Приложение № 2 к Регламенту расчетного обслуживания клиентов АКБ «Заречье» (ОАО) (юридических лиц и индивидуальных предпринимателей) с использованием системы дистанционного банковского обслуживания «Банк+»

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:

1. 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;
2. как работающими, так и уволенными ИТ-сотрудниками организации, а так же нештатными, приходящими по вызову, ИТ-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;
3. 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.

Как правило, действия злоумышленников направлены:

1. на похищение секретных ключей;
2. на похищение паролей доступа к Системе;
3. 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+» АКБ «Заречье» (ОАО) рекомендует 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 наделяется следующими обязанностями:

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

2. 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.

3. Пароль должен:

- быть не менее 6 символов;
- содержать цифры, строчные и заглавные буквы;
- содержать хотя бы 1 символ, не являющийся буквой или цифрой.

4. Пароль пользователя в операционной системе, а также в системе ДБО «Банк+» менять не реже одного раза в квартал.

5. Пароль доступа к ключу ЭП хранить отдельно. Не записывать пароль доступа к секретному ключу на этикетке внешнего носителя.

6. Подключать внешний носитель, содержащий ключ ЭП, только в момент подписания электронных документов. Не оставлять внешний носитель, содержащий ключ ЭП, постоянно подключенным к компьютеру.

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

8. Не 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+».

9. Не копировать содержимое внешнего носителя, содержащего ключ ЭП, и не передавать его никому даже на короткое время.

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. Применять на рабочем месте средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.

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

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

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

15. 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+».

16. Необходимо блокировать встроенные локальные учетные записи «Администратор» и «Гость» в операционной системе Windows.

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

18. Запрещено восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с системой ДБО «Банк+» разрешено проводить только на новом компьютере после смены всех ключей ЭЦП клиента.

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

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

21. Отключить возможность терминального соединения к компьютерам, используемым для работы по Системе, заблокировать 3389 (RDP Remote desktop).

22. Включить в операционной системе журнал безопасности Windows.

Помимо указанных выше требований рекомендуется также:

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, включая систему ДБО «Банк+».

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 ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.