БАЗОВЫЕ РЕКОМЕНДАЦИИ

по защите информации при работе в ДБО

и возможные риски получения несанкционированного доступа к защищаемой информации

Москва

Июнь 2026 / Редакция №3

Настоящие Базовые рекомендации по защите информации от воздействия программных кодов (вредоносного кода), приводящих к нарушению штатного функционирования средств вычислительной техники, в целях противодействия осуществлению переводов денежных средств без согласия клиента, разработаны в соответствии с в Положением Банка России № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории российской федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента целях ознакомления с возможными рисками и мерами по минимизации рисков несанкционированного доступа к защищаемой информации», а также информационными письмами Банка России по вопросам выявления и противодействия атак с вредоносным программным обеспечением (ВПО).

В ходе работы с системой дистанционного банковского обслуживания (ДБО) **возможны следующие риски** получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения денежными средствами:

- Заражение компьютера используемого для подключения к системе ДБО.

  Заражение обычно происходит путем посещения неблагонадежных веб-сайтов в сети «Интернет», на которых размещаются вредоносные вложения или настроена скрытая переадресация на вредоносные веб-сайты.

- Заражение устройства через съёмные носители информации.

  Заражение через съёмные носители информации (внешние жесткие диски, флэш-носители, CD или DVD-диски) может быть реализовано путем использования носителей с непроверенным содержимым и полученных от неизвестных. Это могут быть копии вредоносного ПО, замаскированные под различные приложения.

- Целевые фишинговые рассылки по электронной почте.

  Фишинговые рассылки содержат в себе «привлекательное» содержание и вложение для клиентов с целью перехода клиентов по ложным ссылкам и компрометации критичной информацией. При открытии такого вложенного файла или перехода по ссылке в письме на устройство загружается вредоносное программное обеспечение. Под фишинговыми рассылками также подразумевается отправка файлов и документов от партнеров и знакомых клиентов.

В результате реализации перечисленных рисков возможны:

- Утечка конфиденциальной информации, логинов/паролей.
- Выполнение на компьютере злонамеренных действий.
- Проникновение вирусов-шифровальщиков и иного ПО, которое может привести к неработоспособности компьютера.
- Непосредственно операции по выводу денег.

В целях противодействия осуществлению переводов денежных средств без согласия Клиента АО «Мидзухо Банк (Москва)» (далее по тексту – «Банк») рекомендует следующие меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого Клиентом осуществлялся перевод денежных средств необходимо внедрить следующие меры по предотвращению несанкционированного доступа к защищаемой информации:

- Не используйте компьютер с системой ДБО для посещения сайтов в сети Интернет. Используйте выделенный компьютер только для работы с ДБО.
- На выделенном для работы с ДБО компьютере установите антивирусное программное обеспечения для защиты от вредоносного ПО.
- Не подключайте компьютер, используемый для работы с ДБО, к общественным Wi-Fi сетям.
- Не открывайте письма, полученные из неизвестных источников на компьютере, используемых для работы с ДБО, не открывайте вложенные файлы и не переходите по ссылкам на веб-сайты.
- Не подключайте к компьютеру, используемому для работы с ДБО флэш-носители, CD или DVD-диски с непроверенным содержимым.
- Не устанавливайте и не открывайте вложения от Банка, полученным по нетипичным каналам связи.
- Используйте информацию с официального сайта Банка для установки и настройки системы ДБО. Не используйте переход к указанным сервисам и установку клиентской части системы ДБО по ссылке из других источников.
- В операционной системе работайте под учетной записью обычного пользователя (не администратор). Защитите вход в операционную систему надежным сложным паролем.
- Блокируйте компьютер при временном отсутствии на рабочем месте, а при длительном отсутствии обязательно выключайте компьютер. Настройте автоматическую блокировку компьютера по истечении определённого времени (не более 5 минут).
- Не оставляйте без контроля ключевой носитель, используемый для работы с системой ДБО. Извлекайте ключевой носитель после завершения работы с системой ДБО. Храните носитель отдельно от компьютера в местах, исключающих несанкционированный доступ к носителю.

В целях соблюдения требований по информационной безопасности Банк рекомендует регулярное проведение следующих мероприятий:

- Использование и своевременное обновление антивирусных средств защиты;
- Использование антифишинг-систем, в том числе автоматического анализа ссылок (вложений);
- Регулярное обучение персонала по противодействию социальной инженерии и фишингу;
- Ограничение бесконтрольного доступа работников в сеть «Интернет»;

- Ограничение возможности импортирования сертификатов электронной подписи на рабочие персональные компьютеры работников бухгалтерии, финансовых подразделений, осуществляющих проведение платежей со счетов юридического лица.

В целях повышения уровня защищенности объектов инфраструктуры, Банк рекомендует регулярное проведение следующих мероприятий:

- Использование решений для мониторинга и выявления киберугроз и оперативного реагирования на инциденты (например, MDR-решений);
- С помощью аппаратных или программных средств сетевой защиты (например, Firewall, корпоративные прокси-серверы) ограничить доступ в сеть «Интернет». Маршрутизировать трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами;
- Не допускать использования работниками организации рабочих устройств для личного использования, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах.
- С учетом возможного перехвата вредоносным программным обеспечением SMS сообщений рекомендовать сотрудникам установление и периодическое обновление антивирусного программного обеспечения для защиты от вредоносного ПО на мобильные телефоны;
- Соблюдать требования безопасности при эксплуатации аппаратного ключа (токена), производить его извлечение из USB-порта сразу после подписания платежных поручений.

Каналы коммуникации с Банком

- Используйте для коммуникаций с АО «Мидзухо Банк (Москва)» только официальные каналы коммуникации.
- Система ДБО является защищенным каналом связи, поэтому она более предпочтительна для обмена электронными копиями документов.
- Представитель Банка может обратиться к уполномоченным представителям организации по записывающему телефону для подтверждения платежа в рамках исполнения обязанностей Банка по предотвращению переводов денежных средств со счета организации без согласия или запроса, полученного от организации через дополнительные каналы коммуникации (почта, курьер, личная электронная почта и т.п.).
- Представитель Банка никогда не будет запрашивать у уполномоченных представителей организации какую-то иную конфиденциальную информацию, связанную с такими сотрудниками, кроме той, что необходима для подтверждения уже полученного Банком для исполнения платежа. Тем более не будет предлагать совершить какие-то срочные действия.
- Если у Вас (у Клиента) возникли сомнения в том, что к Вам обращается именно представитель Банка, рекомендуем обратиться в Банк по официальным каналам и получить подтверждение.

При выявлении инцидента информационной безопасности, такие как:

- операции, которые не совершали — смена пароля, создание платежей,
- видите на компьютере действия, которых не совершаете: перемещение курсора, открытие и закрытие окон, заполнение полей документа,
- данные для входа стали известны посторонним.

Банк рекомендует незамедлительно:

1) **Связаться со службой поддержки Банка по телефону 8-495-212-03-40.**
2) **Произвести следующие действия:**

- не перезагружать компьютер, не запускать антивирусные решения, извлечь токены доступа и съемные носители информации;
- отключить устройство от локальной сети и сети Интернет;
- выполнить процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения (например, «FTK Imager») для дальнейшего проведения расследования;
- сохранить образец вредоносного программного обеспечения для проведения анализа и последующей передачи его в Банк (в рамках анализа компьютерного инцидента);
- в случае заражения мобильного устройства, необходимо включить авиа-режим и извлечь SIM-карту. Если в устройстве используется электронная сим-карта, допустимо выключить устройство. Сбрасывать устройство до заводских настроек не рекомендуется, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.