Законодательная и нормативная правовая база обеспечения информационной безопасности Российской Федерации

Л. А. Шивдяков, к. в. н.,
руководитель Управления ФСТЭК России
по Дальневосточному федеральному округу

В статье проанализированы требования основных законодательных и нормативных актов в области информационной безопасности и технической защиты информации, действующих на территории Российской Федерации. На основе правоприменительной практики отмечены положительные моменты и недостатки действующей законодательной и нормативно-правовой базы в области информационной безопасности.

В нашей стране теоретические разработки законодательства в области информатизации были начаты специалистами Института государства и права АН СССР еще в 60-е годы. Однако на практике эти вопросы начали рассматриваться лишь в 70-е годы в связи с развитием автоматизированных систем управления различных уровней, ориентированных главным образом на использование больших ЭВМ.

В условиях монопольного распоряжения правами владения, использования и распоряжения национальными информационными ресурсами деятельность специалистов по защите информации в нашей стране сводилась к организации защиты секретной информации, а прерогатива защиты и контроля защищенности засекреченной информации сводилась к исключительной компетенции государства[1].

Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности в своем решении от 02.12.97 определила следующие основные направления развития законодательства в области обеспечения информационной безопасности:

- внесение изменений в действующее законодательство для развития обеспечения информационной безопасности в целях устранения противоречий нормам Конституции Российской Федерации и международным соглашениям, к которым присоединилась Российская Федерация, противоречий между законодательными актами федерального уровня и актами субъектов Российской Федерации, а также конкретизации норм ответственности за правонарушения в области информационной безопасности;
- законодательное разграничение уровней правового регулирования проблем обеспечения информационной безопасности (федеральный уровень, уровень субъекта РФ, уровень местного самоуправления);

[1] *Минаев В. А., Скрыль С. В., Фисун А. П., Потанин В. Е., Дворянкин С. В. Основы информационной безопасности. – Воронеж: Воронежский институт МВД России, 2001. – с. 233.*

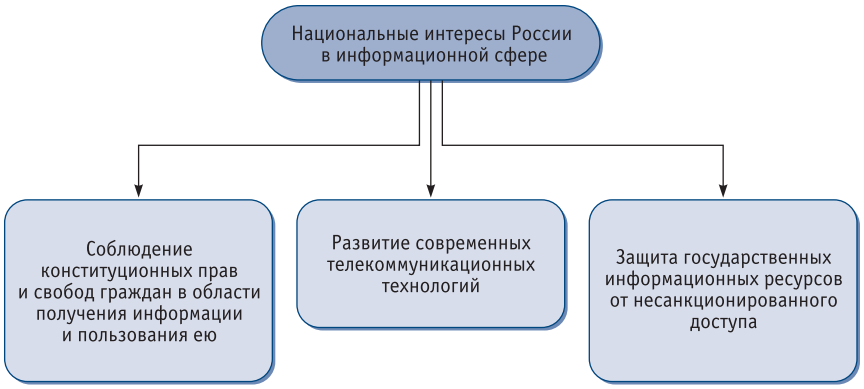
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- разработка Национальной программы развития общедоступных компьютерных сетей, включая определение правового статуса провайдера интернет-услуг и правовое регулирование их деятельности, представление в Интернет информации о деятельности органов государственной власти и органов местного самоуправления, защиту русского языка в Интернете;
- создание правовой базы для функционирования в Российской Федерации системы региональных центров обеспечения информационной безопасности;
- правовое регулирование развития негосударственного компонента в формировании информационного общества и обеспечения информационной безопасности Российской Федерации[2].

Важнейшим рычагом для обеспечения информационной безопасности Российской Федерации является соответствующая законодательная база.

Концепция национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 17.12.97 № 1300, определила национальные интересы России в информационной сфере (см. рисунок):

- соблюдение конституционных прав и свобод граждан в области получения информации и пользования ею;
- развитие современных телекоммуникационных технологий;
- защита государственных информационных ресурсов от несанкционированного доступа[3].

Основным законом Российской Федерации, затрагивающим вопросы информационной безопасности, является Конституция Российской



Рисунок

Федерации, принятая 12.12.93. На основании ст. 23 Конституции РФ человеку предоставляется и гарантируется право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений[4]. Данное право ограничивается исключительно по судебному решению, о чем говорит тот факт, что личная информация незыблема и неотчуждаема, и никто не вправе вторгаться в нее без разрешения судебного органа.

В соответствии со ст. 24 Конституции РФ, 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[5].

Статья 29 Конституции РФ предоставляет каждому гражданину право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. При этом указывается, что перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Статья 41 Конституции РФ гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, ст. 42 – право на знание достоверной информации о состоянии окружающей среды[6].

Одним из наиболее важных документов в области информационной безопасности, продолжившем развитие Концепции национальной безопасности Российской Федерации применительно к информационной сфере, является Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09.09.2000 № Пр-1895.

Она является базовой основой для достижения следующих задач:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения ИБ Российской Федерации[7].

В Доктрине под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Доктрина выделяет четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

[2] *Уфимцев Ю. С., Ерофеев Е. А. и др. Информационная безопасность России. – М.: Изд-во «Экзамен», 2003. – с. 68.*

[3] *Концепция национальной безопасности Российской Федерации. Разд. 2.*

[4] *Конституция Российской Федерации. Гл. 2. Ст. 23.*

[5] *Там же. Гл. 2. Ст. 24.*

[6] *Там же. Гл. 2. Ст. 29, 41, 42*

[7] *Доктрина информационной безопасности Российской Федерации. Преамбула.*

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.

2. Информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России[8].

К правовым методам обеспечения информационной безопасности Российской Федерации Доктрина относит разработку нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась РФ, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов РФ, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов РФ, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- законодательное закрепление приоритета развития национальных сетей связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в РФ региональных структур обеспечения информационной безопасности[9].

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации. Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативно-правовых актов в информационной сфере и выработку программы их совершенствования;
- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
- разработку нормативно-правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ[10].

[8] *Доктрина информационной безопасности Российской Федерации. Разд. 1. Гл. 1.*

[9] *Там же. Разд. 2. Гл. 5.*

[10] *Там же. Разд. 3. Гл. 8.*

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

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 информационной безопасности серверов.

Федеральным законом Российской Федерации от 30.12.2001 № 195-ФЗ (с изменениями и дополнениями от 29.04.2008 № 58-ФЗ) с 01.07.2002 введен в действие Кодекс РФ об административных правонарушениях, предусматривающий административную ответственность физических, юридических и должностных лиц, в частности, за правонарушения в области информации.

Кодекс Российской Федерации об административных правонарушениях выделяет два вида нарушений в области защиты информации:

- в соответствии со ст. 13.12 – нарушение правил защиты информации;
- в соответствии со ст. 13.13 – незаконная деятельность в области защиты информации[11].

Они предусматривают ответственность за несоблюдение лицензионных требований и условий в области защиты информации.

Статья 13.14 уделяет внимание факту разглашения информации с ограниченным доступом. Защищая конфиденциальность персональных данных, ст. 13.11 Кодекса устанавливает санкции за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). В ст. 19.7 Кодекс устанавливает санкцию за непредставление сведений (информации) в своевременный срок государственному органу или должностному лицу, которые обязательны для представления в соответствии с законом и необходимы для осуществления этим органом (должностным лицом) его законной деятельности, а равно за представление сведений в неполном объеме или в искаженном виде[12].

Законодательство об административных правонарушениях преследует цель выявить и пресечь правонарушения в области защиты информации и установить санкции в отношении данных правонарушителей в области связи и информации, управления. Кодекс Российской Федерации об административных правонарушения определяет также органы, в компетенцию которых входит:

- осуществление государственного контроля в области обращения и защиты информации (ст. 23.46);
- осуществление государственного надзора за связью и информатизацией (ст. 23.44);
- осуществление контроля за обеспечением защиты государственной тайны (ст. 23.45).

Весьма конкретно определяет меры ответственности за совершение преступлений в сфере информационной безопасности Уголовный кодекс Российской Федерации[13], введенный в действие Федеральным законом РФ от 13.06.96 № 63-ФЗ (с изменениями и дополнениями от 08.04.2008 № 43-ФЗ).

Статья 138 УК Российской Федерации, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, переговоров, сообщений и тем самым устанавливает правовой барьер нарушению нормы ст. 23 Конституции. Статья 140 УК РФ устанавливает санкции за отказ в предоставлении гражданам информации, требуемой на законных основаниях, и, безусловно, также защищает конституционные права и свободы граждан, которые гарантированы, в частности, в ст. 29 Конституции Российской Федерации. Необходимо упомянуть ст. 183 УК РФ, в которой определены наказания за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Не следует также забывать ст. 237 УК РФ, предусматривающую санкцию за нарушение ст. 41 Конституции Российской Федерации, а именно за сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей. Безусловно, в этом вопросе должностные лица органов государственной власти обязаны строго придерживаться конституционных норм и следовать конституционным гарантиям и правам человека. Как логическое завершение сказанному, необходимо отметить также гл. 26 УК РФ и провести параллель со ст. 42 Конституции Российской Федерации, где оптимально построена защита в области эко-

[11] *Кодекс Российской Федерации об административных правонарушениях. Гл. 13. Ст. 13.12, 13.13.*

[12] *Там же. Гл. 13. Ст. 13.11, 13.14, 19.7.*

[13] *Уголовный кодекс Российской Федерации. Ст. 138, 140.*

логии и где человек имеет право на достоверную информацию о состоянии окружающей среды.

Весьма актуальна в условиях современного информационного мира гл. 28 УК РФ «Преступления в сфере компьютерной информации». Статья 272 устанавливает ответственность за неправомерный доступ к охраняемой законом информации, находящейся в электронном виде (на машинном носителе, в ЭВМ, системе ЭВМ или их сети), то есть пресекает посягательство на конфиденциальность; ст. 273 устанавливает меры ответственности нарушителей, незаконно создающих программы для ЭВМ или вносящих изменения в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, нарушения работы ЭВМ, их систем или сетей, тем самым наносящих существенный вред информационным интересам государства. Статья 274 делает упор на противодействие нарушению целостности охраняемой законом информации, содержащейся в базе данных ЭВМ, и этим самым подтверждает приоритет сохранения единой информационной системы[14].

Перед выходом Указа Президента РФ от 30.11.95 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне», в целях разработки данного перечня и установления правил по разграничению сведений, отнесенных к государственной тайне, было утверждено Постановление Правительства Российской Федерации от 04.09.95 № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

В Постановлении ставятся задачи определить степень секретности конкретных сведений, учет ведомственной и отраслевой специфики. Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности государства вследствие распространения данных сведений.

Настоящее Постановление, опираясь на закон Российской Федерации «О государственной тайне», определяет принципы засекречивания сведений: законность, обоснованность, своевременность, а также обращает внимание экспертных комиссий на данные принципы, которыми они должны руководствоваться при подготовке проекта перечня, анализе всех видов деятельности органов государственной власти, предприятий, учреждений и организаций с целью определения сведений, распространение которых может нанести ущерб безопасности Российской Федерации.

Также в Постановлении указано, что утвержденные перечни могут пересматриваться, дополняться и изменяться в случае необходимости не реже, чем через пять лет, и в том же порядке, что и при их разработке[15].

В дальнейшем Указ Президента Российской Федерации № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне», упоминавшийся выше, был изложен в редакции Указа Президента РФ от 30.04.2008 № 654.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в законе «О государственной тайне» от 21.07.93 № 5485-1 (с изменениями и дополнениями от 01.12.2007 №№ 294-ФЗ и 318-ФЗ).

В нем государственная тайна 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. Согласно данному закону, 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[16]. Следует отметить важность последней части определения. Она выражается в обеспечении надежности защиты сведений, отнесенных к государственной тайне, а также в выборе приоритетной задачи по усовершенствованию технических средств защиты информации.

В данном законе делается акцент на то, что законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, законе Российской Федерации «О безопасности», включает настоящий закон и другие положения, регулирующие отношения, связанные с защитой государственной тайны.

Рассматриваемый закон выделяет принципы, которым обязаны следовать органы государственной власти и должностные лица при отнесении сведений к гостайне и их засекречиванию, а именно такие принципы, как законность, обоснованность, своевременность. Законность заключается в соответствии засекречиваемых сведений положениям законодательства Российской Федерации о государственной тайне и настоящему закону.

В законе определен порядок засекречивания и рассекречивания сведений, составляющих государственную тайну, регламентированы правила по распоряжению и использованию секретных сведений. Перечислен ряд органов по защите государственной тайны и их полномочия, указан ряд обязательств, которые берут на себя должностные лица и граждане при допуске к государственной тайне, льготы и права.

Устанавливаются формы допуска к государственной тайне должностных лиц и граждан, сроки и порядок переоформления допуска, осно-

[14] *Уголовный кодекс Российской Федерации. Гл. 28. Ст. 272–274.*

[15] *Постановление Правительства Российской Федерации от 04.09.95 № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности». П. 6.*

[16] *Федеральный закон «О государственной тайне». Разд. 1. Ст. 2.*

вания для отказа в допуске к государственной тайне должностному лицу и гражданину.

Установлена ответственность за нарушения законодательства Российской Федерации о государственной тайне. В заключительном разделе указаны лица и органы, осуществляющие контроль и надзор за обеспечением защиты государственной тайны.

Следует затронуть в кратком аспекте еще один немаловажный Федеральный закон «О безопасности» от 05.03.92 № 2446-1 (в редакции от 02.03.2007 № 24-ФЗ), устанавливающий и рассматривающий, в том числе, вопросы обеспечения информационной безопасности. Закон определяет жизненно важные интересы таких основных объектов безопасности, как личность с ее правами и свободами, общества с его материальными и духовными ценностями и государство с его конституционным строем, суверенитетом и территориальной целостностью, а также ставит цель обеспечить безопасность данных объектов и их взаимоотношений, в ходе которых удовлетворяются потребности всех основных объектов безопасности, тем самым обеспечивая возможность прогрессивного развития личности, общества и государства. И наконец, преследует цель закрепить систему безопасности на правовом уровне, определив и утвердив элементы и функции системы безопасности, принципы обеспечения безопасности (законность, взаимоответственность, интеграция с международными системами безопасности). Примечателен тот факт, что в Законе имеет место разграничение полномочий органов власти в системе безопасности, что, безусловно, исключает доминирующее положение одного из органов и не допускает путаницы.

Законодательством по обеспечению безопасности ставятся такие задачи, как:

- определение важных интересов личности, общества и государства, выявление внутренних и внешних угроз объектам безопасности и их оценка;
- разработка основных направлений стратегии обеспечения безопасности и организация подготовки федеральных программ ее обеспечения;
- анализ и обработка информации о функционировании системы обеспечения безопасности РФ;
- организация научных исследований в области обеспечения безопасности[17].

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. Данный закон принят в развитие Доктрины информационной безопасности Российской Федерации вместо действовавшего ранее закона «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ.

В нем даются основные определения таким понятиям, как «информация», «доступ к информации», «конфиденциальность информации» и другим.

Также закон устанавливает следующие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

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[18].

Как указано в законе, государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации.

Отметим, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации[19].

Закон на ведущее место ставит сохранение конфиденциальности информации.

В соответствии со ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» на обладателя

[17] *Федеральный закон «О безопасности». Разд. 1. Ст. 1, 4, 5; Разд. 2. Ст. 10.*

[18] *Федеральный закон «Об информации, информационных технологиях и о защите информации». Ст. 3.*

[19] *Там же. Ст. 16.*

информации, оператора информационной системы в случаях, установленных законодательством РФ, возлагается обязанность 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[20].

Положительным явлением можно признать то, что новый закон подтвердил следующее: профессиональная тайна, то есть информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации (п. 5 ст. 9)[21]. Тем самым, с учетом положения ст. 41 закона о СМИ, возникает еще одно основание считать видом такой тайны профессиональную тайну журналиста.

Новый закон, как и прежний, продекларировал, что нарушение его требований влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации. Учитывая продолжающуюся закрытость от граждан государственных ресурсов и тотальную открытость сведений о гражданах на «черном рынке» информации, возникают сомнения в эффективности и «новых старых» норм. Одна из причин таких сомнений – отказ законодателя от принятой повсеместно в Европе и мире практики учреждения специального органа по контролю над соблюдением информационного законодательства, своего рода информационного омбудсмена с широкими полномочиями.

К сожалению, в ст. 9 («Ограничения доступа к информации») закон ушел и от введения принципа, принятого в цивилизованных странах мира: ограничения должны быть четко установлены законом, быть необходимыми в демократическом обществе и пропорциональными целям защиты. Другими словами, ограничения права на доступ к информации должны быть оспоримыми, они могут быть признаны в установленном порядке недействующими в случае преобладания общественного интереса в разглашении информации.

Проведем некоторый обзор наиболее значимых нормативных правовых актов законодательства Российской Федерации, в содержании которых затронуты вопросы о сведениях, входящих в Перечень конфиденциальной информации.

1. Перечень персональных данных раскрыт в таких нормативных правовых актах, как Трудовой кодекс Российской Федерации от 30.12.2001 (гл. 14, ст. 85–90), закон Российской Федерации от 27.12.91 № 2124-1 «О средствах массовой информации», Федеральный закон от 15.11.97 № 143-ФЗ «Об актах гражданского состояния» (ст. 12), Налоговый кодекс Российской Федерации (ст. 84).

26 января 2007 года в России вступил в действие новый Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных». Закон принят, главным образом, для борьбы с утечками баз данных.

Ранее определение персональных данных было изложено в Указе Президента Российской Федерации «О Перечне сведений конфиденциального характера» от 06.03.97 № 188. В частности, там сказано, что персональные данные – это сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность. Под этим самым понималось, что персональные данные – это та же конфиденциальная документированная информация, как и коммерческая информация, служебная, доступ к которой ограничен федеральными законами и которая должна быть также зафиксирована на материальном носителе, снабженном реквизитами. Конституция Российской Федерации также оговаривает в ст. 23, что человек имеет право на личную тайну.

С принятием нового документа создается целостная система регулирования персональных данных: если раньше защищались сами базы данных, то теперь законом охраняется и их содержимое.

Само понятие персональных данных определено в новом законе шире, чем ранее: под ними понимается «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу[22]». К числу персональных данных, наряду с фамилией, именем, отчеством, датой и местом рождения, относятся также семейное, социальное, имущественное положение, образование, профессия, доходы, национальность, наличие судимости и другая информация.

Исходя из разъяснений Правового Управления Аппарата Государственной Думы Российской Федерации, под термином «другая информация» следует понимать, например, информацию о фактах, событиях и обстоятельствах жизни физического лица, его политических, религиозных и иных взглядах и убеждениях, любую информацию медицинского характера и т. д. При этом персональными данными является любая отдельная информация (любой набор данных) о физическом лице,

[20] *Федеральный закон «Об информации, информационных технологиях и о защите информации». Ст. 16.*

[21] *Там же. Ст. 9.*

[22] *Федеральный закон «О персональных данных». Ст. 3.*

если она соответствует критериям, указанным в определении понятия «персональные данные»: она относится к определенному физическому лицу (независимо от характера и состава информации); она позволяет определить физическое лицо.

Согласно новому Закону, обработка персональных данных (в том числе сбор, систематизация, хранение, передача) может осуществляться только с согласия субъекта персональных данных. При этом в установленных законом случаях требуется письменное согласие на обработку, которое должно содержать, в частности, перечень персональных данных, на обработку которых дается согласие, сведения о лице, которому разрешается такая обработка, перечень действий, которые разрешается совершать с персональными данными, а также срок, в течение которого действует согласие. Исключением требования согласия лица могут стать случаи, когда обработка этих данных необходима для защиты его жизни и здоровья. Кроме того, разрешается обрабатывать персональные данные на основании закона, предусматривающего такую обработку, например правоохранительными органами.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев обезличивания персональных данных, а также в отношении общедоступных персональных данных.

Также закон определяет, что государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных.

Статья 19 закона «О персональных данных» определяет меры по обеспечению безопасности персональных данных при их обработке:

- при обработке персональных данных оператор обязан использовать необходимые организационные и технические меры, в том числе применять шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;
- Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных;
- контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных;
- использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения[23].

Кроме этого, Постановлением Правительства Российской Федерации от 17.11.2007 № 781 утверждено Положение об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных. Положение устанавливает требования к обеспечению безопасности передачи данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Под техническими средствами, позволяющими обрабатывать персональные данные, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации, принимаемые в информационных системах[24].

2. Сведения, составляющие тайну следствия и судопроизводства, отражены в ст. 12 Федерального закона от 12.08.95 № 144-ФЗ «Об оперативно-розыскной деятельности», а также в ст. 298 и 341 Уголовно-процессуального кодекса Российской Федерации от 18.12.2001.

3. Служебные сведения (служебная тайна) представлены в п. 1.2 «Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденном Постановлением Правительства Российской Федерации от 03.11.94 № 1233 и Указе Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера».

4. Сведения, связанные с профессиональной деятельностью, базируются в таких нормативно-правовых актах, как «Основы законодательства Российской Федерации об ох-

[23] *Федеральный закон «О персональных данных». Ст. 19.*

[24] *Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных», п. 2.*

ране здоровья граждан» от 22.06.93 № 5487-1 (ст. 61 – врачебная тайна), «Основы законодательства РФ о нотариате» от 11.02.93 № 4462-1 (ст. 5 и 16 – нотариальная тайна), Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (ст. 8 – адвокатская тайна), Федеральный закон от 17.07.99 № 176-ФЗ «О почтовой связи» (ст. 15 – тайна связи), Федеральный закон от 02.12.90 № 395-1 «О банках и банковской деятельности» (ст. 26 – банковская тайна).

Вопросы, связанные с защитой информации, относящейся к профессиональной тайне, предоставлением такой информации третьим лицам, а также сроками исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, изложены в пп. 5–7 ст. 9 Федерального закона «Об информации, информационных технологиях и о защите информации».

5. Сведения, связанные с коммерческой деятельностью, представлены Федеральным законом «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

6. Сведения об авторских правах, сущности изобретения или промышленного образца (права на результаты интеллектуальной деятельности и средства индивидуализации) имеют место в части четвертой Гражданского кодекса от 18.12.2006 № 230-ФЗ (с изменениями и дополнениями от 01.12.2007 № 318-ФЗ).

На основании краткого обзора нормативно-правовых актов законодательства Российской Федерации, в содержании которых затронуты сведения, относящиеся к конфиденциальной информации, можно констатировать, что выполнение в полном объеме данной нормативно-правовой базы обеспечивает безопасность информации.

Важный закон «Об электронной цифровой подписи» за № 1-ФЗ был подписан Президентом Российской Федерации 10.01.2002. Напомним, что в п. 3 ст. 11 Федерального закона «Об информации, информационных технологиях и о защите информации» также содержатся нормы по отнесению документов, подписанных электронной цифровой подписью, к электронным документам, равнозначным документам, подписанным собственноручной подписью. Роль закона «Об электронной цифровой подписи» поясняется в первой его статье.

1. Целью настоящего Федерального закона является обеспечение правовых условий использования ЭЦП 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[25].

Согласно закону, ЭЦП 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 ЭЦП в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон также определяет сведения, которые должен содержать сертификат ключа подписи.

Законодательной базой лицензионной деятельности в области защиты информации являются:

- закон Российской Федерации от 21.07.93 № 5485-1 «О государственной тайне»;
- Федеральный закон от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности»;
- Постановление Правительства РФ от 15.04.95 № 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»;
- Постановление Правительства РФ от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства РФ от 27.05.2002 № 346 «Об утверждении положений о лицензировании деятельности в области авиационной техники»;
- Постановление Правительства РФ от 21.06.2002 № 455 «Об утверждении Положения о лицензировании производства оружия и основных частей огнестрельного оружия»;
- Постановление Правительства РФ от 21.06.2002 № 456 «О лицензировании деятельности в области вооружения и военной техники»;
- Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства РФ от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

Продолжим рассмотрение нормативно-правовой базы обеспечения информационной безопасности законом «О лицензировании отдельных видов деятельности» № 128-ФЗ (в редакции от 06.12.2007 № 334-ФЗ).

Основными лицензирующими органами в области защиты информации являются Федеральная служба безопасности Российской Федерации и Федеральная служба по техническому и экспортному контролю. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Все эти вопросы регламентированы со-

[25] *Федеральный закон «Об электронной цифровой подписи». Ст. 1.*

ответствующими указами Президента и постановлениями Правительства Российской Федерации, в частности, в ст. 2 Постановления Правительства «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 оказанием услуг по защите государственной тайны» от 15.04.95 № 333 (в редакции от 06.01.2007 № 50). В данном постановлении утверждены нормы, в которых установлены:

- условия и порядок предоставления соответствующих документов для получения лицензии (ст. 5);
- сроки, по которым уполномоченный орган принимает решение о выдаче или об отказе в выдаче лицензии (ст. 6);
- на основании чего и при соблюдении каких требований выдаются лицензии (ст. 7);
- основания отказа в выдачи лицензии (ст. 9) и приостановление или аннулирование действия лицензии (ст. 12);

а также указываются:

- органы, осуществляющие специальные экспертизы и порядок их проведения (ст. 10);
- порядок организации и проведения государственной аттестации (ст. 11)[26].

Постановление преследует цель: защита сведений, составляющих государственную тайну, осуществление контроля компетентными органами методом лицензирования.

Постановлением Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности» утверждены перечни федеральных органов исполнительной власти, осуществляющих лицензирование, перечни видов деятельности, лицензирование которых осуществляется органами исполнительной власти субъектов Российской Федерации, перечни федеральных органов исполнительной власти, разрабатывающих проекты положений о лицензировании этих видов деятельности.

Ранее требования и условия осуществления лицензируемой деятельности по технической защите конфиденциальной информации были изложены в «Положении о лицензировании деятельности по технической защите конфиденциальной информации», утвержденном Постановлением Правительства Российской Федерации от 30.04.2002 № 290. Данное Положение утратило силу с опубликованием Постановления Правительства Российской Федерации от 15.08.2006 № 504, утвердившего новое «Положение о лицензировании деятельности по технической защите конфиденциальной информации».

Положение определяет порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

Положение берет за основу техническую защиту конфиденциальной информации как «комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней»[27].

Положением определены лицензионные требования и условия при осуществлении деятельности по технической защите конфиденциальной информации, которыми являются:

а) наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;

б) наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;

в) наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

г) использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

д) использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

е) наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю[28].

Также установлены права органа по лицензированию, сроки о выдаче или об отказе в выдаче лицензии, ее действия. Определен порядок ведения реестра лицензий лицензирующим органом, а также контроль за

[26] *Постановление Правительства Российской Федерации «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 оказанием услуг по защите государственной тайны». Ст. 5–7, 9–12.*

[27] *«Положение о лицензировании деятельности по технической защите конфиденциальной информации». П. 2.*

[28] *Там же. П. 4.*

лицензиатом в виде плановых и внеплановых проверок за выполнением требований и условий и их сроки.

Постановлением Правительства Российской Федерации от 31.07.2006 № 532 утверждено «Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

Данное Положение определяет порядок лицензирования деятельности по разработке и (или) производству средств защиты конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

В нем также устанавливается, что лицензирование деятельности по разработке и (или) производству средств защиты конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю, а в части разработки и (или) производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента РФ, Совета Безопасности РФ, Федерального Собрания РФ, Правительства РФ, Конституционного суда РФ, Верховного Суда РФ и Высшего Арбитражного Суда РФ, – Федеральная служба безопасности Российской Федерации[29].

Важную роль со дня принятия 04.07.96 сыграл закон № 85-ФЗ «Об участии в международном информационном обмене», которым было установлено, что основным защитным средством являются лицензии и сертификаты[30].

Статья 9: «Защита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена».

Статья 17: «Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

При ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора.

Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации»[31].

Вышеуказанные статьи закона придерживались такого общепризнанного принципа, как законность, то есть четкого следования нормам, по которым осуществляется контроль за лицензированием конкретных видов деятельности в области защиты информации.

Со времени вступления в силу Федерального закона «Об информации, информационных технологиях и о защите информации» Федеральный закон «Об участии в международном информационном обмене» утратил силу.

Правовой базой деятельности Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 являются:

- закон РФ «О государственной тайне», федеральные законы «О техническом регулировании», «Об информации, информационных технологиях и о защите информации»;
- Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
- Постановление Правительства РФ от 26.06.95 № 608 «О сертификации средств защиты информации»;
- Правила по проведению сертификации в Российской Федерации, утвержденные постановлением Госстандарта России от 10.05.2000 № 26 и Порядок проведения сертификации продукции в РФ, утвержденный постановлением Госстандарта России от 21.09.94 № 15, «Положение о сертификации средств защиты информации по требованиям безопасности информации», введенное в действие приказом председателя Гостехкомиссии России от 27.10.95 № 199.

Постановление Правительства Российской Федерации № 608 (в редакции от 17.12.2004. № 808) «О сертификации средств защиты информации» демонстрирует и устанавливает в интересующей нас области информационной безопасности порядок сертификации средств защиты информации в РФ и за рубежом. Настоящее постановление основывается на Федеральных законах «О государственной тайне» от 21.06.93 № 5485-1 и «О сертификации продукции и услуг» от 10.06.93 № 5151-1. Под средствами защиты информации понимаются технические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, а также средства их реализации и контроля эффективности защиты информации[32]. Указанные средства подлежат обязательной сертификации в рамках систем сертификации средств защиты информации.

Сертификация осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством РФ и федеральными органами по сертификации (ФСТЭК России, ФСБ России). Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны. Постановление представляет участников сертификации средств защиты информации и определяет их сферу деятельности.

Заслуживает внимание схема проведения сертификации средств за-

[29] *«Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации». Ст. 2.*

[30] *Федеральный закон «Об участии в международном информационном обмене». Ст. 9.*

[31] *Там же. Ст. 17.*

[32] *Постановление Правительства Российской Федерации «О сертификации средств защиты информации». Ч. 1.*

щиты информации: «Для единичных образцов средств защиты информации – проведение испытаний этих образцов на соответствие требованиям по защите информации; для серийного производства средств защиты информации – проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль стабильности характеристик сертификационных средств защиты информации, определяющих выполнение этих требований»[33].

Указанное Постановление преследует цель утвердить и обеспечить участниками сертификации средств защиты информации порядок сертификации средств защиты информации и тем самым обеспечить защиту государственной тайны и других конфиденциальных сведений.

Следует упомянуть Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», в котором установлено, что «подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети Интернет, не допускается»[34].

Законодательство Российской Федерации в области информационной безопасности в настоящее время продолжает совершенствоваться. Принимаются новые нормативные правовые документы, вносятся изменения в уже действующие.

Немаловажное значение имеют положения Концепции региональной информатизации до 2010 года. Данная Концепция одобрена 17 июля 2006 года Распоряжением Правительства Российской Федерации № 1024 и направлена на реализацию государственной политики в сфере региональной информатизации в соответствии с задачами модернизации государственного управления и социально-экономического развития регионов РФ.

В целях эффективной координации деятельности по реализации программ и проектов региональной информатизации создается совет региональной информатизации при федеральном органе исполнительной власти, обеспечивающем нормативное правовое регулирование в сфере информационных технологий[35].

Концепция региональной информатизации до 2010 года определяет основные принципы функциональных подсистем и элементов инфраструктуры электронного правительства региона. К одной из таких подсистем отнесена подсистема обеспечения информационной безопасности электронного правительства региона.

В п. 5 Приложения к Концепции определено, что в целях обеспечения защиты электронного правительства региона должна быть сформирована единая политика обеспечения информационной безопасности и реализована соответствующая подсистема.

Политика обеспечения информационной безопасности должна устанавливать:

- общую модель угроз в сфере информационной безопасности электронного правительства региона;
- классификацию объектов электронного правительства региона по необходимому уровню обеспечения защиты информации и общие требования к ним;
- критерии отнесения объектов системы электронного правительства региона к системам, требующим защиты, и перечень необходимых мер по обеспечению их защиты;
- порядок согласования требований к отдельным подсистемам электронного правительства региона, а также аттестации объектов электронного правительства региона;
- порядок доступа к подсистемам электронного правительства региона.

Подсистема обеспечения информационной безопасности электронного правительства региона должна включать функции осуществления доступа к подсистемам, регистрации и учета действий пользователей при работе с системой, мониторинга нарушений в области информационной безопасности, обеспечения антивирусной защиты, а также обеспечения защиты информации при ее передаче и обработке с использованием сертифицированных средств[36].

Правовой базой деятельности системы подготовки, переподготовки и повышения квалификации специалистов в области технической защиты информации являются федеральные законы:

- «Об образовании» от 10.07.92 № 3266-1;
- «О высшем и послевузовском профессиональном образовании» от 22.08.96 № 125-ФЗ;
- Положение о лицензировании образовательной деятельности, утвержденное Постановлением Правительства Российской Федерации от 18.10.2000 № 796.

На этом можно завершить краткий обзор основных законов и других нормативных правовых актов Российской Федерации, относящихся к вопросам информационной безопасности.

Как уже отмечалось выше, важно (и, вероятно, трудно) на зако-

[33] *Постановление Правительства Российской Федерации «О сертификации средств защиты информации». Ч. 8.*

[34] *Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», подпункт «а» п. 1.*

[35] *«Концепция региональной информатизации до 2010 года». П. 3.*

[36] *Приложение к «Концепции региональной информатизации до 2010 года». П. 5.*

нодательном уровне создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет.

Необходимо отметить, что ограничительные меры в области информационной безопасности представлены в российском законодательстве существенно лучше, чем координирующие и направляющие. Глава 28 УК РФ достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.

Необходимо отметить, что значительное количество нормативных правовых актов Российской Федерации по вопросам информационной безопасности РФ, других документов в области технической защиты информации является общедоступным ресурсом. Такие документы опубликованы в открытой печати, размещены на сайтах государственных учреждений. В информационно-справочной системе, размещенной на сайте ФСТЭК России (www.fstec.ru), кроме правовых и организационно-распорядительных документов широко представлены также и специальные нормативные документы ФСТЭК России по технической защите информации.

Следует напомнить, что под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (из Доктрины информационной безопасности).

Цель защиты информации *состоит в создании условий, способствующих реализации политики Российской Федерации в сфере обеспечения национальной безопасности, содействии устойчивому социально-экономическому развитию области, региона и государства в целом путем предотвращения или существенного снижения ущерба национальной безопасности с использованием методов и средств защиты информации.*

В заключение можно наметить основные направления, по которым должна двигаться законотворческая деятельность в сфере информационной безопасности:

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

Новости компаний

Aladdin усиливает состав директоров московского офиса компании

В целях повышения эффективности управления компания Aladdin реформирует и расширяет состав топ-менеджеров.

Aladdin объявляет о проведении внутренней реструктуризации, вызванной принятием новой стратегии компании, призванной укрепить позиции на профильных для компании сегментах рынка ИБ путем повышения клиентоориентированности бизнеса.

Для реализации новой стратегии проведена реорганизация, которая преследовала цель сделать структуру более удобной для взаимодействия с партнерами и заказчиками, а также повысить уровень эффективности и управляемости компании.

Изменения в штате затронули, прежде всего, директорский состав: заместителем генерального директора компании назначен Алексей Сабанов, ранее занимавший должность коммерческого директора Aladdin, позицию директора по персоналу Aladdin заняла Анна Баратова, до прихода в компанию Aladdin работавшая на посту директора по персоналу в компании HeadHunter, директором по маркетингу стала Шахноза Салманова, более 7 лет занимавшая должность заместителя директора соответствующего подразделения в «Информзащите», исполнительным директором компании теперь является Константин Розанцев. До прихода в Aladdin Константин занимался решением аналогичных задач в компаниях «Комбеллга», «Протек» и крупных российских информационных холдингах.

Сертифицирована система управления средствами аутентификации eToken TMS

Сертификат ФСТЭК на eToken TMS (Token Management System) обеспечивает возможность создания сертифицированной системы управления средствами аутентификации, полностью соответствующей требованиям отраслевых стандартов и законодательства РФ.

Компания Aladdin официально объявляет о завершении сертификации уникальной системы управления аппаратными средствами аутентификации пользователей в масштабах предприятия eToken TMS ФСТЭК России.

На практике получение сертификата ФСТЭК Российской Федерации означает, что комплексная система eToken TMS, предназначенная для внедрения, учета, управления и аудита использования аппаратных средств аутентификации пользователей (USB-ключей и смарт-карт eToken) в масштабах предприятия, может применяться в информационных системах органов государственной власти. Кроме того, решение Aladdin могут использовать предприятия, планирующие внедрение технологий защиты информации на базе инфраструктуры открытых ключей (PKI) с использованием цифровых сертификатов, а также организации, политика информационной безопасности которых требует применения исключительно сертифицированных продуктов и решений.