РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

С. Ф. Нехорошев,
начальник отдела безопасности и информатизации УИТАС, Компания ИВК

В последнее время руководители организаций различных форм собственности и сфер деятельности все большее внимание уделяют множеству аспектов сохранности данных в корпоративных информационных системах. При этом, как правило, значительное внимание уделяется технологическим и программным средствам защиты информации. А особенности, специфика Российской и западной законодательной базы, регулирующей вопросы информационной безопасности, зачастую остаются без должного внимания. Возможной причиной этого является исторически сложившаяся специфика нормативно-правовой базы российского законодательства в этой области.

Одной из таких специфических особенностей российской нормативно-правовой базы является то, что основа ее создавалась еще в период, предшествующий массовой компьютеризации и информатизации общества, когда большая часть информации хранилась на бумажных носителях, и к сохранности информации предъявлялись особые требования, за выполнение которых отвечали уполномоченные на то государственные структуры. Этот же фактор зачастую встает на пути гармонизации российских и зарубежных стандартов в области информационной безопасности.

Другой, не менее важной особенностью, является то, что в наше время технологии, направленные на обеспечение информационной безопасности, развиваются настолько бурными темами, что нормативно-правовая база не в полной мере успевает за техническим прогрессом в этой области. В связи с этим в настоящее время сложилась ситуация, при которой имеющаяся нормативно-правовая база не полностью соответствует реально сложившейся практике работы предприятий, разрабатывающих решения в сфере информационной безопасности.

Целью данной статьи является знакомство читателя с основными особенностями нормативно-правовой базы российского законодательства, регулирующей различные аспекты обеспечения информационной безопасности.

В настоящее время в области обеспечения информационной безопасности достаточно много нормативных документов и законодательных актов, охватывающих широкий круг вопросов защиты информации, однако имеются до сих пор нерешенные проблемы. В СМИ идет интенсивное обсуждение создавшейся ситуации, над разработкой дополнительных нормативных документов работают как гражданские институты, так и институты силовых структур, в первую очередь, тех, в чьих информационных системах обрабатывается данные, составляющие государственную тайну. В качестве основы нормативно-правового регулирования информационной безопасности в настоящий момент можно выделить следующие типы документов: законы и подзаконные акты, постановления правительства, руководящие документы ФСТЭК, государственные стандарты (ГОСТы), отраслевые стандарты (ОСТы), ведомственные приказы и распоряжения, лицензии, сертификаты.

Законы и подзаконные акты. Составляют основу всей нормативно-правовой базы по обеспечению информационной безопасности. Действующие в настоящее время законы и подзаконные акты направлены на регулирование взаимоотношений различных субъектов, работающих в области обеспечения информационной безопасности, а также являются правовой основой органов, осуществляющих лицензирование различных видов деятельности в области информационной безопасности.

Постановления правительства. Вводят перечень органов государственной власти, уполномоченных проводить лицензирование различных видов деятельности, а также регламентируют деятельность органов, осуществляющих сертификацию решений в области информационной безопасности.

Руководящие документы ФСТЭК. Вводят различные категории и показатели защищенности средств по обеспечению информационной безопасности.

Государственные стандарты (ГОСТы). Устанавливают стандарты на различные технологические аспекты обеспечения информационной безопасности, применимые на всей территории Российской Федерации.

Отраслевые стандарты (ОСТы). Устанавливают стандарты на различные технологические аспекты обеспечения информационной безопасности, применимые лишь в рамках деятельности какой-либо отрасли, работающей в сфере обеспечения информационной безопасности, на которую распространяется стандарт. Отдельный отраслевой стандарт в части обеспечения информационной безопасности имеет Центральный банк Российской Федерации.

Ведомственные приказы и распоряжения. Составляют основу работы различных ведомств, работающих в сфере информационной безопасности.

Лицензии. По существующим правилам разрабатывать, производить и реализовывать средства защиты информации может только предприятие, имеющее лицензию на эти виды деятельности. Лицензии выдаются на ограниченный срок, если условия для заявленного вида деятельности удовлетворят Орган по лицензированию. При этом в течение срока действия лицензии Орган по лицензированию следит за неизменностью (не ухудшением) условий заявленного вида деятельности. В случаях, предусмотренных Федеральным Законом «О лицензировании отдельных видов деятельности», действие лицензии может быть приостановлено или аннулировано.

Сертификаты. Наличие сертификата у продукта, обеспечивающего информационную безопасность, подтверждает его соответствие определенным требованиям, изложенным в Руководящих документах Гостехкомиссии, а также отсутствие в продукте незадекларированых возможностей.

Среди наиболее важных действующих в настоящее время законов, направленных на регулирование различных аспектов информационной безопасности, можно выделить следующие:

Федеральный закон № 24-ФЗ, «Об информационной безопасности и защите информации», принятый 20 февраля 1995 г. и утвержденный Указом Президента Российской Федерации от 20 февраля 1995 г. Отличительной особенностью данного закона является его направленность на регулирование отношений, возникающих при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации, создании и использовании информационных технологий и средств их обеспечения, защите информации, прав субъектов, участвующих в информационных процессах и информатизации. Необходимо отметить, что настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах».

Другим не менее важным правовым актом является Федеральный закон № 128-ФЗ «О лицензировании отдельных видов деятельности», принятый 8 августа 2001 г. и утвержденный Указом Президента Российской Федерации от 8 августа 2001 г. (с изменениями и дополнениями от 13 марта, 21 марта 2002 г.). Важнейшей особенностью этого закона является то, что он устанавливает правовую основу работы лицензирующих органов. Этот закон регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности. При этом, его действие не затрагивает деятельность, связанную с защитой государственной тайны. Согласно этому закону, обязательному лицензированию подлежат следующие виды деятельности: деятельность по распространению шифровальных (криптографических) средств; деятельность по техническому обслуживанию шифровальных (криптографических) средств; предоставление услуг в области шифрования информации; разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем; деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей; и т. д.

Отдельно стоит упомянуть и о Федеральном законе о техническом регулировании, который был принят Государственной думой 15 декабря 2002 г. и одобрен Советом Федерации 18 декабря 2002 г. Основная роль этого закона сводится к регулированию отношений, возникающих при разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также при разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг.

Говоря об основных нормативно-правовых актах в части информационной безопасности, нельзя не упомянуть о Постановлениях Правительства Российской Федерации. Наиболее важными из них являются следующие:

Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны». Данное постановление вводит перечень органов исполнительной власти, осуществляющих лицензирующую деятельность.

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». Закон является основным документом, регламентирующим деятельность органов по сертификации средств защиты информации.

Среди руководящих документов Гостехкомиссии необходимо обратить внимание на следующие: Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), в которых приведен максимально полный состав требований к объектам информатизации, где обрабатывается конфиденциальная информация, а также Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР), максимально полно описывающие требования к объектам информатизации, где обрабатывается информация, составляющая государственную тайну.

Также не менее важными документами, входящими в состав нормативно-правовой базы, касающейся обеспечения информационной безопасности, являются ГОСТы. Среди них особо следует выделить ГОСТ Р 50739—95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», в котором приведены наиболее полные определения сути защиты информации от несанкционированного доступа, а также ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», который содержит наиболее значимые факторы воздействия на информацию. Однако самым полным и современным на сегодняшний день оценочным стандартом является ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий», который, по сути, является стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования, однако он не содержит предопределенных классов безопасности. Основными идеями этого стандарта являются: возможное сокращение затрат на сертификацию продуктов; международное признание сертификатов, по-

лученных в России (данный стандарт является полностью гармонизированным с международным стандартом ISO); сохранение национальных требований, включая защиту информации, содержащей государственную тайну, для высших уровней сертификации.

Для подтверждения соответствия характеристик продукта требованиям, изложенным в стандартах по обеспечению информационной безопасности, в отношении него проводится процедура сертификации. В России функционируют четыре Федеральные системы сертификации по требованиям безопасности информации (определено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608). В каждой есть собственные специфические закрытые особенности, за исключением открытой добровольной системы сертификации ФСТЭК, ее руководящие документы открыто публикуются. При этом средства криптографической защиты информации имеет право сертифицировать только Федеральная служба безопасности РФ, а остальные службы производят сертификацию продуктов, не содержащих криптографического функционала. Сертификацию организуют органы по сертификации, а сертификационные испытания проводят аккредитованные лаборатории по методикам, утвержденным Органом по сертификации. Сначала лаборатория готовит протоколы испытаний на основе завершенных испытаний и Техническое заключение. Далее результаты испытаний проверяют эксперты, отдельно назначенные Органом по сертификации. При положительных выводах Технического заключения и экспертов Орган принимает решение о выдаче сертификата на определенный срок (3-5 лет). Сертификация осуществляется либо партии изделий (фиксированной), либо по схеме «тип образца». В итоге в случае сертификации по схеме «тип образца» может быть принято решение о выдаче лицензии на применение т. н. «знака соответствия», но только если производство сертифицированной продукции удовлетворяет требованиям Органа по сертификации. В период действия сертификата Органом по сертификации проводится периодический инспекционный контроль производимой продукции, допускающий отзыв лицензии на применение знака соответствия в случае грубых нарушений, вплоть до приостановки действия выданного сертификата. При этом существует довольно интересная российская особенность, связанная с сертификацией продуктов в области информационной безопасности. Связана она с тем, что зачастую заказчик защищенного продукта (изделия), понимая, что затраты на предстоящую сертификацию по требованиям безопасности информации включаются в себестоимость изделия и проявляя естественное стремление не тратить «лишних» денег, включает в Техническое задание на разработку только обязательные требования для соответствующего класса защиты, определенные Руководящими документами ФСТЭК. Разработчик защищенного продукта, опираясь на устаревшие, но дающие необходимый класс защиты нормы, также минимизирует трудозатраты, пытаясь и исключительно формально реализовать эти требования по безопасности, за исключением базового функционала, который должен работать безупречно. Разработанная система успешно сертифицируется по требованиям безопасности информации, и довольны все, кроме реального потребителя этого продукта. Обработка информации на реальном объекте информатизации «вдруг» приводит к компрометации информации, искажениям, утрате либо блокируется доступ к ней. И тупиковость ситуации в том, что виноватых нет. Все нормы действующего законодательства соблюдены, все штатно выполнили (выполняли свои обязанности).

В связи с этим вполне благоприятным может оказаться перенос зарубежных стандартов на российский рынок, особенно с учетом некоторого застоя в части эволюции нашей нормативно-правовой базы. В соответствии со сложившейся на Западе практикой работы, этапу создания средств защиты информации предшествует оценка (сертификация) так называемого Профиля защиты, на базе требований которого разрабатывается Техническое задание, а в предсертификационный период – Задание по безопасности. И выглядит это все на деле существенно менее консервативно, статично и непродуманно, чем на российском IT-рынке. Заказчик может разработать Профиль защиты, учитывающего все особенности его объекта информатизации, и сертифицировать вновь разработанный продукт на соответствие так называемому Заданию по безопасности для обработки конфиденциальной информации. Пусть дополнительная «компетентная» экспертиза определит достаточность требований Профиля или Задания по безопасности для обработки конфиденциальной информации. В этой схеме есть явный плюс: появляется фигура «компетентного эксперта», которого можно «наказать, если что». И этот эксперт будет следить за всеми новациями в индустрии.

Существует также еще одно различие между российским и зарубежным законодательством в части информационной безопасности и связана она с особенностями принятия нормативно-правовой базы. В практику работы российских разработчиков средств защиты информации в настоящее время ложатся уже существующие нормы законодательной базы, в то время как на Западе иногда уже сложившаяся практика работы и специфика работы крупных корпораций, имеющих устоявшуюся положительную репутацию, ложится в основу законодательства. По сути, закон обобщает и закрепляет уже сложившаяся практика работы крупных корпораций.

В целом, мир, в котором мы живем, становится все более компьютеризированным и информационным. Это явление продиктовано веянием времени и в равной мере пронизывает как коммерческие структуры, так и государственные ведомства, в том числе силовые. В связи с тем, что в настоящее время различные государства активно взаимодействуют друг с другом по экономическим, политическим, оборонным и другим вопросам, очевидна необходимость взаимодействия информационных систем этих стран. Вместе с тем необходимо, чтобы при этом взаимодействии в полной мере соблюдалось законодательство этих стран, регулирующее нормативно-правовые аспекты информационной безопасности, специфика которых не всегда соотносится с особенностями нормативно-правовой базы российского законодательства. Вероятно, этот принцип в обозримом будущем будет одной из важнейших задач в области применения политики безопасности.