Рекомендации
по соблюдению требований информационной безопасности при работе
в Системе дистанционного банковского обслуживания

1. Ограничения при использовании Системы

1.1. Для доступа к Системе необходим персональный компьютер, ноутбук, планшет, устройство мобильной связи или иное устройство, предназначенное для выхода в Интернет (далее – Устройство доступа), подключенное к сети Интернет.

1.2. В случае проведения технических работ на стороне Банка, может быть введено временное ограничение на предоставление информации по счетам Клиента в Банке. О наличии таких ограничений Банк уведомляет Клиента путем размещения сообщения в Системе.

2. Случаи повышенного риска, связанные с использованием Системы.

2.1. Клиент соглашается на получение услуги с использованием Системы, осознавая, что сеть Интернет не всегда является безопасным каналом связи и 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. Банк информирует Клиента о следующих случаях повышенного риска, связанных с использованием Системы посредством доступа с Устройства доступа:

2.2.1. Использование Системы с помощью Устройства доступа, размещенного в общественном месте. В случае необходимости такого использования Клиент может максимально обезопасить себя, выполнив условия обеспечения безопасности соединения в сети Интернет (п.3.3 настоящих Рекомендаций);

2.2.2. Кража или потеря мобильного телефона, на номер которого приходят SMS-сообщения с Разовыми секретными паролями для подтверждения операций по счету посредством Системы. В случае подозрения на кражу или потерю мобильного телефона Клиент обязан незамедлительно обратиться в офис Банка для временной блокировки доступа к Системе (до восстановления SIM-карты) или изменения номера мобильного телефона;

2.2.3. Невыполнение условий обеспечения безопасности Устройства доступа, с которого осуществляется вход в Систему (п.3.4 настоящих Рекомендаций);

2.2.4. Использование Пароля, не соответствующего минимальным требованиям к безопасности (п.3.5 настоящих Рекомендаций).

2.2.5. Получение доступа к Системе посредством браузера с устройства, содержащего вредоносный или модифицированный код, а также с устройств, на которых 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 посредством доступа с Устройства доступа.

3.1. Клиент обязан исключить доступ третьих лиц к Паролю (в том числе Временному паролю, Разовому секретному паролю) и Логину:

3.1.1. Хранить Пароль и Логин раздельно в недоступных для третьих лиц местах.

3.1.2. Незамедлительно обратиться в Банк для смены Пароля в случае появления подозрений в том, что Пароль мог оказаться известен третьим лицам.

3.2. Клиент обязан при работе с Системой через устройство мобильной связи, не использовать это же устройство для получения Разовых секретных паролей.

3.3. Клиент должен обеспечить безопасность соединения в сети Интернет (при доступе с Устройства доступа, если не указано иное):

3.3.1. Собственноручно набирать в адресной строке браузера адрес Системы https://my.k-bnk.ru, либо переходить по ссылке, размещенной на официальном Интернет-сайте Банка www.koshelev-bank.ru.

3.3.2. Не переходить на сайт Системы по ссылкам, размещенным в электронных письмах или размещенным на сайтах в сети Интернет (кроме официального Интернет-сайта Банка www.koshelev-bank.ru).

3.4. Клиент должен обеспечить безопасность Устройства доступа, с которого осуществляется вход в Систему:

3.4.1. Обеспечить физическую безопасность Устройства доступа в Систему.

3.4.2. Использовать на Устройстве доступа только лицензионное программное обеспечение.

3.4.3. Использовать Устройство доступа, на котором установлена только одна операционная система.

3.4.4. Работать в операционной системе компьютера, ноутбука под локальной учетной записью с ограниченными правами доступа.

3.4.5. Установить на Устройство доступа специальные программные и если возможно аппаратные средства защиты (антивирусное программное обеспечение, средства обнаружения вредоносных программ, средства защиты информации от воздействия вредоносного кода, персональный межсетевой экран), которые должны регулярно обновляться.

3.4.6. Регулярно проводить полную антивирусную проверку Устройства доступа.

3.4.7. Своевременно обновлять операционную систему, браузеры, антивирус и другие программы для защиты от хакерских атак, установленные на Устройстве доступа.

3.4.8. Производить регулярное обновление программного обеспечения, установленного на Устройстве доступа.

3.4.9. 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.

3.4.10. Установить парольную защиту на вход в Устройство доступа.

3.4.11. Регулярно проводить смену Паролей.

3.5. При установке Пароля рекомендуется придерживаться следующих правил:

3.5.1. Длина Пароля – не менее 8 символов.

3.5.2. Пароль не должен совпадать ни с одним из последних 3 (Трех) Паролей, ранее использованных Клиентом.

3.5.3. Пароль не должен совпадать с Логином.

3.5.4. В Пароле должны присутствовать символы из разных регистров (большие и маленькие буквы) и цифры. Для предотвращения возможных осложнений, связанных с различной кодировкой, рекомендуется использовать «латиницу».

3.5.5. Пароль не должен целиком состоять из комбинации символов, несущей смысловую нагрузку. Не рекомендуется использовать имена, названия, общепринятые аббревиатуры, адреса или другие общеизвестные слова и их сочетания, в том числе русское слово, набранное в латинской транскрипции **(например: ФАМИЛИЯ - AFVBKBZ);**

3.5.6. Последовательность символов Пароля не должна иметь очевидных закономерностей (например: Пароли 11111111, 12121212, 12345678, QWERTY имеют очевидные зависимости между своими символами).

3.6. Клиент обязан внимательно знакомиться с информационными сообщениями Банка по безопасности, размещенными на Интернет-сайте Банка, на странице авторизации для входа в Систему, направленными по электронной почте или посредством SMS-сообщения. Если имеются сомнения в достоверности адреса отправителя сообщения, необходимо обратиться в Банк по телефону, указанному на Интернет-сайте Банка.