InfoDiode: эффективная защита сетей в финансовой отрасли

Наиболее разрушительные современные атаки на финансовый сектор имеют целенаправленный и многоступенчатый характер. Успех таких атак во многом определяется наличием технической возможности организовать канал удаленного управления системой-жертвой. Для банков и финансовых организаций весьма болезненной является не только проблема остановки деятельности и отказа в обслуживании, следующая за эффективно организованной атакой. Не менее серьезной является и проблема утечки данных клиентов, деталей финансовых операций, другой инсайдерской информации, хранящейся во внутренних ИТ-системах. Последующая публикация или продажа похищенных данных может нанести организации существенный репутационный и экономический ущерб.

Эффективный способ исключения несанкционированного доступа злоумышленников к сети – это ее надежная сегментация, то есть выделение в общей сетевой инфраструктуре критических сегментов с их последующей гарантированной изоляцией. Как правило, в финансовых организациях к критическим сетевым сегментам относят: сетевые сегменты размещения АРМ Банка России (АРМ КБР), сегменты размещения АРМ дистанционного банковского обслуживания (АРМ ДБО) с банками-корреспондентами, сегменты выполнения операций процессинга, сегменты хранения резервных копий, сегменты с различными внутренними ИТ-системами, сегменты площадок ведения разработки и тестирования, сегменты размещения продуктивных систем. То есть все те сегменты, доступ к которым извне банковской сети недопустим ни при каких обстоятельствах.

Для решения задач гарантированной изоляции сетевых сегментов многие финансовые организации применяют физическую изоляцию, разделяя сегменты сети между собой «воздушным зазором», в то время как перемещение данных между сегментами допускается лишь с использованием учтенных съемных носителей. Такой подход, наряду с очевидными достоинствами с точки зрения безопасности, имеет ряд недостатков, а именно - он исключает возможность передачи данных в реальном времени, затрудняет автоматизацию бизнес-процессов и влияет на непрерывность бизнеса, несет дополнительную трудоемкость выполнения операций, характерную для использования съемных носителей информации в условиях значительных объемов циркулирующей информации, провоцирует эксплуатирующий персонал на создание скрытых соединений между сегментами, использование неучтенных носителей информации и формирование нерегламентированных каналов коммуникации.

Внедрение устройств однонаправленной передачи данных **InfoDiode** устраняет указанные выше ограничения, сохраняя возможность передачи данных между сегментами сети в одном направлении и обеспечивая при этом «воздушный зазор» в обратном направлении. Устройства **InfoDiode** изолируют сетевые сегменты, исключая возможность организации обратного (в том числе двунаправленного) соединения на физическом уровне и обеспечивая гарантированную защиту сегмента от внешних информационных атак по сети. Таким образом, с помощью решений **InfoDiode** возможно сочетать высочайший уровень защиты и удобство передачи данных по сети.

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

Решение InfoDiode от АМТ-ГРУП

Сетевая сегментация с применением аппаратных средств находит свое применение и в финансовых организациях. Она позволяет надежно отделить критичные сегменты от остальной сети передачи данных и одновременно обеспечить необходимые взаимодействия между сегментами.

АМТ-ГРУП предлагает решения InfoDiode, которые гарантированно разделяют критические сегменты сети на физическом уровне модели OSI, сохраняя при этом возможности однонаправленной передачи информации из одного сегмента в другой. Для передачи 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, NTP, Netflow и т.д.).

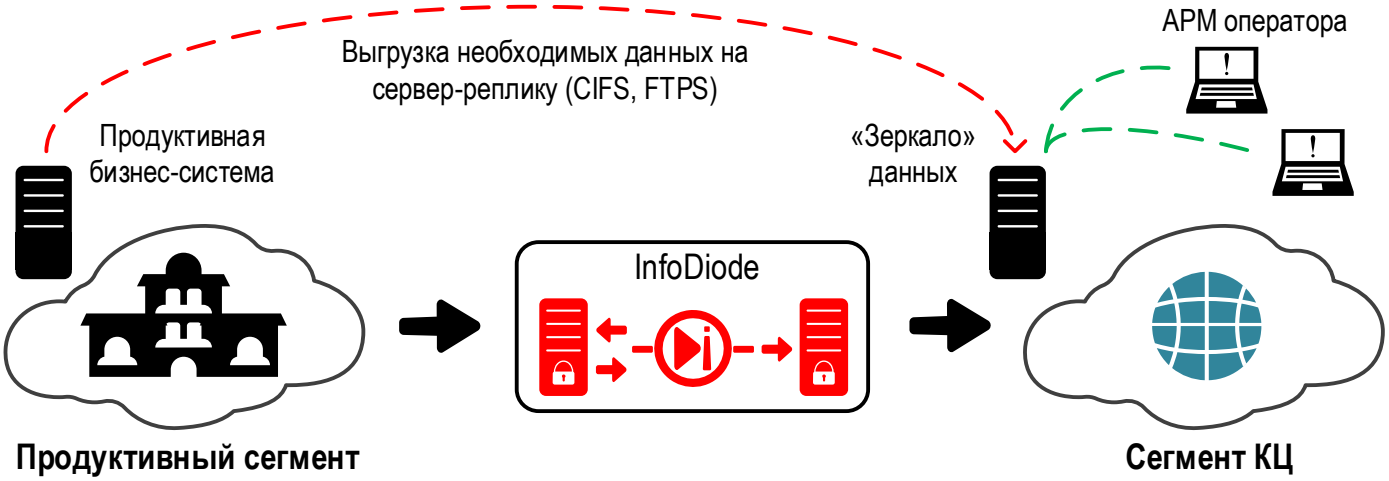
Продукты InfoDiode поставляются на рынок уже более 6 лет и включают в себя аппаратные (АК) и аппаратно-программные (АПК) комплексы, решения в различных форм-факторах (настольный, DIN-рейка, RACK), решения в отказоустойчивых конфигурациях.

Решения InfoDiode имеют сертификат ФСТЭК УД4 и проходят регулярный контроль на соответствие стандартам безопасности. Специалисты АМТ-ГРУП готовы оказывать консультационную поддержку и сопровождать процессы пуско-наладки устройств, встраивание их в единый контур безопасности банка или финансовой организации.

АМТ-ГРУП предлагает комплексную техническую поддержку своих решений в различных и удобных клиентам режимах: 8x5 или 24x7, ЗИП для клиента или ремонт оборудования, выезд технического специалиста для ремонта и др.

Сценарии применения в финансовой отрасли

Сценарий 1. Исключение воздействия сотрудников контакт-центра на продуктивный сегмент сети



Задача: Предоставить контакт-центру доступ к актуальной и частично обезличенной информации из клиентской базы банка, но гарантированно исключить любое воздействие на продуктивную систему банка со стороны контакт-центра.

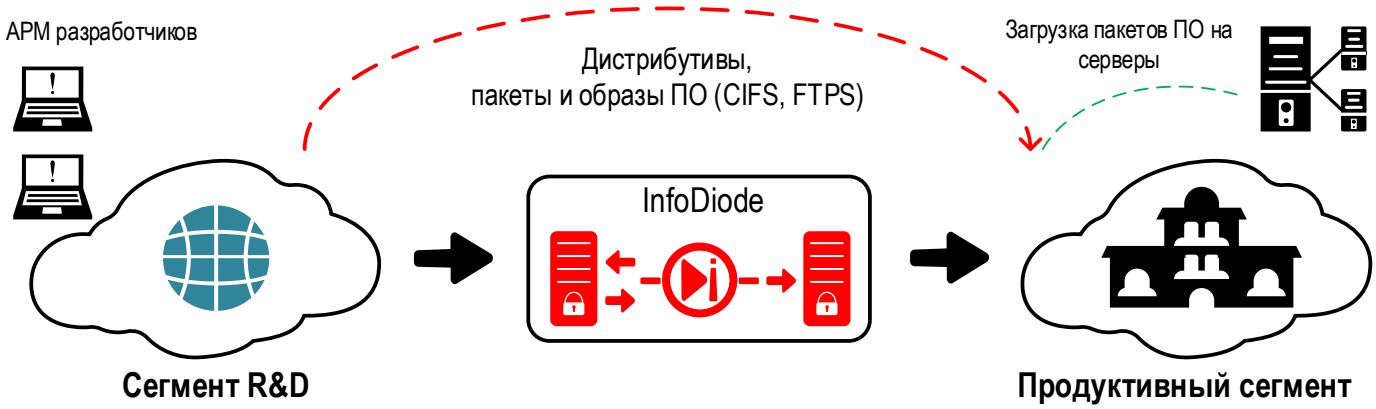
Решение: Операторы контакт-центра при коммуникации с клиентами работают с максимально обезличенной репликой информации из базы данных банка. Необходимые им данные периодически выгружаются из продуктивного сегмента организации через АПК InfoDiode PRO. Таким образом, на физическом уровне исключается возможность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

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

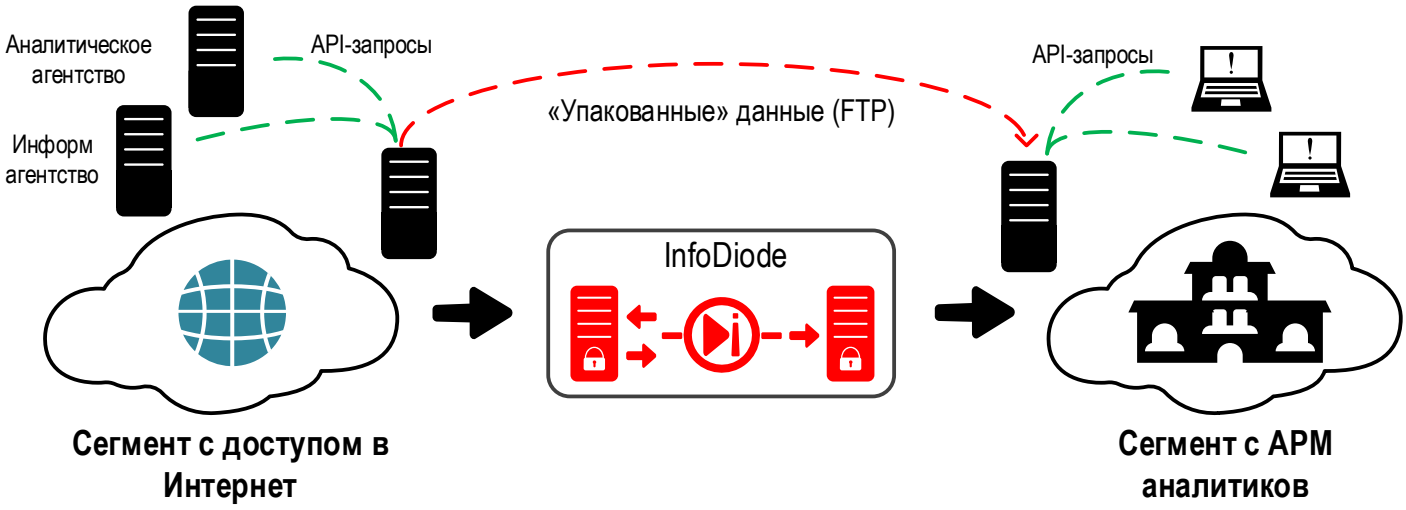
Сценарий 2. Передача обновлений ПО от вендоров в продуктивный сегмент сети



Задача: Гарантированно отделить сегмент разработки ПО (в том числе, сегмент подрядчиков и вендоров) от продуктивной среды банка и обеспечить при этом возможность передачи дистрибутивов и образов ПО в продуктивный контур.

Решение: После успешного тестирования ПО в среде разработки и тестирования осуществляется его загрузка через АПК InfoDiode PRO в продуктивный сегмент банка. Исключается риск утечки продуктивных данных в сегмент разработки, исключается возможность воздействия на продуктивные системы со стороны внешних подразделений и сотрудников.

Сценарий 3. Доставка информации от новостных агентств в защищаемый сегмент



Задача: Доставить в защищаемый сегмент банка информацию от новостных агентств (таких как Reuters, Bloomberg и др.), биржевых площадок, размещенных в сети Интернет или в отдельных VPN сетях. Учитывая высокую ценность результатов работы банковских аналитиков и значимость данных, с которыми они работают, организации требуется исключить утечку данных из сегмента АРМ аналитиков, которые имеют доступ к данным во внутренних бизнес-системах.

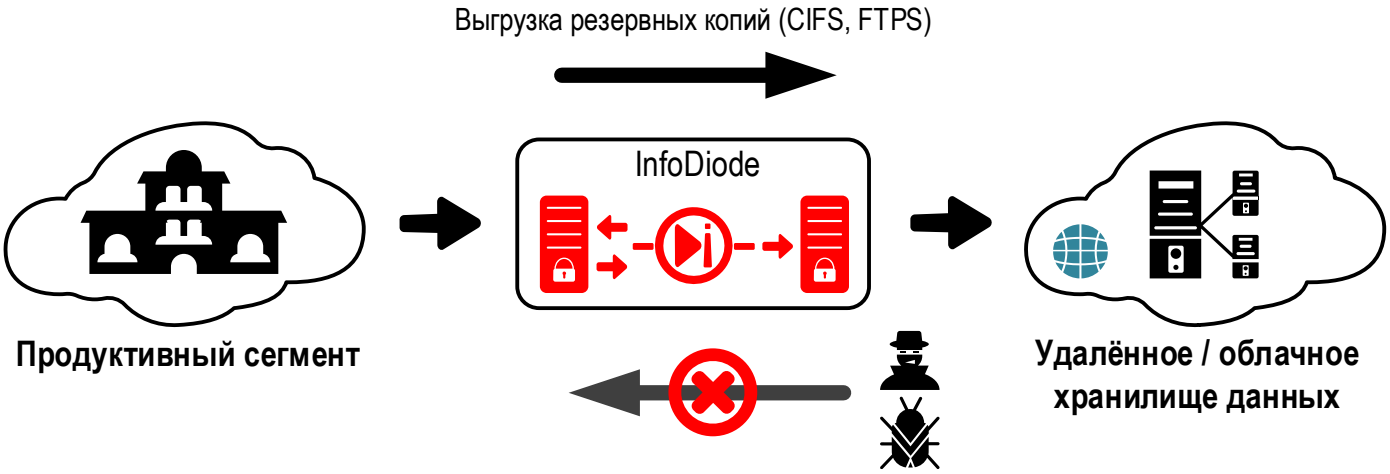
Решение: Размещение АПК InfoDiode PRO на границе сегмента АРМ аналитиков и сегмента Интернет гарантирует невозможность утечки конфиденциальной информации, а также предотвращает кибератаки, основанные на двунаправленном взаимодействии. При этом сохраняется возможность получения актуальной информации из внешних источников, находящихся за пределами банковской сети.

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

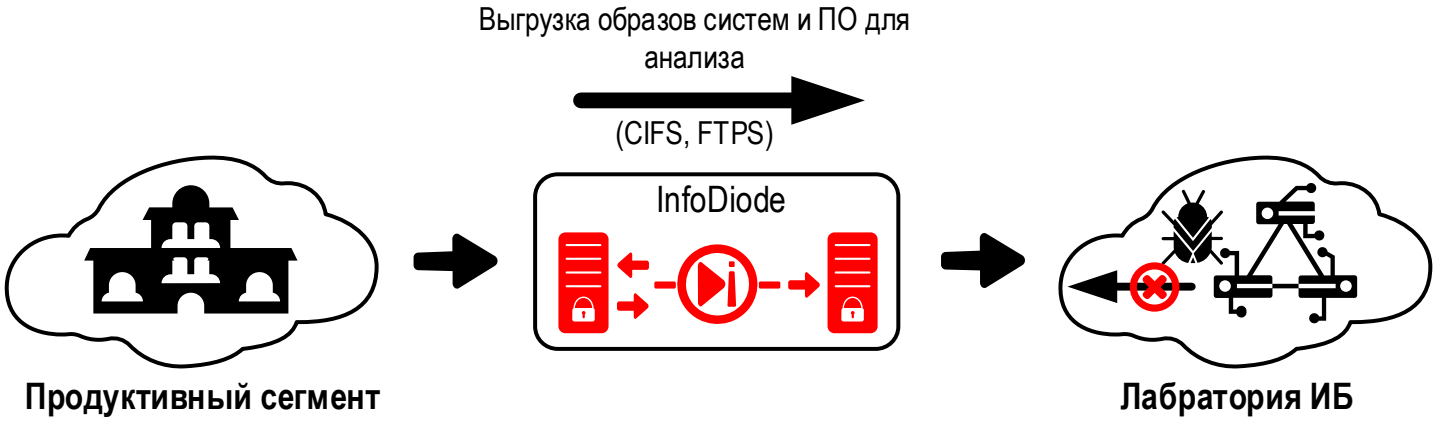
Сценарий 4. Резервное копирование данных на внешний изолированный ресурс



Задача: Отделить сегмент хранения резервных копий систем банка от остальной сети банка и гарантированно исключить воздействие на него извне. Требуется реализовать периодическое резервное копирование данных и ПО на случай критической ситуации и в случае возможной утери данных продуктивного сегмента. Сценарий актуален для финансовой организации, регулярно осуществляющей резервное копирование своих данных в удалённый ЦОД или «облако».

Решение: Выгрузка резервных копий в хранилище осуществляется через АПК InfoDiode PRO. Исключается риск атаки на хранилище со стороны открытых сетей передачи данных и в случае компрометации продуктивного контура.

Сценарий 5. Предотвращение заражения из ИБ лаборатории

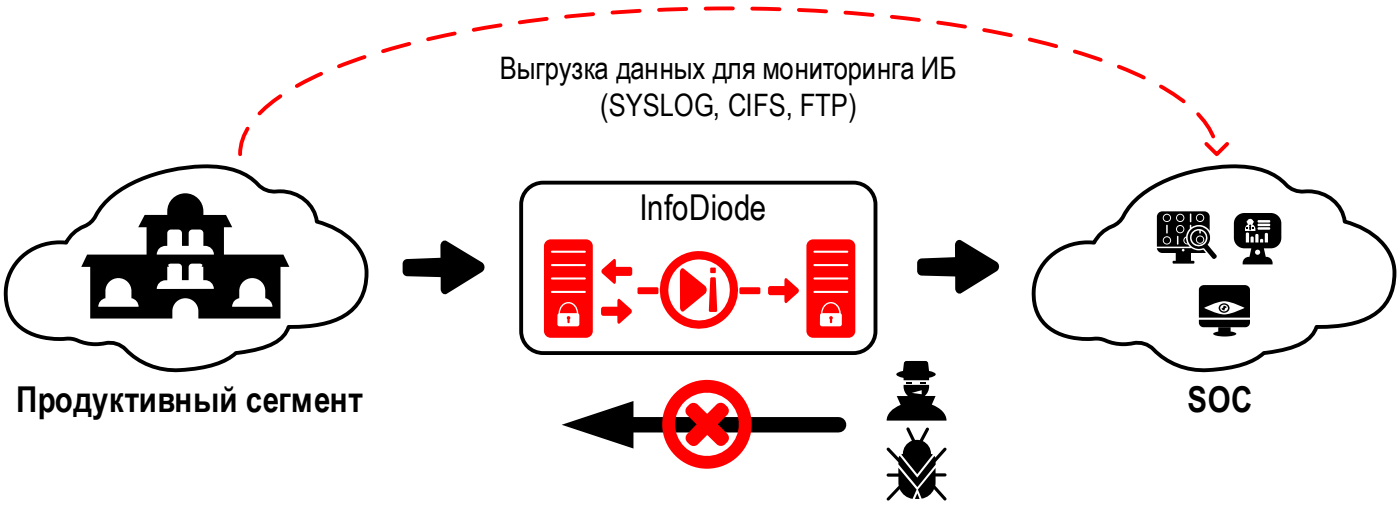


Задача: Исключить возможность заражения банковской сети из сети ИБ лаборатории, сохранив возможность копирования копий подозрительного ПО, виртуальных машин, образов систем для проверки на наличие вирусов и обнаружения угроз.

Решение: АК InfoDiode или АПК InfoDiode PRO на границе сети ИБ лаборатории и продуктивной сети гарантируют невозможность проникновения скомпрометированного ПО и вирусов из «ИБ-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 объектов и данных.

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

Сценарий 6. Мониторинг состояния сети и продуктивного контура



Задача: Реализовать возможность передачи данных для анализа в Ситуационный Центр Информационной Безопасности, расположенный в отдельной подсети банка или в «облаке». Мониторинг трафика банковской сети на наличие потенциальных угроз и обнаружения фактов утечек данных зачастую выполняется в SOC (Security Operations Center или Ситуационный Центр Информационной Безопасности). Передача событий и данных из защищаемого сегмента происходит с использованием syslog и netflow во внешнюю систему мониторинга SOC.

Решение: Передача трафика для регулярного анализа специалистам безопасности через АК InfoDiode или 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 банка в случае, если подсеть ИБ сопрягается с внешними серверами в целях обновления продуктов ИБ, получения сигнатур вирусов, баз репутации и т.п.

Заключение

На сегодняшний день можно отметить все возрастающий интерес организаций финансовой отрасли к повышению уровня защищенности своих ИТ-систем и бизнес-процессов.

Одновременно наблюдается расширение сценариев применения систем однонаправленной передачи данных для реализации более серьезных мер защиты и одновременного повышения удобства их использования .

Выше рассмотрены лишь некоторые сценарии применения комплексов однонаправленной передачи данных InfoDiode для повышения уровня безопасности организаций финансового сектора: сегментирование сетей, хранилища резервных копий, лаборатории безопасности, удалённый мониторинг, SOC, взаимодействие с вендорами ПО и т.д.

Как видно из приведенных примеров, однонаправленная передача данных может повысить безопасность во многих сценариях, как самостоятельно, так и в комплексе с другими классическими средствами защиты, такими как Firewall, антивирусы, DMZ сегменты, SOC и т.п.

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