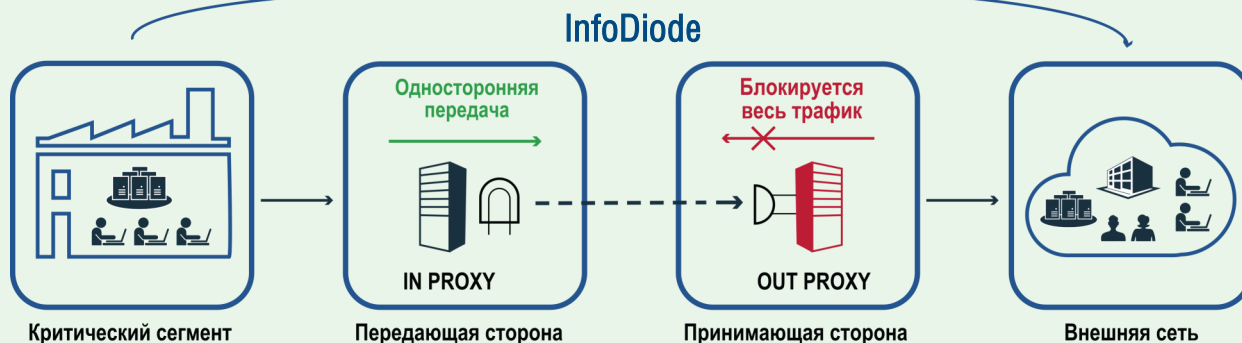




Реализована конструктивно и на аппаратном уровне, невозможно «включить» обратный канал

Не зависит от конфигурации. Ошибка в конфигурации не приводит к нарушению функции безопасности, данные всегда передаются в одном направлении

Эксплуатация уязвимостей не приводит к нарушению функции безопасности, данные всегда передаются в одном направлении

Никакие программные техники не позволяют передавать данные в обратном направлении

Невозможны, что гарантированно защищает от удаленного несанкционированного доступа или сканирования сети

Реализация функции безопасности

Зависимость от корректной конфигурации

Влияние уязвимостей на функцию безопасности

Обход функции безопасности

Использование двунаправленных соединений

Реализована на программном уровне, блокировка соединений реализована в программном обеспечении, можно разрешить нелегитимное соединение

Зависит от конфигурации. Ошибка в конфигурации может привести к нелегитимному или запрещенному политиками соединению

Эксплуатация уязвимости может привести к компрометации и нелегитимному или запрещенному политиками соединению

Возможны уязвимости к специальным техникам сетевых атак: фишинг, шифрование трафика, туннелирование и др.

Возможны, могут использоваться не только для штатного взаимодействия между системами, но и для организации атаки

Программные СЗИ сегментации сети



Критический сегмент

Разрешенный трафик →

Запрещенный трафик ✗

Разрешенный трафик ←

FIREWALL	
POLICY	
ANTIVIRUS	
FILTERING	
IPS/IDS	
VPN	
SANDBOX	
WAF	

Разрешенный трафик →

Запрещенный трафик ✗

Разрешенный трафик ←



Внешняя сеть



Программные «диоды данных»

Программное ограничение передачи данных в обратном направлении. Функция безопасности зависит от программной конфигурации. Уязвимости «нулевого дня» могут нарушить функцию безопасности. Передача двунаправленного трафика возможна в определенных режимах.

Многофункциональные межсетевые экраны уровня сети

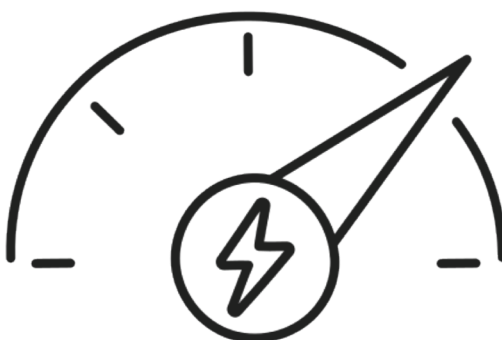
Программное ограничение соединений по таблице правил. Возможны ошибки в конфигурации, вероятно наличие уязвимостей «нулевого дня».

Может включать в себя функции других СЗИ (антивирус, DLP, криптошлюз). Возможно взаимодействие по двунаправленным протоколам.

Классические межсетевые экраны

Программное ограничение соединений по таблице правил. Возможны ошибки в конфигурации, вероятно наличие уязвимостей «нулевого дня». Требуется дополнительных СЗИ для нейтрализации иных угроз.

Возможно взаимодействие по двунаправленным протоколам.



Защита сетевого сегмента

InfoDiode (аппаратные «диоды данных»)

Гарантированное (конструктивное) ограничение передачи данных в обратном направлении. Функция безопасности не зависит от программной конфигурации. Уязвимости «нулевого дня» не позволяют нарушить функцию безопасности. Передача двунаправленного трафика невозможна, только проксирование в однонаправленном режиме.

«Воздушный зазор»

Гарантированная изоляция сетевого сегмента.

Невозможно никакое взаимодействие с изолированным сегментом, что может быть недопустимо для нормального функционирования предприятий и организаций. Большие накладные расходы на обмен информацией.

Как выбрать эффективное средство защиты сетевых сегментов критической инфраструктуры?

- СЗИ должно иметь сертификаты профильных регуляторов, а его применение должно соответствовать требованиям действующих нормативных актов и требованиям в области ИБ, включая модель угроз и нарушителя и внутренние организационно-распорядительные документы. В частности, для защиты значимых КИИ высоких категорий требуется наличие сертификата ФСТЭК соответствующего уровня доверия, например УД4.
- СЗИ должно быть обеспечено гарантийной и технической поддержкой в соответствии с требованиями законодательства. Следует убедиться в наличии у производителя сети сервисных партнеров и/или дистрибуторов. Немаловажным критерием является наличие у производителя опыта применения СЗИ в различных отраслях промышленности и наличие решений с технологическими партнерами в различных отраслях. Целесообразно убедиться, что производимое СЗИ не единично. Как правило, серьезный производитель поддерживает линейку и/или версионирование своих решений.
- В случае выбора средства для изоляции сетевого сегмента (например, сегмента АСУ ТП, хранилища данных) следует иметь в виду, что гарантированную изоляцию могут обеспечить только те СЗИ, которые реализуют функции безопасности на физическом уровне, то есть с применением физических принципов гальванической и оптической развязки сетевых сегментов. Именно при такой реализации гарантируется полная изоляция сетевого сегмента.
- СЗИ должно уметь проксировать трафик значительного количества прикладных, в том числе промышленных, протоколов. Разрыв протоколов защищает изолированный сегмент от деструктивного воздействия, в том числе с использованием уязвимостей сетевых протоколов.
- СЗИ должно иметь интерфейсы взаимодействия с профильными СЗИ для нейтрализации угроз других классов, таких как вирусное заражение, утечка данных, перехват сетевого трафика. СЗИ должно представлять данные о своем состоянии для мониторинга и передавать события во внешние ИБ системы, например SIEM, для контроля состояния безопасности.