Приложение № 14
к Общим условиям открытия, обслуживания и закрытия банковских счетов юридических лиц (кроме кредитных организаций), индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, в «Банке Заречье» (АО)

Риски клиентов при работе в системе дистанционного банковского обслуживания «Банк+» (далее – «Система»)

За последнее время в ряде российских банков участились случаи хищения денежных средств с расчетных счетов корпоративных клиентов путем совершения платежей с использованием системы дистанционного банковского обслуживания. Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

как работающими, так и уволенными ответственными сотрудниками предприятия, имевшими доступ к паролю доступа, секретным ключам, к компьютерам, с которых осуществлялась работа по системе дистанционного банковского обслуживания;

как работающими, так и уволенными IT-сотрудниками организации, а так же нештатными, приходящими по вызову, IT-специалистами, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютерах, с которых осуществляется работа по системе дистанционного банковского обслуживания;

злоумышленниками путем заражения вредоносными программами компьютеров клиентов в связи с уязвимостью системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением секретных ключей и паролей, а также путем использования ложных (фальсифицированных) ресурсов сети Интернет с целью получения персональных данных и реквизитов банковских карт клиентов.

Как правило, действия злоумышленников направлены:

- на похищение секретных ключей;
- на похищение паролей доступа к Системе;
- на передачу в банк электронных платежных документов, заверенных похищенным ключом.

Документы, направляемые злоумышленниками с использованием действующих секретных ключей клиентов, могут не вызывать подозрений у сотрудников банков, поскольку такие документы имеют корректную электронную подпись, вполне обычные реквизиты получателей и типовое назначение платежа. Благодаря этому, полученные платежные документы признаются банками поступившими от клиента – владельца расчетного счета, и банки обязаны их исполнять. Таким образом происходит хищение злоумышленниками денежных средств с расчетных счетов клиентов. **При этом вся ответственность за убытки безусловно и полностью возлагается на клиентов как единственных владельцев секретных ключей.**

В целях повышения безопасности при работе с системой дистанционного банковского обслуживания «Банк+» «Банка Заречье» (АО) представляет комплекс требований и рекомендаций, выполнение которых позволит снизить указанные выше риски при работе в Системе.

Требования по обеспечению информационной безопасности при работе в Системе «Банк+»

В целях обеспечения информационной безопасности при работе в Системе Клиент обязан:

1. Использовать только программное обеспечение системы ДБО «Банк+», 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 Системе «Банк+».
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 6 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 «Банк+» не реже одного раза в квартал.
7. Хранить пароль доступа к ключу ЭП отдельно от ключа ЭП. Запрещено записывать пароль доступа к секретному ключу на этикетке внешнего носителя.
8. Подключать внешний носитель, содержащий ключ ЭП, только в момент подписания электронных документов. Запрещено оставлять внешний носитель, содержащий ключ ЭП, постоянно подключенным к компьютеру.
9. Использовать внешний носитель, содержащий ключ ЭП, только для подписания электронных документов. Запрещено использовать внешний носитель, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с системой ДБО «Банк+».
10. Закончив работу в системе ДБО «Банк+» или прервав её (даже на несколько минут), извлечь внешний носитель, содержащий ключ ЭП, и убрать его в недоступное другим лицам место.
11. Запрещено копировать содержимое внешнего носителя, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
12. Закончив работу в системе ДБО «Банк+» или прервав её (даже на несколько минут), необходимо извлечь внешний носитель, содержащий ключ ЭП, и убрать его в недоступное другим лицам место.
13. Обеспечить защиту клиентского модуля системы ДБО «Банк+» от несанкционированного доступа, а также заражения вредоносным кодом (вирусами).
14. Применять на рабочем месте лицензионные средства защиты от вредоносного кода. Обеспечить регулярное обновление антивирусных баз и их поддержание в актуальном состоянии. При увольнении штатных IT-сотрудников, а также после любых действий внештатных IT-специалистов или других работников, выполнявших какие-либо операции с компьютерами, предназначенными для работы в системе ДБО «Банк+», проводить проверку компьютеров на отсутствие вредоносных программ.

15. Своевременно обновлять ПО системы ДБО «Банк+». Обновление системы ДБО «Банк+» разрешено через меню системы ДБО «Банк+» («Операции» - «Обновление программы»).

16. Не работать с системой ДБО «Банк+» с компьютеров, которые располагаются в общественных местах (Интернет-кафе, салонах, киосках и т.д.).

17. Осуществлять постоянный контроль отправляемых платежных документов при работе с системой ДБО «Банк+», а также за состоянием своего расчетного (банковского) счета.

18. В случае выявления признаков компрометации ключей ЭП или выявления вредоносного кода в компьютере, используемом для работы в системе ДБО «Банк+», 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.

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 «Банк+», в том числе, возникающих в связи с попытками нарушения информационной безопасности;

– увольнение ответственного сотрудника, имевшего доступ к закрытому ключу ЭП ДБО «Банк+».

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

20. При обнаружении несанкционированных платежных операций или утрате системы ДБО «Банк+» немедленно проинформировать руководителя своей организации (индивидуального предпринимателя в случае, если договор ДБО заключен с индивидуальным предпринимателем), обязательно уведомить Банк и написать уведомление об утрате Системы или использовании Системы без согласия Клиента в порядке, установленном пунктом 10.4 Условий, а также обратиться с соответствующим заявлением в правоохранительные органы.

21. Не восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с системой ДБО «Банк+» в это время разрешено проводить только на другом компьютере после смены всех ключей ЭП клиента.

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

23. Не использовать автоматический вход в операционной системе. Использовать режим идентификации пользователя (например, по логину/паролю).

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

25. Включить в операционной системе журнал безопасности Windows.

26. Использовать подключение к сети Интернет на компьютерах, используемых для работы в Системе, исключительно для работы в Системе. Необходимо запретить доступ к социальным сетям и развлекательным ресурсам сети Интернет.

27. Помнить и соблюдать меры безопасности при формировании расчетов в сети Интернет, быть внимательным при обращении к ссылкам на сайт Банка. В случае, если был обнаружен: ложный web-сайт Банка, отличный от ссылки - zarech.ru или

мошенники пытаются связаться по электронной почте или иным способом с требованиями о предоставлении персональных идентификаторов доступа к Системе, необходимо незамедлительно сообщить об этом в Банк.

В целях обеспечения информационной безопасности при работе в Системе также 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 «Банк+».
4. Доступ в помещение, где размещен компьютер с системой ДБО «Банк+», рекомендуется предоставлять только уполномоченным лицам.
5. Компьютер, с которого осуществляется подготовка и отправка электронных документов в Банк, рекомендуется выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети клиента Банка.
6. С целью обеспечения безопасности платежей рекомендуется использовать услугу SMS–информирования.
7. Исключить доступ к компьютерам, используемым для работы по Системе, посторонним лицам и персоналу предприятия, не уполномоченному на работу по Системе и/или обслуживание компьютеров.
8. При обслуживании компьютера IT-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 и т.п.).