# РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" и информирует владельцев квалифицированной электронной подписи об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

Применение квалифицированной электронной подписи в информационных системах сопровождается рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием квалифицированной электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется работа с квалифицированной электронной подписью. В связи с этим необходимо выполнение приведенных ниже мер по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи.

1. Владелец квалифицированной электронной подписи должен обеспечить конфиденциальность ключей электронной подписи.
2. Доступ к компьютеру, который используется для работы с ключевой информацией и подписания документов электронной подписью должен быть ограничен. Не доверяйте Ваш компьютер для обслуживания посторонним лицам, исключите бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.
3. Перед первым использованием носителя ключа электронной подписи (JaCarta, eToken и т.п.) необходимо изменить назначенный по умолчанию PIN-код. Новый PIN-код должен содержать не менее восьми символов цифро-буквенной последовательности.
4. Не передавайте никому личный ключевой носитель и не сообщайте PIN-код доступа к нему кому бы то ни было! Доступ к ключевым носителям должен быть только у их владельцев!
5. Запрещается оставлять личный ключевой носитель и\или PIN-код доступа к нему без присмотра!
6. Обеспечьте безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.
7. Запретите доступ по сети в Вашей организации (офисе) к каталогам на компьютере, где установлены средства электронной подписи, посторонним лицам.
8. Используйте на компьютере только лицензионное ПО. Своевременно устанавливайте обновления безопасности операционной системы.
9. Работайте под учетной записью обычного пользователя (рекомендуется защищать вход в Windows надежным паролем). Отключите стандартную учетную запись «Гость».
10. Обеспечьте непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского ПО и других вредоносных программ лицензионным антивирусным ПО с рекомендуемым разработчиком периодом обновления баз данных, с включенной защитой паролем и сетевой защитой, выставленной на максимальный уровень безопасности. Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения

расширений файлов. Проводите полную еженедельную проверку компьютера на наличие вирусов.

11. В случае необходимости доступа в информационно-телекоммуникационную сеть «Интернет», установите и настройте на компьютере персональный межсетевой экран, разрешив доступ только к доверенным ресурсам сети «Интернет».

12. Для предотвращения удаленного управления Вашим компьютером злоумышленниками не допускайте установки кем бы то ни было на компьютер программ удаленного администрирования. Периодически контролируйте установленное и запущенное (работающее) на компьютере ПО.

13. Блокируйте компьютер при уходе с рабочего места, при длительном отсутствии – обязательно выключайте компьютер.

14. Если Вы работаете на ноутбуке (переносном компьютере), не храните его вместе со всеми атрибутами доступа (личный ключевой носитель, PIN-коды к нему, логин и пароль).

15. Подсоединяйте ключевой носитель к компьютеру только для подписания электронных документов, и в обязательном порядке извлекайте его из компьютера сразу после окончания работы.

16. Блокируйте компьютер и извлекайте ключевой носитель при уходе с рабочего места.

17. Не допускается снимать несанкционированные копии с ключевых носителей, знакомить или передавать ключевые носители лицам, к ним не допущенным.

18. Применяйте для формирования электронной подписи только действующий ключ электронной подписи и с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy), если такие ограничения были установлены.

19. В случае утраты личного ключевого носителя или PIN-кода доступа к нему для блокировки использования Вашего ключа подписи посторонними лицами немедленно известите Удостоверяющий центр о нарушении конфиденциальности ключа электронной подписи. Не применяйте ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

20. Немедленно обратитесь в Удостоверяющий центр с заявлением на аннулирование квалифицированного сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

21. Используйте для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные по требованиям ФСБ России средства электронной подписи.

22. ЗАПРЕЩАЕТСЯ устанавливать режим «Включить кэширование» в настройках режима работы криптопровайдера. Кэширование заключается в том, что считанные с ключевого носителя ключи останутся загруженными в памяти службы хранения ключей и будут доступны любому приложению после извлечения ключевого носителя из считывателя и до завершения работы компьютера. Это означает, что в случае хакерской атаки на Ваш компьютер, злоумышленник сможет воспользоваться загруженными ключами для выработки ЭП от Вашего имени.

23. В организации соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств электронной подписи, назначены владельцы средств электронной подписи и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств. Средства электронной подписи и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах. (В соответствии с требованиями Приказа ФАПСИ от 13 июля 2001 г. № 152).