (песочниц).

Однако, когда на границе сегментов используются только программные средства межсетевого экранирования, существует риск, что даже в случае использования средств детектирования, вредоносное ПО всё же может проникнуть за границу защищаемого сетевого периметра. В таком случае злоумышленник, используя удаленные возможности по его активации и управлению, может получить несанкционированный доступ к доверенному сегменту, закрепиться в инфраструктуре и развить атаку. Поэтому для защиты критических сетевых сегментов необходимы решения, которые не только обнаруживают вредоносный код в файловом потоке, но и предотвращают возможность удаленной эксплуатации вредоносного ПО, попавшего в защищаемый сегмент.

Такими решениями являются комплексные междоменные решения на базе продукта **InfoDiode** и эффективные средства детектирования AVSOFT ATHENA. 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.

AVSOFT ATHENA – система защиты от целенаправленных атак, работает на базе технологий антивирусного мультисканера и песочницы и способна проверять файлы и ссылки множеством инструментов статического и динамического анализа с высокой скоростью.

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 системы защиты от целенаправленных атак AVSOFT ATHENA 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

26.03.2025

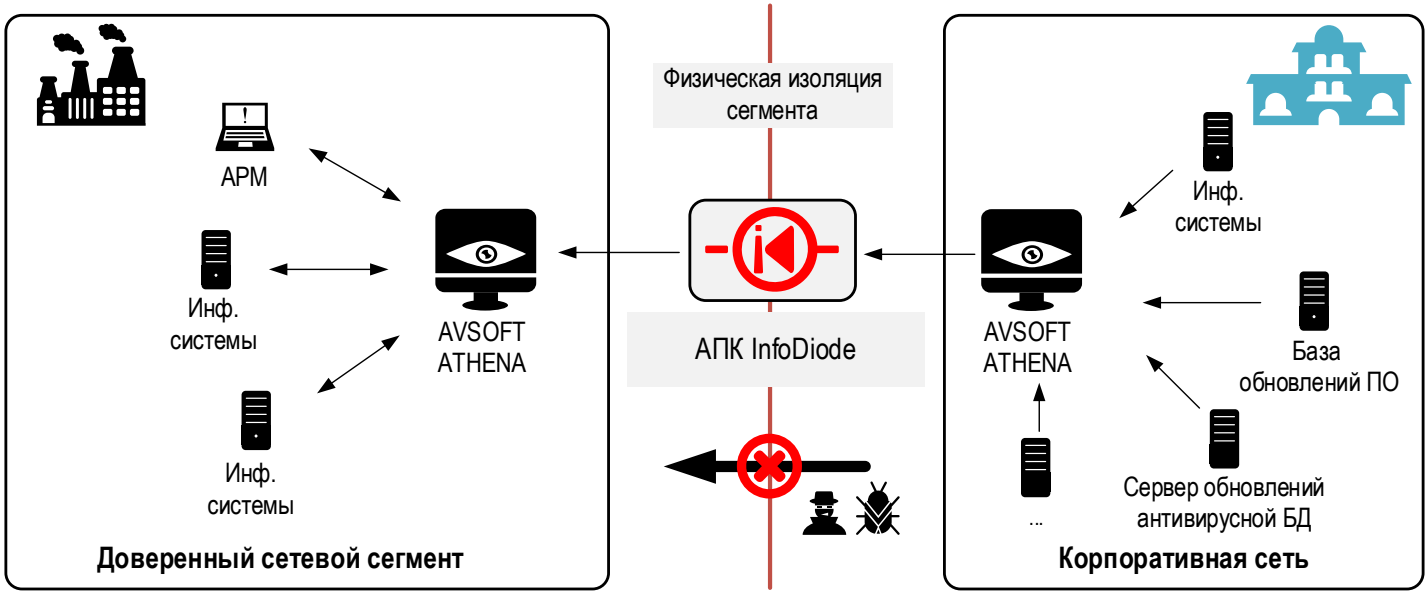
Сценарий передачи файлов в более доверенные сетевые сегменты

На практике использование комплекса однонаправленной передачи данных **InfoDiode** и системы защиты от целенаправленных атак AVSOFT ATHENA 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 систему AVSOFT ATHENA, 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. В случае 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 AVSOFT ATHENA, 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 ограничивает попадание 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 защиты от целенаправленных атак

«AVSOFT ATHENA»

правообладателем которой является

ООО «АВ Софт»

(127106, г. Москва, Гостиничная ул., д. 5, э 4 п I ком 27 оф 1-410)

в дальнейшем именуемыми **«AVSOFT ATHENA»** и **«АВ Софт»** соответственно

и

Комплексом однонаправленной передачи данных

«AMT InfoDiode»,

являющийся продукцией компании

АО «АМТ-ГРУП»

119121, Россия, Москва, Ружейный переулок, д. 6, стр. 1

в дальнейшем именуемыми **«InfoDiode»** и **«АМТ-ГРУП»** соответственно

AMT GROUP -Diode info

AVSOFT

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.

AVSOFT ATHENA – система защиты от целенаправленных атак, работающая на базе технологий антивирусного мультисканера и песочницы. Система способна проверять файлы и ссылки множеством инструментов статического и динамического анализа с высокой скоростью.

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

«АМТ-ГРУП» и **«АВ Софт»** провели всесторонние тесты **AVSOFT ATHENA** в сетях передачи данных с разграничением доступа на базе **InfoDiode** в следующем сценарии:

- Файловый поток, передаваемый из менее доверенного сетевого сегмента, проходит статический и динамический анализ в системе **AVSOFT ATHENA** 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

Результаты тестирования:

- продукты могут использоваться совместно в указанном сценарии, с учетом их индивидуальных системных требований;
- подтверждена полная совместимость продуктов в заявленном сценарии использования.

АО «АМТ-ГРУП»

27 февраля 2025 года

Технический директор

Подпись_____

(Б.В. Молчанов)

ООО «АВ Софт»

27 февраля 2025 года

Генеральный директор

Подпись _____

(А.П. Чухнов)