**Правила обеспечения информационной безопасности при работе в Системе «iBank»**

1. Ответственность за безопасное хранение и использование Ключа электронной подписи лежит на Клиенте.

В целях минимизации рисков мошенничества и предотвращения атак ВК при работе с Системой «Банк-Клиент, Банк рекомендует Клиенту выполнять следующие действия и правила, включая требования ***Приложения № 4*** *к настоящему Договору:*

2.1. Для обеспечения информационной безопасности Ключа электронной подписи обязан:

2.1.1. по завершении работы с Системой «iBank» не оставлять ТОКЕН без присмотра;

2.1.2. обеспечить хранение ТОКЕНа в месте, исключающем доступ к носителю третьих лиц (в сейфе, личной запираемой ячейке и т. п.), не оставлять без присмотра и в легкодоступных местах;

2.1.3. исключить передачу Ключа электронной подписи или его копий третьим лицам, а также передачу по публичным сетям (например, в информационно-телекоммуникационную сеть «Интернет»);

2.1.4. исключить хранение Ключа электронной подписи на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах;

2.1.5. при смене уполномоченного представителя Клиента, отвечающего за формирование и проведение Распоряжений с использованием Системы «iBank», сменить криптографические ключи;

2.2. Для обеспечения безопасности устройства, с которого осуществляется работа с Системой «iBank», Клиент обязан:

2.2.1. использовать только лицензионные общее и прикладное программное обеспечение, средства антивирусной защиты;

2.2.2. обеспечить на устройстве непрерывное функционирование средств антивирусной защиты и межсетевого экранирования (брандмауэр, firewall);

2.2.3. ограничить права пользователя на внесение изменений в настройку операционной системы и установку каких-либо программ на устройство. При использовании для работы в Системе «iBank» нескольких компьютеров, желательно поместить их в отдельный сегмент сети;

2.2.4. обеспечить своевременное обновление операционной системы, антивирусного программного обеспечения, а также антивирусных баз данных;

2.2.5. осуществлять автоматическую периодическую (не реже одного раза в неделю) проверку устройства на наличие вирусов, при обнаружении вирусов, шпионских программ и т. п. немедленно их удалять;

2.2.6. установить парольную политику на ТОКЕН, средствах доступа к Системе «iBank» в соответствии с требованиями Приложения №3 к настоящему Договору;

2.2.7. соблюдать правила информационной безопасности при работе в информационно- телекоммуникационной сети «Интернет» (не посещать подозрительные сайты, не устанавливать программы из «недоверенных» источников, не открывать письма и вложения от неизвестных отправителей и пр.).

2.3. Для обеспечения информационной безопасности при работе в Системе «iBank» Клиент обязан:

2.3.1. использовать вход в систему только с <https://dbo-zemcombank.ru>, обращать внимание на правильность адреса (ссылки). При выявленном несоответствии – немедленно прекратить проведение операций и проинформировать Банк;

2.3.2. ежедневно контролировать состояние Счета(ов) (путем просмотра выписки). При выявлении расхождений – немедленно прекратить проведение операций и проинформировать Банк;

2.3.3. обращать внимание на дату и время последних входов в Систему «iBank» (данные фиксируются на первой странице после входа в Систему «iBank», а также в специальном разделе «Безопасность» - «Журнал сеансов работы»);

2.4. Признаки нарушений режима безопасности:

2.4.1. хищение, утеря (безвозвратная или с последующим обнаружением), повреждение ТОКЕНа;

2.4.2. увольнение сотрудников, имевших доступ к Ключам электронной подписи, изменения функциональных обязанностей сотрудника Клиента, имевшего доступ к распоряжению Счетом;

2.4.3. возникновение подозрений на утечку информации или ее несанкционированное изменение в Системе «iBank»;

2.4.4. подозрение на несанкционированный доступ третьих лиц к Счетам, программно-аппаратным средствам Клиента, Ключу электронной подписи,

несанкционированные операции по банковскому Счету Клиента с использованием Системы «iBank»;

2.4.5. нарушение целостности замков, печатей (при наличии) на сейфе, где хранится ТОКЕН в момент нахождения в нем ТОКЕНа.

2.5. Обязательная замена Ключа электронной подписи:

2.5.1. истек срок действия Ключа электронной подписи;

2.5.2. произошла компрометация Ключа электронной подписи.

3. Настоящим Клиент подтверждает, что до присоединения к настоящим Условиям и заключения Договора Клиент ознакомлен и полностью согласен с тем, что до момента блокировки Ключа электронной подписи Банк не несет ответственности за платежи, совершенные с использованием этого Ключа электронной подписи, даже в случае его компрометации, в т.ч. при воздействии на клиентское АРМ вредоносных кодов.

4. В случае возникновения подозрения на компрометацию Ключа электронной подписи, Клиенту необходимо незамедлительно обратиться в Банк по телефону +7(863)280-00-64 и инициировать процедуру смены всех потенциально скомпрометированных Ключей электронной подписи или блокировку Системы «iBank».