БелИнфоНалог
Удостоверяющий центр с 2003 года

Телефон: (495) 642-95-88, (4722) 232-702,
8 800 511-82-81
e-mail: uc@belinfonalog.ru
сайт: http://belinfonalog.ru

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

Термины и определения:

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром;

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

Спам — рассылка коммерческой и иной рекламы или иных видов сообщений (информации) лицам, не выражавшим желания их получать

Хакерская атака— действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании.

Антивирусное программное обеспечение — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.

1.2. Ограничить доступ к компьютеру, который используется для работы с ключевой информацией и подписания документов электронной подписью. Исключить бесконтрольный доступ в помещения, в которых размещаются средства электронной подписи.

1.3. Не оставлять личный ключевой носитель и/или PIN-код доступа к нему без присмотра.

1.4. Обеспечить безопасное хранение ключей электронной подписи на ключевом носителе в сейфе или запираемом ящике стола.

1.5. Подсоединять ключевой носитель к компьютеру только для подписания электронных документов, и в обязательном порядке извлекать его из компьютера сразу после окончания работы. Блокировать компьютер и извлекать ключевые носители при уходе с рабочего места.

1.6. Не извлекать ключевой носитель во время его работы, т.к. это может привести к потере данных на нем.

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

1.8. Использовать на компьютере только лицензионное программное обеспечение. Своевременно устанавливать обновления безопасности операционной системы.

1.9. Применять для формирования электронной подписи только действующий ключ электронной подписи.

1.10. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.11. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или

подозрения в нарушении конфиденциальности ключа электронной подписи, либо в случае утраты личного ключевого носителя и/или PIN-кода доступа к нему.
1.12. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, 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.
1.13. Использовать 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.

2. Порядок применения средств квалифицированной электронной подписи

2.1 Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.
2.2 Если вам в течение сеанса работы со средствами ЭП приходится многократно использовать ключевой носитель, то для ускорения работы используйте настройку криптопровайдера «Запомнить пароль». После завершения сеанса работы обязательно удалите запомненные пароли, для чего используйте возможности криптопровайдера.
2.3 Для предотвращения заражения компьютера с установленными средствами квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.
2.4 В организации должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств квалифицированной электронной подписи, назначены владельцы средств квалифицированной электронной подписи и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств.
2.5 Используемые или хранимые средства квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители ключей проверки электронной подписи подлежат поэкземплярному учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».