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)

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 цифрового 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 рамках проведения операции без использования методов 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, используемого для доступа к системе «Интернет-банк», и/или мобильного устройства, с последующим совершением/подменой в Системе операций.

Целью рекомендаций, указанных в настоящей Памятке, является доведение до Клиентов информации:

- о возможных рисках получения несанкционированного доступа к защищаемой информации, в том числе с целью осуществления операции в Системе лицами, не обладающими правом их осуществления;
- о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) Клиентом устройства, с использованием которого им совершались действия в целях осуществления операции в Системе, контролю конфигурации устройства, с использованием которого Клиентом

совершаются операции в Системе, и своевременному обнаружению воздействия вредоносного кода (программы).

Несоблюдение рекомендаций повышает риск хищения денежных средств при работе с Системой. Пользователь обязан обеспечить выполнение требований Памятки.

1. Общие рекомендации

1.1. Указывать для регистрации номера Пользователя Системы в Банке только СВОЙ личный номер телефона[1]. Указание номеров телефонов третьих лиц недопустимо. На регистрируемые номера телефонов поступает информация об операциях по счетам/картам клиентов, коды/пароли для совершения операций. Указание телефонов третьих лиц предоставляет им возможность совершать операции без контроля владельца счёта/карты и лишает Пользователя возможности контролировать состояние счёта/карты.

Подключение к Системе Банк осуществляет в случае успешной верификации номера мобильного телефона Клиента.

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

При подключении к Системе в устройствах самообслуживания, Клиенту необходимо самостоятельно, без помощи посторонних, осуществить ввод кода подтверждения, направленного Банком посредством SMS-сообщения 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 посредством SMS-сообщения на номер мобильного телефона Клиента, зарегистрированный в Банке для получения 3-D паролей.

В случае если код подтверждения 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. Сверять при проведении операций реквизиты перевода, в том числе сумму перевода/платежа на экране монитора с информацией, полученной в SMS-сообщении, в котором направлен одноразовый пароль или 3-D пароль для подтверждения операции/Push-уведомлении.

1.3. Не проводить действия в Системе и устройствах самообслуживания Банка по указанию или по рекомендациям третьих лиц, в том числе не передавать/сообщать результаты действий в Системе и устройствах самообслуживания Банка (любую цифровую или буквенную информацию) третьим лицам, в том числе представляющимся работниками Банка.

1.4. Бережно относиться к устройству, выданному Банком для генерации паролей для доступа к Системе «Интернет-банк» и проведения операций с использованием Системы. При утрате пароля или временного пароля необходимо в срочном порядке самостоятельно осуществить его изменение или обратиться в Контакт-центр Банка в соответствии с пунктом 1.8 настоящей Памятки.

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

1.6. Вернуть устройство в Банк при его порче/отказе от использования Системы либо представить в Банк заявление об утрате устройства.

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

---

[1] Номер телефона, оформленный оператором связи на персональные данные клиента, аналогичные тем, которые были переданы в Банк при оформлении банковского продукта или услуги.

1.8. Обращаться в Контакт-центр Банка по номерам телефонов 8(800)200-6099 (звонок по Российской Федерации бесплатный) и +7(495)651-6099 круглосуточно по следующим вопросам, в случаях:

- утраты 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 Системы, то до момента разблокировки Системы в подразделении Банка направление Пользователю временного пароля недоступно. Также возможно изменение пароля (временного пароля) при обращении в любое подразделение Банка;
- утраты логина. В случае утраты логина доступ к Системе блокируется в Контакт-центре Банка по распоряжению Пользователя. В случае если Пользователь забыл 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.

1.9. В целях обеспечения безопасности покупок по картам Банка в сети Интернет, Банк в автоматическом режиме осуществляет подключение способа получения 3-D паролей посредством SMS-сообщений на Зарегистрированный номер Пользователя системы «Интернет-банк» и «Мобильный банк», являющегося держателем действующей платежной карты Банка.

2. Рекомендации по предотвращению несанкционируемого доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства Клиента, контролю конфигурации устройства, и своевременному обнаружению воздействия вредоносного кода

2.1. Меры по обеспечению защиты от несанкционированного доступа неуполномоченных лиц к устройству Пользователя, с которого осуществляется доступ к системе «Интернет-банк» и «Мобильный банк»

2.1.1. 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, цифровой образ узора кожи на пальце/цифровой образ отсканированного лица, 3-D пароль.

2.1.2. 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. При использовании Системы в вышеуказанных местах незамедлительно произвести смену логина/пароля при возникновении первой возможности, не используя публичные беспроводные сети.

2.1.3. Заходить в систему «Интернет-банк» только с официального сайта Банка в сети Интернет по адресу: http://www.rshb.ru и при переходе по ссылке https://online.rshb.ru (адрес страницы должен совпадать полностью, каждый знак).

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

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

2.1.6. 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.

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

2.1.8. При каждом входе в Систему проверять на соответствие дату и время последнего входа. Если дата и время последнего входа не соответствуют, то необходимо проверить, не произведены ли несанкционированные списания со счета третьими лицами, а также незамедлительно изменить логин и пароль.

2.1.9. 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.

2.1.10. 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 Системе по причине ранее произведенной блокировки, при первом входе в систему «Интернет-банк» рекомендуется произвести изменение логина.

2.1.11. Ни при каких обстоятельствах не следует отвечать на подозрительные звонки, электронные письма, сообщения в мессенджерах или социальных сетях и SMS-сообщения, в том числе переходить по указанным в них ссылкам, и письма из социальных сетей, в которых запрашивается конфиденциальная информация (логин, пароль, одноразовый пароль, 3-D пароль и т.п. информацию), в том числе от работников Банка. Банк никогда не обращается к Пользователям с подобными просьбами. О факте подобного обращения следует немедленно сообщить в Банк.

При получении писем/сообщений даже от известных лиц – не переходить по вложенным ссылкам, не активировать какие-либо элементы сообщений без предварительного получения подтверждения от отправителя корректности ссылки/элемента по альтернативному каналу связи. Например, получена ссылка или видео в сообщении мессенджера WhatsApp и в устной форме без использования мессенджера получено подтверждение, что отправлялось именно такая ссылка или видео. Добавление вредоносных ссылок или объектов могли произойти не по воле отправителя.

2.2. Меры по обеспечению защиты устройства Клиента от воздействия вредоносных программ

2.2.1. Не рекомендуется устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщениях/электронной почте, в том числе якобы от имени Банка.

2.2.2. На устройство, в том числе мобильное, устанавливать только лицензионное программное обеспечение (далее – ПО), регулярно и своевременно обновляемое; на устройство не должно устанавливаться ПО, полученное из сомнительных источников (например, скачанное с файлообменников или торрентов). Своевременно обновляемое антивирусное ПО должно работать в автоматическом режиме; не реже одного раза в неделю должно проводиться полное антивирусное сканирование устройства; в случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления – заблокированы; антивирусное ПО не должно отключаться ни при каких обстоятельствах; рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов.

2.2.3. На устройство, в том числе мобильное, не допускается установка специализированного ПО для удаленного администрирования (например, Radmin, TeamViewer и др.).

2.2.4. На установленное на устройстве ПО необходимо своевременно устанавливать обновления безопасности операционной системы устройства, а также обновления безопасности прикладного ПО (желательно в автоматическом режиме).

2.2.5. Необходимо уделять внимание расширениям получаемых файлов. Файлы, зараженные вредоносной программой, часто маскируются под обычные графические, аудио,

видео файлы или файлы приложений MS Office и Adobe Reader (с расширением .pdf), а также архивы, содержащие вышеперечисленные файлы. Режим отображения расширения файлов должен быть включен постоянно. Не рекомендуется открывать вложения электронных писем, полученных от неизвестных вам адресатов. Такие письма лучше немедленно удалить, как и любые подозрительные сообщения.

2.2.6. При использовании браузера не переходить по ссылке и не нажимать кнопки во всплывающих окнах. При получении ссылок по электронной почте или в мессенджерах рекомендуется скопировать ссылку, вставить в адресную строку используемого браузера и убедиться, что адрес соответствует интересующему запросу.

2.2.7. Рекомендуется избегать сайтов, которые могут иметь незаконное и/или вредоносное содержание. Не следует устанавливать и/или сохранять без предварительной антивирусной проверки файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте или полученные из иных ранее неизвестных пользователю источников.

2.2.8. Рекомендуется регулярно выполнять резервное копирование важной информации, а также иметь системный загрузочный диск на случай подозрения на заражение компьютера.

2.3. Специальные рекомендации по обеспечению информационной безопасности при пользовании приложениями на мобильных устройствах Пользователя

2.3.1. Категорически не рекомендуется сохранять ПИН-код к генератору паролей и постоянный пароль на мобильное устройство, на которых запускается мобильное приложение Системы, применяемое для совершения финансовых операций.

2.3.2. Не рекомендуется сохранять ПИН-код к генератору паролей и постоянный пароль в текстовых файлах на компьютерах либо на других электронных носителях информации.

2.3.3. При получении временных паролей/одноразовых паролей посредством SMS-сообщений обращать внимание на отправителя. Банк отправляет сообщения только от абонентов RSHB.

2.3.4. Рекомендуется своевременно устанавливать доступные обновления операционной системы и приложений на мобильное устройство.

2.3.5. Рекомендуется завершать работу с мобильным приложением через завершение сессии с использованием специальной кнопки «Выход».

2.3.6. 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 Системы, обратившись в Контакт-центр Банка.

2.3.7. При утрате мобильного устройства, на которое установлено мобильное приложение, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты, заблокировать доступ в мобильное приложение при помощи специалистов Банка, а также обратиться в Банк для выявления возможных несанкционированных операций.

2.3.8. При смене номера телефона необходимо незамедлительно сообщить об этом в Банк.

2.3.9. Рекомендуется регулярно контролировать состояние своих счетов и незамедлительно сообщать сотрудникам Банка о несанкционированных операциях.

2.4. Требования, предъявляемые к паролям для обеспечения защиты информации

2.4.1. Требования к формированию пароля:

- пароль должен содержать не менее 8 символов;
- пароль должен содержать как минимум по одному символу из букв нижнего и верхнего регистра, цифры и знаки препинания;
- в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны неуполномоченными лицами путем анализа информации о пользователе;

- в качестве пароля не должен использоваться один и тот же повторяющийся символ либо комбинация из нескольких рядом стоящих символов;
- не рекомендуется ставить один и тот же пароль для доступа к различным системам;

2.4.2. Требования к хранению пароля:

- не рекомендуется записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам;
- не рекомендуется сохранять пароль от доступа к системе «Интернет-банк» в браузере.

2.4.3. Прочие требования:

- при осуществлении первого входа в Систему изменить временный пароль на пароль, который сможете запомнить. Рекомендуется изменять пароль не реже 1 раза в месяц;
- пароль в обязательном порядке подлежит изменению в том случае, если он стал известен постороннему лицу или у пользователя есть подозрения, что пароль стал известен постороннему лицу.

3. Действия Пользователя при компрометации

3.1. 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;
- цифрового образа отсканированного лица Пользователя, хранящегося в защищенном хранилище мобильного устройства Пользователя;
- цифрового образа узора кожи на пальце Пользователя, хранящегося в защищенном хранилище мобильного устройства;
- кода активации;
- кода подтверждения,

а также в случае 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, а также незамедлительно произвести замену логина и пароля.

3.2. При получении информации от Пользователя о наступлении любого события, указанного в пункте 3.1 настоящей Памятки, Банк незамедлительно производит блокировку Системы и информирует Пользователя о данном событии.

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