Часть 2

5. ЗАКОНОДАТЕЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В деле обеспечения информационной безопасности успех может принести только комплексный подход. ***Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:***

- *законодательного;*
- *административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);*
- *процедурного (меры безопасности, ориентированные на людей);*
- *программно-технического.*

5.1 Понятие о законодательном уровне информационной безопасности

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.

На законодательном уровне различают две группы мер:

- *меры, направленные на создание и поддержание в обществе негативного* (в том числе с применением наказаний) *отношения к нарушениям и нарушителям информационной безопасности* (назовем их мерами ограничительной направленности);
- *направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности* (меры созидательной направленности).

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

5.2 Обзор российского законодательства в области информационной безопасности

5.2.1 Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

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.*

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

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции *гарантирует право на 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 Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна. *Согласно* ***статье 139 ГК РФ****, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.* Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма шепетильным в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года).

Глава 28 УК РФ - «Преступления в сфере компьютерной информации» *- 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.*

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ*, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.*

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.* Там же дается определение ***средств 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.* Подчеркнем важность последней части определения.

5.2.2 Закон «Об информации, информатизации и защите информации»

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать ***закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ*** (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

- ***информация*** *- сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;*

- **документированная информация (документ)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- **информационные процессы** - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- ***информационная система*** - *организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;*
- ***информационные ресурсы*** - *отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);*
- **информация о гражданах (персональные данные)** - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- ***конфиденциальная информация*** - *документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;*
- ***пользователь (потребитель) информации*** - *субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.*

Обратим внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

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.*

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности («предотвращение несанкционированных действий по ... блокированию информации») сказано довольно мало.

Продолжим цитирование:

«Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу».

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений. 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.»*

Здесь явно выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Процитируем **статью 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.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...

И еще несколько пунктов, теперь из **статьи 22**:

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.
3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.
4. 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 его ресурсов и систем и получения консультаций.
5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Из пункта 5 следует, что должны обнаруживаться все (успешные) атаки на ИС. Вспомним в этой связи один из результатов опроса (см. лекцию 1): около трети респондентов-американцев не знали, были ли взломаны их ИС за последние 12 месяцев. По нашему законодательству их можно было бы привлечь к ответственности...

Далее, **статья 23 «Защита прав субъектов в сфере информационных процессов и информатизации»** содержит следующий пункт:

2. 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:
3. 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.
4. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы «неотказуемости» (невозможности отказаться от собственной подписи).

Таковы важнейшие, на наш взгляд, положения Закона «Об информации, информатизации и защите информации». На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

5.2.3 Другие законы и нормативные акты

Следуя логике Закона «Об информации, информатизации и защите информации», продолжим наш обзор ***Законом «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ*** (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

Лицензия - *специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.*

Лицензируемый вид деятельности - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.

Лицензирование - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за

соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

Лицензирующие органы - *федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.*

Лицензиат - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.»

Статья 17 Закона «О лицензировании отдельных видов деятельности» устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Основными лицензирующими органами в области защиты информации являются

- ***Федеральное агентство правительственной связи и информации (ФАПСИ)*** *ведает всем, что связано с криптографией,*
- ***Гостехкомиссия*** *лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности.*

Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ, которые мы здесь перечислять не будем.

В эпоху глобальных коммуникаций важную роль играет ***Закон «Об участии в международном информационном обмене» от 4 июля 1996 года номер 85-ФЗ*** (принят Государственной Думой 5 июня 1996 года). В нем, как и в Законе «Об информации...», основным защитным средством являются лицензии и сертификаты.

10 января 2002 года Президентом был подписан очень важный ***закон «Об электронной цифровой подписи» номер 1-ФЗ*** (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона «Об информации...». Его роль поясняется в **статье 1.**

1. 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.
2. 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 - документ, в котором информация представлена в электронно-цифровой форме.

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.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

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

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

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности

электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина «сертификат», которое, впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе «Об информации...», поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

На этом заканчиваем обзор законов РФ, относящихся к информационной безопасности.

5.3 Обзор зарубежного законодательства в области информационной безопасности

Очертим некоторые законы нескольких стран (в первую очередь - США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет ***американский «Закон об информационной безопасности» (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988***). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в начале Закона называется конкретный исполнитель - Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

В 1997 году появилось продолжение описанного закона - **законопроект «О совершенствовании информационной безопасности»** (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Для защиты федеральных ИС рекомендуется более широко применять технологические решения, основанные на разработках частного сектора.

Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи -FIPS 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений - аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законотворческая деятельность идет в ногу с прогрессом информационных технологий.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем на них останавливаться. Желающие могут прочитать раздел «Законодательная база в области защиты информации» в превосходной статье О. Беззубцева и А. Ковалева «О лицензировании и сертификации в области защиты информации» (Jet Info, 1997, 4).

В законодательстве ФРГ выделим весьма развернутый (44 раздела) ***Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)***). Он целиком посвящен защите персональных данных.

Как, вероятно, и во всех других законах аналогичной направленности, в данном случае устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу. Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни «субъекта данных», как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании упомянем семейство так называемых ***добровольных стандартов BS 7799***, помогающих организациям на практике сформировать программы безопасности. В последующих лекциях мы еще вернемся к рассмотрению этих стандартов; здесь же отметим, что они действительно работают, несмотря на «добровольность» (или благодаря ей?).

В современном мире глобальных сетей законодательная база должна быть согласована с международной практикой. В этом плане поучителен

пример Аргентины. В конце марта 1996 года компетентными органами Аргентины был арестован Хулио Цезар Ардита, 21 года, житель Буэнос-Айреса, системный оператор электронной доски объявлений «Крик», известный в компьютерном подполье под псевдонимом «El Griton». Ему вменялись в вину систематические вторжения в компьютерные системы ВМС США, НАСА, многих крупнейших американских университетов, а также в компьютерные системы Бразилии, Чили, Кореи, Мексики и Тайваня. Однако, несмотря на тесное сотрудничество компетентных органов Аргентины и США, Ардита был отпущен без официального предъявления обвинений, поскольку по аргентинскому законодательству вторжение в компьютерные системы не считается преступлением. Кроме того, в силу принципа «двойной криминальности», действующего в международных правовых отношениях, Аргентина не может выдать хакера американским властям. Дело Ардита показывает, каким может быть будущее международных компьютерных вторжений при отсутствии всеобщих или хотя бы двусторонних соглашений о борьбе с компьютерной преступностью.

5.4 О текущем состоянии российского законодательства в области информационной безопасности

Как уже отмечалось, ***самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий.*** Пока такого механизма нет и, увы, не предвидится. Сейчас бессмысленно задаваться вопросом, чего не хватает российскому законодательству в области ИБ, это все равно, что интересоваться у пунктирного отрезка, чего тому не хватает, чтобы покрыть всю плоскость. Даже чисто количественное сопоставление с законодательством США показывает, что наша законодательная база явно неполна.

Справедливости ради необходимо отметить, что ограничительная составляющая в российском законодательстве представлена существенно лучше, чем координирующая и направляющая. *Глава 28 Уголовного кодекса РФ достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.*

Положения базового Закона «Об информации, информатизации и защите информации» носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно. Характерно, что Закон разъясняет вопросы ответственности в случае использования несертифицированных средств, но что делать, если нарушение ИБ произошло в системе, построенной строго по правилам? Кто возместит

ущерб субъектам информационных отношений? Поучителен в этом отношении рассмотренный выше закон ФРГ о защите данных.

Законодательством определены органы, ведающие лицензированием и сертификацией. (Отметим в этой связи, что Россия - одна из немногих стран (в список еще входят Вьетнам, Китай, Пакистан), сохранивших жесткий государственный контроль за производством и распространением внутри страны средств обеспечения ИБ, в особенности продуктов криптографических технологий.) Но кто координирует, финансирует и направляет проведение исследований в области ИБ, разработку отечественных средств защиты, адаптацию зарубежных продуктов? Законодательством США определена главная ответственная организация - НИСТ, которая исправно выполняет свою роль. В Великобритании имеются содержательные добровольные стандарты ИБ, помогающие организациям всех размеров и форм собственности. У нас пока ничего такого нет.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии России, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

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. 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.

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.*