ПРИЛОЖЕНИЕ № 12
ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

В целях обеспечения информационной безопасности при работе в системе дистанционного банковского обслуживания (далее – Система) **Клиент обязуется**:

1. Осуществлять вход в Систему только через Сайт Банка *москомбанк.рф (https://www.moscombank.ru).*
2. 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, (495) 609-19-19 . 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.
3. Извлекать из компьютера USB-токен или другой носитель, содержащий ключ электронной подписи, сразу после завершения работы с ним в Системе.
4. Обеспечить использование USB/MAC-токенов только ответственным сотрудником, уполномоченным на то соответствующим распорядительным документом.
5. 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.
6. 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
7 Для получения сообщений для SMS-аутентификации ограничить доступ к устройству (телефону) подвижной радиотелефонной связи, которое зарегистрировано для этих целей.
7.1. 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).
7.2. Обеспечить сокрытие отображения текстов смс-сообщений или PUSH-уведомлений на заблокированном мобильном устройстве.
7.3. Не подключаться к общедоступным Wi-Fi сетям.
7.4. Незамедлительно произвести блокировку сим-карты в случае утери или кражи мобильного устройства или сим-карты.
7.5. Написать заявление сотовому оператору о запрете принимать обращения на блокировку/разблокировку/замену сим-карты от третьих лиц по доверенности.

7.6. В случае обнаружения блокировки Вашей сим-карты без Вашего ведома немедленно заблокировать доступ в системе ДБО, обратившись в службу поддержки по телефону на сайте Банка.
7.7. При подписании платежного документа в системе ДБО осуществлять сверку реквизитов, полученных в смс-сообщении, с кодом подтверждения, с реквизитами документа, отображаемыми в интерфейсе системы ДБО.
7.8. При использовании услуг смс/e-mail-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.
8. 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, (495) 609-19-19, 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.

9. Обеспечивать конфиденциальность использования пароля Клиента для доступа к ключу ЭП. Пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.
10. Применять на рабочем месте лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, спам-фильтры.
11. Производить периодическую (не реже 1 раза в 3 месяца) смену пароля ключей ЭП, а так же в случае Компрометации ключа или по требованию Банка.
12. Самостоятельно настроить используемое оборудование и программное обеспечение для работы с сетью Интернет по защищенному протоколу https.
13. Не использовать на рабочем месте любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer и др.). Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

Помимо указанных выше требований Банк настоятельно рекомендует:

1. 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.
2. 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.
3. 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.

4. Перед началом работы проверить наличие защищенного (зашифрованного) соединения с сервером системы: символ замка и буква «S» в адресной строке – https://www.moscombank.ru, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.
5. Не использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, имена, фамилии, даты рождения, не записывать его там, где доступ к нему могут получить посторонние.
6. В качестве дополнительной меры по обеспечению информационной безопасности использовать MAC-токен. Использование одноразовых цифровых кодов позволяет в Системе дополнительно идентифицировать Клиента, подтверждать платежи больше лимита и вести список доверенных получателей электронных платежей.
7. 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.
8. Для хранения ключей ЭП использовать только аппаратное средство хранения и генерации ключей ЭП – USB-токен(ы) или другие средства, которые Банк примет решение применять для повышения безопасности платежей Клиентов.
9. 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.
10. 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).