Приложение 4
к Условиям дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк» с использованием системы «Интернет-банк» и «Мобильный банк»
(приказ АО «Россельхозбанк» от 31.05.2018 № 461-ОД)
(в редакции приказов АО «Россельхозбанк» от 22.04.2019 № 516-ОД, от 21.05.2019 № 670-ОД)

Памятка по использованию системы «Интернет-банк» и «Мобильный банк» АО «Россельхозбанк»

Соблюдение рекомендаций, содержащихся в настоящей Памятке, являющейся неотъемлемой частью Условий дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк» с использованием системы «Интернет-банк» и «Мобильный банк» (далее – Условия ДБО), позволит обеспечить максимальную сохранность денежных средств, а также снизит возможные риски при совершении операций в системе «Интернет-банк» и «Мобильный банк» АО «Россельхозбанк» (далее – система, Банк), в частности, при осуществлении платежей в пользу поставщиков услуг (мобильные операторы, интернет-провайдеры и т.д.), переводах денежных средств как внутри Банка, так и в другие кредитные организации.

Возможные риски использования системы:

- в рамках предоставления метода SMS-аутентификации – несанкционированное получение сторонними лицами информации о логине, пароле/временном пароле, одноразовом пароле (несанкционированное получение сторонними лицами информации о цифровой последовательности символов), в том числе в результате заражения вредоносным кодом/вредоносным программным обеспечением компьютерного средства, используемого для доступа к системе «Интернет-банк», и/или мобильного устройства, используемого для получения SMS-сообщений с одноразовыми паролями, с последующим совершением в системе операций;
- в рамках предоставления метода программной аутентификации – несанкционированное получение сторонними лицами информации о логине, пароле, коде активации и/или ПИН-коде к генератору паролей, в том числе в результате заражения вредоносным кодом/вредоносным программным обеспечением компьютерного средства (мобильного устройства), используемого для доступа к системе «Интернет-банк» («Мобильный банк»), и/или мобильного устройства, используемого для выработки одноразовых паролей (в том числе с использованием образа отпечатка пальца/сканированного лица), с последующим совершением в системе операций;
- в рамках предоставления метода аппаратной аутентификации – несанкционированное получение сторонними лицами устройства, привязанного к учетной записи Пользователя, позволяющее получать одноразовые пароли без использования платежной карты и ПИН-кода к платежной карте.

В целях минимизации рисков хищения денежных средств при работе с системой, Пользователь обязан обеспечить выполнение следующих требований Памятки.

1. Общие рекомендации

1.1. Подключение к системе Банк осуществляет в случае успешной верификации номера мобильного телефона.

Если подключение к системе осуществляется в офисе Банка, то для проведения верификации, Клиенту необходимо сообщить код подтверждения, направленный Банком в SMS-сообщении на номер мобильного телефона Клиента, работнику Банка.

При подключении к системе в устройствах самообслуживания, Клиенту необходимо самостоятельно осуществить ввод кода подтверждения, направленного Банком в SMS-сообщении на номер мобильного телефона, указанный Клиентом в устройстве

самообслуживания при подключении к системе, в специальное поле на экране устройства самообслуживания.

При подключении к системе на основании распоряжения, сформированного на сайте Банка в сети Интернет, по адресу https://online.rshb.ru, Клиенту необходимо самостоятельно осуществить ввод кода подтверждения, направленного Банком в SMS-сообщении на номер мобильного телефона, зарегистрированный в Банке для получения 3-D паролей.

В случае, если код подтверждения ошибочно введен Клиентом не верно (в устройствах самообслуживания/ на сайте Банка в сети Интернет, по адресу https://online.rshb.ru), Клиенту необходимо осуществить заново процедуру подключения к системе.

1.2. При подключении к системе хранить в секрете информацию, полученную от Банка для осуществления аутентификации в Системе: логин, временный пароль, одноразовый пароль, код активации, а также сформированный и используемый Пользователем пароль и ПИН-код к генератору паролей, отпечаток пальца/сканирования лица, 3-D пароль.

1.3. Не осуществлять вход в систему в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, Интернет-кафе или общественный транспорт.

1.4. До входа в систему убедиться в том, что устройство (компьютер, смартфон, планшет, телефон), с которого осуществляется работа с системой, не заражен вирусами/вредоносным ПО, установлено и работоспособно[1] лицензионное антивирусное программное обеспечение, регулярно и своевременно обновляются антивирусные базы.

1.5. Для осуществления входа в систему «Интернет-банк» рекомендуется использовать виртуальную клавиатуру.

1.6. Не оставлять без присмотра систему в активном состоянии, не осуществив выход из системы специальной кнопкой «Выход». В случае бездействия Пользователя в течение 15 минут, в целях безопасности Банк автоматически завершит сеанс использования системы. Пользователю необходимо заново произвести аутентификацию в системе.

1.7. Заходить в систему «Интернет-банк» только с официального сайта Банка http://www.rshb.ru и при переходе по ссылке https://online.rshb.ru (адрес страницы должен совпадать полностью, вплоть до любого знака).

1.8. При осуществлении входа в систему «Интернет-банк», убедиться в безопасности соединения, включая наличие символа замка в адресной строке браузера.

1.9. При каждом входе в систему проверять на соответствие дату и время последнего входа.

1.10. Для использования системы «Мобильный банк» осуществлять скачивание и установку приложения только при переходе по ссылкам с официального сайта Банка https://online.rshb.ru, или через официальные магазины приложений (Google Play https://play.google.com , Apple AppStore https://appstore.com).

1.11. Устанавливать систему «Мобильный банк» с встроенным генератором паролей, в том числе с активированной функцией входа по отпечатку пальца/сканированию лица, исключительно на мобильные устройства, находящиеся в индивидуальном пользовании, защищать паролем доступ к такому мобильному устройству, не передавать мобильное устройство третьим лицам для временного использования.

1.12. Не отвечать на подозрительные звонки, электронные письма (в т.ч. переходить по ссылкам в электронных письмах) и сообщения из социальных сетей, в которых запрашивают конфиденциальную информацию (логин, пароль, одноразовый пароль, 3-D пароль и т.п. информацию), в том числе от работников Банка и их родственников. Банк никогда не обращается к клиентам с подобными просьбами.

1.13. В целях безопасности, в системе «Интернет-банк» рекомендуется изменять логин на любой другой, удобный для запоминания, с регулярностью изменения не реже 1 раза в квартал. Также, после возобновления доступа к ДБО по причине ранее произведенной

[1] Не отключено и/или не закончился срок действия лицензии.

блокировки, при первом входе в систему «Интернет-банк» рекомендуется произвести изменение логина.

1.14. При осуществлении первого входа в системы изменить временный пароль на пароль, который сможете запомнить. Рекомендуется изменять пароль не реже 1 раза в месяц. Необходимо применять в качестве паролей сложные комбинации заглавных и строчных букв и цифр. Не использовать в качестве паролей:

- простые последовательности букв и цифр (например: Abc123, Qwerty789);
- номера телефонов и паспортов;
- даты рождения и имена своих ближайших родственников;
- названия компьютеров, мониторов, окружающей вас оргтехники и любимых компаний (например: Apple123, Subaru222).

1.15. В случае самостоятельного изменения (создания) ПИН-кода к карте посредством ДБО Пользователю не рекомендуется использовать ПИН-коды, состоящие из четырех одинаковых цифр, например, «0000», «1111», связанные с персональными данными, например, дата рождения, а также из цифр, идущих подряд, например, «1234», «3456».

1.16. Не хранить в мобильном телефоне информацию, полученную от Банка в виде SMS-сообщений.

1.17. При получении временных паролей/одноразовых паролей по SMS обращать внимание на отправителя. Банк отправляет сообщения только от абонентов – RSHB.

1.18. При проведении операций сверяйте реквизиты перевода, в том числе сумму перевода/платежа на экране монитора с информацией в SMS-сообщении, в котором направлен одноразовый пароль или 3-D пароль для подтверждения операции/Push-уведомлении.

1.19. В случае внезапного приостановления работы SIM-карты для номера телефона, который является зарегистрированным номером для направления Банком SMS-сообщений незамедлительно обратиться к оператору мобильной связи для выяснения причин блокировки (возможно незаконное изготовление третьими лицами дубликата SIM-карты). В случае необходимости, осуществить блокировку ДБО, обратившись в Контакт-центр Банка.

1.20. Бережно относится к устройству, выданному Банком для генерации паролей для доступа к системе «Интернет-банк» и проведения операций с использованием системы.

1.21. Вернуть устройство в Банк при его порче/отказе от использования системы, либо представить в Банк заявление об утрате устройства.

1.22. Не передавать третьим лицам устройство, привязанное к учетной записи Пользователя, позволяющее получать одноразовые пароли без использования платежной карты и ПИН-кода к платежной карте.

1.23. Использовать систему, руководствуясь инструкциями Банка, размещенными на официальном сайте Банка в сети Интернет по адресу: www.rshb.ru.

1.24. Контакт-центр Банка по номерам телефонов 8(800)200-6099 (звонок по Российской Федерации бесплатный) и +7(495)651-6099 круглосуточно:

- принимает сообщения об утрате пароля (временного пароля) с возможностью его изменения в Контакт-центре Банка с прохождением процедуры идентификации в установленном в Банке порядке и с использованием кодового слова. В случае, если была осуществлена блокировка ДБО, то до момента разблокировки ДБО в подразделении Банка направление Пользователю временного пароля недоступно. Также возможно изменение пароля (временного пароля) при обращении в любое подразделение Банка;
- принимает сообщения об утрате логина. В случае утраты логина доступ к системе блокируется в Контакт-центре по распоряжению Пользователя. В случае, если Вы забыли логин, то информация о текущем логине может быть предоставлена Пользователю в Контакт-центре Банка с прохождением процедуры идентификации в установленном в Банке порядке и с использованием кодового слова. Также доступны иные способы получения информации о логине, в соответствии с Условиями ДБО. Для изменения логина Пользователь может обратиться в любое подразделение Банка для оформления заявления на изменения логина. За изменение логина на основании письменного заявления Пользователя, поданного в подразделение Банка, взимается комиссия в соответствии с Тарифами.

2. Действия Пользователя при компрометации

2.1. При подозрении на компрометацию (возникновение подозрений на утечку информации) или утрате:

- логина;
- пароля (в т.ч. временного пароля);
- одноразового пароля;
- 3-D пароля;
- устройства, привязанного к учетной записи Пользователя;
- ПИН-кода к генератору паролей;
- сканирования лица;
- отпечатка пальца;
- кода активации;
- кода подтверждения,

а также после обнаружения факта совершения в системе операции без согласия Пользователя, но не позднее дня, следующего за днем получения от Банка уведомления о совершении такой операции, Пользователю необходимо незамедлительно направить в Банк соответствующее уведомление, обратившись в Контакт-центр Банка или в любое подразделение Банка.

2.2. При получении информации от Пользователя о наступлении любого события, указанного в пункте 2.1 настоящей Памятки, Банк незамедлительно производит блокировку ДБО и информирует Пользователя о данном событии.

2.3. Для разблокировки доступа к ДБО, в случае, если блокировка ДБО была произведена по инициативе Пользователя, Пользователю необходимо обратиться в любое подразделение Банка с документом, удостоверяющим личность, для подачи заявления на подключение. При разблокировке ДБО Банком предоставляются прежний логин и новый временный пароль.