Правила безопасного использования системы «iBank 2»

Использование системы «iBank 2» потенциально несет в себе риски неблагоприятных последствий, связанных с хищением денежных средств, для его держателя, которые могут возникнуть в случае несанкционированного доступа к системе «iBank 2».

Технологии защиты операций в системе «iBank 2» 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. Для защиты ключей электронной подписи (далее-ЭП) от хищения вредоносными программами рекомендуется использовать USB-токен или смарт-карту «iBank 2 Key»;

Подключайте носитель с ключами электронной подписи **только** на время работы в системе «iBank 2» (в частности при синхронизации с сервером системы в РС-банкинге и во время подписания ЭД). Не предоставляйте доступ к Вашему ключу электронной подписи неуполномоченным лицам.

2. При вводе нового пароля для доступа к ключу ЭП не используйте простые комбинации. Лучше всего, если пароль будет длинной не менее восьми символов, состоять из заглавных и строчных букв, а также цифр. Это обеспечит усиление защиты от взлома пароля.

3. Запомните пароль для доступа к ключу ЭП. Никогда не записывайте его в местах, легко доступных посторонним лицам (на стикерах на мониторе, в файлах на рабочем столе ПК и т.д.).

4. Никому не передавайте носитель с ключами и не сообщайте пароль от ключа. Пароль на доступ к ключу ЭП должен быть известен только Вам как владельцу

5. Максимально ограничьте число сотрудников, допущенных к работе с ключами электронной подписи и местам хранения носителей ключей. Помните, что сотрудники ПАО КБ «САММИТ БАНК» никогда и ни в какой форме не будут запрашивать пароль Вашего ключа ЭП.

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 произведите внеплановую смену ключа при увольнении сотрудника, имевшего доступ к секретному ключу Вашей электронной подписи.

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

8. При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк с просьбой заблокировать ключи ЭП.

9. Установите и используйте персональный брандмауэр (межсетевой экран) и средства защиты от несанкционированного доступа на вашем компьютере. Это позволит предотвратить или усложнить доступ мошенников к информации на компьютере.

10. Устанавливайте самые последние обновления Вашего браузера, операционной системы и Java.

11. Включите SMS-оповещение о движении средств по счету.

12. Обеспечивайте сохранность и целостность клиентской части РС-банкинг программного комплекса системы «iBank 2».

13. По требованию Банка прекратить использовать указанный Банком ключ ЭП, сгенерируйте новый ключ ЭП и зарегистрируйте новый ключ проверки ЭП в Банке.

14. В случае прекращения использования системы «iBank 2» уничтожьте программное обеспечение системы «iBank 2».
15. Ежедневно проверяйте расходные и приходные операции в системе «iBank 2» по выписке из Банка.
16. Храните материальный носитель, содержащий ключ ЭП Клиента в надежном месте, исключающем несанкционированный доступ к нему и его повреждение.
17. Не осуществляйте посредством системы «iBank 2» незаконные финансовые операции, незаконную торговлю и любые другие операции в нарушение законодательства РФ.
18. При наличии технической возможности получения у провайдера сети Интернет статического **IP-адреса** – сообщить в Банк, что Вы будете подключаться к системе ДБО «iBank 2» с указанного адреса.
19. Рекомендуется использовать отдельный компьютер исключительно для работы в РС-банкинге. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
20. Работа на компьютере с системой “iBank 2” «РС-Банкинг - 'САММИТ БАНК'» **должна производиться** только под учетной записью с правами «Пользователь». **Административный доступ** для этой учетной записи **должен быть запрещен.**

Выполнение Вами данных мероприятий позволит значительно снизить риски совершения несанкционированных операций в системе «iBank 2».

Дополнительная мера обеспечения безопасности -Многофакторная аутентификация

Для предотвращения возможности использования похищенных ключей ЭП клиента в «iBank 2» может быть использован механизм многофакторной аутентификация клиента в системе.
Корпоративным клиентам с включенным механизмом «Многофакторная аутентификация» при выполнении синхронизации данных в РС-Банкинг необходимо дополнительно вводить в своих АРМ одноразовый пароль (см. Рисунок 1).

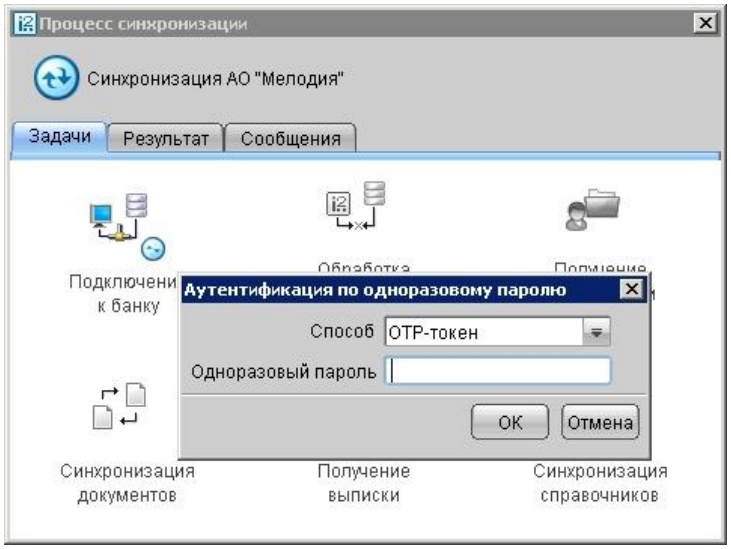

Рисунок 1. Синхронизация с банком при многофакторной аутентификации

Источником одноразовых паролей может выступать OTP-токен или **SMS**.

При любых подозрениях на компрометацию ключа электронной подписи, в том числе при утрате (потере, хищении) устройства, с использованием которого осуществлялся перевод денежных средств, а также при возникновении любых необычных ситуаций при работе с системой «iBank2» – немедленно обратитесь в Банк по телефону (42355) 56211, (423) 246-83-12, а также предоставьте информацию о необычных ситуациях по адресу электронной почты auto@kbsammit.ru.