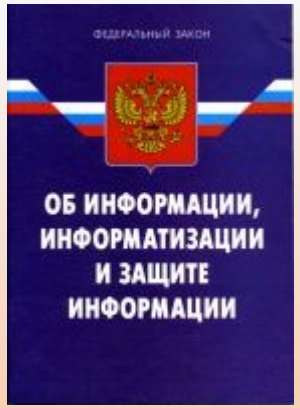
Основы законодательства об информации и её защите

Подготовил студент группы ЦОС 32 ПИ

Ляпустин Павел Витальевич

Введение

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года (принят Государственной Думой РФ 25 января 1995 года; актуальная версия закона от 21.07.2014). В нём даются основные определения и намечаются направления развития законодательства в данной области.



Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.
- Согласно закону "Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу". Далее, "Режим защиты информации устанавливается:
- в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации — собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных — Федеральным законом".

Еще несколько пунктов закона (статья 22, пункты 2-5):

1. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.
2. Риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из не сертифицированной системы, лежит на потребителе информации.
3. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты ресурсов собственника и систем и получения консультаций.
4. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем обо всех фактах нарушения режима защиты информации.

Лицензирование и сертификация (статья 19):

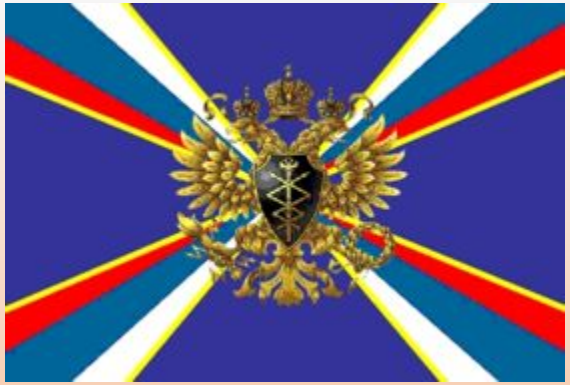
1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".
2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.
3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.
4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации"

1. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба. Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи.
2. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.
3. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Лицензирующие органы

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ). ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. (Устаревшие данные: 1 июля 2003 года Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) было упразднено



Закон "Об электронной цифровой подписи"

- Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.
- Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия:

- электронный документ;
- электронная цифровая подпись;
- владелец сертификата ключа подписи;
- средства электронной цифровой подписи
- сертификат средств электронной цифровой подписи;
- закрытый ключ электронной цифровой подписи;
- сертификат ключа подписи;
- пользователь сертификата ключа подписи;
- информационная система общего пользования;

Об нормативно-правовой базе

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность.

Заключение

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.