ПРИЛОЖЕНИЕ № 12
РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

МОСКОМБАНК
Commercial Bank of Moscow

РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА В ДБО

В области информационной безопасности АО «МОСКОМБАНК» рекомендует Клиенту:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Системы. Признаком установки защищённого соединения является наличие информации о протоколе https в адресной строке используемого клиентом браузера, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.

2. Осуществлять вход в Систему только через Сайт Банка *москомбанк.рф (https://www.moscombank.ru)*.

3. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену *москомбанк.рф (https://www.moscombank.ru)*, сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефонам: (495) 109-00-14. Банк не осуществляет рассылку электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Системы.

4. Извлекать из компьютера USB-токен или другой носитель, содержащий ключ электронной подписи, сразу после завершения работы с ним в Системе.

5. Обеспечить использование USB/MAC-токенов только ответственным сотрудником, уполномоченным на то соответствующим распорядительным документом.

6. Не передавать токены или другие носители, содержащие ключ электронной подписи неуполномоченным сотрудникам Клиента (в том числе ИТ-сотрудникам, а также сотрудникам Банка) для проверки работы Системы, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить USB-токен или другой носитель ЭП к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентской части Системы, и лично ввести пароль, сохраняя его конфиденциальность.

7. Хранить токены или другие носители, содержащие ключи электронной подписи, в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя. Вся ответственность за сохранность и использование ключей ЭП полностью лежит на Клиенте, как единственном их владельце

8. Не отлучаться от устройства с установленным ДБО в период активной сессии с Системой, либо завершить активную сессию ДБО.

9. Использовать виртуальную клавиатуру. Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками. Виртуальная клавиатура появляется при входе в Систему. При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе (если пароль содержит заглавную букву или символ, нажмите клавишу Shift, переключение между русским и английским алфавитом - клавиша Рус/Lat, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите Enter.

10. Для получения сообщений для SMS-аутентификации ограничить доступ к устройству (телефону) подвижной радиотелефонной связи, которое зарегистрировано для этих целей.

11. Обеспечить отсутствие доступа третьих лиц к устройству и сим-карте, посредством которых осуществляется доступ к номеру телефона, используемого при работе в системе ДБО (в том числе для формирования простой электронной подписи), в том числе с использованием штатных средств ограничения доступа (PIN-код, графический ключ, Touch ID, Face ID и т.п).

12. Обеспечить сокрытие отображения текстов смс-сообщений или PUSH-уведомлений на заблокированном мобильном устройстве.

13. Не подключаться к общедоступным Wi-Fi сетям.

14. Не записывать используемый Пароль там, где доступ к нему могут получить посторонние лица.

15. Незамедлительно произвести блокировку сим-карты в случае утери или кражи мобильного устройства или сим-карты.

16. Написать заявление сотовому оператору о запрете принимать обращения на блокировку/разблокировку/замену сим-карты от третьих лиц по доверенности.

17. В случае обнаружения блокировки Вашей сим-карты без Вашего ведома немедленно заблокировать доступ в Системе, обратившись в службу поддержки по телефону на сайте Банка.

18. При подписании платежного документа в системе ДБО осуществлять сверку реквизитов, полученных в SMS-сообщении, с кодом подтверждения, с реквизитами документа, отображаемыми в интерфейсе Системы.

19. При использовании услуг SMS-информирования об операциях проверять реквизиты в направляемых Банком информационных сообщениях о проведенных операциях. В случае возникновения подозрений о мошеннических действиях незамедлительно сообщать Банку по официальному номеру телефона, указанному на сайте Банка.

20. В случае выявления явных или косвенных признаков Компрометации ключей ЭП или вредоносных программ в компьютере, используемом для работы в Системе, незамедлительно уведомить об этом Банк по телефонам: (495) 109-00-14, либо лично явившись в Банк с целью блокирования скомпрометированных ключей ЭП с последующей их заменой. К событиям, связанным с Компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- утеря USB-токена или другого устройства, содержащего ключ электронной подписи, в том числе с последующим обнаружением;
- выход USB-токена или другого устройства, содержащего ключ электронной подписи, когда невозможно достоверно определить причину этого события (доказательно не

опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

- обнаружение факта или угрозы использования (копирования) ключа ЭП и/или доступа к Системе с использованием ключа ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение вредоносных программ в компьютере, используемом для работы в Системе;
- увольнение ответственного сотрудника Клиента, имевшего доступ к ключу ЭП.

21. Обеспечивать конфиденциальность использования пароля Клиента для доступа к ключу ЭП. Пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.

22. Применять на рабочем месте лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, спам-фильтры.

23. Производить периодическую (не реже 1 раза в 3 месяца) смену пароля ключей ЭП, а так же в случае Компрометации ключа или по требованию Банка. Пароли должны выбираться исходя из следующих требований:

- длина пароля не менее 8 символов;
- пароль должен состоять из больших и маленьких букв, цифр и специальных символов (+ = * и т.д.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (qwerty, qwerty123, 12345678 и т.д.);
- при смене пароля он должен отличаться от предыдущего не менее чем в 2х позициях.

24. Самостоятельно настроить используемое оборудование и программное обеспечение для работы с сетью Интернет по защищенному протоколу https.

25. Не использовать на рабочем месте любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer, AnyDesk, Ammy Admin и др.). Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

26. При использовании мобильного устройства установить на него антивирусное программное обеспечение и пароль доступа к устройству, не использовать мобильное устройство с расширенными правами (Jailbreak/Root), так как это значительно снижает уровень обеспечения безопасности устройства. Регулярно устанавливать обновления для Вашего устройства и установленного антивирусного программного обеспечения, защитить свое мобильное устройство кодом блокировки экрана, паролем или отпечатком пальца.

27. Не устанавливать на мобильное устройство, используемое для приема SMS-сообщений с подтверждающим одноразовым Паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим Клиентам ссылки или указания на установку приложений.

28. При утрате мобильного устройства или SIM-карты, используемых для приема SMS-сообщений с подтверждающим одноразовым Паролем, немедленно обратиться к своему оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Системе и проверки последних платежей.

29. Выделить для использования в Системе отдельный компьютер, настроенный на работу только с сервером Банка, а при наличии двух ключей электронной подписи – двух выделенных компьютеров, так как вероятность вирусного заражения обоих компьютеров резко снижается.

30. Исключить доступ к компьютерам, используемым для работы в Системе, посторонним лицам и персоналу организации Клиента, не уполномоченному на работу в Системе и/или обслуживание компьютеров.

31. На компьютерах, используемых для работы в Системе, исключить посещение всех интернет-сайтов, кроме используемых для входа в Систему, а также исключить установку развлекательных и игровых программ.

32. Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО, исключить использование самодельных «сборок» и взломанного программного обеспечения.

33. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями. Обеспечить использование ключей электронной подписи и MAC-токенов только ответственными сотрудниками, не оставлять USB-токен подключенным к компьютеру постоянно, использовать USB-токен только для подписания документов в Системе.

34. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе только с указанных Клиентом IP адресов/сетей).

В области социальной инженерии АО «МОСКОМБАНК» рекомендует Клиенту:

1. Обращать внимание на следующие признаки мошенничества:
   - мошенник обращается с неизвестного номера телефона;
   - мошенник представляется сотрудником Банка, Центрального Банка, Федеральных органов исполнительной власти (полиция, следователи, сотрудники Федеральной службы безопасности), операторов связи;
   - Клиенту предлагается или какая-то выгода или описывается проблема и предлагается путь решения;
   - от Клиента требуют сообщить номера карты, ПИН-код, логин и пароль от банковских приложений, подтвердить код по СМС, перейти по ссылке в СМС или e-mail сообщении, т.е. провести компрометацию конфиденциальных данных;
   - от Клиента требуют провести мгновенную оплату, перевод денежных средств;
   - от Клиента требуют быстрого принятия решения, немедленной реакции;
   - возражают против того, чтобы Клиент позвонил позже, препятствуют разъединению телефонного звонка.