Тема 3.2 Основные законы России в области компьютерного права.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом развития современного общества, в частности информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это может привести к снижению информационной безопасности.

Законодательство в сфере информационной безопасности в Российской Федерации начало развиваться только в начале девяностых годов прошлого столетия. Ряд законодательных актов довольно долго действовал в старых редакциях, часть документов утратили свою самостоятельность и были включены в Гражданский кодекс РФ. В рамках данной темы дается возможность проследить судьбу некоторых актуальных документов.

Одним из основным законом Российской Федерации является **Конституция**, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации*.

В **Уголовном кодексе Российской Федерации** Глава 28 носит название «Преступления в сфере компьютерной информации», которая содержит три статьи:

- Статья 272. Неправомерный доступ к компьютерной информации;

- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 272 УК РФ описывает ситуации неправомерного доступа к охраняемой законом компьютерной информации лицом или группами лиц, повлекшее за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Здесь описаны штрафные и уголовные меры за содеянное.

Статья 273 УК РФ знакомит с мерами пресечения действий в отношении создания программ для ЭВМ или внесения изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т.д.

Статья 138 УК РФ, защищает конфиденциальность персональных данных и предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи интересны руководящие документы выпущенные Федеральной службой по техническому и экспортному контролю Российской Федерации, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно можно выделить документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В информационном обществе 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. Есть целый ряд оснований для того, чтобы это сделать. Одно из них - необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) - доминирование аппаратно-программных продуктов зарубежного производства.

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. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных), может представлять угрозу национальной безопасности (в том числе информационной безопасности), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В

таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

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.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Предлагаем ознакомится с некоторыми важными нормативно-правовыми документами в области информационных технологий и информационной безопасности более подробно.

Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992г. № 3523-1). Закон «Об авторском праве и смежных правах» (от 09.07.1993г. №5351-1 с последующим изменением и дополнением). Четвертая часть Гражданского кодекса РФ (от 18.12.2006г №230-ФЗ). Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от 18.12.2006г. №231-ФЗ.).

Два важных документа - Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992г. № 3523-1) и Закон «Об авторском праве и смежных правах» (от 09.07.1993г. №5351-1) были введены в действие с целью регулирования правовых норм в отношении авторского права т охране программ для ЭВМ. Законы работали самостоятельно до 1 января 2008 года, в связи с введением в действие ФЗ «О введении в действие части четвертой гражданского кодекса РФ» (от 18.12.2006г. №231-ФЗ).

Четвертая часть гражданского кодекса РФ (от 18.12.2006г №230-ФЗ), в текстах которого прописаны нормы правовой охраны программ для ЭВМ и баз данных, затрагивает права на результаты интеллектуальной деятельности и средства индивидуализации (к которым и относятся программы для ЭВМ и базы данных); авторское право; права, смежные с авторскими; патентное

право и т.д. Отсюда можно узнать как используется авторское право, как оно действует, какие есть ограничения в использовании авторских прав, как составляются договора и документы по авторскому праву и охране программ для ЭВМ, какие санкции могут применяться относительно неправомерного использования авторского права и т.д.

Закон «О государственной тайне» (от 21.07.1993г. № 5485-1 с последующим изменением и дополнением).

Рассмотрим подробнее закон «О государственной тайне» (от 21.07. 1993г. № 5485-1) с последующим изменением и дополнением). Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О государственной тайне» (с изменениями и дополнениями от 6 октября 1997 года). В нем ***гостайна*** определена, как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Согласно данному Закону, ***средства защиты информации*** - это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О Безопасности» и включает в себя настоящий закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Федеральный закон «О связи» (от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением).

Данный Федеральный закон впервые был принят в редакции от 16.02.1995г. за номером 15-ФЗ. В настоящее время имеют дело с редакцией от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением. Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Целями настоящего Федерального закона являются:

- создание условий для оказания услуг связи на всей территории Российской Федерации;

- содействие внедрению перспективных технологий и стандартов;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российскими радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Статья 63 «Тайна связи» Главы 9 «Защита прав пользователей услугами связи» затрагивает проблему конфиденциальности передаваемой информации операторами связи.

Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006г. №149-ФЗ).

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В настоящее время его название видоизменено и звучит следующим образом – «Об информации, информационных технологиях и защите информации». Закон в обновленном виде действует с 27 июля 2006г. за номером 149-ФЗ.

Настоящий Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

В нем даются основные определения и намечаются направления развития законодательства в данной области.

Приведем основные определения согласно статье 2:

1) **информация** - сведения (сообщения, данные) независимо от формы их представления;

2) **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) **информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) **доступ к информации** - возможность получения информации и ее использования;

7) **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) **предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) **распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) **электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) **документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации прописаны в статье 3. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 16 носит название «Защита информации» и затрагивает следующие аспекты:

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

А Статья 17 предусматривает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Исходя из того, что практические умения и навыки по указанным выше вопросам представляется целесообразным формировать в условиях, приближенных к жизненным, наиболее подходящим средством для этого являются ситуационные задачи, т. е. задачи, которые формулируются в виде описания жизненных ситуаций. Для закрепления вышеизложенного материала предлагается проанализировать эти ситуации, выявить в них моменты правонарушений, обосновав выдержками из упомянутых выше нормативных документов, и по необходимости сделать выводы.