РЕКОМЕНДАЦИИ КЛИЕНТУ
о мерах снижения рисков при работе
в системе дистанционного банковского обслуживания «Internet-Банкинг»

АО «КОШЕЛЕВ-БАНК» использует современные меры обеспечения безопасности системы дистанционного банковского обслуживания «Internet-банкинг» и предоставляет удобство пользования услугой, обеспечивая при этом высокий уровень надежности и безопасности системы. Вместе с тем, эффективность данных мер зависит во многом и от соблюдения Вами следующих мер безопасности при работе в Системе ДБО.

В соответствии с п.3 ст.9 Федерального закона от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе» Банк информирует Клиента:

1. Условия использования электронного средства платежа, в частности любые ограничения способов и мест использования Системы ДБО определены положениями Договора ДБО.

2. Случаи повышенного риска, связанные с использованием Системы ДБО

2.1. Клиент соглашается на получение услуги с использованием Системы ДБО, осознавая, что сеть Интернет не всегда является безопасным каналом связи для передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности, и иные риски, возникающие вследствие использования такого канала доступа, в частности риск осуществления переводов денежных средств Клиента лицами, не обладающими правом распоряжения этими денежными средствами.

2.2. Клиент понимает повышенный риск несанкционированного использования Системы ДБО, включая компрометацию ключей ЭП и несанкционированное удаленное управление Системой ДБО, при ненадлежащем соблюдении Клиентом мер безопасности, определенными настоящими Рекомендациями.

2.3. К случаям повышенного риска, связанным с использованием Системы ДБО, относится:

2.3.1. использование Системы ДБО с помощью устройства доступа, размещенного в общественном месте. В случае такого использования Клиент может максимально обезопасить себя, выполнив условия обеспечения безопасности соединения в сети Интернет (п.п. 3.1.1, п.п.3.1.2 настоящих Рекомендаций);

2.3.2. кража (потеря) устройства мобильной связи, на номер которого приходят SMS-сообщения с разовыми паролями для подтверждения операций по счету посредством сервиса информирования Системы ДБО, либо SMS-сообщения о проведенных платежах. В случае подозрения на кражу или потерю устройства мобильной связи Клиент обязан незамедлительно прекратить использование Системы ДБО до восстановления SIM-карты или изменения номера устройства мобильной связи;

2.3.3. невыполнение условий обеспечения безопасности устройства доступа в Систему ДБО (п.п. 3.3 настоящих Рекомендаций);

2.3.4. использование пароля на вход в устройство доступа и пароля доступа к ключам ЭП, не соответствующего минимальным требованиям к его безопасности (п.п. 3.4 настоящих Рекомендаций).

2.3.5. получение доступа к Системе ДБО посредством браузера с устройства доступа, содержащего вредоносный или модифицированный код, а также на котором произведена модификация системы с целью получения доступа к файловой системе или иных прав, не предусмотренных разработчиками операционной системы.

3. Меры обеспечения безопасности при пользовании Системы ДБО

3.1. **Обеспечьте безопасность работы в Системе ДБО:**

3.1.1. Перед вводом пароля для доступа в Систему ДБО убедитесь, что соединение установлено именно со стартовой страницы системы и в адресной строке web-браузера отображается «https://online.k-bnk.ru/ ». Если Вы заметили, что адрес сайта отличается или есть иные признаки, вызывающие подозрения подлинности сайта (например, сообщение web-браузера о перенаправлении на другой сайт), не вводите никакой конфиденциальной информации и незамедлительно сообщите о данном факте по телефону Банка 8 (846) 251 00 00.

Рекомендуется вводить адрес Системы ДБО только вручную в новом окне web-браузера в адресной строке и НЕ переходить на данную страницу по ссылкам из Интернет-ресурсов (за исключением http://www.koshelev-bank.ru/) или из e-mail/SMS-сообщений, даже если они отправлены от имени Банка.

3.1.2. Перед началом работы в Системе ДБО удостоверьтесь, что соединение установлено в защищенном режиме SSL: в префиксе в адресной строке web-браузера должен появиться символ S - httpS://online.k-bnk.ru/, а также отобразится иконка «закрытый замок» (может отличаться для разных web-браузеров).

3.1.3. Установите пароль доступа к ключам электронной подписи, хранящимся на персональном аппаратном криптопровайдере (USB-токене).

3.1.4. Обязательно отключайте от устройства доступа в Систему ДБО персональный аппаратный криптопровайдер (USB-токен) даже при кратковременном прекращении работы в системе. Используйте его исключительно для входа в систему и для подписания электронного документа (платежного поручения, письма и т.п.) при отправке в Банк. Для удобства работы с USB-токеном используйте USB-удлинители.

3.2. В перерывах между использованием USB-токена храните его в месте, доступном только владельцам ключей электронной подписи. Не передавайте носитель ключей третьим лицам.

3.2.1. После окончания работы в Системе ДБО обязательно завершайте сеанс работы с помощью кнопки «Выход» (в правом верхнем углу экрана).

3.2.2. Контролируйте состояние Ваших счетов. Регулярно не менее 1 (Одного) раза в день (с 15:00 до 17:00) проверяйте в системе (особенно перед проведением операции) разделы «Рублевые документы» («Валютные документы») (история операций и платежей, совершенных в Системе), «Сеансы работы» (история успешных и неуспешных попыток входа в Систему с отображением IP-адреса и используемого браузера, все операции совершенные в Системе с отображением даты и времени операции), раздел «Шаблоны» в разделе «Рублевые документы» (перечень сохраненных шаблонов операций). В случае если Вы обнаружили подозрительные записи в журналах событий (например, события входа в систему с неизвестных Вам IP-адресов или в не типичное для Вас время суток; несколько неуспешных попыток входа, которые Вы не совершали; операции, которые Вы не выполняли; шаблоны, которые Вы не создавали) незамедлительно заблокируйте Вашу учетную запись в системе, позвонив в Банк по телефону 8 (846) 251 00 00 и произнеся блокировочное слово администратору системы.

3.2.3. Для повышения уровня безопасности работы в Системе ДБО подключите режим усиленной защиты: вход в систему потребует подтверждения одноразовым паролем, получаемым в виде SMS-сообщения.

3.2.4. При смене/увольнении уполномоченного лица, осуществляющего работу с Системой ДБО, проинформируйте Банк о произошедших изменениях и произведите замену ключевой пары.

3.2.5. При изменении контактной информации (электронный почтовый адрес, телефон) своевременно сообщайте обновленные данные специалистам Банка.

3.2.6. Внимательно ознакомиться с информационными сообщениями Банка по безопасности, размещенными на сайте Банка и/или направляемыми по Системе ДБО. Если имеются сомнения в достоверности адреса отправителя сообщения, необходимо обратиться в Банк, по телефону, указанному на сайте Банка.

3.3. **Обеспечьте безопасность устройства доступа, с использованием которого осуществляется работа в Системе ДБО:**

3.3.1. Допускать к работе на устройстве доступа только уполномоченных лиц, обеспечить физическую безопасность устройства, на котором осуществляется работа в Системе ДБО.

3.3.2. Перед входом в Систему ДБО необходимо удостовериться в том, что на устройстве доступа установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Если существуют подозрения или основания считать, что устройство доступа может быть заражено вирусами – не осуществляйте с него работу в системе.

3.3.3. Использовать на устройстве доступа только лицензионное программное обеспечение.

3.3.4. Своевременно обновлять операционную систему устройства доступа, браузеры и прикладное программное обеспечение. Обновления следует устанавливать только из доверенных источников (с официального сайта производителя)

3.3.5. Использовать устройство доступа, на котором установлена только одна операционная система.

3.3.6. Осуществлять работу с Системой ДБО с использованием отдельной учетной записи в операционной системе устройства доступа, защищенной сложным паролем, известным только Вам (см п.п.3.4 настоящих Рекомендаций) с ограниченными правами доступа.

3.3.7. Установить на устройство доступа специальные программные и аппаратные средства защиты (антивирусное программное обеспечение, средства обнаружения вредоносных программ, средства защиты информации от воздействия вредоносного кода, персональный межсетевой экран), которые должны регулярно обновляться. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Устройства доступа только к северу Системы (httpS://online.k-bnk.ru/) и серверам обновлений разработчиков программного обеспечения, любые иные подключения рекомендуется запретить.

3.3.8. Регулярно проводить полную антивирусную проверку устройства доступа.

3.3.9. Рекомендуется избегать работы в Системе ДБО с использованием «недоверенных» устройств доступа, таких как компьютеры в интернет-кафе или другие общедоступные устройства, «чужие» устройства, временно используемые Вами и т.п. Крайне нежелательна работа с Системой из публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользуйтесь «мобильным интернетом» (GPRS / EDGE / HSPA / 3G / LTE соединение). Если же данные рекомендации не могут быть Вами выполнены, то при первой же возможности измените пароль, войдя в Систему с «доверенного» Устройства доступа.

3.3.10. Не оставлять без присмотра Ваше устройство доступа с активной сессией работы в Системе ДБО, блокировать доступ к устройству при помощи пароля на время Вашего отсутствия.

3.3.11. Запускать на устройстве доступа программы, полученные только из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет); не рекомендуется открывать и использовать без проведения соответствующих проверок файлы, полученные из общедоступных сетей передачи данных, для исключения программных закладок и вирусов.

Помните, что Банк не рассылает своим Клиентам диск с программным обеспечением Системы ДБО и средством криптографической защиты информации (СКЗИ) по почте; ссылки или указания на установку программного обеспечения через SMS/MMS/Email – сообщения. Получить программно-технические средства можно только в Банке.

3.3.12. Исключить посещение с устройства доступа потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы, файлообменные сервисы и т.д.), а также работу с почтовыми сообщениями, полученными из недостоверных источников.

3.4. **При выборе пароля и его хранении придерживайтесь следующих правил:**

3.4.1. Установить парольную защиту на вход в устройство доступа, а также на устройство мобильной связи, используемое для получения сообщений от сервисов SMS-подтверждения, SMS-информирования Системы ДБО. Регулярно проводить смену паролей.

3.4.2. Для работы с Системой ДБО необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

3.4.2.1. пароль должен иметь длину от 8 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков !#$%&()*+-./:;<=>?[\, используйте буквы верхнего и нижнего регистра.

3.4.2.2. обратите внимание, что регистр и язык букв пароля имеет значение.

3.4.2.3. пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.)

3.4.2.4. пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера банковской карты и т.п.)

3.4.2.5. пароль не должен содержать словарных слов (password, football, русские слова, набранные в английской кодировке, например, gfhjkm – пароль).

3.4.2.6. пароль не должен совпадать с шестью предыдущими паролями и не должен совпадать с именем входа (логином).

3.4.2.7. пароль не должен быть копией или комбинаций паролей, используемых Вами в других системах или Интернет-ресурсах (вход в операционную систему устройства доступа, на электронную почту, социальные сети, развлекательный ресурсы в сети Интернет и т.п.).

3.4.3. Никогда не сообщайте свой пароль третьим лицам, в том числе родственникам и сотрудникам Банка, вводите пароль только при работе в Системе ДБО. Помните, что сотрудник Банка не имеет права запрашивать у Вас пароль, даже если Вы самостоятельно обратились в Банк. Вводите пароль только в Системе ДБО, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.

3.4.4. Не записывайте и не храните пароль в местах доступа третьих лиц. Запрещается хранить пароль на устройстве доступа, мобильном устройстве, используемом для получения одноразовых SMS подтверждений, а также на иных электронных носителях, доступ к которым могут получить третьи лица, в том числе в случае заражения устройства вирусом.

3.4.5. Рекомендуется осуществлять смену пароля доступа к ключам ЭП (к Системе ДБО) и не реже одного раза в 3 месяца.

3.4.6. При возникновении подозрений, что Ваш пароль доступа к ключу ЭП (в Систему ДБО) стал известен третьим лицам, либо еще не введенные в систему одноразовый код стали известны третьим лицам (в том числе представившимся сотрудниками Банка), незамедлительно заблокировать доступ в Систему ДБО, обратившись в Банк по телефону 8 (846) 251 00 00 и произнеся блокировочное слово администратору системы.

3.5. **Остерегайтесь мошенничества**

3.5.1. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли, параметры банковских карт и другие конфиденциальные данные). Не отвечайте на такие сообщения.

3.5.2. Не открывайте подозрительные файлы, присланные Вам по электронной почте. При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении.

3.5.3. При работе с Системой ДБО обращайте внимание на страницу входа и интерфейс системы. Если у Вас возникли подозрения в подлинности сайта, необходимо незамедлительно прекратить работу и связаться с Банком по телефону 8 (846) 251 00 00 (никогда не связывайтесь по телефону, указанному на подозрительной странице).

3.5.4. Для входа в Систему ДБО необходимо ввести пароль (а в случае усиленного режима защиты дополнительно одноразовый пароль). Если Вам предлагается также заполнить иные поля (телефон, номер карты и т.п.) немедленно прекратите работу в системе и сообщите об этом в Банк.

3.5.5. Банк никогда не запрашивает одноразовый пароль или пароль на вход в Систему ДБО (к ключам ЭП) для отмены операций. При вводе пароля Вы даете Банку право на проведение операции, отменить ее с помощью пароля нельзя.

3.5.6. Если Вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему ДБО или одноразовый пароль.

3.5.7. Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Системе ДБО. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности системы вследствие проведения каких-либо регламентных работ. Если Вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону 8 (846) 251 00 00 (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).

3.5.8. В случае возникновения перечисленных ниже событий незамедлительно отключите носитель с ключами ЭП от устройства доступа, прекратите работу в Системе ДБО и обратитесь в Банк по телефону контакт-центра 8 (846) 251 00 00:

3.5.8.1. при невозможности доступа к сайту Системы ДБО и нестабильной работы системы («зависания») при нормальной работе других Интернет-ресурсов;

3.5.9. при выходе из строя устройства доступа;

3.5.9.1. при обнаружении на устройстве доступа вредоносного программного обеспечения, если зараженное устройство уже использовалось для доступа к Системе ДБО;

3.5.10. при отказе в доступе к ключам ЭП по причине некорректности пароля (PIN-кода), если уверены, что вводите корректный пароль;

3.5.11. при обнаружении отсутствия ключей ЭП на USB-токене;

3.5.12. при появление подозрительной активности на устройстве доступа, например, самопроизвольные движение курсора на экране, набор текста и т.п.

3.5.13. при обнаружении факта несанкционированного удаленного управления вашим устройством доступа;

3.5.14. при обнаружении ошибочно отправленного платежного поручения;

3.5.15. при несоответствии остатка денежных средств на расчетном счете.

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.