Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи (СКПЭП):
1.1. Обеспечить конфиденциальность ключей электронных подписей (ЭП).
1.2. Перед первым использованием ключевого носителя изменить назначенный по умолчанию ПИН-код (пароль на контейнер). ПИН-код (пароль на контейнер) должен содержать не менее 6-ти символов случайной цифро-буквенной последовательности.
1.3. Применять для формирования ЭП только действующий ключ ЭП.
1.4. Не применять ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
1.4. Применять ключ ЭП с учетом ограничений, содержащихся в СКПЭП (в расширениях Extended Key Usage, Application Policy СКПЭП), если такие ограничения были установлены.
1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия СКПЭП в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа ЭП.
1.6. Не использовать ключ ЭП, связанный с СКПЭП, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.
1.7. Не использовать ключ ЭП, связанный с СКПЭП, заявление на приостановление, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.
1.8. Не использовать ключ ЭП, связанный с СКПЭП, который аннулирован, действие которого прекращено или приостановлено.
1.9. Использовать для создания и проверки квалифицированных ЭП, создания ключей ЭП и ключей проверки ЭП сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

2. Порядок применения средств квалифицированной электронной подписи
2.1. Средства квалифицированной ЭП должны применяться владельцем квалифицированного СКПЭП в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.
2.2. Для предотвращения заражения компьютера с установленными средствами квалифицированной ЭП необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского ПО и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления баз данных.
2.3. В организации юридического лица соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств квалифицированной ЭП, назначены владельцы средств квалифицированной ЭП и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств; средства квалифицированной ЭП и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.

3. Риски использования электронной подписи:

При подписании электронного документа электронной подписью, срок действия которой истек, данный документ будет признан недействительным.

Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.

Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.

Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.

Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.

Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.