Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи Удостоверяющего Центра АО «Тинькофф Банк»

Использование усиленной электронной подписи предусматривает работу со средствами криптографической защиты информации (далее - СКЗИ). Безопасность их использования в значительной мере основывается на конфиденциальности носителей, содержащих криптографические ключи, и обеспечении пользователем доверенной компьютерной среды, в которой функционирует криптографическое средство.

Для обеспечения безопасности квалифицированной электронной подписи и СКЗИ Удостоверяющим Центром АО «Тинькофф Банк» разработаны следующие рекомендации.

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи по обеспечению его безопасности:

1.1. Обеспечить конфиденциальность ключей электронных подписей, в том числе не передавать ключи электронной подписи третьим лицам.

1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в квалифицированном сертификате (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.5. Немедленно обратиться в Удостоверяющий Центр по телефону 88007551110 или электронной почте ca@tinkoff.ru с заявлением о прекращении действия (отзыва) или приостановления действия квалифицированного сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

1.6. Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление на прекращение действия (отзыв) или приостановление действия, которое подано в Удостоверяющий Центр, в течение времени, исчисляемого с момента времени подачи заявления по момент времени официального уведомления о прекращении действия (отзыве) или приостановлении действия сертификата.

1.7. Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, действие которого прекращено или приостановлено.

1.8. Использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи СКЗИ, сертифицированные в соответствии с правилами пользования на данные СКЗИ.

2. Меры по обеспечению безопасности средств квалифицированной электронной подписи:

2.1. Сертифицированные СКЗИ должны применяться владельцем квалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство.

2.2. Для предотвращения заражения компьютера с установленными СКЗИ необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

2.3. В организации - обладателя конфиденциальной информации о должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ, назначены владельцы СКЗИ и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств.

2.4. Помещения, в которых установлены СКЗИ или хранятся носители ключей электронной подписи должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

2.5. В помещениях пользователей СКЗИ для хранения выданных им носителей ключей электронной подписи, эксплуатационной и технической документации 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 средств электронной подписи.

2.6. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, носители ключей электронной подписи подлежат поэкземплярному учету в соответствии с требованиями п. 26 Приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».