РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Читинский филиал




Электронная подпись

Лапа Алексей Александрович

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Нормативно-правовая база защиты информации:

Главные законы об информации и информационной безопасности

Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» — устанавливает основные права и обязанности, касающиеся информации и информационной безопасности.

Федеральный закон Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных» — описывает правила работы с персональными данными.

Федеральный закон Российской Федерации от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» — дает определение электронной подписи и описывает, как и когда ее можно применять, какой юридической силой она обладает.

Федеральный закон Российской Федерации от 26 июля 2016 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» — описывает правила защиты IT-инфраструктуры на предприятиях, работающих в сферах, критически важных для государства. К таким сферам относится здравоохранение, наука, оборона, связь, транспорт, энергетика, банки и некоторая промышленность.

Федеральный закон Российской Федерации от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» — определяет, что относится к коммерческой тайне компаний.

Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»:

цели:

- Необходимость создания законодательной базы для внедрения цифровой подписи в системы электронного документооборота органов государственной власти.
- Гармонизация российского законодательства с международным.
- Создание правовой основы для интеграции внутренних и международных систем электронной торговли.
- Упрощение процедур ведения «электронного» бизнеса.

Теоретически принятие закона «О цифровой подписи» несло потенциальные выгоды и потребителям услуг, позволяя им вступать в правоотношения без предварительного заключения договора в бумажном виде.

Итог:

Закон не соответствует объективным обстоятельствам, в которых предполагается его реализовывать.

Закон противоречит интересам общества и государства

Закон, практически не достигает поставленных целей.

Определение:

электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Статья 1. Сфера действия настоящего Федерального закона:

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Гражданский кодекс РФ закрепил возможность использования ЦП, наряду с иными аналогами собственноручной подписи (АСП) в электронном документообороте.

Сферы применения:
Электронные торги
Электронный документооборот
Электронная отчетность
Защита информации.

https://iecp.ru/law-review-list

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) 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;

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание соответствия удостоверяющего центра требованиям настоящего Федерального закона;

8.1) аккредитация доверенной третьей стороны - признание уполномоченным федеральным органом соответствия юридического лица требованиям настоящего Федерального закона к доверенной третьей стороне;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

9) 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;

10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане;

12) корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

14) вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра созданного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

15) подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата;

16) заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе:

17) доверенная третья сторона - юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные настоящим Федеральным законом;

18) средства доверенной третьей стороны - программные и (или) аппаратные средства, используемые для оказания услуг доверенной третьей стороной, прошедшие процедуру подтверждения соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

19) метка доверенного времени - достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая и проверяемая доверенной третьей стороной, удостоверяющим центром или оператором информационной системы и полученная в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 3. Правовое регулирование отношений в области использования электронных подписей:

1. Отношения в области использования электронных подписей регулируются настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 4. Принципы использования электронной подписи:

Принципами использования электронной подписи являются:
1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 5. Виды электронных подписей:

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.
2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
3. Неквалифицированной электронной подписью является электронная подпись, которая:
1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2) позволяет определить лицо, подписавшее электронный документ;
3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4) создается с использованием средств электронной подписи.
4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
1) ключ проверки электронной подписи указан в квалифицированном сертификате;
2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Носители ключевой информации:

Дискета
USB Flash накопитель
Реестр
Мобильный телефон

\-

не обеспечивают защиту от считывания ключа и подвергают электронную подпись высокой вероятности компрометации.

Защищенные накопители:

\+

Рутокен
Рутокен ЭЦП 2.0
JaCarta-2
и т.д.

?

Защищенное облако?

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

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

1. Уполномоченный федеральный орган определяется Правительством Российской Федерации.

2. Уполномоченный федеральный орган:

1) осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений;

2) осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров;

3) осуществляет аккредитацию доверенных третьих сторон, проводит проверки соблюдения доверенными третьими сторонами требований, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в порядке, установленном уполномоченным федеральным органом, и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

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

5. Федеральный орган исполнительной власти в области обеспечения безопасности:

1) по согласованию с уполномоченным федеральным органом устанавливает требования к форме квалифицированного сертификата и правила подтверждения владения ключом электронной подписи;

2) устанавливает требования к средствам электронной подписи, средствам удостоверяющего центра, за исключением указанных в пункте 2.1 настоящей части, и средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи;

2.1) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра, применяемым для реализации функций, предусмотренных частью 2.2 статьи 15 настоящего Федерального закона, включающие в себя в том числе требования по:

а) хранению ключей квалифицированной электронной подписи и автоматическому созданию такой подписи с их использованием по поручению соответствующих владельцев квалифицированных сертификатов;

б) аутентификации владельцев квалифицированных сертификатов, по поручению которых аккредитованный удостоверяющий центр создает и проверяет квалифицированную электронную подпись;

в) защите информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и аккредитованным удостоверяющим центром, осуществляющим создание и проверку квалифицированной электронной подписи по поручению такого владельца;

г) доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной электронной подписи;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Федеральным законом, и публикует перечень таких средств;

4) осуществляет подтверждение соответствия средств доверенной третьей стороны требованиям, установленным в соответствии с настоящим Федеральным законом, и публикует перечень таких средств.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 9. Использование простой электронной подписи:

1. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:
1) простая электронная подпись содержится в самом электронном документе;
2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.
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:
1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;
2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.
3. К отношениям, связанным с использованием простой электронной подписи, в том числе с созданием и использованием ключа простой электронной подписи, не применяются правила, установленные статьями 10 - 18 настоящего Федерального закона.
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

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

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

1. 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.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 11. Признание квалифицированной электронной подписи:

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 12. Средства электронной подписи:

1. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:
1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;
2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;
3) позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

Приказ ФСБ РФ от 27 декабря 2011 г. № 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

Статья 13. Удостоверяющий центр
Статья 14. Сертификат ключа проверки электронной подписи
Статья 15. Аккредитованный удостоверяющий центр
Статья 16. Аккредитация удостоверяющего центра
Статья 16.1. Федеральный государственный контроль (надзор) в сфере электронной подписи
Статья 17. Квалифицированный сертификат
Статья 18. Выдача квалифицированного сертификата
Статья 18.1. Доверенная третья сторона
Статья 18.2. Аккредитация доверенной третьей стороны
Статья 19. Заключительные положения

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»

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

-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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, в части обращения со средствами криптографической защиты информации;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66, в части эксплуатации средств криптографической защиты информации;

-- эксплуатационной документации к средствам электронной подписи;

Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

-должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

Требования к персоналу

Должен быть определен и утвержден список лиц, имеющих доступ к ключевой информации.

К работе на АРМ с установленным СКЗИ допускаются только определенные для эксплуатации лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документацией на СКЗИ, а также другими нормативными документами по использованию электронной подписи.

К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются доверенные лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

Рекомендуется назначение в организации, эксплуатирующей СКЗИ, администратора безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.)

На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.

На АРМ должна быть установлена только одна операционная система. При этом не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Необходимо установить и использовать на АРМ антивирусное программное обеспечение.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения АРМ (Service Packs, Hot fix и т п.), обновлять антивирусные базы.

Обращение с ключевыми носителями

Должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с ключами ЭП и шифрования, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

Запрещается:
Снимать несанкционированные администратором безопасности копии с ключевых носителей.
Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) АРМ или принтер.
Устанавливать ключевой носитель в считывающее устройство ПЭВМ АРМ в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие ПЭВМ.
Записывать на ключевой носитель постороннюю информацию.

Обращение с ключевыми носителями

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Обращение с ключевой информацией

Владелец сертификата ключа проверки ЭП обязан:

Хранить в тайне ключ ЭП (закрытый ключ).
Не использовать для электронной подписи и шифрования ключи, если ему известно, что эти ключи используются или использовались ранее.

Немедленно требовать приостановления действия сертификата ключа проверки ЭП при наличии оснований полагать, что тайна ключа ЭП (закрытого ключа) нарушена (произошла компрометация ключа).

Обновлять сертификат ключа проверки ЭП в соответствии с установленным регламентом.

Учет и контроль

Действия, связанные с эксплуатацией СКЗИ, должны фиксироваться в журналах, которые ведет лицо, ответственное за обеспечение информационной безопасности на АРМ. В журнал кроме этого записываются факты компрометации ключевых документов, нештатные ситуации, происходящие в системе и связанные с использованием СКЗИ, проведение регламентных работ, данные о полученных у администратора безопасности организации ключевых носителях, нештатных ситуациях, произошедших на АРМ, с установленным ПО СКЗИ.

В журнале может отражаться следующая информация:

дата, время;

запись о компрометации ключа;

запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;

запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;

запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя;

запись о получении сертификата ключа проверки ЭП, полный номер ключевого носителя, соответствующий сертификату;

записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;

события, происходившие на АРМ пользователя с установленным ПО СКЗИ,

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Необходимый минимум нормативных документов в организации:

1. Приказ о назначении администратора безопасности криптосредств инструкция администратора криптосредст
2. Приказ о назначении пользователей криптосредств инструкция пользователя
3. Перечень помещений и Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств
4. Перечень лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств
5. Инструкция по антивирусной и парольной защите
6. Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов
7. Журнал учета и выдачи носителей с ключевой информацией
8. Журнал обучения пользователей правилам работы с криптосредствами

РАНХиГС

РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Читинский филиал

Спасибо за внимание!