ПАМЯТКА
по обеспечению безопасности при работе
в системе дистанционного банковского обслуживания
для корпоративных клиентов

В целях повышения безопасности при работе с системой дистанционного банковского обслуживания «Банк Заречье» (АО) представляет комплекс требований и рекомендаций, выполнение которых позволит снизить возможные риски при работе в системе дистанционного банковского обслуживания (далее - ДБО) .

Требования по обеспечению информационной безопасности

В целях обеспечения информационной безопасности при работе в ДБО Клиент должен:

1. Использовать только программное обеспечение ДБО скачанное с официального сайта «Банка Заречье» (АО) (www.zarech.ru).

2. Хранить Ключи электронной подписи (далее по тексту – ЭП) только на внешнем носителе информации в недоступном для посторонних лиц месте (персональный сейф, металлический шкаф).

3. Соблюдать запрет на копирование ключей ЭП на жесткий диск компьютера, с которого осуществляется работа в ДБО а также передачу носителя ключей ЭП третьим лицам.

4. Не использовать в качестве пароля:

– последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
– последовательности повторяющихся букв или цифр;
– идущие подряд в раскладке клавиатуры или в алфавите символы;
– имена и фамилии;
– ИНН или другие реквизиты клиента.

5. Использовать пароль содержащий:

– не менее 8 символов;
– цифры, строчные и заглавные буквы;
– хотя бы 1 символ, не являющийся буквой или цифрой.

6. Менять пароль пользователя в операционной системе, а также в системе ДБО не реже одного раза в квартал.

7. Хранить пароль доступа к ключу ЭП отдельно от ключа ЭП. Не следует записывать пароль доступа к секретному ключу на бумажных и прочих носителях и хранить их в доступном посторонним лицам месте, записывать пароль доступа к секретному ключу на на этикетке внешнего носителя.

8. Подключать внешний носитель, содержащий ключ ЭП, только в момент подписания электронных документов.

9. Использовать внешний носитель, содержащий ключ ЭП, только для подписания электронных документов.

10. Закончив работу в системе ДБО или прервав её (даже на несколько минут), извлечь внешний носитель, содержащий ключ ЭП, и убрать его в недоступное другим лицам место. Не оставлять внешний носитель, содержащий ключ ЭП, постоянно подключенным к компьютеру

11. Применять на рабочем месте средства защиты от вредоносного кода, позволяющее блокирование несанкционированного удаленного доступа к компьютеру по

сети Интернет, с возможностью автоматического обновления баз данных сигнатур вредоносного кода.

12. Своевременно обновлять програмное обеспечение (далее - ПО) системы ДБО.

13. Осуществлять постоянный контроль отправляемых платежных документов при работе с ДБО а также за состоянием своего расчетного (банковского) счета.

В случае выявления признаков компрометации ключей ЭП, выявления несанкционированного удалённого доступа или вредоносного кода в компьютере, используемом для работы в системе ДБО необходимо немедленно извлечь ключ ЭП, выключить компьютер и уведомить Банк по телефонам: **(843) 557-59-74, (843) 557-59-88 с 8 часов 00 минут до 17 часов 00 минут (в рабочие дни)**, либо лично явиться в Банк с целью блокирования скомпрометированных закрытых ключей ЭП с последующей их заменой.

Не рекомендуется осуществлять доступ в ДБО поврежденного компьютера до проведения технической экспертизы. Работу в ДБО возможно проводить на новом компьютере после смены всех ключей ЭП клиента.

К событиям, связанным с компрометацией ключей ЭП, в том числе, относятся:

– утеря (утрата) носителя ЭП, в том числе, с последующим его обнаружением;

– обнаружение факта или угрозы использования (копирования) ключей ЭП и/или пароля доступа к ключам ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);

– обнаружение ошибок в работе системы ДБО в том числе, возникающих в связи с попытками нарушения информационной безопасности;

– увольнение ответственного сотрудника, имевшего доступ к закрытому ключу ЭП ДБО

14. Блокировать встроенные локальные учетные записи «Администратор» и «Гость» в операционной системе Windows.

15. При обнаружении несанкционированных платежных операций или утрате системы ДБО немедленно проинформировать руководство, обязательно уведомить Банк и написать уведомление об утрате доступа ДБО или использовании ДБО без согласия Клиента в порядке, установленном Соглашением о расчетном обслуживании с использованием системы дистанционного банковского обслуживания а также обратиться с соответствующим заявлением в правоохранительные органы.

16. Отключить службу «Telnet» и её автоматический запуск операционной системе Windows.

17. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.

18. Отключить возможность терминального соединения к компьютерам, используемым для работы в ДБО, заблокировать 3389 (RDP Remote desktop). Не рекомендуется использование сторонних приложений, позволяющих осуществление удаленного доступа к компьютерам, используемым для работы ДБО (таких как ‘Team Viewer’, ‘Radmin’ и т.п.).

19. Включить в операционной системе журнал безопасности Windows.

Использовать подключение к сети Интернет на компьютерах, используемых для работы ДБО, исключительно для работы в системе ДБО. Необходимо запретить доступ к социальным сетям и развлекательным ресурсам сети Интернет. Крайне не рекомендуется работать с системой ДБО с компьютеров, которые располагаются в общественных местах (Интернет-кафе, салонах, киосках и т.д.).

Также Клиенту рекомендуется:

1. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).

2. Обеспечить возможность своевременного обновления системного и прикладного ПО.

3. Выделить стационарный компьютер только для работы с системой ДБО

4. Доступ в помещение, где размещен компьютер с системой ДБО предоставлять только уполномоченным лицам.

5. Компьютер, с которого осуществляется подготовка и отправка электронных документов в Банк, выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети клиента Банка.

6. С целью обеспечения безопасности платежей использовать услугу СМС-информирования.

7. Исключить доступ к компьютерам, используемым для работы ДБО, посторонним лицам и персоналу предприятия, не уполномоченному на работу в ДБО и/или обслуживание компьютеров.

8. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.

9. Оборудовать устройство, с которого осуществляется перевод денежных средств, средством защиты информации, позволяющим осуществлять контроль конфигурации устройства (Аккорд-АМДЗ, ПАК Соболь и т.п.).