Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

Основные риски при использовании электронной подписи (далее - ЭП) связаны с несанкционированным доступом к ключам ЭП (т.е. использованием без ведома их владельца), вследствие чего становится возможным возникновение электронных документов, порождающих нежелательные юридически значимые последствия в отношении владельца сертификата ЭП.

Источниками несанкционированного доступа могут быть как преднамеренные либо неумышленные действия человека, так и активность вредоносного программного обеспечения. Далее приводится краткий перечень основных мер безопасности для владельцев ЭП, направленных на избежание указанных рисков.

1. Определить круг лиц, имеющих доступ с согласия владельца сертификата ЭП к ключам и средствам ЭП, а также обязанности и ответственность этих лиц по обеспечению конфиденциальности ключей ЭП.
2. Исключить пребывание посторонних лиц в помещениях с ключами и средствами ЭП, их доступ к рабочему месту, либо, в случае необходимости пребывания, обеспечить контроль над их действиями.
3. Определить порядок обращения с ключевыми носителями при использовании и хранении, исключающий возможность несанкционированного доступа к ним.
4. Установить и использовать на рабочем месте лицензионное программное обеспечение (далее - ПО) стабильных версий, полученное из вызывающих доверие источников. Не использовать изменённые, взломанные или неподдерживаемые производителем версии ПО.
5. Установить и использовать на рабочих местах антивирусное ПО.
6. Установить или использовать уже имеющиеся на рабочих местах средства межсетевого экранирования (Firewall) с определением правил доступа к сетевым ресурсам.
7. Установить и использовать средства ЭП строго в соответствии с эксплуатационной документацией, поставляемой в комплекте или опубликованной на сайте удостоверяющего центра.
8. Регулярно отслеживать и устанавливать обновления безопасности для ПО, обновлять антивирусные базы.
9. 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).
10. Использовать ключ электронной подписи только для тех целей, которые указаны в дополнениях keyUsage и extendedKeyUsage квалифицированного сертификата ключа проверки электронной подписи.
11. При наличии оснований полагать, что конфиденциальность ключа ЭП нарушена (произошла компрометация), немедленно принять меры по прекращению действия сертификата ЭП в порядке, предусмотренном Регламентом удостоверяющего центра.
12. 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.

13. Не использовать для создания ЭП ключи, если известно, что эти ключи используются или использовались ранее лицами, не имеющими доступа к ним.