

## ПАМЯТКА

### Клиенту о возможных угрозах хищений денежных средств со счетов с использованием системы «iBank 2» и способах защиты

1. Настоящей Памяткой Банк информирует Вас о возможных случаях хищения денежных средств с Ваших расчетных счетов при использовании Системы «iBank 2», мерах соблюдения безопасности и способах пресечения данного хищения.

2. Хищение денежных средств с расчетных счетов возможно при получении злоумышленниками тем или иным образом доступа к Секретным ключам ЭЦП и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица похищенным ключом ЭЦП, что предположительно могут осуществить:

- ответственные сотрудники Вашей Компании, ранее имевшие доступ к Секретным ключам ЭЦП для Системы «iBank 2», например: уволенные директора, бухгалтеры и их заместители, а также совладельцы Компании;
- штатные ИТ-сотрудники Вашей Компании, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с Секретными ключами ЭЦП, а также доступ к компьютерам Компании, с которых осуществлялась работа по Системе «iBank 2»;
- нештатные, приходящие по вызову, ИТ-специалисты, обслуживающие компьютеры Вашей Компании, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого программного обеспечения на компьютеры, с которых осуществлялась или осуществляется работа по Системе «iBank 2»;
- другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами, используя уязвимости системного и прикладного программного обеспечения (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением Секретных ключей ЭЦП и паролей.

3. Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием корректных и действующих Секретных ключей ЭЦП Клиента, имеющие вполне обычные реквизиты получателей и типовые назначения платежа. И правомерное, в данном случае, исполнение таких платежей Банком приведет к хищению денежных средств с Вашего расчетного счета.

4. Важно понимать, что Банк не имеет доступа к Вашим Секретным ключам ЭЦП и не может от Вашего имени сформировать корректную ЭЦП под электронным платежным поручением.

5. Вся ответственность за конфиденциальность Ваших Секретных ключей ЭЦП полностью лежит на Вас, как единственных владельцах Секретных ключей ЭЦП.

6. Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать Секретный ключ ЭЦП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

7. Если Вы сомневаетесь в конфиденциальности своих Секретных ключей ЭЦП или есть подозрение в их компрометации (копировании), Вы должны заблокировать свои ключи ЭЦП.

8. Изменение пароля доступа к Секретному ключу ЭЦП не защищает от использования злоумышленником ранее похищенного ключа.

9. Банк настоящим еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования Секретных ключей ЭЦП и о необходимости ограничения доступа к персональным компьютерам, с которых осуществляется работа по Системе «iBank 2».

10. Чтобы воспрепятствовать хищению и использованию Вашего Секретного ключа ЭЦП злоумышленниками, требуется придерживаться приведенных ниже правил и рекомендаций:

- использовать для хранения файлов с секретными ключами ЭЦП отчуждаемые носители: дискеты, флеш-диски, специализированные устройства – USB-токены «iBank 2 Key» (см. ниже);
- отключать, извлекать носители с ключами ЭЦП, если они не используются для работы с Системой «iBank 2»;
- выделить отдельный компьютер, который использовать только для работы с Системой «iBank 2» и никакие другие задачи на этом компьютере не выполнять;
- ограничить доступ к компьютерам, используемым для работы с Системой «iBank 2»;
- исключить доступ к компьютерам персонала, не имеющего отношения к работе с Системой «iBank 2»;
- на компьютерах, используемых для работы с Системой «iBank 2», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п.;
- перейти к использованию лицензионного программного обеспечения (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного программного обеспечения;
- применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз;

- применять на рабочем месте специализированные программные средства безопасности: персональные фаерволы, антишпионское программное обеспечение и т.п.;
- исключить обслуживание компьютеров, используемых для работы с Системой «iBank 2», нелояльными ИТ-сотрудниками;
- при обслуживании компьютера ИТ-сотрудниками – обеспечивать контроль за выполняемыми ими действиями;
- никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы Системы «iBank 2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и лично ввести пароль, исключая подсматривание посторонними лицами;
- при увольнении ответственного сотрудника, имевшего доступ к Секретному ключу ЭЦП, обязательно заблокировать его ключ ЭЦП;
- при увольнении сотрудника, имевшего технический доступ к секретному ключу ЭЦП, обязательно заблокировать его ключ ЭЦП;
- при увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с Системой «iBank 2», принять меры для обеспечения отсутствия вредоносных программ на компьютерах;
- при возникновении любых подозрений на компрометацию (копирование) Секретных ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно заблокировать ключи ЭЦП;
- если Вы заметили проявление необычного поведения программного обеспечения Системы «iBank 2» или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – заблокировать ключи ЭЦП.

11. Наличие потенциальной угрозы хищения денежных средств требует не только соблюдения традиционных мер безопасности, перечисленных выше, но и перехода на качественно новый уровень защищенности. Чтобы полностью исключить угрозу хищения Секретных ключей ЭЦП, а соответственно и несанкционированного доступа к расчетному счету, необходимо использовать для хранения файлов с Секретными ключами ЭЦП специализированные устройства – USB-токены «iBank 2 Key».

12. При использовании «iBank 2 Key» секретный ключ ЭЦП генерируется самим USB-токеном один раз при инициализации.

13. Секретный ключ ЭЦП используется только самим токеном и никогда, никем и ни при каких условиях не может быть считан из токена. USB-токен может отдать внешним приложениям только открытый ключ ЭЦП для проверки формируемой им подписи.

14. USB-токен принимает на вход подписываемый электронный документ и возвращает на выходе ЭЦП под данным документом. Формирование ЭЦП клиента под электронным документом осуществляется непосредственно внутри USB-токена.

15. Пресечь использование ключей ЭЦП злоумышленниками позволяет также сервис электронного оповещения Системы «iBank 2».

16. Сервис электронного оповещения позволяет организовать рассылку сообщений по следующим каналам связи: SMS, e-mail, icq.

17. Использование услуги электронного оповещения Системы «iBank 2» позволит Вам самостоятельно настроить адреса и телефоны для автоматических, оперативных оповещений о следующих событиях:

- вход в систему «iBank 2»;
- поступление в Банк платежного поручения;
- списание средств с расчетного счета;
- текущие остатки на счёте.

18. Если Вы получили уведомление о совершении данных действий от имени Вашей Компании, но Вы или Ваши сотрудники не совершали этих действий – необходимо срочно связаться с Банком и заблокировать ключи ЭЦП. Таким образом, получение данных сообщений позволит Вам своевременно узнать о несанкционированном доступе и оперативно предпринять необходимые меры.

19. Электронное оповещение осуществляет серверный модуль Системы «iBank 2».

20. Все сообщения, которыми обмениваются серверный модуль с SMS-центрами российских сотовых операторов, подписываются ЭЦП и для обеспечения целостности передаваемых данных шифруются.

21. У Банка существует возможность разрешить каждому Клиенту работать только с заданных для данного Клиента IP-адресов и IP-подсетей. Список разрешенных IP-адресов и IP-подсетей задается в индивидуальных настройках клиента в банковском АРМе «Администратор» на основании поданного в Банк заявления Клиента. Использование встроенного в систему «iBank 2» механизма IP-фильтрации ограничивает возможности Клиента работать с системой при подключении к Интернету из произвольного места, но при этом делают задачу хищения средств злоумышленником практически неосуществимой.

**Для получения дополнительной информации обращайтесь в банковскую службу поддержки пользователей Системы «iBank 2» по телефону (495)721 3107**