Приложение 14
к Условиям дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Россельхозбанк» с использованием системы
«Банк-Клиент»/«Интернет-Клиент»

Памятка
для Клиентов АО «Россельхозбанк» при использовании систем дистанционного банковского обслуживания «Банк-Клиент»/«Интернет-Клиент»

В последнее время в ряде российских банков участились случаи (попытки) хищения денежных средств Клиентов при использовании Систем ДБО.

Цели злоумышленников:

- получение персональных данных Клиента;
- возможность доступа к Системе ДБО от имени Клиента;
- отслеживание состояния счетов Клиента;
- хищение денежных средств (несанкционированный перевод денежных средств со счетов Клиентов на счета физических и юридических лиц).

Как правило, хищения (попытки хищения) осуществляются:

- работающими (или уволенными) ответственными работниками Клиента, имеющими (имевшими) доступ к ключам ЭП, носителям ключей ЭП или компьютерам, на которых реализована работа в Системе ДБО;
- штатными IT-специалистами Клиента, имеющими (имевшими) доступ к ФКН eToken или компьютерам, на которых реализована работа в Системе ДБО;
- нештатными IT-специалистами, вызываемыми для выполнения профилактических работ и подключения компьютеров Клиента к сети Интернет, для установки, настройки и обновления бухгалтерских и информационно-справочных программ или другого программного обеспечения на компьютерах Клиента, на которых реализована работа в Системе ДБО;
- злоумышленниками, использующими уязвимости системного и прикладного программного обеспечения Клиента, отсутствие действенной актуальной антивирусной защиты, фильтрации сетевого трафика и воздействующими вредоносными программами на компьютеры Клиента через сеть Интернет с последующим дистанционным хищением ключей ЭП Клиентов, логинов и паролей доступа к Системе ДБО.

Следует понимать, что направленные злоумышленниками электронные документы, подписанные действующими ключами ЭП Клиента, имеющие обычные реквизиты отправителя и получателя и типовое назначение платежа должны быть исполнены Банком. При этом вся ответственность за убытки безусловно и полностью возлагается на Клиентов как единственных владельцев ключей ЭП.

Исходя из вышеизложенного, в целях обеспечения информационной безопасности при использовании Системы ДБО Банк рекомендует:

1. Соблюдать меры безопасности по режиму:

- размещать компьютеры в помещениях, которые обеспечивают безопасность конфиденциальной информации, СКЗИ, ключей ЭП;
- исключить доступ к компьютерам, использующимся в Системе ДБО, персонала, не имеющего отношения к работе в Системе ДБО;
- обеспечить контроль за действиями IT-специалистов при обслуживании компьютеров, подключенных к Системе ДБО;
- размещение и установка СКЗИ должны удовлетворять требованиям документации на СКЗИ.

2. Обеспечить безопасность ключей ЭП:

- хранить ключи ЭП только на ФКН eToken;

- не использовать съемные носители информации, предназначенные для хранения ключей ЭП, для каких-либо иных целей;

- работу с ключами поручать только специально выделенным работникам, которые должны нести персональную ответственность за сохранность ключей;

- незамедлительно сообщать Уполномоченным работникам Банка о фактах компрометации или подозрения в компрометации ключей, в том числе, о переводе на другую работу или увольнении работников, имевших доступ к ключевой информации (использование скомпрометированного ключа должно быть немедленно прекращено);

- предусмотреть хранение носителей с ключами ЭП в надежном хранилище (сейф, металлический шкаф), допуская их извлечение только на период непосредственной работы с ключами;

- обеспечить контроль носителей с ключами при их нахождении вне хранилища (в случае даже кратковременного отсутствия на рабочем месте работника, ответственного за ключи, носители ключей должны быть убраны в хранилище);

- при использовании системы «Интернет-Клиент» устанавливать в компьютер носители с ключами только для авторизации Клиента и подписания ЭД ЭП (после выполнения отмеченных операций носители с ключами должны быть извлечены из компьютера);

- при использовании системы «Банк-Клиент» устанавливать в компьютер носители с ключами только для простановки ЭП на ЭД и извлечь из компьютера сразу же после завершения сеанса связи с Банком в Системе ДБО;

- не передавать ключи ЭП, а также логин и пароль доступа к Системе ДБО кому-либо, в том числе IT-специалистам при проверке работоспособности Системы ДБО, установке параметров и настройке аппаратуры;

- находясь в общественном месте (выставка, библиотека, магазин, интернет-кафе и др.) по возможности исключить какие-либо действия с ключами ЭП, логином и паролем доступа к Системе ДБО, а также использование публичных компьютеров, находящихся в общественном месте, для обмена сообщениями с Банком.

3. Применять необходимые меры антивирусной защиты:

- применять на рабочем месте лицензионные средства антивирусной защиты; обеспечить регулярное обновление антивирусных баз и их поддержание в актуальном состоянии; еженедельно проводить полную антивирусную проверку;

- исключить посещение интернет-сайтов сомнительного содержания (в первую очередь, игровых, спортивных, сайтов развлекательного характера) с компьютеров, подключенных к Системе ДБО;

- при работе с электронной почтой не открывать письма и вложения к ним, поступившие от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам (не активизировать ссылки);

- не отвечать на письма, поступившие якобы от имени Банка, с предложениями (просьбами, требованиями) зайти на сайт, не принадлежащий домену Банка;

- использовать только программное обеспечение Системы ДБО, предоставленное Банку;

- если компьютер, предназначенный для работы в Системе ДБО, неожиданно перестал запускаться или выдает непонятные сообщения, необходимо незамедлительно проинформировать об этом Уполномоченных лиц Банка и исключить использование действующих рабочих ключей ЭП (извлечь носитель с ключами в случае его нахождения в компьютере);

- при увольнении штатных IT-специалистов, осуществлявших обслуживание компьютеров, используемых для работы в Системе ДБО, а также после любых действий внештатных IT-специалистов или других работников, выполнявших какие-либо операции с компьютерами, предназначенными для работы в Системе ДБО, провести проверку компьютеров на отсутствие вредоносных программ;

- при возникновении подозрений о наличие в компьютере вредоносных программ, незамедлительно исключить использование действующих рабочих ключей ЭП (извлечь

носитель с ключами в случае его нахождения в компьютере) и сообщить об инциденте в Банк (возобновление работы с ключами допустимо только после проверки компьютера и устранения зараженности).

4. Формировать пароль доступа к Системе ДБО с учетом следующих требований:

- пароль должен содержать не менее 8 символов латиницы и кириллицы (цифры, специальные символы и буквы алфавита в верхнем и нижнем регистрах);
- последовательность символов не должна содержать очевидных закономерностей;
- пароль не должен содержать:
  - комбинации символов, несущих смысловую нагрузку (имена, фамилии, названия);
  - последовательность символов, состоящих только из цифр (в том числе, номера телефонов, памятные даты, реквизиты Клиента и т.п.) или букв;
  - последовательности повторяющихся букв и цифр;
  - подряд идущие в алфавите или раскладке клавиатуры символы;
- регулярно проводить смену пароля (не реже 1 раза в месяц).

5. Помнить, что Банк никогда не запрашивает у Клиентов информацию (в том числе, путем рассылки электронных писем) об их персональных данных, ключах ЭП, логине и пароле доступа к Системе ДБО. При поступлении таких запросов, не отвечая на них, следует незамедлительно поставить в известность Уполномоченных лиц Банка.

6. Строго соблюдать положения документов Банка, регламентирующих условия доступа Клиента к Системе ДБО, требования по использованию, хранению, уничтожению криптографических ключей ЭП, СКЗИ, логинов, паролей, а также выполнять все рекомендации Банка по эксплуатации технических средств.

7. Обращаться в Банк по всем вопросам организации электронного документооборота по телефонам, переданным Клиенту при открытии банковского счета или указанным в договоре банковского обслуживания с использованием Системы ДБО.