Приложение 9
к Соглашению Дистанционного Банковского Обслуживания
«Клиент-Банк»

ПРАВИЛА БЕЗОПАСНОСТИ КЛИЕНТА ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (ДАЛЕЕ – ДБО)

- Для работы с Системой ДБО необходимо иметь персональный компьютер (далее – ПК).
- Операционная система и необходимое программное обеспечение (далее – ПО) данного ПК должны быть только лицензионными.
- Используемый ПК должен быть оснащен антивирусным ПО.
- При первом входе в систему, а так же регулярно, каждый месяц меняйте пароли на систему ДБО.
- Ежегодно производите перегенерацию криптографических ключей.

Доступ к данному ПК и его использование внутри организации Клиента должен быть регламентирован, в том числе список хостов, доступных для данного ПК. Список должен исключать хосты, содержащие рекламный, новостной и развлекательный контент, и содержать только список IP адресов Банковских Систем ДБО или подобных государственных служб.

- Очень опасно хранить секретные ключи на жестком диске в каком-либо виде и создавать копии. Необходимо хранить секретные ключи на съемном носителе e-Token и держать их в надежном, недоступном для третьих лиц месте (например, сейф)
- Использование секретных Ключей должно производиться в момент работы с Системой ДБО и контролироваться Вами как Владельцем данного Ключа. Используя нелицензионное ПО и оставляя секретные Ключи без присмотра, Вы рискуете их скомпрометировать и сделать доступными для третьих лиц, т.к. такое ПО может заведомо содержать вредоносный код.
- Никогда и никому не сообщайте логины \ пароли Систем ДБО и тем более не доверяйте секретные ключи. Даже если этого попросит сотрудник Банка.
- В случае, если Вы, как Владелец секретного Ключа, доверяете управление своим банковским счетом посредством ДБО другому лицу, такая передача управления должна быть зафиксирована юридически, с обязательным письменным уведомлением Банка и предоставлением заверенной нотариально копии доверенности.
- Избегайте использования Системы ДБО на чужих компьютерах или в интернет-кафе.

В случае, если у Вас:

- Неожиданно сломался компьютер, на котором у Вас установлена Система ДБО;
- Заблокировался логин;
- Невозможно зайти в Систему ДБО;
- Потерян контроль над носителем с секретными ключами;
- Потерян контроль над программой «Клиент-Банк»;
- Возникли подозрения в несанкционированном доступе к Системе ДБО:
    - Появляются \ *исчезают* \ документы, контрагенты;
    - Остатки на расчетном счете Клиента в Системе ДБО не соответствуют Вашим расчетам;
    - Любое другое подозрение

Вы должны немедленно обратиться в Банк с тем, чтобы решить все возникшие вопросы.

Соблюдая эти простые правила, Вы существенно снизите риски несанкционированного доступа к вашему расчетному счету посредством ДБО.
Помните! Согласно раздела 5 Соглашения на обслуживание с использованием Системы ДБО «Ответственность сторон и риски убытков», все риски, связанные с утратой и компрометацией секретных ключей, несет Владелец ключа.

С правилами безопасности эксплуатации Системы ДБО ознакомлен _____/_____/