**Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи"**

Принят

Государственной Думой

25 марта 2011 года

Одобрен

Советом Федерации

30 марта 2011 года

*(в ред. Федеральных законов от 01.07.2011 № 169-ФЗ, от 10.07.2012 № 108-ФЗ, от 05.04.2013 № 60-ФЗ, от 02.07.2013 № 171-ФЗ, от 02.07.2013 № 185-ФЗ, от 12.03.2014 № 33-ФЗ, от 28.06.2014 № 184-ФЗ, от 30.12.2015 № 445-ФЗ)*

**[Извлечение]**

**Статья 8. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи**

[…]

5. Федеральный орган исполнительной власти в области обеспечения безопасности:

[…]

4) по согласованию с уполномоченным федеральным органом устанавливает дополнительные требования к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, а также к обеспечению информационной безопасности аккредитованного удостоверяющего центра.

[…]

**Статья 9. Использование простой электронной подписи**

[…]

2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

[…]

2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

[…]

4. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

[…]

**Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей**

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

**Статья 12. Средства электронной подписи**

[…]

4. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

[…]

**Статья 13. Удостоверяющий центр**

2. Удостоверяющий центр обязан:

[…]

2) обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

[…]

4) обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

[…]

**Статья 16. Аккредитация удостоверяющего центра**

[…]

3. Аккредитация удостоверяющего центра осуществляется при условии выполнения им следующих требований:

[…]

4) наличие в штате удостоверяющего центра не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, имеющих высшее профессиональное образование в области информационных технологий или информационной безопасности либо высшее или среднее профессиональное образование с последующим прохождением переподготовки или повышения квалификации по вопросам использования электронной подписи.

[…]

3.1. Удостоверяющий центр наряду с указанными в части 3 настоящей статьи требованиями вправе также обеспечить свое соответствие установленным федеральным органом исполнительной власти в области обеспечения безопасности по согласованию с уполномоченным федеральным органом дополнительным требованиям к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, а также к обеспечению информационной безопасности аккредитованного удостоверяющего центра в случаях, если необходимость соблюдения таких дополнительных требований в определенных отношениях предусмотрена федеральным законом.

[…]

**Статья 17. Квалифицированный сертификат**

[…]

6. Владелец квалифицированного сертификата обязан:

1) не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена; […]