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

1. Основные положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также мерах, необходимых для обеспечения безопасности использования квалифицированной электронной подписи.

Настоящее руководство обязательно для ознакомления пользователями Удостоверяющего центра, которые должны соблюдать требования по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Основные риски при использовании электронной подписи связаны с несанкционированным доступом к ключам электронной подписи и в помещения, в которых они размещаются средства вычислительной техники с установленными на них средствами электронной подписи (т.е. использованием без ведома их владельца), вследствие чего становится возможным возникновение электронных документов, порождающих нежелательные юридически значимые последствия в отношении владельца сертификата электронной подписи.

Источниками несанкционированного доступа могут быть как преднамеренные либо неумышленные действия человека, так и активность вредоносного программного обеспечения.

2. Размещение технических средств

Размещение средств вычислительной техники с установленными на них средствами электронной подписи и квалифицированными электронными подписями должно исключать возможность несанкционированного доступа посторонних лиц в помещениях, в которых размещены такие средства.

Допускается присутствие посторонних лиц в помещениях при обеспечении контроля за их действиями со стороны допущенных лиц.

3. Установка и эксплуатация программного обеспечения

Владельцы квалифицированных электронных подписей должны выполнять меры безопасности по отношению к установленному программному обеспечению, направленные на избежание вышеуказанных рисков.

Рекомендовано не использовать нестандартные, измененные и отладочные версии операционных систем, а также исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой.

Регулярно устанавливайте пакеты обновлений безопасности операционной системы.

Режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень.

Необходимо устанавливать и использовать лицензионное программное обеспечение стабильных версий, полученное из вызывающих доверие источников. Запрещается использовать изменённые, взломанные или неподдерживаемые производителем версии программного обеспечения.

Необходимо установить и использовать на рабочих местах антивирусное программное обеспечение, а также уже имеющиеся на автоматизированных рабочих местах средства межсетевого экранирования (Firewall) с определением правил доступа к сетевым ресурсам.

Необходимо исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

Средства электронной подписи необходимо установить и использовать строго в соответствии с эксплуатационной документацией, поставляемой в комплекте или опубликованной на сайте удостоверяющего центра.

Регулярно отслеживайте и устанавливайте обновления безопасности для программного обеспечения, обновлять антивирусные базы.

Необходимо также разрабатывать и использовать политику назначения и смены паролей (на вход в операционную систему, параметры BIOS, экранную заставку и т.д.) в соответствии с общепринятыми рекомендациями по созданию сильных паролей. При покидании рабочего места с активным сеансом пользователя блокировать его паролем (сочетанием клавиш win+L). Личный пароль пользователь не должен никому сообщать, а также пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также сокращения (user, admin, root 12345678 и т.д.).

4. Обращение с ключевыми носителями

Определите круг лиц, имеющих доступ с согласия владельца сертификата электронной подписи к ключам и средствам электронной подписи, а также обязанности и ответственность этих лиц по обеспечению конфиденциальности ключей электронной подписи.

Определите порядок обращения с ключевыми носителями при использовании и хранении, исключающий возможность несанкционированного доступа к ним.

Использовать ключ электронной подписи необходимо только для тех целей, которые указаны в дополнениях keyUsage и extendedKeyUsage квалифицированного сертификата ключа проверки электронной подписи.

Ключ квалифицированной электронной подписи должен быть записан на типы ключевых носителей, которые поддерживаются используемым средством квалифицированной электронной подписи согласно эксплуатационной и технической документации к ним.

Ключи квалифицированной электронной подписи на ключевом носителе рекомендовано защищать паролем (pin-кодом). Ответственность за конфиденциальность сохранения пароля (pin-кода) возлагается на владельца ключа квалифицированной электронной подписи.

После получения квалифицированной электронной подписи в Удостоверяющем центре рекомендуется произвести смену стандартного пароля (pin-кода) на свой собственный усиленный. Рекомендованная длина пароля не менее 8 символов.

Недопустимо пересылать файлы с ключевой информацией другим лицам, за исключением открытых ключей.

Размещение (запись) ключевой информации на локальном диске технического средства должно предусматривать выполнение ряда требований, предъявляемых к техническому средству, как к ключевому носителю.

Ключевые носители должны храниться в местах, недоступных сторонним лицам (индивидуальное хранилище, сейф, закрывающийся металлический ящик). Двери от хранилищ должны быть оборудованы средствами, сигнализирующими о их вскрытии.

Ключевой носитель должен быть подключен к техническому средству только на время осуществления процедуры формирования и проверки квалифицированной электронной подписи, шифрования или дешифрования.

На ключевом носителе недопустимо хранить иную информацию.

В случае увольнения или перевода в другое подразделение (на другую должность) представителя юридического лица, имеющего доступ к ключевому носителю, должна быть проведена смена ключей электронной подписи.

5. Компрометация

К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей, в том числе с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушения правил хранения ключевых носителей;
- возникновение подозрений на утечку информации;
- несанкционированное копирование ключевых носителей.

Пользователь Удостоверяющего центра должен самостоятельно определить факт компрометации ключа электронной подписи и оценить значение этого события. Мероприятия по розыску и локализации последствий компрометации конвенционной информации, переданной с использованием средств электронной подписи, организует и осуществляет сам пользователь Удостоверяющего центра.

При наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена (произошла компрометация), немедленно принять меры по прекращению действия сертификата электронной подписи в порядке, предусмотренном Порядком реализации функций Удостоверяющего центра.

Запрещается использовать для создания электронной подписи ключи, если известно, что эти ключи используются или использовались ранее лицами, не имеющими доступа к ним.

6. Запрещается

- Разглашать содержимое электронных носителей, передавать сами носители лица, к ним не допущенным, выводить информацию о средствах электронной подписи на дисплей и принтер;

– Подсоединять электронный носитель к usb-порту компьютера при проведении работ, не являющихся штатными процедурами использования средств электронной подписи;

– Носить какие-либо изменения в программное обеспечение и средства электронной подписи;

– Осуществлять несанкционированное копирование ключевой информации на ключевом носителе.

7. Заключение

После того как Удостоверяющий центр передал владельцу сертификата ключа проверки электронной подписи ключи электронной подписи, содержащиеся на носителе ключевой информации, а также информацию о pin-коде для доступа к ключу электронной подписи, конфиденциальность полученных данных полностью зависит от того, насколько ответственно владелец сертификата ключа проверки электронной подписи отнесется к их использованию и хранению.