

ПОЛОЖЕНИЕ

О безопасной работе в системе «iBank2» и противодействии злонамеренным действиям третьих лиц

1. Порядок хранения НЭК

- 1.1. Хранение НЭК следует осуществлять в сейфе, или в другом месте, недоступном для лиц, не имеющих прав доступа к системе «iBank2».
- 1.2. Вне времени работы с системой «iBank2», НЭК должны храниться в указанных п. 1.1. местах.

2. Требования к рабочему месту, с которого происходит работа в системе «iBank2».

- 2.1. На компьютере, используемом Клиентом для создания и подписания платежных документов, должно быть установлено только лицензионное программное обеспечение.
- 2.2. Программное обеспечение должно включать в себя антивирусную программу, с регулярно (по мере выпуска производителем) обновляемыми вирусными базами.
- 2.3. Расположение рабочего места должно исключать возможность незаметного доступа к компьютеру, на котором осуществляется формирование и подписание платежных документов, посторонним лицам.
- 2.4. На рабочем месте обязательно должна использоваться система парольной защиты.
- 2.5. Рекомендуется использование на рабочем месте программ защиты от несанкционированного доступа из внешних сетей (межсетевые экраны, антишпионские программы и т.д.)

3. Порядок работы с НЭК

- 3.1. При работе с НЭК не допускается:
 - знакомить с содержанием НЭК или передавать НЭК лицам, к ним не допущенным;
- 3.2. Генерация и хранение секретных ключей ЭЦП Клиента должно осуществляться исключительно на НЭК.
- 3.3. Рекомендуется подключать НЭК к компьютеру только непосредственно перед началом работы с системой, и извлекать его сразу после окончания работы.

4. Порядок действий при компрометации секретного ключа ЭЦП Клиента

- 4.1. Если НЭК был утерян, а также если у Клиента или у Банка появилось подозрение, что НЭК или его содержимое могло попасть в руки посторонних лиц, то содержащаяся на носителе ключевая информация считается скомпрометированной.
- 4.2. При компрометации секретного ключа ЭЦП Клиент и Банк обязаны:
 - Немедленно прекратить использование и предпринять все меры для прекращения любых операций Клиента с использованием этого НЭК.
 - Клиент обязан немедленно сообщить о факте компрометации секретного ключа ЭЦП в Банк по телефону, произнеся уникальное блокировочное слово; Банк обязан немедленно прекратить приём и исполнение документов Клиента, заверенных всеми ЭЦП, находящимися на скомпрометированном НЭК.
 - Клиент вместе с ответственным сотрудником Банка обязан принять согласованное решение о сроках замены скомпрометированной пары ключей ЭЦП и дальнейших действиях по обмену сообщениями до проведения смены скомпрометированной информации.
- 4.3. Банк имеет право отказать Клиенту в приеме от него распоряжения на проведение операции по банковскому счету, подписанному ЭЦП, и затребовать от Клиента оформления электронного документа на бумажном носителе, подписанного уполномоченными лицами и заверенного печатью Клиента (в соответствии с письмом ЦБ РФ от 27.04.2007 N 60-Т).

5. Внеплановая смена пары ключей ЭЦП Клиента

- 5.1. Внеплановая смена ключей ЭЦП Клиента обязательно производится в следующих случаях:
 - При компрометации секретного ключа ЭЦП;
 - В случаях увольнения сотрудника, работавшего с НЭК.
- 5.2. Клиент имеет право в любой момент по своему усмотрению досрочно прекратить действие своего активного открытого ключа ЭЦП, потребовать от Банка заблокировать этот активный открытый ключ

ЭЦП, сгенерировать новую пару ключей ЭЦП и зарегистрировать в Банке новый открытый ключ ЭЦП Клиента.

5.3. Банк имеет право в любой момент по своему усмотрению блокировать активный открытый ключ ЭЦП Клиента и (или) потребовать от Клиента смены пары ключей ЭЦП Клиента.

6. Рекомендации по работе с системой «iBank2»

6.1. Если в процессе рабочего дня через систему «iBank2» проводились операции, рекомендуется проверять остатки на счетах не менее 2-х раз в день.

6.2. Если операций в текущий день не проводилось, рекомендуется проверять остатки на счетах один раз в день.

6.3. Исполнитель самостоятельно контролирует состояние счёта в результате проведения операций с использованием системы «iBank2». В случае обнаружения неисполнения банком поручений клиента, переданных по системе «iBank2» в течение 1 часа, а также в случае обнаружения ошибочных списаний со счёта, необходимо связаться с Банком. Основным документом, подтверждающим осуществление операции по счёту, является выписка. Информация в остальных разделах системы «iBank2» является справочной.

6.4. Рекомендуется использование автоинформатора для получения сообщений Клиентом о входе в систему и операциях по счёту.

6.5. Рекомендуется использовать разовые сеансовые ключи при работе с системой.

6.6. Рекомендуется использовать IP-фильтрацию для ограничения доступа в систему с компьютеров с IP-адресами, отличными от адресов Клиента.

7. Способы повышения безопасности при работе с системой «iBank2»

7.1. **USB-токен.** При работе в системе «iBank2» используется аппаратный криптопровайдер в виде USB-токена «iBank2 Key». USB-токен формирует ЭЦП клиента под электронным документом по российскому криптоалгоритму согласно ГОСТ Р34.10-2001 непосредственно внутри SIM-карты токена. На вход USB-токена передается электронный документ, а на выходе USB-токена – ЭЦП под данным документом. При этом секретный ключ ЭЦП генерируется самим токеном при инициализации и хранится в защищенной памяти токена. Доступ ко всем криптографическим функциям USB-токена предоставляется только после ввода корректного пароля.

7.2. Смарт-карта — интеллектуальная пластиковая карта со встроенным криптографическим микроконтроллером, позволяющим осуществлять криптографические операции и вычисления.

7.3. **IP – фильтрация.** Составление индивидуального списка разрешенных IP – адресов для работы с системой «iBank2» и входящих в «доверительную зону» Клиента (операции, проводимые с IP – адресов, не указанных Клиентом, будут блокированы банком до получения Вашего согласия на их проведение). Для того, чтобы подключить данную услугу, необходимо написать письмо в Банк со списком разрешенных IP-адресов. Комиссия за оказание данной услуги не взимается.

7.4. **ОТР-токен** - это аппаратное устройство, предназначенное для генерации одноразовых паролей, которые применяются при подтверждении авторства документов, составленных Клиентом.

8. Ответственность

8.1. Ответственность за выполнения требований настоящего документа возлагается на Клиента.

8.2. Банк не несет ответственности за ущерб, причиненный Клиенту в результате действий третьих лиц.

«___» _____ 20___ г.

_____ / _____ /
должность

подпись

Ф.И.О.

М.П.