

ООО НКО «МОБИ.Деньги»

Рекомендации по снижению рисков осуществления перевода денежных средств без добровольного согласия клиента

В целях снижения рисков осуществления перевода денежных средств без добровольного согласия клиента и реализации части 3.6 статьи 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» ООО НКО «МОБИ.Деньги» (далее - НКО) доводит до своих клиентов информацию о существующих рисках получения злоумышленниками несанкционированного доступа к защищаемой информации клиентов с целью хищения денежных средств клиентов, а также дает рекомендации по снижению данных рисков.

Операция без добровольного согласия клиента (далее - операция БСК) - операция, соответствующая признакам осуществления перевода денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием. Признаки осуществления перевода денежных средств без добровольного согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети «Интернет» (Приложение к настоящим рекомендациям).

К операциям БСК могут относиться (включая, но не ограничиваясь):

- операции по оплате товаров и услуг через сеть Интернет с использованием электронного устройства клиента (компьютер, электронный планшет, смартфон, мобильный телефон, далее – ЭУ) в том числе по реквизитам ЭСП клиента;
- операции по переводу денежных средств, предоставленных клиентом оператору связи в качестве оплаты услуг связи, в том числе перечисление денежных средств на «короткие номера»;
- операции, осуществляемые с использованием системы МОБИ.Деньги, предоставляемой НКО и установленной клиентом на ЭУ (далее – Система);
- операции по оплате товаров и услуг с использованием иных приложений, установленных на ЭУ клиента.

Несанкционированный перевод денежных средств может проводиться вследствие заражения ЭУ клиента вредоносным программным обеспечением (далее - ВПО) или посредством удалённого доступа к устройствам клиента.

Заражение ЭУ клиента осуществляется через спам-рассылку SMS или MMS-сообщений, сообщений электронной почты, содержащих ссылки на внешние ресурсы, или при переходе по ссылкам на ресурсы сети Интернет. При переходе по таким ссылкам ВПО устанавливается на ЭУ клиента.

ВПО может обладать различными возможностями, в том числе:

- формировать и отправлять от имени клиента распоряжения на перевод денежных средств, в том числе в виде SMS-сообщений на «короткие номера»;
- формировать и отправлять от имени клиента распоряжения на перевод денежных средств с использованием Системы и иных приложений, предназначенных для оплаты товаров и услуг;

- перехватывать сообщения с кодами подтверждения, приходящие на ЭУ в целях подтверждения операции.

Наибольший риск таких операций связан с тем, что в ряде случаев в ВПО скрывает от клиента приходящие от НКО или оператора связи уведомления о списании денежных средств. Таким образом, клиент, не зная о несанкционированной операции с его денежными средствами, не может направить в НКО в определённые законодательством сроки уведомление о факте перевода денежных средств без согласия.

Также злоумышленники, используя методы социальной инженерии (представившись сотрудниками НКО, оператора связи), могут обманом вынудить клиента сообщить данные для проведения операции – коды доступа, коды SMS-подтверждения и осуществить с использованием таких сведений несанкционированные операции.

В случае обнаружения списания денежных средств необходимо в сроки, установленные законодательством РФ, обратиться в НКО или к оператору связи (если произошло списание денежных средств, предоставленных оператору связи в оплату услуг связи, в том числе перечисление денежных средств на «короткие номера»).

Клиентам следует учитывать следующие рекомендации для снижения риска хищения денежных средств:

1. Не следует сообщать посторонним лицам свою персональную информацию (ФИО, реквизиты ЭСП, логин, пароль, номер карты, счета, паспорта и т.д.). Сотрудник НКО имеет право уточнять у клиента подобную информацию только в случае, если клиент самостоятельно обратился в НКО.

2. В случае утери ЭУ, используемым для работы с Системой, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи и обратиться в НКО для блокировки доступа в Систему;

3. В случае изменения номера телефона ЭУ для работы в Системе нужно обратиться в НКО для изменения телефонного номера, по которому осуществляется доступ к сервисам НКО. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время;

4. Если у Вас неожиданно перестала работать SIM-карта – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как это может быть одним из признаков совершаемых в отношении Вас третьими лицами мошеннических действий;

5. Для работы с Системой используйте защищенные ЭУ – не пытайтесь обходить установленные производителем ЭУ программные средства защиты. Не перепрошивайте свое ЭУ программным обеспечением сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению ВПО.

6. Не допускается работать в Системе через публичные беспроводные сети (free Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через оператора мобильной связи (3G, 4G) или через доверенную защищенную беспроводную сеть;

7. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой НКО Системы, и (или) использующих зарегистрированные товарные знаки и наименование НКО, необходимо удостовериться, чтобы при подключении к Системе защищённое SSL-соединение было установлено исключительно с официальными сайтами Системы: <https://www.mobi-money.ru/> и <https://wallet.mobi-money.ru/> (в случае использования сервиса НКО). Перед началом работы в Системе, необходимо убедиться, что web-адрес в адресной строке браузера совпадает с вышеуказанным адресом соответствующего сервиса.

8. Прежде чем ввести имя пользователя и пароль в Системе, проверьте подлинность сайта по информации из SSL-сертификата. Для этого в адресной строке браузера, например

Internet Explorer, щелкните мышкой на символ замка, далее «Просмотр сертификатов», перейти на закладку «Состав», встать на строку «Субъект», в окне просмотра убедитесь в наличии следующей информации: CN = *.mobi-money.ru. Аналогичным образом можно посмотреть эту информацию и в других браузерах. Центром сертификации, подтверждающим подлинность сайта, является Thawte RSA CA.

9. При создании паролей придерживайтесь следующих правил. Не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы. Пароль должен быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.). Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.);

10. Необходимо хранить код доступа в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать код доступа к Системе там, где доступ к нему могут получить посторонние лица (включая незаблокированное ЭУ);

11. Не сообщать код доступа, SMS-коды, необходимые для проведения операций, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карты (CVV/CVC-код) посторонним лицам, сотрудникам Банка по телефону, электронной почте или иным способом. Использование SMS-кодов допускается только при работе непосредственно с Системой, без участия сотрудников НКО (или иной кредитной организации). При возникновении подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактными телефонам, указанным на официальном сайте НКО;

12. Не оставляйте ЭУ без присмотра, тем более при активированной Системе. Выходите из Системы даже если необходимо отойти на непродолжительное время. Ограничьте доступ посторонних лиц к компьютеру, с которого осуществляется работа в Системе. Установите пароль на доступ к ЭУ и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к ЭУ в случае его утраты;

13. Необходимо корректно завершать работу в Системе, используя для этого пункт меню «Выход»;

14. Необходимо применять на ЭУ, с которых ведётся работа с Системой, лицензионные средства антивирусной защиты, работающие в автоматическом режиме, и регулярно в рекомендуемые разработчиками сроки проводить их обновление;

15. Отключение или несвоевременное обновление антивирусных средств, установленных на ЭУ с которых производятся работы в Системе, не допускается. В случае обнаружения на ЭУ нештатного отключения антивирусных средств – не допускается работа с Системой на ЭУ до устранения причины нештатного отключения;

16. Необходимо осуществлять проверку ЭУ на наличие ВПО перед началом работы с Системой, а также после доступа к Вашему ЭУ сотрудников технической поддержки различных организаций или любых других частных мастеров, выполнивших работу по установке, обновлению и поддержке различных программ;

17. Необходимо на постоянной основе регулярно, например, ежемесячно, проводить полную проверку ЭУ, на котором ведётся работа с Системой, на наличие ВПО.

18. Не рекомендуется передавать ЭУ для использования третьим лицам, в том числе родственникам, т.к. на оставленном без присмотра ЭУ может быть совершён ряд действий, направленных на получение доступа к Системе. Например, злоумышленник может установить ВПО, настроить переадресацию SMS-сообщений на другое устройство и т.п.;

19. Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях из недостоверных источников, в том числе на

известные сайты, а также загружать и устанавливать на ЭУ программное обеспечение из недостоверных источников.

20. Не рекомендуется заходить в Систему и проводить в ней операции с чужих непроверенных ЭУ (интернет-кафе, киоски и т.д.).

21. Не следует реагировать на подозрительные SMS-сообщения, которые запрашивают у Вас конфиденциальную информацию.

22. Пароль доступа к Системе меняйте не реже одного раза в квартал. Помните, что в случае раскрытия пароля доступа существует риск совершения неправомерных действий с Вашими денежными средствами со стороны третьих лиц.

23. В случае если имеются предположения о раскрытии пароля доступа, Ваших персональных данных, позволяющих совершить неправомерные действия с использованием Системы, необходимо немедленно обратиться в НКО и следовать указаниям сотрудника НКО.

24. В случае возникновения подозрений на мошеннические действия необходимо заблокировать доступ к Системе. Для блокировки необходимо позвонить по телефону +8-800-555-3115 для блокировки доступа к Системе.

Приложение
к Рекомендациям по снижению рисков
осуществления перевода денежных средств без
добровольного согласия клиента

**Признаки осуществления перевода денежных средств
без добровольного согласия клиента**

Признаки, выявляемые в отношении переводов денежных средств:

1. Совпадение информации о получателе средств с информацией о получателе средств по переводам денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием (далее при совместном упоминании – перевод денежных средств без добровольного согласия клиента), полученной из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, формирование и ведение которой осуществляются Банком России на основании части 5 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – база данных).

2. Совпадение сведений, относящихся к получателю средств и (или) его электронному средству платежа, со сведениями, размещенными в государственной информационной системе противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, созданной в соответствии с частью 1 статьи 1 Федерального закона от 01.04.2025 N 41-ФЗ "О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации" (применяется с 01.03.2026).

3. Наличие превышения установленного правилами платежной системы времени направления ответа на запрос (APDU (application protocol data unit) - команда) в рамках взаимодействия банкомата и платежной карты или токенизированной (цифровой) платежной карты.

4. Наличие информации об уровне риска осуществления операции без добровольного согласия клиента, о факторах риска компрометации данных электронного средства платежа, направленной в авторизационных сообщениях оператором услуг платежной инфраструктуры, если это предусмотрено правилами платежной системы, или электронных сообщениях, полученных от операционного центра, платежного клирингового центра другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей платежной системы Банка России.

5. Совпадение информации о параметрах устройств, с использованием которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях осуществления перевода денежных средств, с информацией о параметрах устройств, с использованием которых был осуществлен доступ к автоматизированной системе, программному обеспечению в целях осуществления перевода денежных средств без добровольного согласия клиента, полученной из базы данных.

6. Несоответствие характера, и (или) параметров, и (или) объема проводимой операции (время (дни) осуществления операции; место осуществления операции; устройство, с использованием которого осуществляется операция, и параметры его использования; сумма осуществления операции; периодичность (частота) осуществления

операций; получатель средств) операциям, обычно совершаемым клиентом оператора по переводу денежных средств (осуществляемой клиентом деятельностью).

7. Совпадение информации о получателе средств (в том числе его электронном средстве платежа) с информацией о получателе средств (в том числе его электронном средстве платежа), ранее включенном во внутренние перечни (при наличии) оператора по переводу денежных средств в качестве получателя средств по переводам денежных средств без добровольного согласия клиента.

8. Совпадение информации о получателе средств (в том числе его электронном средстве платежа) с информацией о получателе средств (в том числе его электронном средстве платежа), совершившем противоправные действия, связанные с осуществлением перевода денежных средств без добровольного согласия клиента, в связи с чем в отношении такого получателя средств возбуждено уголовное дело (подтвержденное документально).

9. Наличие информации, полученной от операторов связи, владельцев мессенджеров, владельцев сайтов в информационно-телекоммуникационной сети "Интернет" и (или) иных юридических лиц, о том, что в период не менее чем шесть часов до момента направления распоряжения о переводе денежных средств ими выявлены:

телефонные переговоры с применением абонентского номера подвижной радиотелефонной связи, используемого во взаимоотношениях с кредитной организацией, не соответствующие характеру (периодичности (частоте), продолжительности) обычно совершаемых клиентом телефонных переговоров до или во время осуществления переводов денежных средств;

факт (факты) нетипичного получения сообщений, в том числе в мессенджерах и (или) по электронной почте, в частности коротких текстовых сообщений (увеличение количества получаемых сообщений, в том числе от федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" и (или) кредитных организаций, с новых абонентских номеров или от новых адресатов).

10. Наличие информации, полученной от операторов связи, владельцев мессенджеров, владельцев сайтов в информационно-телекоммуникационной сети "Интернет" и (или) иных юридических лиц, а также выявленной оператором по переводу денежных средств в рамках реализуемой им системы управления рисками:

о вредоносном программном обеспечении (вредоносных программах) на устройствах абонента - физического лица, с применением которых осуществляется перевод денежных средств;

о нетипичных для клиента параметрах, событиях в сессии дистанционного банковского обслуживания (использование нетипичного провайдера связи, операционной системы, приложения пользователя, использование инструментов, обеспечивающих сокрытие сессионных данных);

о смене абонентского номера подвижной радиотелефонной связи в личном кабинете дистанционного банковского обслуживания или личном кабинете физического лица в федеральной государственной информационной системе "Единый портал государственных и муниципальных услуг (функций)", осуществленной в течение 48 часов до момента направления распоряжения о переводе денежных средств;

о выявлении факта изменения идентификационного модуля устройства клиента и (или) параметров устройства, с применением которого осуществляется перевод денежных средств, до момента подтверждения принадлежности клиенту абонентского номера подвижной радиотелефонной связи в соответствии с подпунктом 5.2.1 пункта 5 Положения Банка России от 30.01.2025 N 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";

о выявленной в рамках реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента, предусмотренных частью 4 статьи 27 Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе", операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента, в том числе информации, полученной от оператора по переводу денежных средств, обслуживающего получателя средств, а также операторов услуг платежной инфраструктуры.

11. Наличие запроса на внесение наличных денежных средств на банковский счет клиента - физического лица с применением токенизированной (цифровой) платежной карты с использованием банкомата в течение 24 часов с момента осуществления трансграничного перевода денежных средств по распоряжению указанного клиента - физического лица в пользу получателей - физических лиц на сумму более 100 тысяч рублей.

12. Наличие информации о поступлении денежных средств на сумму более 200 тысяч рублей на банковский счет (вклад) физического лица с использованием сервиса быстрых платежей платежной системы Банка России с банковского счета (вклада) указанного физического лица, открытого другим оператором по переводу денежных средств, в период менее чем за 24 часа до момента направления распоряжения о переводе денежных средств физическому лицу, в адрес которого ранее в течение 6 месяцев не совершались переводы денежных средств указанным плательщиком.