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

1. Обеспечьте конфиденциальность ключей электронной подписи.
2. Для предотвращения внештатных ситуаций при использовании ключевой информации **ограничьте доступ к компьютеру**, который используется для работы с ключевой информацией и подписания документов электронной подписью. Не доверяйте Ваш компьютер для обслуживания посторонним лицам, исключите бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.
3. **Не передавайте никому личный ключевой носитель и не сообщайте PIN-код к нему** кому бы то ни было. Доступ к ключевому носителю должен быть только у владельца электронной подписи.
4. **Не оставляйте личный ключевой носитель и/или PIN-код доступа к нему без присмотра.**
5. Обеспечьте безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.
6. **Подсоединяйте ключевой носитель к компьютеру только для подписания электронных документов**, и в обязательном порядке извлекайте его из компьютера сразу после окончания работы. Блокируйте компьютер и извлекайте ключевые носители при уходе с рабочего места.
7. **Не извлекайте ключевой носитель во время его работы**, т.к. это может привести к потере данных на нем. Извлечение ключевого носителя должно производиться через «Безопасное извлечение Запоминающего устройства».
8. **Старайтесь не наносить повреждений своему ключевому носителю**, не ронять и не ударять, а при извлечении из порта компьютера не менять угол наклона и не раскачивать. Механические повреждения могут привести к поломке ключевого носителя.
9. Не допускается снимать несанкционированные копии с ключевых носителей, знакомить или передавать ключевые носители лицам, к ним не допущенным, записывать на ключевой носитель с ключами электронной подписи постороннюю информацию.
10. **Работайте под учетной записью обычного пользователя** (учетная запись должна быть защищена надежным паролем). Не рекомендуется работа с электронной подписью под учетной записью «Администратор». Отключите стандартную учетную запись «Гость».
11. Запретите доступ по сети в вашей организации к каталогам на компьютере, где установлены средства электронной подписи, посторонним лицам.
12. Используйте на компьютере только лицензионное программное обеспечение. Своевременно устанавливайте обновления безопасности операционной системы.
13. **Обеспечьте непрерывную комплексную защиту компьютера от вирусов**, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ лицензионным антивирусным программным обеспечением 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 файлами-вложениями. Обращайте внимание на расширение файла. Проводите полную еженедельную проверку компьютера на наличие вирусов.
14. 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.
15. В случае утраты личного ключевого носителя и/или PIN-кода доступа к нему для блокировки использования Вашего ключа электронной 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.
16. 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.
17. Используйте для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.
18. **Запрещается устанавливать режим «Включить кэширование»** в настройках режима работы средства электронной подписи. 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 электронной подписи от Вашего имени.
19. Если вам в течение сеанса работы со средствами электронной подписи приходится многократно использовать ключевой носитель, то для ускорения работы используйте настройку средства электронной подписи «Запомнить пароль». **После завершения сеанса работы обязательно удалите запомненные пароли**, для чего используйте возможности средства электронной подписи.
20. 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.