Приложение № 1
к Правилам обслуживания банковских счетов юридических лиц,
индивидуальных предпринимателей и лиц, занимающихся частной практикой, в ПАО БАНК «СИАБ»
с использованием системы дистанционного банковского обслуживания «КЛИЕНТ-БАНК»

В редакции Приказа № 155 от 16.11.2015 г.

Требования по обеспечению функционирования и безопасности применяемых средств криптографической защиты информации

1. Средства криптографической защиты информации (СКЗИ) используются для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации.

2. Пользователи СКЗИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящего документа. При этом пользователи должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

3. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

- соблюдением сотрудниками режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;
- точным выполнением сотрудниками требований к обеспечению безопасности конфиденциальной информации;
- надежным хранением сотрудниками СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;
- своевременным выявлением сотрудниками попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;
- немедленным принятием сотрудниками мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

4. Обязанности между сотрудниками должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой документации и документов, а также за порученные участки работы.

5. Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации.

6. Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- исключить возможность несанкционированного доступа к компьютерам, на которых используются СКЗИ;
- использовать антивирусное программное обеспечение на компьютерах, где используются СКЗИ;
- сообщать в ПАО БАНК «СИАБ» о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать в ПАО БАНК «СИАБ» СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять ПАО БАНК «СИАБ» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, выявленных вирусных заражениях компьютеров, на которых используются СКЗИ, а также о причинах и условиях возможной утечки таких сведений.

7. Пользователям СКЗИ запрещается:

- обсуждать конфиденциальную информацию, к которой они допущены, в том числе сведения о криптоключах в присутствии посторонних;
- выполнять операции с использованием СКЗИ в присутствии посторонних;
- оставлять без присмотра СКЗИ, включенные и не заблокированные компьютеры, на которых используются СКЗИ;
- сохранять средствами операционной системы или программного обеспечения СКЗИ ключевую информацию (ключи ЭП и шифрования) вне штатных средств хранения (выданных носителей ключевой информации - ruToken) и пароли доступа (pin-коды) к ключевой информации и СКЗИ;
- работать с СКЗИ на компьютерах без использования антивирусного программного обеспечения.

8. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего инструктажа. Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники ПАО БАНК «СИАБ».

9. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

10. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия. О необходимости вывода криптоключей из действия необходимо сообщить в ПАО БАНК «СИАБ».

11. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в ПАО БАНК «СИАБ». В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

12. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов.

13. Помещения, где установлены СКЗИ или хранятся ключевые документы к ним, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

14. Пользователям СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

15. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и ответственному сотруднику ПАО БАНК «СИАБ».

16. ПАО БАНК «СИАБ» вправе контролировать выполнение пользователями СКЗИ данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение ими условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ и настоящих Требований.

17. Если в использовании СКЗИ обнаружены недостатки, то ПАО БАНК «СИАБ» и пользователи СКЗИ обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки. При необходимости может быть составлен план мероприятий, где предусматривается решение соответствующих вопросов.

Общие рекомендации по обеспечению информационной безопасности

- Своевременно сообщайте в отдел дистанционного банковского обслуживания ПАО БАНК «СИАБ» о всех изменениях в ваших контактных лицах и их телефонах, для обеспечения оперативной связи с ними сотрудников ПАО БАНК «СИАБ».
- Своевременно устанавливайте обновления операционной системы.
- При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Установите на компьютере и регулярно обновляйте антивирусное программное обеспечение. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.
- Используйте межсетевые экраны (firewall), разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.
- При работе в сети Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.
- Не работайте под учетной записью с административными правами, особенно с использованием доступа в интернет.
- Ежемесячно производите смену паролей доступа к системам дистанционного банковского обслуживания.
- На компьютере, используемом для работы в системе «КЛИЕНТ-БАНК», не должно быть учетных записей (пользователей) с пустыми паролями.

Рекомендации по обеспечению информационной безопасности при работе в системе «КЛИЕНТ-БАНК»

- Персональный идентификатор «Рутокен» с ключом ЭП нельзя передавать третьим лицам, оставлять без присмотра, хранить в общедоступном месте.

- В случае компрометации или подозрения на компрометацию следует немедленно произвести смену паролей доступа и замену ключа ЭП. В качестве события, рассматриваемого как компрометация ключа, может выступать как потеря ключевого носителя (даже с последующим обнаружением), так и увольнение или смена лиц, допущенных к этим ключам.

Просим Вас незамедлительно обращаться в ПАО БАНК «СИАБ» при возникновении следующих ситуаций:

- В выписке обнаружены несанкционированные Вами расходные операции.
- Утерян или похищен ключевой носитель с ключом ЭП или компьютер, на котором был установлена система «КЛИЕНТ-БАНК».
- У Вас не работает система «КЛИЕНТ-БАНК» по неизвестным причинам.
- У Вас выявлено вирусное заражение или нетипичная работа (сбои в работе) Вашего компьютера.

Обращаем Ваше внимание, что своевременное обращение в ПАО БАНК «СИАБ» позволит принять оперативные меры по предотвращению мошенничества.