ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

"Экспертиза"

454084, Челябинск ул. Каслинская, дом 5
Каслинская, 5
ИНН 7447133821 КПП 744701001
ОГРН 1087447008550
Расчетный счет 40702810907250004242
в Тракторозаводском ф-ле ОАО «Челиндбанк»

для писем: 454084, г. Челябинск,

Электронная почта: info@e-xp.ru

Утверждено приказом
№ ЭКП-1/11 от
15. 11. 2013 г.

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

1. Общие положения

1.1 Настоящее Руководство:

- определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств (далее - СКЗИ), в информационных системах юридических и физических лиц заказчиков СКЗИ ООО «Экспертиза» (далее - Пользователь);
- является обязательным к исполнению для всех пользователей.

1.2 Настоящее Руководство разработано во исполнение:

- приказа ФСБ России от 9 февраля 2005 года № 66, утвердившего «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);
- приказа руководства 8 Центра ФСБ России от 21 февраля 2008 года № 149/6/6-622 утвердившего «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»
- 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».

1.3 Ключевые документы, СКЗИ с введенными криптоключами относятся к материальным носителям, содержащим информацию ограниченного распространения. С целью их сохранности выполняются требования настоящего Руководства.

2. Термины и определения

2.1. Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ от 6 апреля 2011 года «Об электронной подписи».

2.2. Электронная подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

2.3. Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.4. Ключевой носитель – отчуждаемый носитель, содержащий закрытый ключ электронной подписи (например, USB-ключ eToken, USB-ключ ruToken, Смарт-Карты и т.п.).

2.5. Средства электронной подписи – средства криптографической защиты информации, обеспечивающие реализацию следующих функций: создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждение подлинности электронной подписи в электронном документе с использованием открытого ключа электронной подписи, создание закрытых и открытых ключей электронных подписей.

2.6. Закрытый ключ электронной подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

2.7. Открытый ключ электронной подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому лицу и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

2.8. Средства криптографической защиты информации (далее СКЗИ) – программное обеспечение, предназначенное для работы с ключами шифрования и электронной подписью.

3. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи:

3.1 Обеспечить конфиденциальность ключей электронных подписей.

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

3.3 Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

3.4 Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие были установлены.

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

3.6 Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течении времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо от отказе в прекращении в прекращении действия.

3.7 Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течении времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо от отказе в приостановлении действия.

3.8 Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

3.9 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.

4. Владельцам квалифицированного сертификата ключа проверки электронной подписи запрещено:

4.1. Использовать СКЗИ для защиты сведений, составляющих государственную тайну.

4.2. Осуществлять несанкционированное администратором безопасности копирование ключевых носителей.

4.3. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данным Руководством).

4.4. Записывать на ключевые носители с ключами постороннюю информацию.

4.5. Вносить какие-либо изменения в программное обеспечение СКЗИ.

4.6. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования.

4.7. Исполнять и открывать файлы, полученные из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.

4.8. Оставлять без присмотра ключевые носители, передавать их в пользование третьим лицам.

Директор  Е.А.Петриди