Памятка
для клиентов АО «Россельхозбанк» при использовании информационной системы «Цифровой канал обслуживания юридических лиц «Свой бизнес»

В последнее время в ряде российских банков участились случаи (попытки) хищения денежных средств Клиентов при использовании систем дистанционного банковского обслуживания юридических лиц.

Цели злоумышленников:

- получение персональных данных Клиента;
- возможность доступа к системам дистанционного банковского обслуживания 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/мобильным устройствам, на которых реализована работа систем дистанционного банковского обслуживания;
- штатными IT-специалистами Клиента, имеющими (имевшими) доступ к КН или компьютерам/мобильным устройствам, на которых реализована работа систем дистанционного банковского обслуживания;
- нештатными IT-специалистами, вызываемыми для выполнения профилактических работ и подключения компьютеров/мобильных устройств Клиента к сети Интернет, для установки, настройки и обновления бухгалтерских и информационно-справочных программ или другого программного обеспечения на компьютерах/мобильных устройствах Клиента, на которых реализована работа систем дистанционного банковского обслуживания;
- злоумышленниками, использующими уязвимости системного и прикладного программного обеспечения Клиента, отсутствие действенной актуальной антивирусной защиты, фильтрации сетевого трафика и воздействующими вредоносными программами на компьютеры/мобильные устройства Клиента через сеть Интернет с последующим дистанционным хищением ключей ЭП Клиентов, логинов, паролей и PIN-кодов доступа к системам дистанционного банковского обслуживания.

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 ИС Свой Бизнес Банк рекомендует:

1. Соблюдать меры безопасности по режиму:

- размещать компьютеры/мобильные устройства в помещениях, которые обеспечивают безопасность конфиденциальной информации, СКЗИ, ключей ЭП;
- исключить доступ к компьютерам/мобильным устройствам, использующимся в ИС Свой Бизнес, персонала, не имеющего отношения к работе в ИС Свой Бизнес;
- обеспечить контроль за действиями IT-специалистов при обслуживании компьютеров/мобильных устройств, подключенных к ИС Свой Бизнес;
- размещение и установка СКЗИ должны удовлетворять требованиям документации на СКЗИ.

2. Обеспечить безопасность ключей ЭП:

- хранить ключи ЭП только на КН;

- не использовать съемные носители информации, предназначенные для хранения ключей ЭП, для каких-либо иных целей;
- работу с ключами ЭП поручать только специально выделенным работникам, которые должны нести персональную ответственность за сохранность ключей ЭП;
- ключи ЭП каждого уполномоченного лица Клиента должны храниться на отдельном КН;
- незамедлительно сообщать Уполномоченным работникам Банка о фактах компрометации или подозрения в компрометации ключей ЭП, в том числе, о переводе на другую работу или увольнении работников, имевших доступ к ключевой информации (использование скомпрометированного ключа ЭП должно быть немедленно прекращено);
- предусмотреть хранение КН с ключами ЭП в надежном хранилище (сейф, металлический шкаф), допуская их извлечение только на период непосредственной работы с ключами ЭП;
- обеспечить контроль КН с ключами ЭП при их нахождении вне хранилища (в случае даже кратковременного отсутствия на рабочем месте работника, ответственного за ключи ЭП, КН ключей ЭП должны быть убраны в хранилище);
- при использовании системы Интернет-банк Свой Бизнес с УНЭП устанавливать в компьютер КН с ключами ЭП только для авторизации Клиента и подписания ЭД ЭП (после выполнения отмеченных операций носители с ключами ЭП должны быть извлечены из компьютера);
- не передавать ключи ЭП/КН, а также логин и пароль/PIN-код доступа к ИС Свой Бизнес кому-либо, в том числе IT-специалистам при проверке работоспособности ИС Свой Бизнес, установке параметров и настройке аппаратуры;
- находясь в общественном месте, где услуги Интернета являются общедоступными, и/или предоставляются с использованием публичных беспроводных сетей (выставка, библиотека, магазин, интернет-кафе и др.) по возможности исключить какие-либо действия с ключами ЭП/КН, логином и паролем/PIN-кодом доступа к ИС Свой Бизнес, а также использование публичных компьютеров, находящихся в общественном месте, для обмена сообщениями с Банком.

3. Применять необходимые меры антивирусной защиты:

- применять на компьютере/мобильном устройстве Клиента, на которых реализована работа в ИС Свой Бизнес, 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/мобильных устройств, подключенных к ИС Свой Бизнес;
- при работе с электронной почтой не открывать подозрительные письма и вложения к ним, поступившие от неизвестных отправителей, в том числе сообщения в мессенджерах или социальных сетях и не переходить по содержащимся в таких письмах/сообщениях ссылкам (не активизировать ссылки);
- не отвечать на письма, поступившие якобы от имени Банка, с предложениями (просьбами, требованиями) зайти на сайт, не принадлежащий домену Банка или в которых запрашивается конфиденциальная информация (логин, пароль, иная конфиденциальная информация Клиента);
- использовать только необходимое программное обеспечение для функционирования ИС Свой Бизнес, предоставленное Банком;
- устанавливать Мобильное приложение на мобильном устройстве Клиента только из доверенных источников, размещенных в «Play Маркет», «App Store», «App gallery» «Galaxy Store», «RuStore» и «NashStore»;
- если компьютер/мобильное устройство Клиента, предназначенные для работы в ИС Свой Бизнес, неожиданно перестали запускаться или выдают непонятные сообщения,

необходимо незамедлительно проинформировать об этом Уполномоченных лиц Банка и исключить использование ключей ЭП (извлечь КН с ключами ЭП в случае его нахождения в компьютере);

- при увольнении штатных IT-специалистов, осуществлявших обслуживание компьютеров/мобильных устройств Клиента, используемых для работы в ИС Свой Бизнес, а также после любых действий внештатных IT-специалистов или других работников, выполнявших какие-либо операции с компьютерами/мобильными устройствами Клиента, предназначенными для работы в ИС Свой Бизнес, провести проверку компьютеров/мобильных устройств Клиента на отсутствие вредоносных программ (вирусов);
- при возникновении подозрений о наличие в компьютере вредоносных программ (вирусов), незамедлительно исключить использование ключей ЭП (извлечь КН с ключами ЭП в случае его нахождения в компьютере) и сообщить об инциденте в Банк (возобновление работы с ключами ЭП допустимо только после проверки компьютера и устранения зараженности);
- исключить использование специализированного программного обеспечения для удаленного администрирования («RAdmin», «TeamViewer», «Ammyy Admin» и другого программного обеспечения с подобным функционалом) на компьютере/мобильном устройстве Клиента, подключенного к ИС Свой Бизнес. Если на компьютере/мобильном устройстве Клиента, с которого осуществляется взаимодействие с ИС Свой Бизнес, установлено специализированное программное обеспечение для удаленного администрирования, то Банк не несет ответственности за несанкционированный доступ к данным Клиента Банка сторонними лицами, в том числе к счетам и/или депозитам Клиента.
- при взаимодействии с контрагентами и получении по электронной почте реквизитов на перевод денежных средств необходимо дополнительно проверить и подтвердить у контрагента реквизиты по альтернативным каналам передачи данных. После перевода денежных средств получить информацию от контрагента об успешном получении денежных средств.

4. Формировать пароль доступа к ИС Свой Бизнес 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/PIN-коде доступа к ИС Свой Бизнес. 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 ИС Свой Бизнес, требования по использованию, хранению, уничтожению криптографических ключей ЭП, СКЗИ, логинов, паролей/PIN-кодов, 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 ИС Свой Бизнеса.