Приложение № 14
к Правилам об использовании электронного
средства платежа Система «IBank»

РЕКОМЕНДАЦИИ ДЛЯ КЛИЕНТА ПО СНИЖЕНИЮ РИСКОВ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА

1. Никому не сообщать одноразовый пароль, полученный от банка в SMS/push.
2. Отключать, извлекать носители с ключами электронной подписи (токены), если они не используются для работы с системой ДБО iBank, рекомендуется применять дополнительные средства подтверждения при переводе денежных средств.
3. Не пользоваться системой ДБО iBank с гостевых рабочих мест. При использовании гостевых рабочих мест повышается риск несанкционированного использования ключей электронной подписи и паролей.
4. Ограничить доступ к компьютерам, используемым для работы с системой ДБО iBank.
5. На компьютерах, используемых для работы с системой ДБО iBank, исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения. Указанные сайты и программное обеспечение могут являться разносчиками вредоносного программного обеспечения, предназначенного для кражи денежных средств.
6. Убедиться перед вводом своих данных на сайте Банка, что соединение установлено с официальным Сайтом Банка. Для этого необходимо проверить правильность указания адреса Сайта Банка в строке браузера и наличие сертификата безопасности (https в адресной строке).
7. В случае обнаружения подозрительных сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением Сайта Банка, а также при отсутствии возможности подключения к Сайту Банка – сообщить в Банк по электронной почте is@kremlinbank.ru или по телефону +7 (499) 241-8814 доб. 167, 207.
8. Использовать только лицензионное программное обеспечение или свободно распространяемое программное обеспечение с официальных сайтов (операционные системы, офисные пакеты и пр.).
9. Обеспечить автоматическое обновление системного и прикладного программного обеспечения.
10. Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз.
11. Применять на рабочем месте лицензионные антивирусы, персональные межсетевые экраны, антишпионское программное обеспечение и т.п.
12. Исключить обслуживание компьютеров, используемых для работы с системой ДБО iBank, случайными ИТ-специалистами.
13. При обслуживании компьютера ИТ-специалистами обеспечивать контроль за выполняемыми ими действиями.
14. Никогда не передавать ключи электронной подписи ИТ-специалистам для проверки работы системы ДБО iBank, проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок владелец ключа электронной подписи лично должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентской части системы ДБО iBank, и лично ввести пароль.
15. После обслуживания ИТ-специалистом компьютера, используемого для работы с системой ДБО iBank, убедиться в отсутствии вредоносных программ на компьютере.
16. При возникновении подозрений на несанкционированную работу в системе ДБО iBank или на наличие в компьютере вредоносных программ – немедленно позвонить в Банк и заблокировать ключи электронной подписи.
17. Если замечено проявление необычного поведения системы ДБО iBank или какие-то изменения в интерфейсе системы ДБО iBank – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии системы ДБО iBank. Если нет – заблокировать ключи электронной подписи.