Инструкция Клиента по обеспечению информационной безопасности при работе по Системе «Клиент-Банк» (далее – «Система»)

Требования по обеспечению информационной безопасности при работе по Системе

В целях обеспечения информационной безопасности при работе по Системе **Клиент обязан**:

1. Осуществлять вход в Систему только через сайт https://client.mvbank.ru при вводе логина и пароля пользоваться «Безопасной Авторизацией» посредством виртуальной клавиатуры.
2. Ни в коем случае не отвечать на письма, якобы от имени Системы, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену mvbank.ru., прислать секретный ключ или пароль доступа к нему, а немедленно сообщить о подобном факте Администратору Системы в рабочие часы Банка по телефону: +7 (495) 221-38-70.

Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

3. Хранить ключи ЭП на съемном носителе (дискеты, флеш-диски, CD-диски), а не на жестком диске компьютера.
4. Не отлучаться от компьютера, пока в нем находится съемный носитель, содержащий ключ ЭП.
5. Извлекать из компьютера съемный носитель, содержащий ключ ЭП, сразу после завершения работы в Системе.
6. Не записывать на носитель, содержащий ключ ЭП, какую либо другую информацию.
7. Обеспечить использование ключа ЭП только ответственным сотрудником, уполномоченным на то соответствующим распорядительным актом.
8. Никогда не передавать ключи ЭП ИТ-сотрудникам для проверки работы Системы, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить съемный носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа, и лично ввести пароль, исключая его подсматривание.
9. Хранить съемный носитель, содержащий ключ ЭП, в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя.

Банк информирует Вас, что вся ответственность за конфиденциальность Ваших ключей ЭП полностью лежит на Вас, как единственных владельцах ключей ЭП.

10. В случае выявления явных или косвенных признаков компрометации ключей ЭП или вредоносных программ в компьютере, используемом для работы в Системе, незамедлительно уведомить Банк по тел. +7 (495) 221-38-70.

К событиям, связанным с компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- *утеря материального носителя, содержащего ключ ЭП, в том числе с последующим обнаружением;*
- *выход из строя материального носителя, содержащего ключ ЭП, 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;*
- *увольнение ответственного сотрудника Клиента, имевшего доступ к ключу ЭП.*

11. Обеспечивать конфиденциальность использования пароля Клиента для доступа к ключу ЭП; пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.
12. Применять на рабочем месте средства антивирусной защиты с возможностью автоматического обновления, антивирусных баз и специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.
13. Производить смену ключей ЭП как в случае компрометации, так и по требованию Банка.
14. Периодически производить смену пароля. Рекомендуем не реже 1 раза в месяц.

Помимо указанных выше требований **Банк рекомендует** также:

1. Исключить доступ к компьютерам, используемым для работы по Системе, посторонним лицам и персоналу предприятия, не уполномоченному на работу по Системе и/или обслуживание компьютеров.
2. Ограничить доступ к компьютерам, используемым для работы с Системой. На компьютерах, используемых для работы с Системой, полностью исключить посещение Интернет-сайтов, установку развлекательных и игровых программ.
3. Использовать только лицензионное ПО (операционные Системы, офисные пакеты и пр.), обеспечить автоматическое обновление Системного и прикладного ПО.
4. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль за выполняемыми ими действиями.
5. **В качестве дополнительных мер по обеспечению информационной безопасности АКБ «Московский Вексельный Банк» (ЗАО) предлагает воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе только с указанных Клиентом IP-адресов/сетей) и MAC-фильтрацию (разрешение доступа к Системе только с указанных Клиентом компьютера).**

6. АКБ «Московский Вексельный Банк» (АО), проявляя заботу о безопасности и комфорте своих клиентов, а также с целью исключения возможностей несанкционированного доступа к счетам клиентов третьих лиц, вводит в обязательном порядке использование клиентами аппаратных электронных ключей подписи-шифрования на основе Системы E-token. Электронный ключ E-token представляет собой персональное средство строгой аутентификации и хранения данных, аппаратно поддерживающего работу с цифровыми сертификатами и электронной цифровой подписью. Использование защищенного носителя E-token обеспечивает безопасное хранение ключей ЭП пользователя, полностью исключает в**озможность хищения и копирования ключей, так как** ключ электронно-цифровой подписи клиента никогда и никем не может быть считан из E-token.
Формирование ЭП по ГОСТ Р34.10-2001 осуществляется непосредственно внутри E-token, он использует в своем составе криптобиблиотеку, сертифицированную ФСБ РФ.

Ознакомлен и согласен _____/_____/
подпись *Ф.И.О.*