Рекомендации по защите информации для Клиентов. Правила безопасного использования системы «Клиент-Банк»

Использование системы «Клиент-Банк» потенциально несет в себе риски неблагоприятных последствий для ее пользователя, связанных с хищением денежных средств, которые могут возникнуть в случае несанкционированного доступа к системе «Клиент-Банк».

Технологии защиты операций в системе «Клиент-Банк» используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень ее надежности и безопасности.

Вместе с тем эффективность данных механизмов зависит также от выполнения Вами простых правил:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих вам ключей электронных подписей без Вашего согласия;

2) уведомлять Банк, выдавший сертификат ключа проверки электронной подписи, о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1. Подключайте USB-токен с Закрытым ключом электронной подписи только на время работы в системе «Клиент-Банк». Контролируйте доступ к Вашему USB-токену.

2. При вводе нового постоянного Кода доступа к Закрытому ключу на USB-токене не используйте простые комбинации. Пароль должен отвечать требованиям к сложности пароля - минимальная длина 8 символов, наличие заглавных и строчных букв, цифр (либо спецсимволов). Это обеспечит защиту от взлома пароля.

3. Запомните постоянный Код доступа к Закрытому ключу на USB-токене. Никогда не записывайте его в местах, легко доступных посторонним лицам (на стикерах на мониторе, в файлах на рабочем месте и т.д.).

4. Никому не передавайте USB-токен или мобильное устройство с установленным на нем приложением «УПБ Бизнес» и не сообщайте третьим лицам Код доступа к Закрытому ключу.

5. Помните, что сотрудники АО «УРАЛПРОМБАНК» никогда и ни в какой форме не будут запрашивать Ваш пароль. Игнорируйте любые сообщения по электронной почте, запрашивающие Ваши пароли либо данные счетов или содержащие ссылку на Web-страницу, где Вам предлагается эти данные ввести. Сообщайте в Банк обо всех подобных фактах.

6. Немедленно аннулируйте ЭП при увольнении лица, которому она принадлежала.

7. Используйте современное антивирусное программное обеспечение. Регулярно обновляйте антивирусные базы и проводите полную антивирусную проверку Вашего компьютера для своевременного обнаружения вредоносных программ.

8. Установите и используйте персональный брандмауэр (firewall) на вашем компьютере. Это позволит предотвратить несанкционированный доступ к информации на компьютере.

9. Устанавливайте самые последние обновления Вашего браузера и операционной системы.

10. Подключите SMS-оповещение о движении денежных средств по счету.

11. Обеспечивайте сохранность и целостность программного комплекса системы «Клиент-Банк».

12. Перед установкой приложения «УПБ Бизнес» убедитесь, что:

- Вы скачиваете приложение из официального магазина приложений для данного устройства/операционной системы,
- наименование приложения полностью соответствует следующему написанию «URALPROMBANK», «УПБ Бизнес», а наименование вендора приложения соответствует следующему наименованию: АО «УРАЛПРОМБАНК», JSC Urals Industrial Bank. Избегайте установку приложений, копирующих символику АО «УРАЛПРОМБАНК», но имеющих иные наименования, в том числе иное наименование вендора/разработчика данного приложения.

13. Для мобильных устройств на операционных системах iOS и Android запрещено использование приложений «УПБ Бизнес» в случае присутствия скомпрометированной среды, установленной на мобильном устройстве:

- Для операционной системы Android – получение прав Администратора (root-права) и/или установка альтернативных графических интерфейсов пользователя («прошивок») сторонних разработчиков, и не входящих в пакет обновлений, распространяемых официальным вендором операционной системы и/или производителем мобильного устройства.
- Для операционной системы iOS – джейлбрейк (Jailbreak).

14. По требованию Банка прекратить использовать указанный Банком Закрытый ключ ЭП, сгенерируйте новые Закрытый и Открытый ключи, а также Сертификат открытого ключа.

15. В случае прекращения использования системы «Клиент-Банк» уничтожьте программное обеспечение системы «Клиент-Банк».

16. Не реже, чем ежедневно проверяйте расходные и приходные операции в системе «Клиент-Банк».

17. Храните USB-токен в надежном месте, исключающем несанкционированный доступ к нему и его повреждение.

18. Не осуществляйте посредством системы «Клиент-Банк» незаконные финансовые операции, незаконную торговлю и любые другие операции в нарушение законодательства РФ.

19. При удостоверении распоряжений на перевод денежных средств и иных электронных документов, составленных в системе «Клиент-Банк», через мобильное приложение «УПБ Бизнес» проверяйте реквизиты выводимые на экран мобильного устройства.

20. Не открывайте подозрительные вложения электронной почты на компьютере, в котором работаете с Системой «Клиент-Банк».

21. В случае если Владельцами Закрытых ключей будет принято решение о хранении нескольких Закрытых ключей разных владельцев на одном USB-токене, Банк не несет ответственности за возможное причинение Владельцу Закрытого ключа в связи с этим вреда, Владелец Закрытого ключа самостоятельно несет риск получения убытков.

22. Для работы в системе «Клиент-Банк» рекомендуется использовать отдельное рабочее место, а также запретить все входящие и исходящие соединения к сети Интернет на этом компьютере за исключением соединений необходимых для работы в системе «Клиент-Банк».

23. Запрещено устанавливать на компьютер, используемый для отправки документов в Банк, средства удаленного управления компьютером, такие как «TeamViewer», «Radmin» и подобные для удаленного управления вашим компьютером.

24. При выявлении подозрительной активности на компьютере, на котором установлен «Клиент-Банк» в большинстве случаев рекомендуется незамедлительно выключить компьютер и обратиться к системным администраторам.

Выполнение Вами данных мероприятий позволит значительно снизить риски совершения несанкционированных операций в системе «Клиент-Банк».

При любых подозрениях на компрометацию ключа электронной подписи, а также при возникновении любых необычных ситуаций при работе с системой «Клиент-Банк» – немедленно обратитесь в АО «УРАЛПРОМБАНК» по телефону (351) 239-65-65, либо на адрес электронной почты post@uralprombank.ru.