Приложение № 1
к Положению о выявлении операций,
соответствующих признакам
осуществления переводов денежных средств
без согласия клиентов

Рекомендации для клиента по снижению рисков повторного 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.
3. Не пользоваться Системой ДБО 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. По возможности исключить / ограничить удаленное управление компьютером с Системой ДБО.
5. На компьютерах, используемых для работы с Системой ДБО, 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: dbo@okbank.ru или safety@okbank.ru или по телефонам +7 (812) 309-21-66 или +7 (812) 309-21-68.
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 персональные межсетевые экраны, антишпионское программное обеспечение и т.п.
12. Исключить обслуживание компьютеров, используемых для работы с Системой ДБО, случайными сотрудниками технической поддержки.
13. При обслуживании компьютера сотрудниками технической поддержки обеспечивать контроль за выполняемыми ими действиями.
14. Никогда не передавать ключи электронной подписи сотрудникам технической поддержки для проверки работы системы ДБО, 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, и лично ввести пароль.

15. При увольнении ответственного сотрудника или сотрудника технической поддержки, имевшего доступ к ключу электронной подписи, обязательно позвонить в Банк с уведомлением о приостановлении использования электронного средства платежа (ключа электронной подписи). При необходимости, выпустить новый ключ электронной подписи.
16. При увольнении сотрудника технической поддержки, осуществлявшего обслуживание компьютеров, используемых для работы с Системой ДБО, убедиться в отсутствии вредоносных программ на компьютерах.
17. При возникновении подозрений на несанкционированную работу в Системе ДБО или на наличие в компьютере вредоносных программ – немедленно позвонить в Банк по телефонам +7 (812) 309-21-66 или +7 (812) 309-21-68 или написать по электронной почте: dbo@okbank.ru или safety@okbank.ru о приостановлении использования электронного средства платежа (ключа электронной подписи).
18. Если замечено проявление необычного поведения Системы ДБО или какие-то изменения в интерфейсе Системы ДБО – позвонить в Банк по телефонам +7 (812) 309-21-66 или +7 (812) 309-21-68 или написать по электронной почте: dbo@okbank.ru или safety@okbank.ru и выяснить, не связаны ли такие изменения с обновлением версии системы ДБО. Если нет – обратиться в Банк с уведомлением о приостановлении использования электронного средства платежа (ключа электронной подписи).