

Угрозы

Современные DDoS-атаки на банковские Интернет-каналы и сервисы – действенный способ нарушения операционной деятельности банка, приводящий, в том числе, к недоступности системы электронного банкинга «iBank 2». Как следствие – уход крупных корпоративных клиентов, судебные иски, имиджевые и финансовые потери.

Услуги по защите от DDoS-атак

Компания «БИФИТ» предлагает банкам подключиться к Центру очистки трафика «ИБАНК2.РУ» для защиты системы электронного банкинга «iBank 2» от DDoS-атак.

Банкам, эксплуатирующим систему «iBank 2», услуги защиты от DDoS-атак с минимальным уровнем сервиса предоставляются **бесплатно**.

Схема работы

Для защиты от DDoS-атак весь трафик клиентов системы «iBank 2» направляется в Центр очистки трафика (далее «ЦОТ»), после чего очищенный легитимный трафик перенаправляется из ЦОТа в банк по выделенному каналу.



Защищаемые сервисы

Центр очистки трафика осуществляет защиту от DDoS-атак двух публичных сервисов системы «iBank 2».

HTTPS-сервер «iBank 2». Используется корпоративными клиентами для загрузки стартовых html-страниц, конфигурационных xml-файлов и Java-апплетов. Используется частными клиентами для работы с Internet-Банкингом. Взаимодействие осуществляется по протоколу HTTPS.

Сервер Приложения «iBank 2». Используется корпоративными клиентами при работе в PC-Банкинге, Internet-Банкинге и Mobile-Банкинге. Взаимодействие осуществляется по проприетарным протоколам IBTP и GSL.

Механизмы защиты

Оба сервиса доступны клиентам через Интернет и работают по TCP с использованием криптографических протоколов. Для защиты этих сервисов от DDoS-атак в Центре очистки трафика используются:

- Фильтрация входящего трафика по IP-адресу отправителя – применяются «белые» и «черные» списки индивидуально по каждому банку для каждого сервиса
- Фильтрация входящего трафика по GeoIP с целью исключения трафика из нежелательных регионов (для каждого банка по каждому сервису)

- Подавление сетевых DDoS-атак с помощью механизмов поведенческой и сигнатурной защиты:
 - TCP SYN Flood
 - UDP Flood
 - ICMP Flood
 - IGMP Flood
 - TCP Fin + Ack Flood
 - TCP SYN + Ack Flood
 - TCP Reset Flood
 - TCP Fragmentation Flood
- Инспекция криптографических протоколов на соответствие спецификациям для предотвращения DDoS-атак, основанных на нарушении корректности криптографических протоколов
- Контроль полосы пропускания и количества соединений в единицу времени по IP-адресу отправителя для блокирования хостов с чрезмерно высоким и аномально медленным трафиком

Для защиты от прикладных DDoS-атак в HTTPS-сервер «iBank 2» и Сервер Приложения «iBank 2» встроены дополнительные механизмы, взаимодействующие в онлайн с Центром очистки трафика.

Данные механизмы системы «iBank 2» на стороне банка анализируют результаты согласования сеансовых ключей в криптопротоколах, результаты аутентификации клиентов, частоту и последовательность прикладных запросов к конкретным ресурсам, корректность данных в прикладных запросах и ряд других критичных параметров.

При выявлении аномалий или превышении пороговых значений контролируемых параметров система «iBank 2» автоматически направляет в ЦОТ информацию о блокировании IP-адреса отправителя на заданный период.

Настройка DNS

Для защиты от DDoS-атак сервисов системы «iBank 2» Центр очистки трафика выделяет банку два IP-адреса – по одному для HTTPS-сервера и Сервера Приложения.

Банк для доменных имен HTTPS-сервера «iBank 2» и Сервера Приложения «iBank 2» добавляет вторыми (первые – основные) выделенные ЦОТом IP-адреса.

О работе клиентов

После подключения банка к Центру очистки трафика работа корпоративных и частных клиентов по системе «iBank 2» внешне никак не меняется.

Взаимодействие банка с ЦОТом возможно в двух режимах – работа клиентов только через ЦОТ и работа клиентов напрямую с банком и через ЦОТ одновременно.

Во втором режиме при отсутствии DDoS-атак клиентские приложения подключаются напрямую к банковским сервисам через банковские Интернет-каналы.

При недоступности основных IP-адресов банка из-за DDoS-атаки клиентские приложения автоматически начинают работать через Центр очистки трафика со вторыми IP-адресами, указанными в доменных именах защищаемых банковских сервисов.

Доступность DNS-серверов банка, их защищенность от DDoS-атак – необходимое условие для работы клиентов по системе «iBank 2». Для работы клиентов при недоступности DNS-серверов банка компания «БИФИТ» организовала резерв.

Единая точка входа

Центр очистки трафика «ИБАНК2.РУ» в качестве резерва организовал единую точку входа для всех корпоративных клиентов всех банков - <https://ibank2.ru>

При подключении к HTTPS-серверу единой точки входа клиент загружает Java-апплет, который автоматически определяет нужный банк по выбранному клиентом секретному ключу ЭЦП. Механизм автоопределения банка использует идентификатор экземпляра системы, хранящийся вместе с секретным ключом ЭЦП клиента.

По идентификатору экземпляра системы Java-апплет определяет банк, загружает с HTTPS-сервера единой точки входа соответствующие конфигурационные файлы и начинает работать с Сервером Приложения «iBank 2» данного банка через Центр очистки трафика.

В клиентскую компоненту РС-Банкинга также встроен механизм работы через Центр очистки трафика при невозможности определить IP-адрес банковского сервиса по доменному имени.

В этом случае клиентская компонента РС-Банкинга подключается к банковскому сервису по доменному имени <id>.ibank2.ru, где <id> – уникальный идентификатор экземпляра системы «iBank 2». По умолчанию доменное имя <id>.ibank2.ru дублирует доменное имя банковского сервиса РС-Банкинга. Описанный механизм включается банком в настройках при формировании единого клиентского дистрибутива РС-Банкинга.

Клиентские запросы от РС-Банкинга, поступающие в Центр очистки трафика, инспектируются и перенаправляются в банк аналогично другим сервисам.

О Центре очистки трафика «ИБАНК2.РУ»

Оборудование Центра очистки трафика «ИБАНК2.РУ» расположено на двух межоператорских площадках – в Москве (ММТС-9) и Киеве (NewTelco).

Центр очистки трафика имеет Интернет-каналы 10 Gbps burstable к нескольким магистральным провайдерам, подключен к точкам обмена трафиком MSK-IX и UA-IX.

Ядро Центра очистки трафика «ИБАНК2.РУ» построено на маршрутизаторах **Cisco 7606-S** с RSP720-3CXL и платами DFC3CXL на всех линейных модулях.

Для защиты от DDoS-атак на обеих площадках Центра очистки трафика используются топовые решения компании Radware с производительностью **8Gbps** и **10Mpps** – **Radware DefensePro 8412 IPS & Behavioral Protection**.

Дополнительно в Центре очистки трафика используется решение для защиты от DDoS-атак **Arbor Peakflow SP**, работающее совместно с маршрутизаторами Cisco 7606-S.

Для предоставления услуг по защите от DDoS-атак региональным банкам компания «БИФИТ» арендует магистральные каналы у федеральных операторов и организует свои точки присутствия на региональных межоператорских площадках.

В настоящее время имеются две точки присутствия на следующих региональных межоператорских площадках:

- г. Санкт-Петербург, ул. Большая Морская, 18
- г. Екатеринбург, ул. Мамина-Сибиряка, 145

Ведутся работы по подключению банков этих регионов к ЦОТу по L2 VPN через местных провайдеров. Планируется дальнейшее расширение географии точек присутствия.

Варианты организации выделенного канала

Подключение банка к Центру очистки трафика осуществляется через выделенный канал. На практике есть четыре варианта его организации.

Вариант 1. Компания «БИФИТ» организует канал L2 VPN от ЦОТа до банка, арендуя L2 VPN у канального провайдера банка по межоператорским ценам. Межоператорская кроссировка осуществляется в Москве на ММТС-9.



Для организации канала L2 VPN до регионального банка компания «БИФИТ» при необходимости арендует магистральный канал до региональной межоператорской площадки, организует свою точку присутствия, осуществляет межоператорскую кроссировку с канальным провайдером банка и арендует у этого провайдера канал L2 VPN от региональной точки присутствия до офиса банка.

Зона ответственности компании «БИФИТ» – порт в банке.

Вариант 2. Банк самостоятельно организует канал L2 VPN до Центра очистки трафика на ММТС-9. Порт 100Mb или 1Gb (UTP, SFP) предоставляется бесплатно.

Зона ответственности компании «БИФИТ» – порт ЦОТа.

На практике данный вариант предполагает, что банк самостоятельно договаривается со своим канальным провайдером о подключении к порту ЦОТа на ММТС-9, об аренде канала L2 VPN. Межоператорскую кроссировку на ММТС-9 обеспечивает канальный провайдер.

Банку следует учитывать, что на практике цена аренды L2 VPN для конечного корпоративного клиента существенно выше межоператорской цены для этого же канала.

Вариант 3. Компания «БИФИТ» предоставляет региональному банку в аренду канал L2 VPN от ЦОТа в Москве до точки присутствия на региональной межоператорской площадке и порт 100Mb или 1Gb (UTP, SFP). При этом банк самостоятельно (при участии своего канального провайдера) организует межоператорскую кроссировку с точкой присутствия БИФИТа и канал L2 VPN от порта точки присутствия до офиса банка.

Зона ответственности компании «БИФИТ» – порт точки присутствия на региональной межоператорской площадке.

Вариант 4. Использование банком резервного Интернет-канала для работы с Центром очистки трафика (L3 VPN).

Данный вариант является наиболее простым в реализации, используется для оперативного подключения банка к ЦОТу на начальном этапе и не требует дополнительных финансовых затрат. Типовое время подключения к ЦОТу через L3 VPN составляет 30 минут.

При этом банку следует учитывать, что в данном варианте сохраняется угроза DDoS-атаки на резервный Интернет-канал банка в обход ЦОТа в случае, если злоумышленникам станут известны IP-адреса резервного канала.

За информацией о решениях для защиты от DDoS-атак и услугах Центра очистки трафика обращайтесь по тел. +7 (495) 797-88-89 и e-mail: antiddos@bifit.com