InfoDiode: эффективная защита сетей в финансовой отрасли

Наиболее разрушительные современные атаки на финансовый сектор имеют целенаправленный и многоступенчатый характер. Начиная с проникновения в сетевую инфраструктуру организации через одну уязвимую точку, злоумышленники распространяют свой контроль на критически важные системы в других сетевых сегментах. Ключевыми целями для злоумышленников являются:

- Вывод денежных средств с банковских или корреспондентских счетов финансовой организации, для чего злоумышленнику необходимо проникнуть в сегмент размещения АРМ дистанционного банковского обслуживания (АРМ ДБО) с банками-корреспондентами или сегмент АРМ клиента Банка России (АРМ КБР).
- Похищение персональных данных клиентов, информации о счетах, деталей финансовых операций, инсайдерской и другой информации, хранящейся во внутренних ИТ-системах, для чего злоумышленнику необходимо проникнуть в сегмент продуктивных систем или хранилище данных.
- Шифрование критической информации организации или парализация работы ИТ-систем с целью получения выкупа, для чего злоумышленнику необходимо проникнуть в сегмент продуктивных систем, сегмент АРМ пользователей или хранилище данных.
- Получение доступа к АРМ руководителей организации для дальнейшего применения социальной инженерии с целью получения выгоды, для чего злоумышленнику необходимо проникнуть в сегмент АРМ пользователей.
- Остановка деятельности и отказ в обслуживании ИТ-систем организации с целью нанести максимальный ущерб организации, для чего злоумышленнику необходимо проникнуть в сегмент продуктивных систем.

Успех любого из вышеприведенных сценариев является для финансовой организации крайне болезненным и приводит если не прямым финансовым потерям, то, как минимум, к упущенной прибыли или репутационному ущербу. Снижения уровня безопасности при взаимодействии между сегментами напрямую связано возможностью двунаправленного сетевого подключения к критичным системам из менее доверенных сегментов.

Двунаправленное взаимодействие несет в себе риски реализации атак по двунаправленному каналу, то есть управляемых атаках, для организации которых необходимое условие - наличие оперативной обратной связи (обмен вида «запрос-ответ»). Такой обмен обеспечивается преимущественно в рамках стека протокола TCP/IP. Примеры известных реализуемых угроз, в основе которых лежит двунаправленный характер информационного обмена — WannaCry, Petya, EternalRocks, Remote Access Trojan (RAT) и другие.

Поэтому одним из наиболее эффективных способов не допустить распространения атаки по сети организации является надежная сегментация сети, то есть выделение в сетевой инфраструктуре критических сегментов (сегменты АРМ КБР, АРМ ДБО, продуктивных систем, хранилища данных и других) с их последующей гарантированной изоляцией.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Взгляд регуляторов на защиту сетей организации

Свой вклад в обеспечение безопасности финансовых организаций вносят регуляторы финансового сектора и некоммерческие организации, занимающиеся стандартизацией вопросов защиты информации. В России регулятором финансового сектора является Центральный банк Российской Федерации (Банк России), который отвечает за регулирование и контроль (надзор) за обеспечением информационной безопасности, киберустойчивости и применением информационных технологий в отношении финансовых организаций. Аналогичным регулятором в США, координирующим, в том числе, вопросы безопасности финансовых организаций, является Министерство торговли США, включающее подведомственный Национальный институт стандартов и технологий США (NIST). Среди некоммерческих организаций стоит выделить Центр безопасности Интернета (CIS), создавший несколько популярных фреймворков по повышению уровня безопасности и его оценке, которые широко применяются в финансовых организаций по всему миру. В регуляторных требованиях, стандартах и иных рекомендациях всех вышеуказанных организаций большое внимание уделено безопасности сетей и контролю взаимодействия между различными сегментами. Среди наиболее приоритетных аспектов сетевой безопасности стоит выделить разделение сети организации на сетевые сегменты различной критичности, изоляцию критических сегментов от «недоверенных сегментов»: сети Интернет, сегментов, имеющий доступ в Интернет, сегментов разработки и тестирования, контроль за взаимодействием между сегментами, ограничение используемых протоколов, портов.

Подходы к сегментации сети финансовой организации

Для решения задачи сегментации сети финансовой организации, а также разграничения сетевых сегментов различной критичности, применяется несколько подходов.

Первым подходом является физическая изоляция, то есть разделение сегментов сети между собой «воздушным зазором». Несмотря на то, что такой поход гарантирует изоляцию сегмента и допускает перемещение данных между сегментами только с использованием учтенных съемных носителей, в современной инфраструктуре финансовой организации он практически не применим. Финансовый сектор является одним из наиболее развитых с точки зрения цифровизации бизнес-процессов, что приводит к невозможности использования съемных носителей информации в условиях значительных объемов циркулирующей информации, провоцирует эксплуатирующий персонал на создание скрытых соединений между сегментами и использование неучтенных носителей информации.

Другой подход — межсетевое экранирование. Современные межсетевые экраны успешно справляются с задачей сегментации сети, но имеют существенный недостаток, не позволяющий рассматривать их как единственное и универсальное решение: фильтрация сетевого трафика производится на программном уровне, и в случае компрометации самого межсетевого экрана (например, в результате ошибок при его конфигурации или уязвимостям платформы, на которой он развернут) злоумышленник может свободно организовать доступ в другой сетевой сегмент.

Альтернативным взглядом на проблему является внедрение устройств однонаправленной передачи данных **InfoDiode,** который устраняет указанные выше ограничения, сохраняя возможность передачи данных между сегментами сети в

Линейка решений InfoDiode

В качестве решения предлагается использовать **InfoDiode**. Линейка решений **InfoDiode** гарантированно разделяет критические сегменты сети на физическом уровне модели OSI, сохраняя при этом возможность однонаправленной передачи информации из одного сегмента в другой. Для передачи данных за границы защищаемого периметра решения **InfoDiode** поддерживают работу по следующим протоколам:

- протоколы файлового обмена (CIFS, FTP/FTPS, SFTP);
- протокол передачи почты SMTP;
- протоколы, использующие в качестве транспорта UDP (SNMP trap, Syslog, Netflow и др).

Продукты **InfoDiode** включают в себя аппаратные (АК) и аппаратно-программные (АПК) комплексы, решения в различных форм-факторах (настольный, DIN-рейка, RACK), решения в отказоустойчивых конфигурациях.

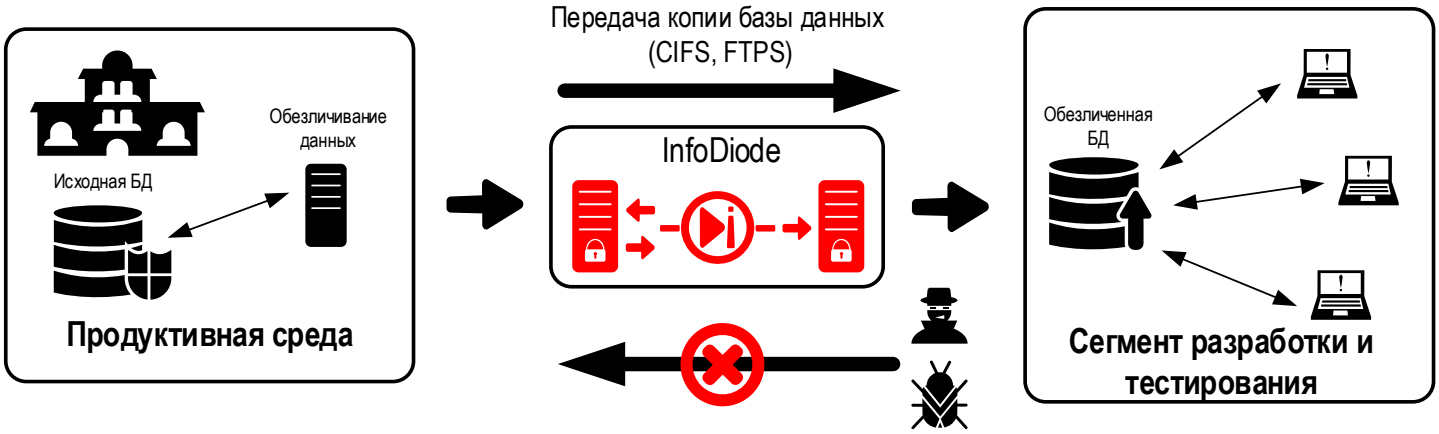
Решения **InfoDiode** имеют сертификат ФСТЭК УД4 и проходят регулярный контроль на соответствие стандартам безопасности.

Предлагается комплексная техническая поддержка решений в различных и удобных клиентам режимах: 8x5 или 24x7, ЗИП или ремонт оборудования, выезд технического специалиста для ремонта и др.

В настоящей брошюре приведены типовые сценарии применения **InfoDiode** в финансовом секторе. В том числе дополнительно указано, как построение взаимодействия между различными сетевыми сегментами с использованием **InfoDiode** позволяет обеспечить надежную защиту критических сегментов и реализовать меры защиты стандартов.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 1. Безопасная передача тестовых данных из продуктивного сегмента сети в сегмент разработки и тестирования



Задача: Реализовать возможность передачи данных продуктивной среды, которые необходимы разработчикам систем финансовой организации или аналитических моделей, в выделенный контур разработки и тестирования. Данный процесс реализуется путем создания резервной копии базы данных (полной или части), её полного или частичного обезличивания и развертывания в другом контуре безопасности — среде разработке и тестирования.

Ключевые меры защиты информации российских и международных стандартов:

ГОСТ Р 57580.1-2017. СМЭ.6 — Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации АС, в том числе тестирования ПО и объектов доступа.

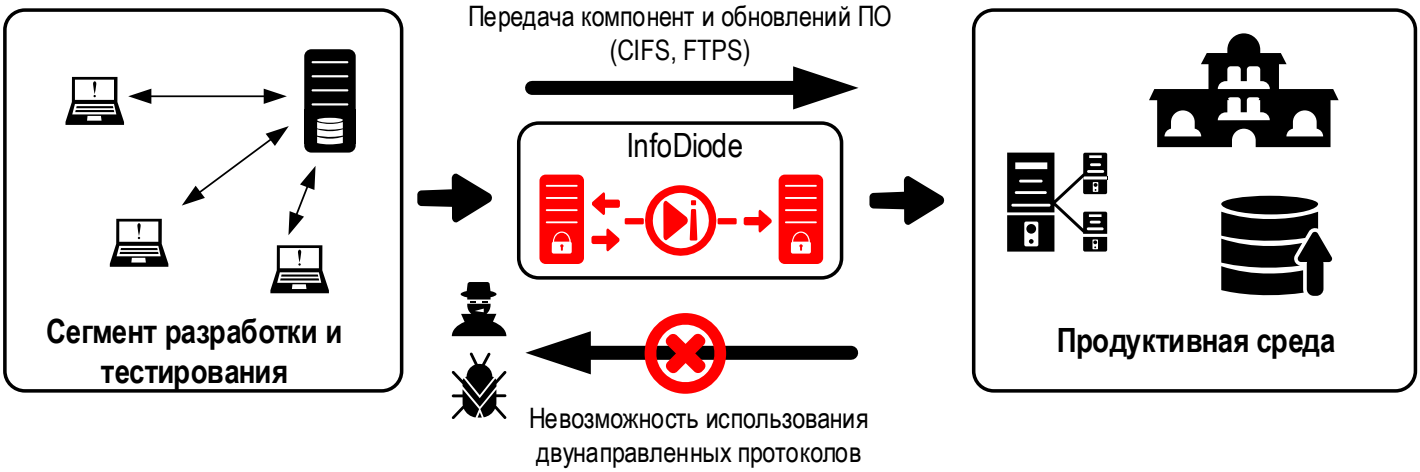
ГОСТ Р 57580.1-2017. СМЭ.7 — Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования.

CIS Critical Security Controls. 16. Безопасность прикладного программного обеспечения. 16.8 Разделение производственных и непроизводственных систем — Поддерживать отдельные среды (сетевые сегменты) для производственных (продуктивная среда) и непроизводственных (среда разработки и тестирования) систем.

Решение: Процесс переноса тестовых данных в среду разработки и тестирования может быть полностью автоматизирован без снижения уровня безопасности продуктивной среды: резервная копия базы данных после обезличивания передается в среду разработки с использованием АПК InfoDiode PRO по однонаправленному каналу. При этом исключается риск атаки на продуктивные системы в случае компрометации среды разработки и тестирования или несанкционированных действий работников организации.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 2. Передача компонент и обновлений программного обеспечения в продуктивный сегмент сети



Задача: Отделить сегмент разработки и тестирования программного обеспечения, который может включать в себя также сегмент взаимодействия с подрядчиками/вендорами, от продуктивной среды финансовой организации и при этом обеспечить возможность передачи дистрибутивов и образов программного обеспечения в продуктивный контур.

Ключевые меры защиты информации российских и международных стандартов:

ГОСТ Р 57580.1-2017. СМЭ.6 — Выделение в вычислительных сетях финансовой организации отдельных сегментов (групп сегментов), предназначенных для размещения информационной инфраструктуры, используемой только на этапе создания и (или) модернизации АС, в том числе тестирования ПО и объектов доступа.

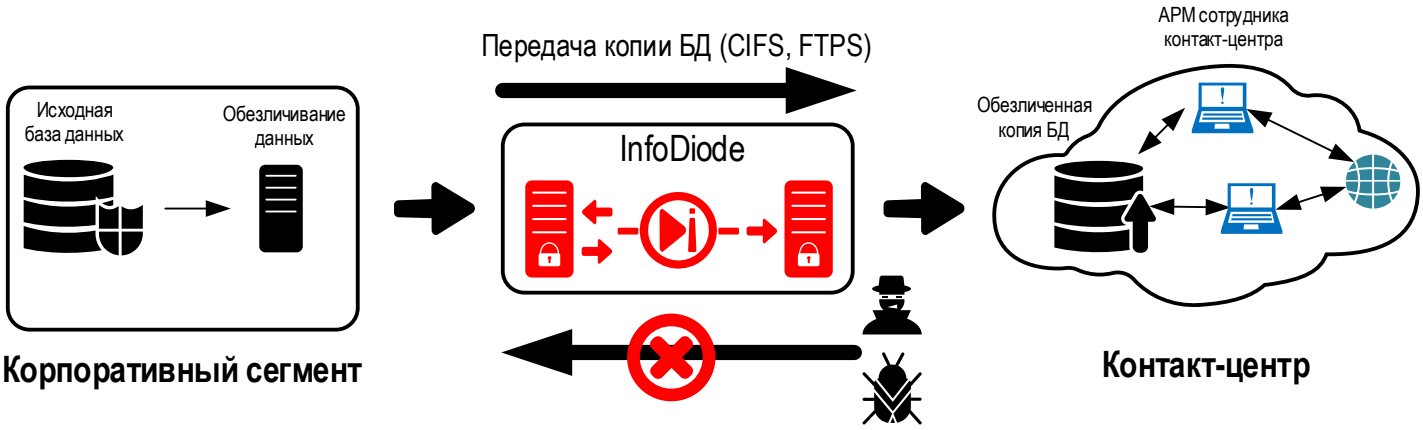
ГОСТ Р 57580.1-2017. СМЭ.7 — Реализация запрета сетевого взаимодействия сегмента разработки и тестирования и иных внутренних вычислительных сетей финансовой организации по инициативе сегмента разработки и тестирования.

CIS Critical Security Controls. 16. Безопасность прикладного программного обеспечения. 16.8 Разделение производственных и непроизводственных систем — Поддерживать отдельные среды (сетевые сегменты) для производственных (продуктивная среда) и непроизводственных (среда разработки и тестирования) систем.

Решение: После успешного тестирования программного обеспечения в среде разработки и тестирования доставка файлов компонент или обновлений в продуктивный сегмент сети осуществляется через интегрированный с конвейером CI/CD АПК InfoDiode PRO по однонаправленному каналу. При этом за счет однонаправленной передачи данных на физическом уровне InfoDiode делает невозможным работу двунаправленных протоколов взаимодействия, что не минимизирует риск атаки на продуктивные системы в случае компрометации АРМ разработчиков организации или подрядчиков или их несанкционированных действиях.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 3. Исключение воздействия со стороны АРМ сотрудников контакт-центра на корпоративный сегмент сети



Задача: Предоставить сотрудникам контакт-центра доступ к актуальной и частично обезличенной информации из клиентской базы финансовой организации, но гарантированно исключить любое воздействие на инфраструктуру финансовой организации со стороны сегмента контакт-центра.

Ключевые меры защиты информации российских и международных стандартов:

ГОСТ Р 57580.1-2017. СМЭ.8 — Выделение в составе сегментов контуров безопасности отдельных пользовательских сегментов, в которых располагаются только АРМ пользователей.

ГОСТ Р 57580.1-2017. СМЭ.13/СМЭ.14 — Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный)/третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет.

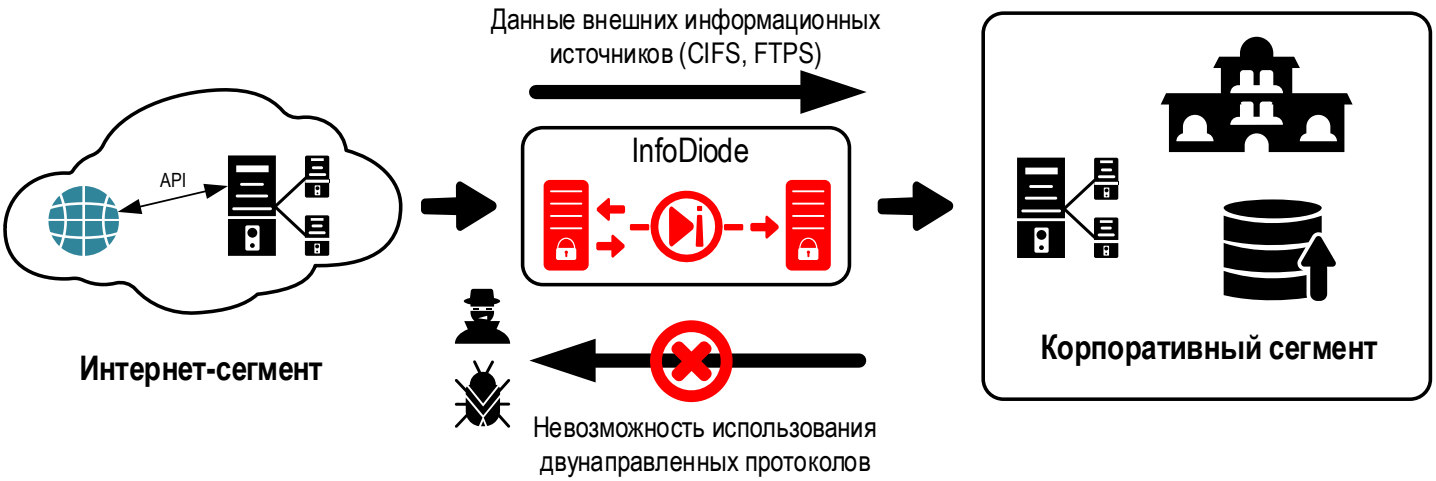
NIST SP 800-53. SC-7: Защита границ — Выделение в подсети общедоступных компонентов систем, и их отделение от внутренней сети организации.

CIS Critical Security Controls. 12. Управление инфраструктурой сети. 12.2 Создание и поддержка безопасной сетевой архитектуры — Безопасная сетевая архитектура должна, как минимум, включать в себя сегментацию сети, минимальные привилегии и доступность.

Решение: Операторы контакт-центра при коммуникации с клиентами работают с максимально обезличенной репликой информации из базы данных банка. Необходимые им данные периодически выгружаются из продуктивного сегмента организации через АПК InfoDiode PRO. Таким образом, на физическом уровне исключается возможность негативного воздействия на системы продуктивного сегмента банка со стороны АРМ операторов и сопрягаемых с ними сегментами сети.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 4. Доставка информации из внешних информационных источников в корпоративный сегмент сети



Задача: Доставить в защищаемый корпоративный сегмент финансовой организации информацию от новостных агентств (таких как Reuters, Bloomberg и др.), биржевых площадок и иных внешних источников данных, размещенных в сети Интернет. При этом необходимо минимизировать возможность несанкционированного проникновения в корпоративный сегмент через данный канал и гарантированно исключить утечку данных из сегмента.

Ключевые меры защиты информации российских и международных стандартов:

ГОСТ Р 57580.1-2017. СМЭ.13/СМЭ.14 — Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный)/третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет.

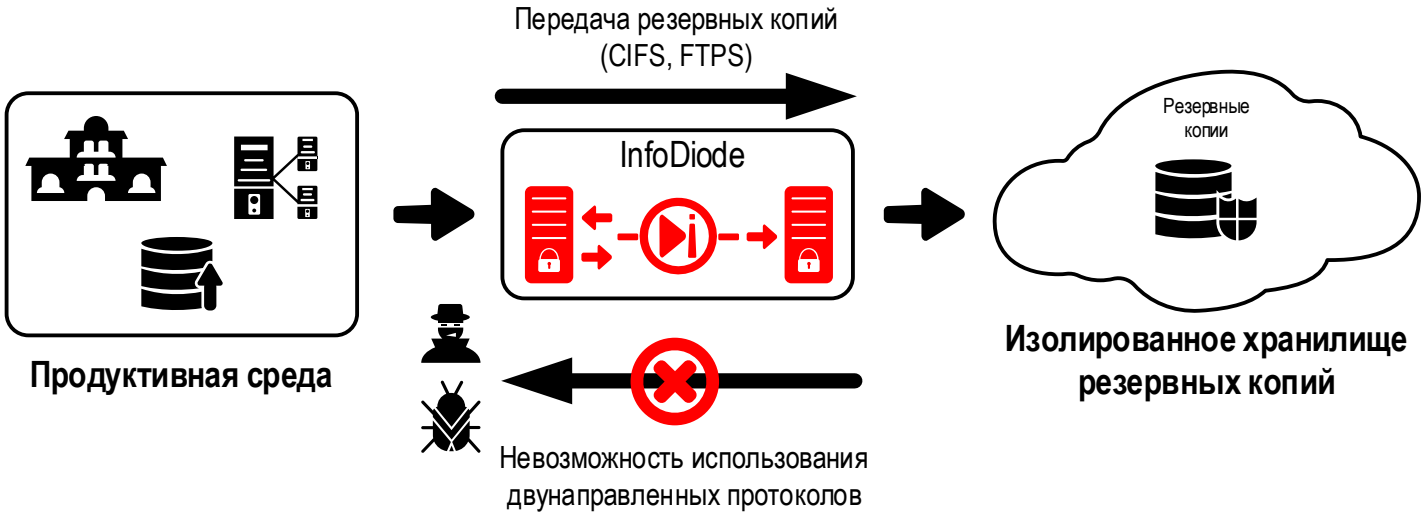
NIST SP 800-53. SC-7: Защита границ — Выделение в подсети общедоступных компонентов систем, и их отделение от внутренней сети организации.

CIS Critical Security Controls. 3. Защита данных. 3.12 Сегментирование обработки и хранения данных на основе уровня их конфиденциальности — Контроль за обработкой конфиденциальных данных в корпоративных сегментах с более низким уровнем конфиденциальности.

Решение: Размещение АПК InfoDiode PRO на границе Интернет-сегмента и корпоративного сегмента, включающего в себя АРМ аналитиков, гарантирует невозможность утечки конфиденциальной информации, сохраняя при этом возможность получения актуальной информации из внешних источников, находящихся за пределами банковской сети, а также предотвращает кибератаки, основанные на двунаправленном сетевом взаимодействии.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 5. Резервное копирование в изолированное хранилище данных



Задача: Требуется реализовать периодическое резервное копирование данных и конфигураций систем финансовой организации на случай критической ситуации и в случае возможной утери данных продуктивного сегмента. При этом необходимо отделить сегмент хранения резервных копий от остальной сети (в том числе возможны сценарии по резервному копированию в удаленный ЦОД или «облако») и гарантированно исключить воздействие на него извне.

Ключевые меры защиты информации российских и международных стандартов:

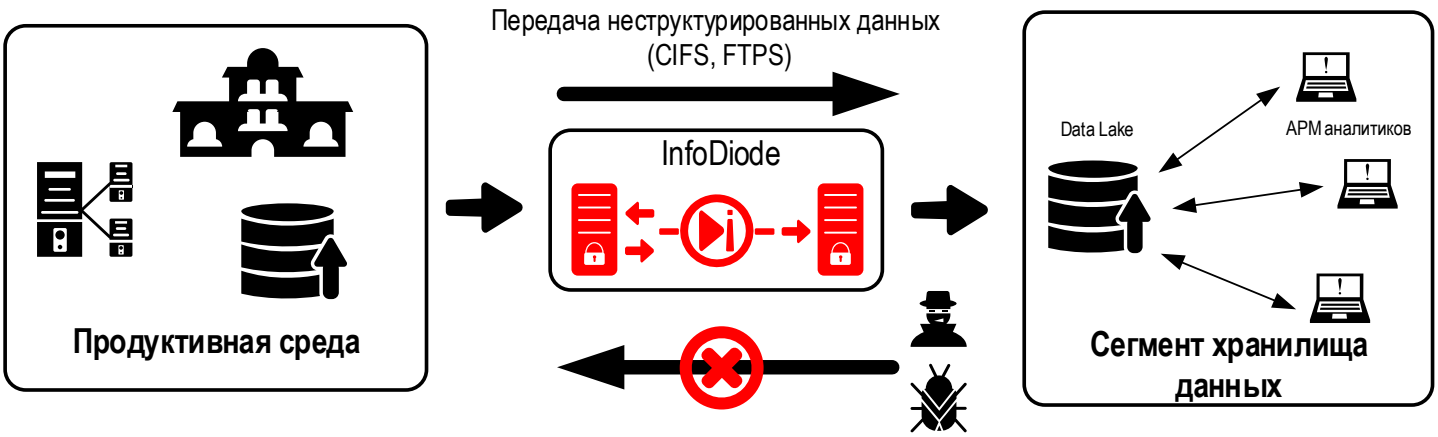
ГОСТ Р 57580.1-2017. СМЭ.10 — Выделение в составе сегментов контуров безопасности отдельных сегментов хранения и обработки данных, в которых располагаются ресурсы доступа, предназначенные для обработки и хранения данных, серверное оборудование и системы хранения данных.

CIS Critical Security Controls. 11. Восстановление данных. 11.4 Создание и поддержка изолированной копии данных резервного копирования.

Решение: Реализация процесса выгрузки резервных копий в хранилище с использованием в качестве транспорта АПК InfoDiode PRO позволяет обеспечить стабильную передачу резервных копий в хранилище и делает невозможным работу двунаправленных протоколов сетевого взаимодействия. Такой решение минимизирует риски атаки на хранилище в случае компрометации корпоративного или продуктового сегментов сети, или несанкционированных действиях работников организации.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 6. Перенос неструктурированных данных продуктивных систем в выделенный сегмент Data Lake



Задача: Процессы современной организации становятся все более датацентричными, и в доступе к данным нуждаются все подразделения компании. Одним из способов организации такого доступа является организация Data Lake. Однако создание каналов передачи данных из продуктивных систем в Data Lake открывает вектор атак на системы из контура АРМ работников организации. Необходима организация взаимодействия между всеми компонентами инфраструктуры, которая позволит обеспечить надежную передачу данных в Data Lake без снижения уровня безопасности продуктивных систем.

Ключевые меры защиты информации российских и международных стандартов:

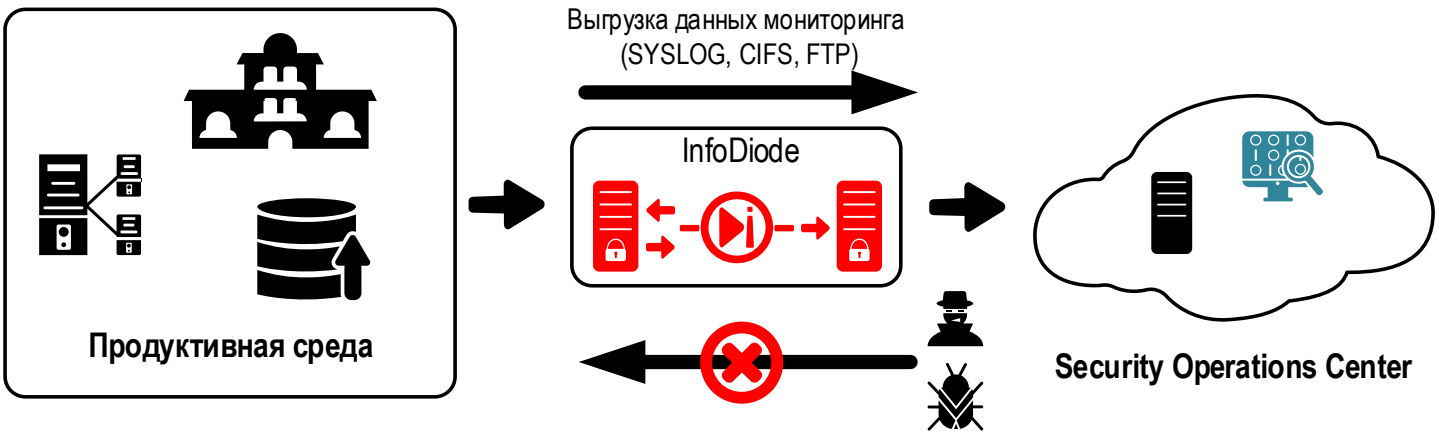
ГОСТ Р 57580.1-2017. СМЭ.10 — Выделение в составе сегментов контуров безопасности отдельных сегментов хранения и обработки данных, в которых располагаются ресурсы доступа, предназначенные для обработки и хранения данных, серверное оборудование и системы хранения данных.

CIS Critical Security Controls. 12. Управление инфраструктурой сети. 12.2 Создание и поддержка безопасной сетевой архитектуры — Безопасная сетевая архитектура должна, как минимум, включать в себя сегментацию сети, минимальные привилегии и доступность.

Решение: АПК InfoDiode PRO, размещенный на границе между продуктивным сегментом и сегментом Data Lake, к которому имеют доступ большая часть сотрудников организации, позволяет обеспечить безопасную передачу файлов и неструктурированных данных продуктивных систем в Data Lake. При этом за счет "воздушного зазора" исключается риск атаки на продуктивные системы в случае компрометации АРМ работников организации или их несанкционированных действиях.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 7. Безопасный мониторинг состояния сети и систем продуктивного контура



Задача: Реализовать возможность передачи данных мониторинга и журналов событий с использованием syslog и net-flow для анализа в Ситуационный центр информационной безопасности (SOC), расположенный в отдельной подсети финансовой организации или в «облаке». При этом необходимо ограничить возможность влияния на продуктивные системы со стороны работников SOC или в случае компрометации АРМ работников SOC.

Ключевые меры защиты информации российских и международных стандартов:

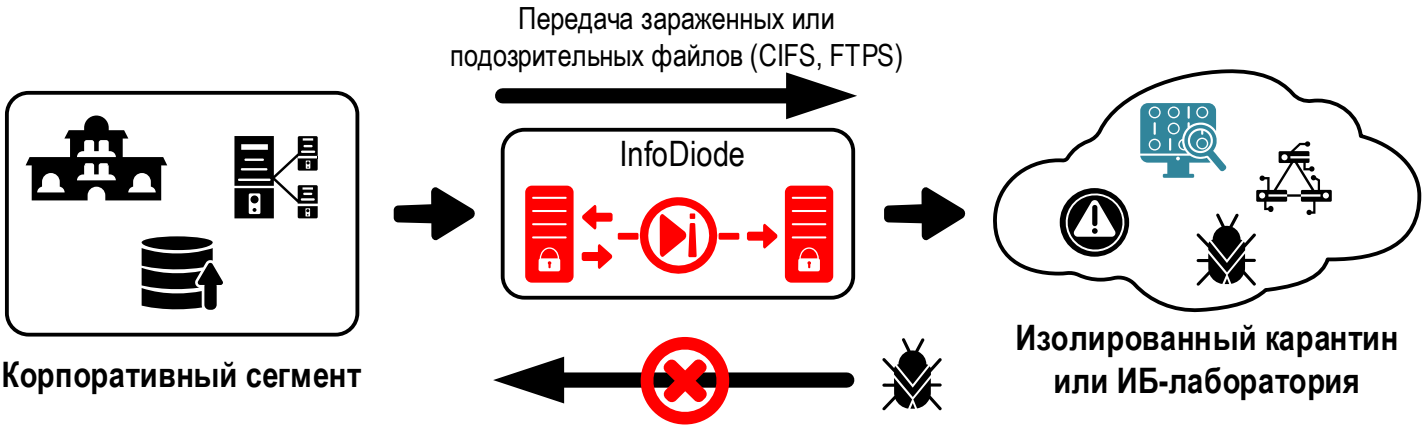
ГОСТ Р 57580.1-2017. СМЭ.4 — Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации в соответствии с установленными правилами и протоколами сетевого взаимодействия.

CIS Critical Security Controls. 12. Управление инфраструктурой сети. 12.2 Создание и поддержка безопасной сетевой архитектуры — Безопасная сетевая архитектура должна, как минимум, включать в себя сегментацию сети, минимальные привилегии и доступность.

Решение: Передача трафика для регулярного анализа специалистам безопасности через АПК InfoDiode PRO позволяет обеспечить доставку информации до целевой системы мониторинга или на файловый сервер в одностороннем порядке. При этом исключается внешнее воздействие на продуктивный сегмент сети финансовой организации, в том числе в случае, если подсеть ИБ сопрягается с внешними серверами в целях обновления продуктов ИБ, получения сигнатур вирусов, баз репутации и т.п.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

Сценарий 8. Предотвращение заражения из закрытого сегмента карантина или ИБ-лаборатории



Задача: Исключить возможность заражения продуктивной сети финансовой организации с ресурсов карантина или из сети ИБ-лаборатории, сохранив возможность передачи на исследование файлов, копий подозрительного ПО, виртуальных машин, образов систем для проверки на наличие вирусов и обнаружения угроз.

Ключевые меры защиты информации российских и международных стандартов:

ГОСТ Р 57580.1-2017. СМЭ.4 — Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации в соответствии с установленными правилами и протоколами сетевого взаимодействия.

CIS Critical Security Controls. 12. Управление инфраструктурой сети. 12.2 Создание и поддержка безопасной сетевой архитектуры — Безопасная сетевая архитектура должна, как минимум, включать в себя сегментацию сети, минимальные привилегии и доступность.

Решение: АПК InfoDiode PRO на границе сети ИБ-лаборатории и корпоративной сети гарантируют невозможность проникновения вирусов из «песочницы» наружу в сеть организации. При этом сохраняется возможность передачи подозрительного ПО и систем для целей проверки в ИБ лаборатории и обеспечивается эффективный карантин зараженных файлов и иных объектов.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru