



**КОММЕНТАРИЙ
К ФЕДЕРАЛЬНОМУ
ЗАКОНУ
ОБ ИНФОРМАЦИИ,
ИНФОРМАТИЗАЦИИ
И ЗАЩИТЕ
ИНФОРМАЦИИ**

О. А. Городов

 **ПИТЕР®**



**КОММЕНТАРИЙ
К ФЕДЕРАЛЬНОМУ
ЗАКОНУ
ОБ ИНФОРМАЦИИ,
ИНФОРМАТИЗАЦИИ
И ЗАЩИТЕ
ИНФОРМАЦИИ**

О. А. Городов



Москва • Санкт-Петербург • Нижний Новгород • Воронеж
Ростов-на-Дону • Екатеринбург • Самара
Киев • Харьков • Минск

2003

ББК 67.623.3-32
УДК 347.78(094.5)
Г70

Городов О. А.

Г70 Комментарий к ФЗ «Об информации, информатизации и защите информации». — СПб.: Питер, 2003. — 272 с: — (Серия «Закон и комментарии»).

ISBN5-94723-539-0

Федеральный закон «Об информации, информатизации и защите информации» является первым в российской истории законодательным актом, посвященным комплексному регулированию отношений, складывающихся по поводу информации, информационных ресурсов, информационных технологий и средств их обеспечения.

Автор комментария ставил перед собой цель не только прокомментировать нормы Закона, но и дать посильные ответы на вопросы, с которыми сталкиваются научные и практические работники, а также граждане, соприкасающиеся с проблемами информационно-правового характера.

ББК 67.623.3-32
УДК 347.78(094.5)

ISBN5-94723-539-0

© ЗАО Издательский дом «Питер», 2003

ОГЛАВЛЕНИЕ

Принятые сокращения.....	6
Введение.....	7

Глава 1 Общие положения

Статья 1. Сфера действия настоящего Федерального закона	15
Статья 2. Термины, используемые в настоящем Федеральном законе, их определения.....	20
Статья 3. Обязанности государства в сфере формирования информационных ресурсов и информатизации.	34

Глава 2 Информационные ресурсы

Статья 4. Основы правового режима информационных ресурсов.....	48
Статья 5. Документирование информации.....	52
Статья 6. Информационные ресурсы как элемент состава имущества и объект права собственности.....	59
Статья 7. Государственные информационные ресурсы.	75
Статья 8. Обязательное представление документированной информации для формирования государственных информационных ресурсов.....	79
Статья 9. Отнесение информационных ресурсов к общероссийскому национальному достоянию.	94
Статья 10. Информационные ресурсы по категориям доступа.....	96

Статья 11. Информация о гражданах (персональные данные).....	117
--	-----

Глава 3

Пользование информационными ресурсами

Статья 12. Реализация права на доступ к информации из информационных ресурсов.....	125
Статья 13. Гарантии предоставления информации.....	131
Статья 14. Доступ граждан и организаций к информации о них.....	136
Статья 15. Обязанности и ответственность владельца информационных ресурсов.....	139

Глава 4

Информатизация. Информационные системы, технологии и средства их обеспечения

Статья 16. Разработка и производство информационных систем, технологий и средств их обеспечения. . . .	144
Статья 17. Право собственности на информационные системы, технологии и средства их обеспечения.....	150
Статья 18. Право авторства и право собственности на информационные системы, технологии и средства их обеспечения.....	155
Статья 19. Сертификация информационных систем, технологий, средств их обеспечения.....	156

Глава 5

Защита информации и прав субъектов в области информационных процессов и информатизации

Статья 20. Цели защиты.....	166
Статья 21. Защита информации.....	169
Статья 22. Права и обязанности субъектов в области защиты информации.....	175

Статья 23. Защита прав субъектов в сфере информационных процессов информатизации.....	177
Статья 24. Защита права на доступ к информации.....	182
Статья 25. Вступление в силу настоящего Федерального закона.....	184
Приложения.....	186

ПРИНЯТЫЕ СОКРАЩЕНИЯ

АПК РФ — Арбитражный процессуальный кодекс Российской Федерации.

БНА — Бюллетень нормативных актов министерств и ведомств РФ, Бюллетень нормативных актов федеральных органов исполнительной власти.

Ведомости РФ — Ведомости Верховного Совета РСФСР, Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.

Вестник ВАС — Вестник Высшего Арбитражного Суда Российской Федерации.

ГК РФ — Гражданский кодекс Российской Федерации.

ГПК РФ — Гражданский процессуальный кодекс Российской Федерации.

КоАП — Кодекс Российской Федерации об административных правонарушениях.

САПП РФ — Собрание актов Президента и Правительства Российской Федерации.

СЗ РФ — Собрание законодательства Российской Федерации.

УК РФ — Уголовный кодекс Российской Федерации.

ВВЕДЕНИЕ

Федеральный закон «Об информации, информатизации и защите информации» (далее— Закон) является первым в российской истории законодательным актом, посвященным комплексному регулированию отношений, складывающихся по поводу информации, информационных ресурсов, информационных технологий и средств их обеспечения. Значение подобного акта трудно переоценить, поскольку информация и информационные технологии все в большей степени определяют ландшафт современного постиндустриального общества, формируют его материальную основу и становятся центральным звеном всей системы общественных отношений. Это звено и образует так называемую информационную сферу, которая все в большей мере становится предметом целенаправленной деятельности законодателя.

Подлежащие правовому опосредованию нормами Закона общественные отношения дифференцированы по трем основным областям.

Первую область составляют отношения, складывающиеся при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и представления потребителю документированной информации. Данная область общественных отношений объемлет два ключевых направления регулирования, которые связаны, во-первых, с формированием и, во-вторых, с использованием информационных ресурсов.

Вторую область образуют отношения, возникающие при создании и использовании информационных технологий и средств их обеспечения.

Третья область включает группу отношений, возникающих при защите информации и защите прав субъектов, участвующих в информационных процессах и информатизации.

Общественная практика последних лет убедительно показала необходимость правового регулирования избранных законодателем направлений.

Закон состоит из 25 статей, сгруппированных в 5 главах.

Первая глава «Общие положения» определяет сферу действия Закона, раскрывает содержание используемых терминов, устанавливает обязанности государства в сфере формирования информационных ресурсов и информатизации.

Вторая глава, именуемая «Информационные ресурсы», посвящена, в частности, установлению правового режима информационных ресурсов, их формированию, порядку предоставления документированной информации для формирования государственных информационных ресурсов, дифференциации информационных ресурсов по категориям доступа.

В главе третьей «Пользование информационными ресурсами» содержатся нормы, регулирующие отношения, связанные с реализацией права на доступ к информации из информационных ресурсов, с гарантиями предоставления информации, с обязанностями и ответственностью владельца информационных ресурсов.

Глава четвертая «Информатизация, информационные системы, технологии и средства их обеспечения» основное внимание уделяет вопросам правового опосредования разработки и производства информационных систем, технологий и средств их обеспечения. В ней делается попытка сочетания права собственности на информационные системы, технологии и средства их обеспечения с правом авторства.

Заключительная, 5-я, глава «Защита информации и прав субъектов в области информационных процессов и информатизации» устанавливает перечень целей защиты, определяет круг объектов, подлежащих защите, а также закрепляет права и формулирует обязанности собственников и владельцев документов в области защиты информации.

Давая общую характеристику Закону, следует отметить его комплексный характер, поскольку он содержит нормы различ-

ной отраслевой принадлежности. Например, ст. 6 «Информационные ресурсы как элемент состава имущества и объект права собственности», а также ст. 17 «Право собственности на информационные системы, технологии и средства их обеспечения», имеют гражданско-правовой характер, а ст. 8 «Обязательное предоставление документированной информации для формирования государственных информационных ресурсов» — административный характер.

Закон призван играть роль базового нормативно-правового акта в информационной сфере и вследствие этого содержит весьма незначительное количество норм прямого действия. Он призван также сыграть роль рамочного и системообразующего правового акта, основополагающие предписания которого должны получить развитие и конкретизацию в иных федеральных законах и подзаконных нормативных актах. Так, согласно п. 2 ст. 9 Закона, отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому национальному достоянию и определение их правового режима устанавливаются федеральным законом. В соответствии с п. 1 ст. 11 перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов РФ, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Согласно абз. 2 п. 1 ст. 8 перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство РФ.

К важнейшим положениям Закона относятся нормы, закрепляющие режим информационных ресурсов, устанавливающие категории доступа к документированной информации, провозглашающие гарантии предоставления информации и за-

кладывающие основы правового регулирования процесса информатизации.

Несмотря на то что Закон не только формирует основы новой комплексной отрасли права, но и придает известное ускорение процессу нормотворчества в информационной сфере, он далеко не безупречен в концептуальном и юридико-техническом аспектах.

Следует признать, что перед законодателем и, главным образом, перед разработчиками законопроекта стояли весьма нетривиальные задачи. Их удалось разрешить лишь отчасти.

Понятно, что неписаной целью Закона было сведение к минимуму отрицательных последствий ухода информации из под контроля государства. Причиной такого ухода явились рыночные преобразования, которые дали жизнь негосударственным информационным системам. Через эти системы на граждан и общество может оказываться нежелательное влияние, а государство фактически лишается возможности контроля, оценки, переработки и распределения информационных потоков, а равно монопольного коммерческого использования государственных информационных ресурсов. Негативные последствия утраты указанных возможностей побуждают государство, защищая свободу информации и сферу своих коммерческих информационных интересов, одновременно накладывать на распространение информации, ее переработку и распределение известные ограничения. В отношении свободы массовой информации указанные ограничения частично налагаются Законом РФ «О средствах массовой информации». Регламентация товарно-денежных отношений, складывающихся по поводу информации, должна быть осуществлена прежде всего ГК РФ. Однако последний лишь констатировал в ст. 128 существование вида объектов гражданских прав, именуемого информацией, а в ст. 139 сформулировал общее дозволение на сохранение информации в режиме служебной и коммерческой тайны. Да и иные федеральные законы, введенные в действие как до, так и после принятия комментируемого

Закона и содержащие нормы, относящиеся к информационной сфере, не универсальны и не исчерпывают возможных форм регулирования отношений, возникающих в обществе по поводу информации. Не универсален в этом отношении и комментируемый Закон, поскольку информация как феномен одного порядка с категориями материи и энергии является для правовой науки не то чтобы загадкой, но объектом, в отношении которого не выработаны универсальные юридические инструменты, способные выполнить регулятивную и охранительную функции. Поэтому законодатель уже в самом названии Закона выдал желаемое за действительное в части вынесения термина «информация» в его заглавие. Закон следовало бы ввести в действие под наименованием «О документированной информации, информатизации и защите документированной информации».

Не вполне удачным концептуальным решением законодателя является юридическая модель информационных ресурсов как объекта права собственности. Институт вещного права собственности должен иметь, и имеет, как и любой иной гражданско-правовой институт, свои границы применимости и эффективен при юридическом закреплении отношений, складывающихся только по поводу материальных носителей информации, да и то далеко не всех. В последнем случае мы имеем в виду физические поля, которые могут выступать носителями информации (что, например, констатируется в ст. 2 Закона РФ «О государственной тайне»), но не могут быть объектами хозяйственного господства в традиционном его понимании и цивилистической интерпретации.

Благодаря решению законодателя легализована «проприетарная» концепция информации, которая не способна, к сожалению, придать последней значение самостоятельного объекта правоотношений иначе как вкупе с материальным носителем сведений. К слову сказать, возможность иметь в собственности материальный носитель как движимую вещь, в том числе с зафиксированными на нем сведениями, и до принятия комменти-

руемого Закона никто не подвергал сомнению. Фиксация сведений на конкретном материальном носителе ничего не меняет в режиме принадлежности самой информации, ибо одни и те же по содержанию сведения могут циркулировать по разным носителям, оставаясь инвариантными им. При этом материальные носители могут на законных основаниях принадлежать различным собственникам. Поэтому правомерное обладание материальным носителем не является достаточным условием правомерного обладания закрепленной на данном носителе информации, как бы того ни желал законодатель. Собственник оригинала документа не может автоматически считаться собственником всех возможных его копий. Следовательно, вещные права не способны выступать тем юридическим институтом, который обеспечивает надлежащую правовую охрану и режим использования сведений как содержательной стороны информации (формальная сторона информации при определенных условиях охраняется нормами авторского права), поскольку содержанием нельзя ни владеть, ни пользоваться, ни распоряжаться. Меры, принимаемые самим обладателем информации для ее защиты (фактическая монополия), не только эффективнее мер по наделению его титулом собственника, но и служат наиболее подходящим из двух возможных способов обеспечения охраны содержательной стороны информации. Второй способ реализуется, при определенных опять же условиях, через институт исключительных прав.

Неадекватной сущности регулируемых отношений следует признать и позицию законодателя в отношении правового режима информационных технологий, которые по смыслу комментируемого Закона являются объектами права собственности (ст. 17).

По прошествии более чем 7 лет с момента принятия Закона мы можем сказать, что отмеченные выше концептуальные решения законодателя, а также иные, вытекающие из них, некоррентные с гражданским законодательством предписания составляют своего рода смысловую ось дискуссии, которая не

могла не возникнуть в среде юристов. Это вполне естественно, поскольку категория информации, и, в частности, документированная ее разновидность, стала объективным фактом, существующим в юридической науке. И как бы эту категорию ни оценивать, не считаться с ней нельзя. Даже если относиться скептически к конструктивным возможностям «проприетарного» подхода к информации, легализация сферы ее приложения при помощи традиционных институтов и средств правового опосредования, несомненно, принесла свои результаты.

Поэтому, давая критическую оценку тем либо иным решениям, получившим отражение в Законе, а равно отдельным его нормам, мы не подвергаем сомнению его позитивную роль в целом.

Принимая во внимание планы законотворческих работ Государственной Думы, в рамках которых предполагается внесение изменений и дополнений в комментируемый Закон, автор предлагает читателю в качестве приложения проект Федерального закона «О внесении изменений и дополнений в статьи 2, 11, 16 ФЗ "Об информации, информатизации и защите информации"», который находится на момент подготовки рукописи комментария на рассмотрении в Государственной Думе. Кроме того, в качестве приложений к комментарию предлагаются Доктрина информационной безопасности Российской Федерации и Федеральная целевая программа «Электронная Россия (2002—2010 гг.)».

Автор комментария ставил перед собой цель не только прокомментировать нормы Закона, но и дать сильные ответы на вопросы, с которыми сталкиваются научные и практические работники, а также граждане, соприкасающиеся с проблемами информационно-правового характера. Это тем более необходимо сделать, поскольку с момента появления первого комментария к Закону, подготовленного авторским коллективом под руководством видных российских ученых И. Л. Бачило и В. А. Копылова, прошло значительное время и он стал библиографической редкостью.

Автор просит с пониманием отнестись к излагаемой точке зрения по ряду вопросов, которая, по-видимому, не всегда может совпадать с мнением читателя, и выражает надежду, что его работа вместе с уже имеющимися публикациями по информационно-правовой тематике расширит общее представление об информации, информатизации и защите информации.

Глава 1

ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие 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.

2. Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах».

1. Комментируемая статья включает в себя положения, устанавливающие сферу действия Федерального закона «Об информации, информатизации и защите информации». В указанную сферу, контуры которой предопределены характером регулируемых отношений, законодатель включил те из них, которые, по его мнению, нуждаются в правовом опосредовании в силу своей значимости для общества, государства и граждан.

Подлежащие правовому регулированию отношения дифференцированы по трем основным областям.

Первую область составляют отношения, складывающиеся при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения; поиска, распространения и представления потребителю документированной информации. Данная область общественных отношений включает в себя два ключевых

направления регулирования, которые связаны с формированием и использованием информационных ресурсов.

Формирование информационных ресурсов предполагает в конечном счете их некое организационное выражение и объективацию. Представленный в объективной форме информационный ресурс и будет выступать в качестве предмета, по поводу которого участники общественных отношений вступают во взаимодействие. Законодатель, в данном случае, пошел по пути придания информационным ресурсам объективированного выражения в форме документированной информации, помещенной в информационную систему. Подобного рода объективация юридически значима и преследует цель установления возможности регулирования отношений, возникающих в сфере формирования информационных ресурсов, да и в сфере их использования, с помощью известных и хорошо изученных правовых институтов, например института вещных прав.

Использование информационных ресурсов предполагает удовлетворение общественных потребностей, а равно потребностей государства и личности в информации.

Вторую область регулируемых комментируемым Законом общественных отношений образуют отношения, возникающие при создании и использовании информационных технологий и средств их обеспечения.

Действующее законодательство не содержит легального понятия информационной технологии. В доктрине под информационной технологией понимают совокупность технологий (использование научного знания для определения способов изготовления вещей в воспроизводимой манере) в микроэлектронике, создании вычислительной техники (машин и программного обеспечения), телекоммуникации, вещании и оптико-электронной промышленности, геной инженерии.¹

¹ Мануэль Кастельс. Информационная эпоха: экономика, общество и культура/Пер, с англ./Под ред. проф. О. И. Шкаратана. М., 2000. С. 50, 77.

Указание законодателя на регулирование отношений, возникающих при создании технологий, нельзя признать удачным. Любая технология создается как результат интеллектуальной деятельности человека, в ряде случаев как охраняемый результат. В этом смысле право не способно воздействовать на процесс создания технологий, поскольку интеллектуальная деятельность человека не подвержена правовой регламентации. Сфера использования информационных технологий и средств их обеспечения действительно требует правового опосредования и подвержена такому опосредованию. Оно может осуществляться по многим направлениям, в частности, в направлении координации деятельности органов публичной власти, ответственных за технологическое развитие, в направлении стандартизации, сертификации, в направлении государственного контроля и надзора, в направлении государственной поддержки наиболее значимых проектов в сфере информационных технологий.

Третья область регулируемых отношений включает группу отношений, возникающих при защите информации, защите прав субъектов, участвующих в информационных процессах и информатизации. В свою очередь область отношений по защите информации и защите прав на нее включает ряд направлений, в рамках которых могут быть решены правовые проблемы данной защиты. Это прежде всего защита информационных ресурсов от неправомерного их использования и неправомерного воздействия на них, защита прав, свобод и охраняемых законом интересов граждан, защита интересов общества, государства и личности от воздействия вредной информации, в том числе путем ограничения информационных прав и свобод.

2. Объектами отношений, урегулированных нормами комментируемого Закона, выступают информационные ресурсы, а также информационные технологии и средства их обеспечения. Предметом регулирования являются общественные отношения, складывающиеся по их поводу. Очевидно, что однород-

ность групп общественных отношений, образующих предметную область законодательного опосредования, относительна. Их объединяет лишь то, что в качестве объектов данных отношений выступают производные от информации продукты, а именно — информационные ресурсы и информационные технологии.

Общественные отношения, складывающиеся по поводу собственно информации, несмотря на название Закона, остаются за пределами предметной области регулирования.

Вполне естественно предположить, что предметная область комментируемого Закона будет со временем содержательно изменяться путем включения в нее новых групп общественных отношений, которые потребуют своего правового опосредования. На современном этапе развития информационного законодательства мы можем лишь с большой долей условности говорить о наличии в предметном поле регулирования отношений, возникающих по поводу информации, т. е. чисто информационных отношений. Законодатель предпочитает сегодня регулировать отношения, объектом которых выступают не информация, а производные от нее продукты и деятельность, связанная с ними.

3. Пункт 2 разграничивает сферу действия комментируемого Закона и Закона РФ «Об авторском праве и смежных правах»¹, которым регулируются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права). Очевидно, что комментируемый Закон, помимо отношений, урегулированных законодательством об авторском праве, не «затрагивает» также и отношений, которые регламентируются иными законами, действующими в сфере правовой охраны интеллекту-

¹ Ведомости РФ. 1993. № 32. Ст. 1242; СЗ РФ. 1995. № 30. Ст. 2866.

альной собственности. Вместе с тем, следует иметь в виду, что объекты авторского права и иные охраняемые результаты интеллектуальной деятельности, получившие объективацию в форме материальных носителей, могут быть включены в состав информационных ресурсов, но это обстоятельство не лишает их правовой охраны нормами законодательства об интеллектуальной собственности.

Что касается официальных документов (законов, судебных решений, иных текстов законодательного, административного и судебного характера, в том числе описаний и чертежей к правоустанавливающим документам на объекты промышленной собственности), их официальных переводов, произведений народного творчества, сообщений о событиях и фактах, имеющих информационный характер, то они не являются объектами авторского права, и отношения по их поводу не входят в сферу правового регулирования нормами законодательства об авторском праве. Вне указанной сферы находятся и отношения, складывающиеся в связи с программами теле- и радиопередач, публикуемыми в газетах и журналах, на что неоднократно указывал Высший Арбитражный Суд РФ. Так, в п. 1 Информационного письма Президиума Высшего Арбитражного Суда РФ от 28 сентября 1999 г. № 47 говорится о том, что программа является доводимой до зрителей (слушателей) информацией о времени выхода в эфир скомпонованных определенным образом теле- и радиопередач. Такая информация, опубликованная ранее в другой газете, становится общедоступной и, кроме того, излагается в обычной (неоригинальной) форме, не образует самостоятельного произведения.¹

Противоположную позицию в отношении программ теле- и радиопередач занимала ныне упраздненная Судебная палата

¹ См.: Вестник ВАС РФ. 1999 № 2. С. 76; 1998. № 6. С. 76.

по информационным спорам при Президенте РФ, которая в своих рекомендациях от 5 мая 1994 г. и от 2 июля 1995 г. высказывалась за охраняемость авторским правом программ теле- и радиопередач.¹

Статья 2. Термины, используемые в настоящем
Федеральном законе, их определения

В настоящем Федеральном законе используются следующие понятия:

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

информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

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;

¹ Информационные споры: как в них победить? Решения, рекомендации, экспертные заключения Судебной палаты по информационным спорам при Президенте РФ/Под ред. А. К. Симонова. М., 2002. С. 303, 311.

конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

средства обеспечения автоматизированных информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

1. Комментируемая статья, следуя англосаксонской законодательской практике, выделяет дефинитивную часть законодательного акта, в которой сосредоточены используемые в нем основные термины. Эти термины имеют значение только для целей комментируемого Закона. В других законодательных актах могут вводиться аналогичные термины, но несущие в себе иную смысловую нагрузку и иное содержание. Так, например, в ст. 1 Федерального закона «О библиотечном деле»¹ дается понятие документа как материального объекта с зафиксированной на нем информацией, а комментируемая

¹ СЗРФ. 1995. № 1. Ст. 2.

статья определяет документ как зафиксированную на материальном носителе информацию с реквизитами.

2. В основу всех информационных процессов, происходящих в общественной жизни, положен феномен информации. Само понятие информации, выступая в качестве центрального по ряду естественно-научных отраслей знания, продолжает тем не менее оставаться одним из наиболее спорных и противоречивых. Первые попытки уточнить понятие информации восходят к работам Р. Фишера 1921 г. (вероятностная концепция) и Р. Хартли 1928 г. (логарифмическая мера количества информации), которые предвосхитили появление классической статистической теории связи Н. Винера — К. Шеннона 1948 г. (количество информации как мера уменьшения неопределенности). Получили научное признание определения информации, данные выдающимися учеными, стоящими у истоков становления теории информации, как «связь, в процессе которой устраняется неопределенность» (К. Шеннон)¹, «разнообразии» (У. Эшби)², «оригинальность и мера сложности» (А. Моль)³, «знание» (Ф. Махлуп)⁴, «обозначение содержания, полученного из внешнего мира, в процессе нашего приспособления к нему и приспособления к нему наших чувств» (Н. Винер)⁵, «данные, которые были организованы и переданы» (М. Кастельс)⁶. Однако выработать универсальное понятие информации, которое отражало бы все многообразные стороны данного феномена, до сих пор было не суждено.

Комментируемая статья определяет информацию через сведения. Из легального термина следует ряд признаков, ха-

¹ Шеннон К. Работы по теории информации и кибернетике. М., 1963. С. 243.

² Эшби У. Р. Введение в кибернетику. М., 1958. С. 18.

³ Моль А. Теория информации и эстетическое восприятие. М., 1966. С. 15.

⁴ Махлуп Ф. Производство и распространение знаний в США. М., 1966. С. 36-37.

⁵ Винер Н. Кибернетика и общество. М., 1968. С. 31.

⁶ Кастельс М. Информационная эпоха: экономика, общество и культура. М., 2000. С. 39 и др.

рактизирующих легальную форму информации, но, понимает-ся, не саму информацию.

Первым признаком следует назвать содержательность. Этот признак проявляется через отождествление информации со сведениями, которые выступают некими символами лиц, предметов, фактов, событий, явлений и процессов. Очевидно, что между сведениями и теми объектами, по поводу которых эти сведения возникли, нет взаимно однозначного соответствия. Данные сведения выступают лишь обозначением содержания, полученного из внешнего мира.

Вторым признаком будет являться независимость формы представления сведений. Этот признак проявляется через возможность существования сведений о чем-либо в любой воспринимаемой форме: устной, письменной, визуальной, акустической и т. п. Сведения, выраженные в знаках, обычно именуют данными.

В литературе приводится множество иных признаков и свойств информации, которые находятся за пределами ее легального определения¹.

Термин «информация» включен и в предметное поле цивилистики. Согласно ст. 128 ГК РФ информация отнесена к видам объектов гражданских прав².

Следует подчеркнуть, что термин «информация» по тексту комментируемого закона используется в качестве самостоятельного весьма редко, но с его помощью конструируется ряд родственных, смежных с ним терминов.

3. Термин «информатизация» раскрывается законодателем через понятие процесса, т. е. последовательной смены состояний определенной сферы общественной жизни. Этой сферой является сфера удовлетворения информационных

¹ См., например, Черняк Ю. Н. Информация и управление. М., 1974. С. 62—64; Бачило И. Л., Лопатин В. И., Федотов М. А. Информационное право: Учебник/Под ред. Б. Н. Топорнина. СПб. 2001. С. 143-145.

² См.: Городов О. А. Информация как объект гражданских прав//Правоведение, 2001. №5. С. 72-83.

потребностей граждан, государства и общества. Указанные потребности должны удовлетворяться посредством формирования и использования информационных ресурсов. Сам процесс должен выступать в качестве организационного и иметь социально-экономическую и научно-техническую направленность. Сегодня в нормативных и литературных источниках широко употребляются производные от термина «информатизация» понятия, например: информатизация образования, информатизация правотворческой деятельности, информатизация правоприменительной и правоохранительной деятельности, государственная политика информатизации и т. п.

Так, понятие «государственная политика информатизации правовой сферы» используется в Указе Президента РФ от 4 августа 1995 г. № 808 «О президентских программах правовой информатизации»¹.

В широком смысле информатизацию рассматривают иногда как один из факторов глобализации².

Процесс информатизации следует отличать от процесса компьютеризации. Компьютеризация предполагает совершенствование и внедрение технической базы, в том числе вычислительной техники, для целей накопления информации, ее переработки и представления в воспринимаемой человеком форме.

4. Термин «документированная информация (документ)» является ключевым для комментируемого закона и основополагающим в избранной законодателем модели регулирования отношений, складывающихся по поводу информации.

Данный термин представлен в качестве легального в ряде федеральных законов. Помимо комментируемого Закона, дефиниция документированной информации сформулирована в ст. 2 Федерального закона «Об участии в международном ин-

¹ Российская газета. 1995. 15 августа.

² Бачило И. Л. Информационное право: основы практической информатики. Учебное пособие. М., 2001. С. 192-197.

формационном обмене»¹, в ст. 1 Федерального закона «О библиотечном деле»² и в ст. 1 Федерального закона «Об обязательном экземпляре документов»³. И если в первом из названных законов термин «документированная информация (документ)» текстуально совпадает с термином, используемым в комментируемом Законе, то в двух других наблюдается существенное расхождение его содержательной стороны.

Так, согласно ст. 1 Федерального закона «О библиотечном деле», документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования. Близка по смыслу к цитируемому термину и дефиниция, содержащаяся в Федеральном законе «Об обязательном экземпляре документов». Здесь документ — это материальный носитель с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, предназначенный для передачи во времени и пространстве в целях общественного использования и хранения.

В отличие от термина «документированная информация (документ)», содержащегося в комментируемой статье, в приведенных понятиях законодатель сместил акцент с фиксации информации на материальном носителе, как необходимого признака документированной информации, на сам материальный носитель, который становится документом при условии фиксации на нем в установленном законодателем виде соответствующих сведений.

Генетически точнее термин комментируемого Закона, который, конечно же, не свободен от субъективных представлений законодателя, но в отличие от приведенных терминов лишен просчетов методологического характера, проистекающих вследствие отхода от базовых представлений о феномене ин-

¹ СЗ РФ 1995. № 8. Ст. 609; 1996. № 28. Ст. 3347.

² СЗ РФ. 1995. № 1. Ст. 2.

³ СЗ РФ. 1995. № 1. Ст. 1, Российская газета. 2002. 14 февраля.

формации. О чем, собственно, идет речь? Прежде всего, о том, что информация при смене носителей остается инвариантной своему носителю, а не наоборот. И, во-вторых, информация циркулирует между носителями, меняя их, но не материальные носители циркулируют между сведениями о лицах, предметах, фактах, событиях, явлениях и процессах. В игнорировании этих аксиом и видятся истоки «проприетаризации» информации, когда во главу угла ставится материальный носитель сведений, а не сами сведения.

Из легального термина «документированная информация (документ)», содержащегося в комментируемой статье, вытекают три основных признака документа.

Первый из них — наличие материального носителя информации. В качестве такового, в принципе, могут рассматриваться любые объекты материального мира, включая вещи и физические поля, в которых находят свое отображение определенные сведения. Одни и те же сведения могут быть зафиксированы на различных материальных носителях. Наибольшее распространение получили бумажные носители, документы, в которых информация представлена в электронно-цифровой форме (электронные документы), видео- и звукозаписи.

Вторым признаком документированной информации является идентифицируемость зафиксированных на носителе сведений. Это достигается путем присовокупления к содержательной стороне сведений данных, именуемых реквизитами, которые позволяют установить источник и назначение информации, время ее документирования, а в ряде случаев и обеспечить защиту того либо иного документа (электронная цифровая подпись). Реквизиты должны быть зафиксированы на том же материальном носителе, что и идентифицируемые сведения.

Третьим признаком документированной информации, который не нашел своего отражения в анализируемом термине, выступает возможность изменения форм ее закрепления. Данный признак проявляется в том, что информация, закреп-

ленная на материальном носителе одного вида, может быть одновременно представлена и на других видах носителей без угрозы утраты своего содержания и реквизитов. По существу, это возможность копирования информации.

5. Термин «информационные процессы» в содержательном плане фиксирует последовательность определенного вида действий. В качестве таких действий законодатель называет сбор, обработку, накопление, хранение, поиск, распространение информации. Эти действия взаимосвязаны, хотя каждое из них само по себе — тоже процесс. Так, процессу хранения информации должен предшествовать процесс ее сбора. Процессу сбора должен предшествовать процесс поиска и т. п.

Несколько иное звучание по сравнению с комментируемым Законом термин «информационные процессы» получил в Федеральном законе «Об участии в международном информационном обмене». Согласно ст. 2 названного Закона, информационные процессы — процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Еще одно значение информационным процессам придается в ГОСТ Р 50922-96. В соответствии с ним информационные процессы представляют собой процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации¹. Существуют и доктринальные определения информационных процессов. Так, О. А. Гаврилов полагает, что это процессы распространения информации в естественной, технической или социальной среде².

6. Термин «информационная система» представлен в комментируемой статье в качестве обозначения организационно упорядоченной совокупности (сочетания) двух элементов.

¹ ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

² Гаврилов О. А. Курс правовой информатики: Учебник для вузов. М., 2002. С. 21.

Первым из них являются документы или их массивы. Вторым — информационные технологии, в том числе с использованием средств вычислительной техники и связи. Информационные технологии должны обладать способностью реализовывать процессы сбора, обработки, накопления, хранения, поиска и распространения информации. Существует множество классификаций информационных систем, в которых они дифференцированы по различным основаниям¹.

По степени автоматизации различают ручные, автоматизированные и автоматические информационные системы.

По сфере применения информационные системы подразделяются на интегрированные, системы организационного управления, системы автоматизированных плановых расчетов. По характеру применения выделяются информационно-поисковые, информационно-решающие, управляющие, советующие системы.

К информационным системам относятся библиотеки, архивы, банки данных, фонды и т. п. хранилища документированной информации. Одной из наиболее известных и значимых информационных систем является Государственная автоматизированная система Российской Федерации «Выборы», отношения по поводу использования которой регулируются Федеральным законом «О Государственной автоматизированной системе Российской Федерации "Выборы"»². Данная информационная система предназначена для реализации информационных процессов при подготовке и проведении выборов и референдумов.

7. Термин «информационные ресурсы» генетически связан с терминами «документ» и «информационная система». В основу термина «информационные ресурсы» положена категория документированной информации. Указанное обстоятельство предопределяет правовой режим информационных ресурсов,

¹ Гаврилов О. А. Указ. соч. С. 78; Бачило И. Л. Информационное право: основы практической информатики. М., 2001. С. 140-152.

² Российская газета. 2003. 15 января.

который построен по модели режима документированной информации и базируется на использовании института вещных прав.

Понятие информационного ресурса уже понятия документированной информации, поскольку последняя для отнесения ее к разряду информационных ресурсов должна находиться в составе информационной системы.

Институт информационных ресурсов занимает особое место в системе информационного законодательства. Этим институтом опосредуется основная форма организационного выражения документированной информации, которая используется при ее сборе, обработке, хранении и потреблении. С другой стороны, и сами информационные ресурсы могут быть представлены различными организационно-упорядоченными формами. Это прежде всего библиотеки, архивы, фонды, депозитарии, банки и базы данных.

В литературе по информационному праву приводятся и иные разновидности информационных ресурсов. И. Л. Бачило, например, выделяет следующие их группы. Первая группа представлена различными массивами информации, которые создаются на основе деятельности различных органов государственной власти, на основе деятельности ведомств, ориентированных на определенные функции государственного управления. Вторую группу образуют ресурсы, ориентированные на решение общегосударственных задач. Третья группа включает информационные ресурсы массовой информации¹ (см. комментарий к ст. 6).

8. Термином «информация о гражданах (персональные данные)» обозначаются сведения, касающиеся биографических данных лица, сведения об имущественном, образовательном, семейном положении, сведения о состоянии здоровья, о месте жительства гражданина, о судимости и т. п.

¹ Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право: Учебник. СПб., 2001. С. 190-196.

Категория персональных данных представлена и в иных законодательных актах РФ. Так, согласно ст. 85 Трудового кодекса РФ, персональные данные работника— информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. В соответствии с Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 6 марта 1997 г. № 188\ под персональными данными понимаются сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность. При этом указанные сведения, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных законом случаях, считаются конфиденциальными.

9. Термином «конфиденциальная информация» в комментируемой статье обозначается разновидность документированной информации, доступ к которой ограничен по основаниям, установленным законодательством РФ. Под законодательством РФ в данном случае понимаются не только законы РФ, но и иные нормативные правовые акты, обязательные для исполнения всеми лицами, пребывающими на территории, находящейся под юрисдикцией России.

К сведениям Конституционного характера согласно Указа Президента РФ от 6 марта 1997 г. № 188 отнесены:

- персональные данные;
- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

¹СЗРФ. 1997. №10. Ст. 1127.

Законодатель достаточно часто оперирует термином «конфиденциальная информация» и семантически созвучным с ним термином «тайна». Так, в качестве конфиденциальной информации могут рассматриваться сведения, находящиеся в режиме коммерческой и служебной тайны (п. 1. ст. 139 ГК РФ), банковской тайны (п. 2 ст. 857 ГК РФ), аудиторской тайны (п. 3 ст. 8 Федерального закона «Об аудиторской деятельности»¹), врачебной тайны (ст. 9 Закона РФ «О психиатрической помощи и гарантиях прав граждан на ее оказание»²), налоговой тайны (ст. 102 Налогового кодекса РФ), тайны страхования (ст. 946 ГК РФ).

10. Термин «средства обеспечения автоматизированных информационных систем и их технологий» обозначает совокупность используемых или создаваемых при проектировании информационных систем и обеспечивающих их эксплуатацию элементов. В качестве таких элементов комментируемая статья выделяет программные, технические, лингвистические правовые и организационные средства. В свою очередь, указанные средства подразделяются на:

- средства вычислительной техники и связи;
- словари, тезаурусы и классификаторы;
- инструкции и методики;
- положения, уставы, должностные инструкции;
- схемы и их описания, другая эксплуатационная и сопроводительная документация.

Очевидно, что при проектировании и эксплуатации могут использоваться и иные средства, которыми вправе оперировать лица, обслуживающие автоматизированную информационную систему или проектирующие ее.

¹ СЗ РФ. 2001. № 33. Ст. 3422; Российская газета. 2002. 12 января.

² Ведомости РФ. 1992. № 33. Ст. 2470.

11. Термин «собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения» означает лицо, которое наделяется юридически обеспеченной возможностью владеть, пользоваться и распоряжаться перечисленными объектами по своему усмотрению и в своем интересе. Власть собственника в отношении принадлежащих ему информационных ресурсов, информационных систем, технологий и средств их обеспечения не безгранична. Реализуя свои правомочия, собственник может совершать любые действия, не противоречащие закону, иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц.

Содержание права собственности на информационные ресурсы и иные объекты образуют принадлежащие собственнику правомочия по владению, пользованию и распоряжению этими ресурсами и объектами. Это традиционная для российского права «триада» правомочий.

Под правомочием владения понимается юридически обеспеченная возможность фактического обладания информационным ресурсом и иными объектами и хозяйственного господства над ними.

Под правомочием пользования понимается юридически обеспеченная возможность извлечения полезных свойств из информационного ресурса и иных объектов, например, путем личного знакомства со сведениями, содержащимися в информационной системе либо путем организации подобного знакомства всем желающим это сделать.

Под правомочием распоряжения понимается юридически обеспеченная возможность определения судьбы информационного ресурса и иных объектов путем совершения юридически или фактически значимых актов в их отношении, например, путем отчуждения по договору, передачи по наследству, закрытию доступа. У собственника информационного ресурса и иных объектов присутствуют одновременно все три названных выше правомочия.

12. Термин «владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения» означает лицо, у которого фактически находятся информационные ресурсы и иные указанные выше объекты. Пока не доказано обратное, предполагается, что данное лицо имеет право на владение информационными ресурсами и иными объектами.

Владелец может быть законным и незаконным. В свою очередь, незаконный владелец может быть добросовестным или недобросовестным.

Объем правомочий, которыми наделяется владелец информационных ресурсов и иных объектов, по смыслу комментируемой статьи, совпадает с объемом правомочий собственника, поскольку последний также ограничен в реализации своих полномочий рамками закона. Поэтому провести четкую грань между юридически обеспеченными возможностями поведения владельца и аналогичными возможностями собственника, ориентируясь на легальные дефиниции ст. 2 комментируемого Закона, не представляется возможным.

13. Термин «пользователь (потребитель) информации» означает лицо, обращающееся за получением необходимой ему информации и пользующийся ею. Источниками получения такой информации выступают информационная система либо посредник. Фигуру посредника законодатель не определяет. Представляется, что таковым может быть как собственник информационных ресурсов или информационных систем, так и их владелец, в том числе временный.

В то же время в роли потребителя информации могут выступать лица, владеющие информационными ресурсами или информационными системами, т. е. все те же собственник или владелец.

Статья 3. Обязанности государства в сфере формирования информационных ресурсов и информатизации

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на созда-

ние условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации.

2. Основными направлениями государственной политики в сфере информатизации являются:

обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

формирование и защита государственных информационных ресурсов;

создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;

создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

поддержка проектов и программ информатизации;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

1. Комментируемая статья определяет обязанности государства в сфере формирования информационных ресурсов и информатизации.

Деятельность государства в информационном секторе многообразна и не сводится только к формированию ресурсов и информатизации. Тем не менее законодатель счел возможным выделить две названные сферы, определив тем са-

мым приоритеты государственного воздействия в предметной сфере информационных отношений. Выбор подобных приоритетов предопределен тем обстоятельством, что многие общественно значимые задачи невозможно решить вне государственно-правового механизма, а формирование информационных ресурсов и информатизация как раз и являются задачами такого класса. Их решение вызвано, как минимум, требованиями охраны публичных интересов.

Осуществляя политику в сфере формирования информационных ресурсов и информатизации, государство действует на нескольких уровнях:

- на федеральном уровне — в качестве представителя интересов всего общества;
- на уровне субъектов РФ — в качестве представителя интересов населения соответствующих территорий.

Основной целью государственной политики в сфере формирования информационных ресурсов и информатизации является создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития РФ.

Государственную политику в названных сферах проводят государственные органы общей и специальной компетенции.

В числе органов общей компетенции ведущую роль по вопросам организации исполнения Конституции РФ, законодательства РФ играет Правительство РФ, которое хотя и не имеет прямых полномочий в решении проблем формирования информационных ресурсов и информатизации, воздействует на указанные проблемы посредством контроля деятельности органов исполнительной власти. К органам специальной компетенции, реализующим государственную политику в сфере формирования информационных ресурсов и информатизации, относятся практически все федеральные органы исполнительной власти, система которых на сегодня определена Указом Президента РФ от 17 мая 2000 г. «О структуре феде-

ральных органов исполнительной власти»¹. Вместе с тем следует назвать те из них, в задачи которых входит прямое решение вопросов информатизации и формирования информационных ресурсов.

Это, прежде всего, Министерство РФ по связи и информатизации, основными задачами которого являются: разработка и реализация государственной политики в области электросвязи, почтовой связи и информатизации, государственный надзор за деятельностью в области связи и информатизации; Министерство РФ по делам печати, телерадиовещания и средств массовых коммуникаций, которое обеспечивает разработку и реализацию государственной политики в области средств массовой информации и массовых коммуникаций, телерадиовещания, информационного обмена, развития компьютерных сетей общего пользования; Государственный комитет РФ по стандартизации и метрологии, в функции которого входит создание, актуализация и использование баз и банков данных нормативных документов, общероссийских классификаторов, научно-технической терминологии, каталогизации продукции и информации в области стандартизации, метрологии, сертификации, аккредитации, государственного контроля и надзора, являющихся федеральными информационными ресурсами; Федеральная архивная служба России, которая осуществляет государственное регулирование в области архивного дела и контроль над сохранностью, комплектованием и использованием документов Архивного фонда РФ.

2. Пункт 2 комментируемой статьи формулирует основные направления государственной политики в сфере информатизации. Указанные направления охватывают наиболее важные, с точки зрения законодателя, комплексные установки, которые должны быть реализованы при исполнении закона уполномоченными органами государственной власти РФ,

¹ СЗ РФ. 2000. № 21. Ст. 2168.

проводящими государственную политику в области информатизации.

В качестве первого направления названо обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы. Речь в данной формулировке идет по существу:

- об обеспечении условий реализации п. 2 ст. 8 Конституции РФ, согласно которому в Российской Федерации признаются и защищаются равным образом частная, государственная, муниципальная и иные формы собственности;
- о признании информационных ресурсов объектом права собственности и элементом материальных ресурсов России;
- о необходимости разграничения информационных ресурсов по формам собственности.

3. Второе направление государственной политики состоит в формировании и защите государственных информационных ресурсов. И если необходимость формирования государственных ресурсов как одна из приоритетных задач государства понятна и объяснима, то акцент на защиту только одной из разновидностей информационных ресурсов, а именно государственной их составляющей, не учитывает конституционной нормы о равенстве защиты всех форм собственности.

Реализация государственной политики по формированию государственных информационных ресурсов имеет целью, прежде всего, обеспечение федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ информацией о деятельности тех либо иных отраслей народного хозяйства и повышение эффективности функционирования механизма экономического регулирования и контроля над их деятельностью. Так, постановлением Правительства РФ от 6 сентября 2002 г. № 663 утверждены Основные положе-

ния формирования и использования государственных информационных ресурсов топливно-энергетического комплекса РФ¹.

Согласно названному нормативно-правовому акту, государственные информационные ресурсы ТЭК являются объектом федеральной собственности и включаются в государственный реестр федерального имущества. Формирование государственных информационных ресурсов ТЭК осуществляется Министерством энергетики РФ за счет средств федерального бюджета.

4. Третье направление государственной политики в сфере информатизации связано с созданием и развитием федеральных и региональных информационных систем и сетей, обеспечения их совместимости и взаимодействия. Реализация данного направления тесно связана с программными установками Федеральной целевой программы «Электронная Россия (2002—2010 гг.)», утвержденной постановлением Правительства РФ от 28 января 2002 г. № 65². Так, основной задачей мероприятий по совершенствованию деятельности органов государственной власти и органов местного самоуправления на основе использования информационных и коммуникационных технологий является повышение эффективности работы органов публичной власти путем обеспечения совместимости стандартов хранения информации и документооборота, подключения к компьютерным сетям органов государственной власти и органов местного самоуправления, бюджетных учреждений, реализации отраслевых программ информатизации, создания межведомственных и местных информационных систем и баз данных.

Важным документом, направленным на регламентацию порядка обеспечения совместимости и взаимодействия информационных сетей, является Руководящий документ «Основные

¹ Российская газета. 2002. 29 октября.

² Российская газета. 2002. 12 февраля.

положения развития Взаимоувязанной сети связи Российской Федерации на перспективу до 2005 г.», утвержденный решением Государственной комиссии по электросвязи при Государственном комитете РФ по связи и информатизации от 20 декабря 1995 г. № 140'.

5. Четвертое направление охватывает комплекс проблем по созданию условий для качественного и эффективного информационного обеспечения граждан, органов публичной власти и организаций на основе государственных информационных ресурсов. Реализация данного направления государственной политики связана, прежде всего, с формированием государственных информационных ресурсов с учетом потребностей граждан, организаций и органов публичной власти и использованием уже имеющихся ресурсов. Для этих целей создаются федеральные библиотеки, библиотеки субъектов РФ, библиотеки министерств и иных федеральных органов исполнительной власти, библиотеки академий, научно-исследовательских институтов, образовательных учреждений (ст. 4 Федерального закона «О библиотечном деле»²), осуществляется пополнение государственных информационных ресурсов путем международного информационного обмена (ст. 11 Федерального закона «Об участии в международном информационном обмене»³), комплектуется государственная часть Архивного фонда РФ (ст. 6, ст. 18, ст. 20 Основ законодательства РФ Об Архивном фонде Российской Федерации и архивах⁴), формируются различные фонды информации, депозитарии, электронные информационные системы, разрабаты-

¹ Сб. норм, документов по вопросам использования радиочастот в радиоэлектронных системах и высококачественных устройствах гражданского применения. М., 1999.

² СЗ РФ. 1995. № 1. Ст. 2.

³ СЗ. РФ. 1996. № 28. Ст. 3347.

⁴ Ведомости РФ. 1993. № 33. Ст. 1311.

ваются классификаторы и осуществляется их адаптация к стандартам промышленно развитых стран.

6. Пятое направление включает вопросы государственной политики по обеспечению национальной безопасности в сфере информации и обеспечению реализации прав граждан, организаций в условиях информатизации. Реализация указанного направления существенным образом замкнута на установки Доктрины информационной безопасности¹, которая является совокупностью официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства. В основу доктринального определения информационной безопасности, равно как и легального, содержащегося в ст. 2 Федерального закона «Об участии в международном информационном обмене», положено родовое понятие безопасности как «состояния защищенности», закрепленное в Законе РФ «О безопасности»².

В соответствии с п. 1 Доктрины, под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В легальной формулировке ст. 2 Федерального закона «Об участии в международном информационном обмене» информационная безопасность — это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Легко заметить, что в легальной формулировке речь идет о защищенности информационной среды (сферы) в интересах граждан и государства, а в доктринальной — о защищенности

¹ Российская газета. 2000. 28 сентября.

² Ведомости РФ. 1992. № 15. Ст. 779; 1993. № 2. Ст. 77; САПП РФ. 1993IN№52. Ст. 5086.

национальных интересов в информационной сфере. Таким образом, в самом выборе объекта защиты кроются противоречия, хотя с формально-юридических позиций в этом качестве должна выступать информационная среда, под которой понимают сферу деятельности, связанную с созданием, использованием, преобразованием и потреблением информации. С другой стороны, доктринальная формула объекта защиты соответствует родовому объекту, идентифицированному в Законе РФ «О безопасности» как жизненно важные интересы.

Учитывая роль и значимость Доктрины, следует признать, что дальнейшее использование и развитие понятия информационной безопасности будет происходить в заданном этим документом направлении, хотя оно и наиболее проблемно, поскольку требует ответа на не найденный до сих пор несколькими поколениями ученых вопрос. Этот вопрос, коль скоро речь идет об объекте защиты, в качестве которого полагаются национальные интересы, определяющиеся совокупностью сбалансированных интересов личности, общества и государства, состоит в определении баланса интересов отдельной личности и общества в целом. Ведь то, что отвечает интересам отдельного индивида, не всегда отвечает интересам общества в целом; и наоборот, то, что соответствует интересам всего общества, может явно противоречить интересу отдельного индивида.

7. Шестое направление государственной политики в сфере информатизации состоит в обязанности государства содействовать формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения. В рамках данного направления, во-первых, признается товарно-денежный характер отношений, складывающихся по поводу информационных ресурсов, информационных услуг, информационных систем, технологий и средств их обеспечения и, во-вторых, определяется необходимость содействия со стороны государства в развитии этих отношений. Задача государства при этом состоит, прежде всего, в органи-

зации экономических условий путем издания соответствующих законов, осуществления контроля над их исполнением и разрешения конфликтов.

Наличие различных форм собственности предполагает государственное регулирование по весьма широкому спектру общественных отношений, связанных с формированием рынка информационных товаров, работ и услуг. Указанное регулирование должно опираться на базовый принцип, закрепленный в ч. 1 ст. 8 Конституции РФ — принцип свободного перемещения на территории РФ товаров, услуг и финансовых средств, поддержки конкуренции и свободы экономической деятельности.

Свободное перемещение информационных ресурсов, услуг, технологий и средств их обеспечения должно подкрепляться едиными стандартами сертификации, едиными правилами лицензирования, отсутствием внутренних таможенных границ, ограничением монополизма в сферах конкурентного предпринимательства и иными мерами, которые могут объективно содействовать развитию рыночных отношений.

Весьма важной задачей, требующей своего решения при реализации данного направления государственной политики, является информационное обеспечение предпринимательской деятельности. Попытки такого обеспечения получили нормативное закрепление в постановлениях Правительства РФ от 1 декабря 1994 г. № 1319 «Об информационном обеспечении предпринимательства в Российской Федерации»¹ и от 29 декабря 1994 г. № 1434 «О сети региональных агентств поддержки малого бизнеса»².

8. Седьмое направление включает обязанность государства по формированию и осуществлению единой научно-технической и промышленной политики в сфере информатизации. Данное направление получило развитие и закрепление в Фе-

деральном законе «О науке и государственной научно-технической политике»¹ и Федеральной целевой программе «Электронная Россия (2002—2010 гг.)».

Согласно ст. 2 Федерального закона «О науке и государственной научно-технической политике», государственная научно-техническая политика — составная часть социально-экономической политики, которая выражает отношение государства к научной и научно-технической деятельности, определяет цели, направления, формы деятельности органов государственной власти РФ в области науки, техники и реализации достижений науки и техники.

Основными целями государственной научно-технической политики являются развитие, рациональное размещение и эффективное использование научно-технического потенциала, увеличение вклада науки и техники в развитие экономики государства, реализация важнейших социальных задач, обеспечение прогрессивных структурных преобразований в области материального производства, повышение его эффективности и конкурентоспособности продукции, улучшение экологической обстановки и защиты информационных ресурсов государства, укрепление обороноспособности государства и безопасности личности, общества и государства, упрочение взаимосвязи науки и образования.

Информационное обеспечение научно-технической деятельности заключается в тех шагах государства, которые оно предпринимает в отношении создания организационных, экономических и правовых условий такого обеспечения. В Российской Федерации создан ряд государственных организаций, в задачи которых входит информационное обеспечение науки и техники, в том числе Всероссийский институт научной и технической информации РАН, Институт научной информации по общественным наукам РАН, Всероссийский научно-технический информационный центр, межотраслевые центры

научно-технической информации. Координация работ по формированию и использованию государственных ресурсов научно-технической информации, разработка и реализация межведомственных программ по информационным технологиям, осуществление мер по развитию научно-информационной сети возложены на Министерство промышленности, науки и технологий РФ¹.

Единая научно-техническая и промышленная политика должна осуществляться с учетом современного мирового уровня развития информационных технологий. На достижение такого уровня направлена Федеральная целевая программа «Электронная Россия (2002—2010 гг.)», реализация которой позволит, в частности, преодолеть отставание России от развитых стран в уровне использования и развития информационных и коммуникационных технологий.

9. Восьмое направление государственной политики заключается в поддержке проектов и программ информатизации. Указанная поддержка рассматривается законодателем как одна из обязанностей государства и должна облекаться в форму плановых актов, т. е. в установленную форму действий государственных органов, с которыми связываются предусмотренные законом правовые последствия. Плановые акты существуют в формах целевых программ, государственных заказов, проектов и т. п. Согласно ст. 1. Закона РФ «О поставках продукции для федеральных государственных нужд»², различаются: федеральные целевые программы, межрегиональные целевые программы, региональные целевые программы. В целях обеспечения особо важных общегосударственных задач федеральным целевым программам может присваиваться статус президентских программ, инициатором которых является Президент РФ. В соответствии со ст. 71 Конституции РФ, установление основ федеральной политики и федеральные

программы в области государственного, экономического, экологического, социального, культурного и национального развития РФ находятся в ведении Российской Федерации. Все целевые программы должны обеспечиваться соответствующими мерами экономического стимулирования (бюджетное ассигнование, льготные кредиты, льготы по налогообложению и т. п.).

В России накоплен значительный опыт разработки и реализации программ и концепций информации. Так, только в области правовой информации были приняты Указ Президента РФ от 29 июня 1993 г. № 996 «Концепция правовой информатизации России»¹, которым определялись пять важнейших направлений информатизации (правотворчество, правоприменительная деятельность, правоохранительная деятельность, правовое образование и воспитание, правовое обеспечение процессов информатизации) и Указ Президента РФ от 4 августа 1995 г. № 808 «О президентских программах правовой информатизации»², которым предусматривалась разработка программ правовой информатизации органов государственной власти РФ, органов исполнительной власти РФ, органов государственной власти субъектов РФ.

Сегодня на повестке дня стоит вопрос реализации Федеральной целевой программы «Электронная Россия (2002—2010 гг.)», утвержденной постановлением Правительства РФ от 28 января 2002 г. № 65. Основными целями данной Программы являются создание условий для развития демократии, повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения информационных и коммуникационных технологий, обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширение подготов-

ки специалистов по информационным и коммуникационным технологиям и квалифицированных пользователей.

10. Девятое направление государственной политики включает обязанность государства по созданию и совершенствованию системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации. Это одно из наиболее актуальных направлений реализации государственной политики в сфере информатизации. Его актуальность обусловлена отсутствием в ряде регионов РФ необходимой телекоммуникационной инфраструктуры и значительными тарифами на подключение к компьютерным сетям. Указанное обстоятельство делает открытые информационные системы недоступными для граждан с низкими доходами, а равно существенно ограничивает возможность их использования образовательными и научными учреждениями, иными бюджетными организациями, местными средствами массовой информации, органами местного самоуправления. Данная проблема вполне осознана и в Федеральной целевой программе «Электронная Россия (2002-2010 гг.)», ее решение планируется осуществить по двум направлениям:

- содействие развитию общей телекоммуникационной инфраструктуры страны;
- создание пунктов подключения к общедоступным информационным системам.

Реализацию мероприятий первого направления планируется обеспечить преимущественно путем снижения административных барьеров и снятия ограничений для предпринимательской деятельности, повышения конкурентоспособности и создания благоприятных условий для притока иностранных инвестиций в сферу информационных и коммуникационных технологий.

Мероприятия второго направления планируется осуществить путем финансирования (в том числе долевого) за счет средств федерального бюджета развития пунктов подключе-

ния к общедоступным информационным системам органов государственной власти, бюджетных и некоммерческих организаций.

Планируется, что общий объем финансовых ресурсов, необходимых для реализации Федеральной целевой программы, составит 77 179, 1 млн рублей (в ценах 2002 г.), из них 15 186 млн рублей из внебюджетных источников.

11. Десятое направление государственной политики в сфере информатизации предполагает развитие законодательства в области информационных процессов, информатизации и защиты информации. Это направление также чрезвычайно важно, поскольку нормативно правовое регулирование общественных отношений, складывающихся по поводу информации и информатизации, существенно отстает от темпов развития данных областей человеческой деятельности и потребностей информационного общества. Принятых и введенных в действие законов РФ и подзаконных актов в предметной области информационного права явно недостаточно. Самого пристального внимания требует решение вопросов разработки теоретико-правовой и цивилистической модели информации как объекта гражданских прав, создания нормативно-правовой базы регулирования отношений, возникающих в связи с использованием глобальной сети Интернет, развития законодательства в сфере информационной безопасности, электронного документооборота, защиты информации от несанкционированного доступа, электронной торговли и т. д.¹

Глава 2

ИНФОРМАЦИОННЫЕ РЕСУРСЫ

Статья 4. Основы правового режима информационных ресурсов

1. Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

2. Правовой режим информационных ресурсов определяется нормами, устанавливающими:

порядок документирования информации;
право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

категорию информации по уровню доступа к ней;
порядок правовой защиты информации.

1. Комментируемая статья посвящена основам правового режима информационных ресурсов, который характеризует специфику правовой регламентации отношений, складывающихся по поводу информационных ресурсов, предопределяя их статику и динамику. Термином «правовой режим» довольно часто оперируют как в нормативно-правовых актах, так и в юридической литературе. Наиболее авторитетное определение этой категории дал в своих работах С. С. Алексеев, который понимает под правовым режимом порядок регулирования, выраженный в «комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создающих особую направленность регулирования»¹.

2. Комментируемый Закон, являющийся базовым для сферы информационных отношений/закрепляет концепцию пра-

вового режима информационных ресурсов, в основу которой положен институт вещного права собственности, характеризующий статику имущественных отношений, объектом которых являются вещи. В рамках этой концепции законодатель уходит от прямого установления правового режима информации, оперируя не термином «право на информацию», а используя термины «право на документ», «право на отдельные массивы документов», «право на документы и массивы документов в информационных системах», что придает последним режим объекта права собственности, хозяйственного ведения и оперативного управления (ст. 6 комментируемого Закона). Специальное субъективное право на информацию не вводится. Это свидетельствует о том, что в сфере правового регулирования информационных отношений сформирована, легализована и признана господствующей «проприетарная» концепция правового режима информации, отождествляющая информацию с вещью. Подобное отождествление осуществлено, прежде всего, с целью определения меры юридической власти конкретного лица в отношении принадлежащей ему информации. По мысли законодателя, обладатель информации, закрепленной на каком-либо материальном носителе, располагает юридически обеспеченной возможностью владеть, пользоваться и распоряжаться принадлежащими ему сведениями по своему усмотрению и в своем интересе, т. е. осуществляет хозяйственное господство над информацией. Важнейшим элементом подобного господства выступает возможность определять доступ к информации и диктовать его порядок. Фактически, институт вещных прав призван играть роль инструмента доступа к тем либо иным блокам сведений. Юридически «загрузив» информацию в материальный носитель и тем самым обособив отдельные ее блоки друг от друга, законодатель решил задачу, аналогичную, по существу, с вариантом закрытия информации, подменив фактическую монополию механизмом вещных прав. Но каковы последствия такой подмены, имеют ли они поло-

жительный эффект, делают ли данный вариант более оптимальным по сравнению с режимом фактической монополии? Представляется, что право собственности на информационные ресурсы и все те юридические возможности, которые вытекают из этого сугубо вещного права, как-то: передача в хозяйственное ведение, оперативное управление, аренду, доверительное управление, в залог, дарение, наследование и т. п., не могут придать режиму информации той ценности, какую придает фактор ее неизвестности третьим лицам и содержательная сторона сведений. Вещные права не являются и не могут являться юридическим инструментом, обеспечивающим надлежащую правовую охрану самих сведений как содержательной стороны информации (формальная сторона охраняется нормами авторского права), поскольку содержанием нельзя ни владеть, ни пользоваться, ни распоряжаться в вещно-правовом смысле. Фиксация сведений на конкретном носителе ничего не меняет, ибо одни и те же сведения могут циркулировать по разным носителям, оставаясь инвариантными им. В данном случае законодатель явно превысил границы применимости института права собственности, придав ему догматическое качество универсальности, позволяющее гарантированное использование данного института для всех возможных объектов. Примечателен в этой связи фрагмент рассуждений И. А. Покровского по поводу продуктов духовной деятельности, получающих общественное признание и вследствие этого делающихся объективными общественными благами. И. А. Покровский пишет: «Не только в правовых системах примитивных народов, но даже еще в праве римском духовная деятельность подобного рода не давала никаких субъективных прав на ее продукты их авторам и не пользовалась никакой правовой защитой. Всякий мог опубликовать или воспроизвести без согласия автора его произведение, осуществить его техническое изобретение. Насколько мало ценилась в римском праве духовная деятельность сама по себе, видно уже из того, что в классическую

эпоху, например, поэма, написанная на чужом писчем материале, или картина, нарисованная на чужой доске, принадлежали не поэту или художнику, а собственнику писчего материала или доски. Правда, для Юстиниана такая норма оказалась уже конфузной и была отменена»¹.

Сведения о лицах, предметах, фактах, событиях, явлениях и процессах юридически безразличны к возможностям собственника и иного титульного владельца материального носителя информации. Поэтому меры, принимаемые самим обладателем информации к ее охране, не только эффективнее мер по надделению его титулом собственника, но это и самый подходящий из возможных способов обеспечения охраны содержательной стороны информации. Еще один способ предусмотрен нормами законодательства об интеллектуальной собственности посредством применения механизма исключительного права.

Отдельные исследователи феномена информационного права преувеличивают юридическую значимость придания информационным ресурсам режима объекта права собственности. На материальные носители информации, в том числе с зафиксированными на них сведениями, право собственности существовало и до принятия комментируемого Закона. В этом отношении революции не произошло и не могло произойти. Для этого требуется, как правильно замечает В. А. Дозорцев, сферу нематериальных интеллектуальных прав «подвергнуть развернутой регламентации практически с начала и до конца»².

3. Пункт 2 комментируемой статьи устанавливает элементы правового режима информационных ресурсов. В качестве таких элементов выступают нормы закона, которыми регламентируются отношения, складывающиеся по поводу порядка документирования информации, права собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, катего-

¹ Покровский И. А. Основные проблемы гражданского права. М., 1998. С. 133.

² Дозорцев В. А. Понятие исключительного права /Проблемы совершенствования гражданского права: Сборник статей. М., 2000. С. 313.

рирования информации по уровню доступа к ней, порядка правовой защиты информации. Указанные нормы содержатся в ст. 5, 6, 10, 21 комментируемого Закона, и мы обратимся к их анализу ниже.

Статья 5. Документирование информации

1. Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов *и* их массивов, безопасность Российской Федерации.

2. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

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.

1. Данная статья устанавливает общие начала документирования информации, которое выступает обязательным условием включения информации в информационные ресурсы. Из смысла первого предложения п. 1 комментируемой статьи следует, что в состав информационных ресурсов может быть включена не любая информация, а лишь та, которая зафиксирована на материальном носителе и сопровождается реквизитами, позволяющими ее идентифицировать. При этом законодатель не уточняет ни тип материального носителя, ни способ знаковой формализации, ни характер содержания зафиксированных сведений. Поэтому поддокументированием в широком смысле следует понимать процесс любой знаковой формали-

зации сведений. В то же время существует и толкование документирования как обоснования документами¹.

В узком смысле под документированием следует понимать осуществляемый в порядке, устанавливаемом уполномоченными органами государственной власти, процесс фиксации на материальном носителе воспринимаемых человеком или техническим устройством сведений.

В качестве уполномоченных органов в комментируемой статье называются органы государственной власти, ответственные за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

За организацию делопроизводства в подведомственных отраслях несут ответственность фактически все министерства и ведомства.

Вопросами стандартизации документов занимается Государственный комитет РФ по стандартизации и метрологии (Госстандарт России), являющийся федеральным органом исполнительной власти, осуществляющим межотраслевую координацию, а также функциональное регулирование в области стандартизации, метрологии и сертификации². Организационно-технические стороны документирования реализуются специальными учреждениями. В их число входят Всероссийский научно-исследовательский институт классификации, терминологии и информации по стандартизации и качеству (ВНИИКИ) Госстандарта России, Всероссийский научно-исследовательский институт документоведения и архивного дела (ВНИИДАД). Указанными организациями, совместно с рядом других заинтересованных структур, разработан и введен в действие постановлением Госстандарта России от 30 декабря 1993 г. № 299 Общероссийский классификатор управленческой документации (ОКУД), который является составной

¹ Ожегов С. И. Словарь русского языка. М., 1967.

² СЗ РФ. 1999. № 20. Ст. 2434.

частью Единой системы классификации и кодирования технико-экономической и социальной информации, и охватывает унифицированные системы документации и формы документов, разрешенных к применению в народном хозяйстве¹.

В области стандартизации документации действует множество государственных стандартов (ГОСТов), которые представляют собой нормативные документы, в которых, в целях добровольного многократного использования, устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения. Назовем некоторые из них:

- ГОСТ 6.10.3.-83. Унифицированные системы документации, запись информации унифицированных документов в коммуникативном формате;
- ГОСТ 6.10.4.-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинопрограмме, создаваемыми средствами вычислительной техники. Основные положения;
- ГОСТ 6.01.1.-87. Единая система классификации и кодирования технико-экономической информации;
- ГОСТ 6.10.5.-87. Унифицированная система документации. Требования к построению формуляра-образца;
- ГОСТ 6.10.6.-87. Единая система внешнеторговой документации. Формуляр-образец;
- ГОСТ Р 6.30.-97. Унифицированные системы документации. Система организационно-распорядительной документации. Требования к оформлению документов.

¹ Общероссийский классификатор управленческой документации. М.: Изд-во стандартов, 1994.

Следует подчеркнуть, что с введением в действие Федерального закона «О техническом регулировании»¹ (27 июня 2003 г.) отношения по поводу стандартизации должны подчиняться новым правилам. В частности, вводятся институты национальных стандартов и общероссийских классификаторов технико-экономической и социальной информации (ст. 15).

Общее методическое руководство организаций архивного дела и документационного обеспечения в организациях РФ осуществляет Федеральная архивная служба России (Росархив). В 1991 г. Росархивом была разработана Государственная система документационного обеспечения управления, Общие положения, Общие требования к документам и службам документационного обеспечения (ГС ДОУ). Названный документ носит рекомендательный характер и считается наиболее полным межотраслевым актом в области организации документированного обеспечения управления. Отдельные положения ГС ДОУ получили развитие и конкретизацию в Типовой инструкции по делопроизводству в министерствах и ведомствах Российской Федерации, введенной в действие в 1993 г.²

2. Пункт 2 комментируемой статьи содержит отсылочную норму, согласно которой полученный из автоматизированной информационной системы документ приобретает юридическую силу только после его подписания должностным лицом. Момент обретения указанным документом юридической силы законодатель связывает с порядком, установленным на этот счет законодательством РФ.

Документы, издаваемые в форме нормативно-правовых актов, вводятся в действие, как правило, по истечении определенного срока после их опубликования. Федеральные законы подлежат опубликованию и вводятся в действие в соответствии с правилами, установленными Федеральным законом «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат

¹ Российская газета. 2002. 27 декабря.

² Типовая инструкция по делопроизводству в министерствах и ведомствах Российской Федерации. М.: Росархив. 1994.

Федерального Собрания»¹. Названные нормативные акты в течение семи дней после их подписания Президентом РФ подлежат официальному опубликованию в «Российской газете» или «Собрании законодательства Российской Федерации». По истечении десяти дней после дня их опубликования законы вступают в силу, если иной порядок не предусмотрен в соответствующем законе. Указы Президента РФ и постановления Правительства РФ подлежат опубликованию и вступают в силу согласно правилам, установленным Указом Президента РФ от 23 мая 1996 г. № 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативно-правовых актов федеральных органов исполнительной власти»². Указы Президента РФ, имеющие нормативный характер, вступают в силу на всей территории РФ одновременно по истечении семи дней после дня их первого официального опубликования в «Российской газете» или в «Собрании законодательства Российской Федерации», если иной срок не определен соответствующим указом. Постановления Правительства РФ, затрагивающие права, свободы и обязанности человека и гражданина, устанавливающие правовой статус федеральных органов исполнительной власти, а равно организаций, вступают в силу одновременно на всей территории России по истечении семи дней после дня их первого официального опубликования в названных выше печатных органах.

Ведомственные нормативно-правовые акты подлежат опубликованию и вступают в силу по правилам, предусмотренным Указом Президента РФ от 23 мая 1996 г. № 763.

Требования к иным документам, полученным из автоматизированной информационной системы, определены в ГОСТ 6.10.4.-84³. Указанный стандарт требует единого комплекса

¹ СЗ РФ. 1994. № 8. Ст. 801; 1999. № 43. Ст. 5124.

² СЗ РФ. 1996. № 22. Ст. 2663.

³ Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинопрограмме, создаваемым средствами вычислительной техники. Основные положения. М.: Изд-во стандартов, 1985.

обязательных реквизитов любых управленческих документов, независимо от материального носителя информации.

Специальные условия придания юридической силы документам, подготовленным с использованием ГАС «Выборы», предусмотрены Федеральным законом «О государственной автоматизированной системе Российской Федерации "Выборы"»¹. В соответствии со ст. 12 указанного Закона, документ на бумажном носителе, подготовленный с использованием ГАС «Выборы» в соответствии с федеральными законами, приобретает юридическую силу после его подписания соответствующими должностными лицами. Электронный документ, подготовленный с использованием ГАС «Выборы», приобретает юридическую силу после его подписания электронными цифровыми подписями соответствующих должностных лиц. Протокол, сводная таблица об итогах голосования, иные сводные документы, подготовленные в электронном виде с использованием ГАС «Выборы», приобретают юридическую силу в аналогичном порядке, но после обязательной проверки в установленном порядке с помощью открытых ключей электронных цифровых подписей подлинности всех исходных электронных документов, на основе которых готовится сводный электронный документ.

3. Пункт 3 комментируемой статьи устанавливает возможность подтверждения электронной цифровой подписью юридической силы документа, который хранится, обрабатывается и передается с помощью автоматизированных информационных и телекоммуникационных систем.

Под электронной цифровой подписью, согласно ст. 3 Федерального закона «Об электронной цифровой подписи»², понимается реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной

¹ Российская газета. 2003. 15 января.

² Российская газета. 2002. 12 января.

цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронная цифровая подпись может использоваться в сфере государственного управления и в корпоративных информационных системах.

Особенности использования электронной цифровой подписи в сфере государственного управления определены в ст. 16 Федерального закона «Об электронной цифровой подписи». Согласно п. 1 указанной статьи, федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

Особенности использования электронной цифровой подписи в корпоративных информационных системах установлены в ст. 17 Федерального закона «Об электронной цифровой подписи». Порядок использования электронных цифровых подписей в корпоративной информационной системе (информационной системе, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы) устанавливается решением владельца системы или соглашением ее участников.

В соответствии с абз. 2 п. 3 комментируемой статьи, юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи и соблюдение установленного режима их использования. Данное правило конкретизировано в ст. 4 Федерального закона «Об электронной цифровой подписи», согласно которой электронная цифровая подпись в электронном документе равнозначна собственноручной под-

писи 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.

Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении прав и исполнении обязанностей, вытекающих из отношений, указанных в сертификате ключа подписи.

Статья 6. Информационные ресурсы как элемент состава имущества и объект права собственности

1. Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.

2. Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

4. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами, независимо от их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

5. Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества,

6. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.

7. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:

назначать лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими; устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

определять условия распоряжения документами при их копировании и распространении.

8. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

1. Концептуальная установка законодателя, предопределяющая правовой режим информационных ресурсов, базируется на использовании института вещных прав применительно к этим ресурсам. Данная установка получила развитие посредством придания информационным ресурсам статуса элемента состава имущества и причисления их к числу объектов права собственности. В соответствии с п. 1 комментируемой статьи, информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Приведенная норма произвольно очерчивает круг субъектов права собственности на информационные ресурсы, называя в их ряду органы государственной власти и органы местного самоуправления. На самом деле, и это подкрепляется правилом, регулирующим отношения по поводу субъектов права собственности, информационные ресурсы (как имущество) могут находиться в собственности граждан и юридических лиц, а также Российской Федерации, субъектов Российской Федерации, муниципальных образований (ст. 212 ГК РФ). Что касается органов государственной власти и органов местного самоуправления, то они ни при каких обстоятельствах, по смыслу отечественной цивилистической доктрины, не могут являться собственниками имущества. Указанные органы могут лишь в рамках их компетенции, установленной актами, определяющими статус этих органов, своими действиями приобретать и осуществлять имущественные и личные неимущественные права и обязанности от имени соответствующего публичного образования (ст. 125 ГК РФ).

Следует подчеркнуть, что в комментируемом Законе классификация информационных ресурсов по основанию их принадлежности произведена крайне неудовлетворительно. Закон, являющийся базовым в информационной сфере, не содержит ясных правил, позволяющих дифференцировать информационные ресурсы на их отдельные разновидности.

сти. Противоречивые правила п. 1, п. 3, абз. 2 п. 5 ст. 6; п. 1. ст. 7 комментируемого Закона не позволяют назвать реальных субъектов, обладающих правом собственности на государственную часть информационных ресурсов.

Попытка классификации информационных ресурсов по формам собственности не является единственной. В соответствии со ст. 10 комментируемого Закона, все государственные информационные ресурсы делятся на две категории:

- открытые и общедоступные информационные ресурсы;
- информационные ресурсы ограниченного доступа.

Последние, в свою очередь, дифференцируются на:

- документированную информацию, отнесенную к государственной тайне;
- документированную информацию конфиденциального характера.

Отступив от принципа единства классификационного основания, законодатель вычленяет еще две разновидности информационных ресурсов, а именно:

- информационные ресурсы, отнесенные к общероссийскому национальному достоянию (ст. 9 комментируемого Закона);
- перечни персональных данных, включенные в состав федеральных информационных ресурсов, информационных ресурсов субъектов РФ, информационных ресурсов органов местного самоуправления, а также получаемые и собираемые негосударственными организациями (п. 1 ст. 11 комментируемого Закона).

Представляется, что существующие легальные классификации информационных ресурсов нуждаются в корректировке и, прежде всего, в части выбора критериев, способных служить в качестве классификационных оснований. Таких классификационных оснований для целей дифференциации родового понятия «информационные ресурсы» может быть несколько.

Наиболее предпочтительными из них являются полагающие нахождение в основании деления:

- форму собственности;
- правовой режим информации.

Первое из них базируется на факторе присвоенное™ (принадлежности) информационных ресурсов, допускаемом существующими формами экономических отношений собственности и принятой законодателем вещно-правовой моделью документированной информации.

Согласно первому классификационному основанию, все информационные ресурсы подразделяются на:

- федеральные информационные ресурсы, в состав которых входят отдельные документы и массивы документов, в том числе в информационных системах, находящиеся в собственности РФ;
- государственные информационные ресурсы, в состав которых входят отдельные документы и массивы документов, в том числе в информационных системах, находящиеся в государственной собственности субъектов РФ;
- муниципальные информационные ресурсы, в состав которых входят отдельные документы и массивы документов, в том числе в информационных системах, находящиеся в собственности муниципальных образований (муниципальной собственности);
- частные информационные ресурсы, в состав которых входят отдельные документы и массивы документов, в том числе в информационных системах, находящиеся в собственности граждан и юридических лиц.

В свою очередь, каждый из четырех видов информационных ресурсов может быть подвергнут более дробной классификации, в основу которой положены правовые режимы информации. В соответствии с последним критерием, федеральные, государственные, муниципальные и частные информацион-

ные ресурсы могут находиться в режимах свободного или ограниченного доступа.

2. В п. 2 комментируемой статьи формулируются основания, по которым физические и юридические лица обретают статус субъекта права собственности на информационные ресурсы. Коль скоро отношения, складывающиеся по поводу права собственности на информационные ресурсы, регулируются гражданским законодательством, основания приобретения права собственности на информационные ресурсы должны отвечать требованиям главы 14 ГК РФ. Принято различать первоначальные и производные способы приобретения права собственности. К первоначальным способам, которые не зависят от прав предшествующего собственника информационных ресурсов, будут относиться:

- создание (формирование) информационного ресурса;
- переработка ранее существовавшего информационного ресурса;
- приобретение права собственности на бесхозяйственный информационный ресурс.

Очевидно, что такие способы первоначального приобретения, как обращение в собственность общедоступных для сбора вещей и самовольная постройка, не применимы к информационным ресурсам.

К производным способам, при которых право собственности на информационный ресурс возникает по воле предшествующего собственника этого ресурса, относятся:

- приобретение права собственности на основании договора либо иной сделки;
- приобретение права собственности в порядке правопреемства при реорганизации юридического лица;
- приобретение права собственности в порядке наследования.

Легко заметить, что в комментируемом пункте перечень способов приобретения права собственности на информаци-

онные ресурсы не совпадает с титулами собственности, сформулированными в ГК РФ. Так, физическое лицо, создавшее документ или сформировавшее массив таких документов «для себя», без доказательств того, что они созданы за свой счет, не может рассматриваться в качестве собственника указанных документов. Аналогичная ситуация возникает и при создании документов за чужой счет.

Ряд проблемных ситуаций связан и с переработкой ранее существующего информационного ресурса. Законодатель не отвечает на вопросы, касающиеся адаптации правил ст. 220 ГК РФ применительно к информационным ресурсам.

3. В пункте 3 комментируемой статьи установлены основания приобретения права собственности на информационные ресурсы Российской Федерацией и субъектами Российской Федерации. Основания приобретения права собственности на информационные ресурсы муниципальными образованиями комментируемый Закон не устанавливает.

Помимо общегражданских способов приобретения права собственности, которых мы кратко коснулись в предыдущем пункте, закон специально выделяет в таком качестве создание, приобретение и накопление информационных ресурсов названными публичными образованиями за счет средств соответствующих бюджетов. Как и в предыдущем пункте, остается открытым вопрос о том, что следует понимать под «созданием информационных ресурсов», поскольку результатом такого создания должна явиться, как минимум, комбинация информации с материальным носителем. Ответов на этот вопрос может быть несколько. Во-первых, под созданием информационного ресурса можно понимать процесс фиксации на существующем материальном носителе воспринимаемых человеком или техническим устройством сведений, т. е. документирование (см. комментарии к п. 1 ст. 5). Во-вторых, под созданием можно понимать изготовление нового материального носителя с последующей фиксацией на нем существующих на другом носителе сведений. В-третьих, под созданием

можно понимать и технический прием декомпилирования, состоящий в преобразовании закодированной информации в воспринимаемый человеком текст. Количество подобных комбинаций можно продолжить, а затем и удвоить, оперируя фактором принадлежности материального носителя. Но это не наша задача. Требуется легальное определение действию? (действий), понимаемого законодателем как создание информационного ресурса.

В комментируемом пункте закреплено право государства на выкуп у физических и юридических лиц документированной информации в случае отнесения этой информации к государственной тайне. Отнесение сведений к государственной тайне представляет собой строго регламентированный процесс, основой которого положено применение Перечня сведений, составляющих государственную тайну, и Перечня должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утвержденных соответственно Указом/Президента РФ от 30 ноября 1995 г. № 1203 (в ред. Указов Президента РФ от 24 января 1998 г. № 61, от 6 июня 2001 г. № 659, от 10 сентября 2001 г. № 1114)¹ и распоряжением Президента РФ от 30 мая 1997 г. № 226-рп (в ред. от 23 июля 1998 г. и от 23 января 1999 г.²). При этом материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре, согласно абз. 2 ст. 10 Закона РФ «О государственной тайне»³, также предусматриваются обязательства собственника информации по ее неразглашению. При отказе собственника информации от подписанного договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну, в

¹ СЗ РФ. 1995. № 49. Ст. 4775; 2001. № 24. Ст. 2418; 2001. № 38.

² СЗ РФ. 1997. № 22. Ст. 2573.

³ СЗ РФ. 1997. № 41. Ст. 4673.

соответствии с действующим законодательством. Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника, его права. Не может быть ограничено Право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства РФ.

В абз. 3 п. 3 комментируемой статьи установлено правило, запрещающее собственнику информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, распоряжаться такими ресурсами без разрешения соответствующих органов государственной власти.

Общественные отношения, возникающие по поводу распоряжения сведениями, составляющими государственную тайну, детально урегулированы в разделе V Закона РФ «О государственной тайне», по направлениям взаимной передачи сведений, органами государственной власти и организациями (ст. 16), передачи сведений в связи с выполнением совместных и других работ (ст. 17), передачи сведений другим государствам (ст. 18).

4. Первое предложение п. 4 комментируемой статьи устанавливает правило, согласно которому лица, предоставляющие в обязательном порядке документированную информацию в органы государственной власти и организации, например в соответствии с Федеральным законом «Об обязательном экземпляре документов»¹, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. На практике это, очевидно, означает возможность изготовления копий предоставляемых документов, поскольку, не владея документом, в данном случае его копией, невозможно использовать зафиксированную в нем информацию.

Второе предложение п. 4 определяет норму, фиксирующую источник формирования информационных ресурсов, нахо-

¹ СЗ РФ. 1995. № 1. Ст. 1; Российская газета. 2002. 14 февраля.

дящихся в совместном владении государства и лиц, предоставляющих эту информацию. Фразу «субъектов, представляющих информацию» следует рассматривать как техническую ошибку которая вкралась в текст закона. Таким источником называете? документированная информация, предоставляемая в обязательном порядке в органы государственной власти и организации юридическими лицами и гражданами по основаниям, установленным ст. 8 комментируемого Закона. По смыслу данного предложения, совладельцами такой документированной информации являются только государство и субъекты, ее предоставившие. Что касается организаций, в которые предоставлен документированная информация, то между ними и субъектами, предоставившими такую информацию, отношений совладения комментируемая статья не устанавливает.

5. Согласно п. 5 комментируемой статьи, информационные ресурсы, являющиеся собственностью организаций, включаются в состав имущества этих организаций в соответствии с гражданским законодательством РФ.

Действующее гражданское законодательство относит «юридическим лицам — собственникам имущества две группы организаций. Первую группу образуют организации, учредители (участники) которых имеют обязательственные права требования к учрежденным им организациям в отношении переданного последним имущества. К таким организациям относятся хозяйственные общества и товарищества, производственные и потребительские кооперативы, некоммерческие партнерства.

Вторую группу составляют организации, на имущество которых их учредители (участники) не имеют ни вещных, ни обязательственных прав. В их число входят общественные и религиозные объединения, ассоциации, союзы, фонды, автономные некоммерческие организации, товарищества собственников жилья.

При создании организации происходит обособление передаваемого ей имущества и его идентификация в новом каче-

стве. Обособленность переданного организации имущества характеризует наличие у нее самостоятельного баланса, который выполняет прежде всего учетную функцию и не персонализирует гражданско-правовой режим имущества.

Нормы гражданского законодательства не содержат указаний относительно возможности включения в состав имущества организаций-собственников информационных ресурсов, если только последние не рассматривать в качестве вещей. Так, согласно п. 6 ст. 66 ГК РФ, вкладом в имущество хозяйственного товарищества или общества могут быть деньги, ценные бумаги, другие вещи или имущественные права либо иные права, имеющие денежную оценку. На этот счет имеется и соответствующее разъяснение Пленумов Верховного Суда РФ и Высшего Арбитражного Суда РФ, которые в п. 17 своего совместного Постановления от 1 июля 1996 г. № 6/8 «О некоторых вопросах, связанных с применением части первой Гражданского кодекса Российской Федерации» указали на следующее обстоятельство: необходимо учитывать, что в качестве вклада в имущество хозяйственного товарищества или общества могут вноситься имущественные права либо иные права, имеющие денежную оценку. В связи с этим таким вкладом не может быть объект интеллектуальной собственности (патент, объект авторского права, включая программу для ЭВМ и т. п.) или ноу-хау. Однако в качестве вклада может быть признано право пользования таким объектом, передаваемое обществу или товариществу в соответствии с лицензионным договором, который должен быть зарегистрирован в порядке, предусмотренном законодательством¹.

При реорганизации юридических лиц права и обязанности в отношении имущества организации переходят в соответствии с передаточным актом или разделительным балансом (ст. 59 ГК РФ).

Абзац 2 п. 5 комментируемой статьи содержит два юридически важных момента. Первый из них состоит в том, что ин-

¹ Российская газета. 1996. 10 августа.

формационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти, что в целом правильно, учитывая режим имущества госорганов. Однако данная норма вступает в известное противоречие с нормой п. 1 комментируемой статьи, согласно которой информационные ресурсы как элемент состава имущества находятся в собственности органов государственной власти (см. комментарии к п. 1 ст. 6). Второй момент касается «ведения» информационными ресурсами организаций. Очевидно, режим «ведения» распространяется на организации - не собственники, учредители которых сохраняют на закрепленном за организациями имуществе право собственности (унитарные предприятия, казенные предприятия, учреждения) или иное вещное право (дочерние унитарные предприятия).

Государственные органы и организации осуществляют «ведение» информационными ресурсами в соответствии со своей компетенцией и правоспособностью (организации). Информационные ресурсы в данном случае подлежат учету и защите в составе государственного имущества. Из общезначимого смысла абз. 2 п. 5 следует, что информационные ресурсы, находящиеся в государственной собственности, не могут включаться в имущество казны (п. 4 ст. 214 ГК РФ).

Отсутствует упоминание об информационных ресурсах как объекте учета федерального имущества и в Положении об учете федерального имущества и ведении реестра федерального имущества, утвержденного постановлением Правительства РФ от 3 июля 1998 г. № 696¹.

6. Комментируемая статья признает за информационными ресурсами качество товара. За изъятиями, предусмотренными законодательством РФ, информационные ресурсы могут выступать в качестве продукта труда, предназначенного для обмена. Следовательно, они должны обладать двумя свойствами!

¹ Российская газета. 1998. 13 июля.

потребительной стоимостью и стоимостью. Денежным выражением стоимости информационных ресурсов является их цена. Вместе с тем классический подход к информационным ресурсам как объекту товарно-денежных отношений уже давно подвергся критическому переосмыслению.

Как показал А. Моль, при определении суммарной стоимости информации как интеллектуальной продукции должен использоваться «иной, нежели у Маркса, характер прибавочной стоимости», а сама ситуация со стоимостью «в корне отличается от картины, которую рассматривает классическая политическая экономия»¹.

Как и любые иные объекты гражданских прав, а информация относится к их числу, согласно ст. 128 ГК РФ, информационные ресурсы могут свободно отчуждаться или переходить от одного лица к другому в порядке универсального правопреемства либо иным способом, если они не изъяты из оборота или не ограничены в обороте. При этом категории информационных ресурсов, нахождение которых в обороте не допускается, по смыслу ст. 129 ГК РФ, должны быть прямо указаны в законе.

7. В пункте 7 комментируемой статьи интерпретируются юридические возможности собственника по отношению к принадлежащим ему информационным ресурсам. Гражданское законодательство признает за собственником имущества группу правомочий, которые исчерпывают все предоставленные ему возможности. Эта группа правомочий раскрывается в ст. 209 ГК РФ с помощью традиционной для отечественного гражданского права триады: владения, пользования и распоряжения. Интерпретацию правомочий собственника, принятую в комментируемом пункте, нельзя признать безупречной. Так, не всякий собственник информационных ресурсов вправе назначать лицо, осуществляющее хозяйственное ведение ими. Это прерогатива субъектов права государственной и муниципальной собственности. При этом права

¹ Моль А. Социодинамика культуры. М., 1973. С. 97.

собственника в отношении информационных ресурсов, находящихся в хозяйственном ведении и оперативном управлении, исчерпывающим образом определены в ст. 295 и 296 ГК РФ.

Очевидно, что не любой субъект права собственности на информационные ресурсы может диктовать и устанавливать правила обработки, защиты и доступа к ним. В ряде случаев деятельность подобного рода требует лицензирования. Согласно ст. 17 Федерального закона «О лицензировании отдельных видов деятельности», лицензированию, в частности, подлежат:

- 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 выявлению электронных устройств, предназначенных для негласного получения информации в помещениях и технических средствах (за исключением случаев, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации ин-

дивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

В соответствии с названными предписаниями законодателя, Правительством РФ утверждены, в частности:

- Положение о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность¹.
- Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации²;
- Положение о лицензировании деятельности по технической защите конфиденциальной информации³;
- Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств⁴;
- Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств⁵.

8. В п. 8 комментируемой статьи регулируются отношения, складывающиеся по поводу информационных ресурсов и средств обработки информации. Право собственности на

¹ Постановление Правительства РФ от 15 июня 2002 г. № 526//Российская газета. 2002. 9 августа.

² Постановление Правительства РФ от 27 мая 2002 г. № 348//Российская газета. 2002. 22 июня.

³ Постановление Правительства РФ от 30 апреля 2002 г. № 290//Российская газета. 2002. 7 мая.

⁴ Постановление Правительства РФ от 23 сентября 2002 г. № 691//Российская газета. 2002. 5 ноября.

⁵ Постановление Правительства РФ от 23 сентября 2002 г. № 691//Российская газета. 2002. 12 ноября. 26 ноября.

средства обработки информации не влечет возникновение права собственности на информационные ресурсы, принадлежащие другим собственникам. Очевидно, что аналогично должно обстоять дело и со средствами хранения, поиска и транспортировки документированной информации.

К средствам обработки документированной информации относятся технические приспособления для физической обработки материального носителя, на котором зафиксирована информация с реквизитами. Такими приспособлениями могут являться фальцевальные, биговальные, перфорирующие, резательные машины, листоподборочное, сортировальное, скрепляющее и переплетное оборудование, машины для нанесения защитных покрытий на документы (ламинаторы), адресовальные, штемпелевальные и франкирующие устройства и др.

Для копирования и тиражирования документов используются средства репрографии и оперативной полиграфии. К средствам репрографии относятся устройства фотокопирования, светокопирования (диазокопирования), электрофотографии, термографии, электронно-искрового копирования, микрофильмирования.

Средства оперативной полиграфии включают: гектографы, ротаторы, малые офисные машины.

Применение средств обработки должно быть направлено на то, чтобы обработанная документальная информация отвечала критериям полноты и достоверности.

Значительная часть процедур обработки документированной информации носит технический либо формально-логический характер. Однако современные средства организационной техники, особенно персональные компьютеры, копировальная техника, могут выполнять и более сложные процедуры, например, обрабатывать как материальный носитель документа, так и его смысловую, содержательную часть. В этом случае не исключается возможность сохранения в памяти компьютера информации, зафиксированной на

обрабатываемом документе. Вследствие этого правило, сформулированное во втором предложении комментируемого пункта, лишается своей продуктивности, поскольку документ, бесспорно, принадлежит своему владельцу, но сама информация благодаря свойству мультиплицирования окажется зафиксированной и в средстве организационной техники, т. е. во владении и сфере хозяйственного господства нового собственника.

Статья 7. Государственные информационные ресурсы

1. Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

федеральные информационные ресурсы;

информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации (далее информационные ресурсы совместного ведения);

информационные ресурсы субъектов Российской Федерации.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспечивают их использование в соответствии с установленной компетенцией.

3. Деятельность органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов «Информатика» («Информационное обеспечение»).

1. Комментируемая статья посвящена регулированию отношений, складывающихся по поводу государственных ин-

формационных ресурсов. В п. 1 установлен порядок формирования государственных информационных ресурсов, основанный на формуле «в соответствии со сферами ведения». Указанная формула близка по смыслу с конституционно-правовым термином «находятся в ведении», поскольку последний обозначает: во-первых, сферы жизни общества, отрасли и подотрасли народного хозяйства и социально-культурной деятельности, технико-экономические системы, виды имущества, его объекты, которые находятся под воздействием государственной власти; во-вторых, названные выше отрасли и иные сферы с дополнением в виде записи о способах государственного воздействия на них; в-третьих, различные области государственного строительства и государственной деятельности с указанием или без указания специфической роли государственной власти применительно к этим областям; в-четвертых, правовое регулирование, осуществляемое федеральной властью, отрасли и подотрасли законодательства, устанавливаемые ею¹.

Итак, в сфере ведения Российской Федерации формируются федеральные информационные ресурсы, в совместном ведении Российской Федерации и субъектов Российской Федерации формируются информационные ресурсы совместного ведения, в сфере ведения субъектов Российской Федерации формируются информационные ресурсы субъектов Российской Федерации. Категория «ведение» относится к числу административно-правовых, поэтому термины «сфера ведения РФ», «сфера совместного ведения РФ и субъектов РФ», «сфера ведения субъектов РФ» не тождественны терминам «находятся в собственности РФ», «совместной собственности РФ и субъектов РФ», «собственности субъектов РФ».

Непосредственное формирование государственных информационных ресурсов осуществляют в пределах своей компе-

¹ Конституция Российской Федерации. Комментарий/Под общей ред. Б. Н. Топорнина, Ю. М. Батурина, Р. Г. Орехова. М., 1994. С. 338 (автор коммент. Б. М. Лазарев).

тенции соответствующие органы государственной власти федерального и регионального уровней.

2. Пункт 2 комментируемой статьи очерчивает круг лиц, осуществляющих формирование государственных информационных ресурсов. Среди них названы граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения.

Вопросы формирования информационных ресурсов, в том числе наиболее обширной их части — государственных ресурсов, должны находиться под контролем государства и являться элементом проводимой им политики (см. комментарий к ст. 3). В рамках реализации государственной политики по формированию информационных ресурсов введен в действие ряд федеральных законов. В их числе следует, прежде всего, назвать Федеральный закон «О библиотечном деле»¹, Основы законодательства РФ об Архивном фонде Российской Федерации и архивах², Федеральный закон «Об обязательном экземпляре документов»³, Федеральный закон «Об участии в международном информационном обмене»⁴. В названных законах получили закрепление отдельные правила, регулирующие отношения, возникающие по поводу формирования государственных информационных ресурсов.

Так, согласно ст. 19 и ст. 21 Федерального закона «О библиотечном деле», органы государственной власти финансируют деятельность государственных библиотек, в том числе выполняющих функции центральных, по созданию условий для взаимопользования их ресурсов. В целях обеспечения рационального использования государственных информационных ресурсов библиотеки взаимодействуют с органами научно-технической информации, архивами, другими пред-

¹СЗ РФ. 1995. № 1. Ст. 2.

ведомости РФ. 1993. № 33. Ст. 1311.

³СЗ РФ. 1995. № 1. Ст. 1; Российская газета. 2002. 14 февраля.

⁴СЗ РФ, 1996. № 28. Ст. 3347.

приятными, учреждениями, которые имеют информационные банки данных разных уровней.

Одним из важнейших направлений формирования государственных информационных ресурсов выступает организация хранения, учета и использования архивных документов. Это направление составляет особую сферу общественных отношений, которая, как и библиотечное дело, подвергнута правовому опосредованию специальным законодательством. Центральным звеном этого законодательства выступают Основы законодательства РФ об Архивном фонде РФ и архивах и принятый в целях совершенствования управления Архивным фондом РФ Указ Президента РФ от 17 марта 1994 г. № 552 (в ред. Указов Президента РФ от 1 апреля 1996 г. № 460, от 1 декабря 1998 г. № 1447) «Об утверждении положения об Архивном фонде Российской Федерации»¹. В соответствии со ст. 18 Основ законодательства РФ об Архивном фонде РФ и архивах, государственные архивы комплектуются архивными документами (документами, сохраняемыми или подлежащими сохранению в силу их значимости для общества, а равно имеющими ценность для собственника), образующимися в деятельности органов государственной власти, государственных учреждений и организаций или приобретенными указанными архивами, а также документами, передаваемыми негосударственными учреждениями, организациями и гражданами.

Федеральный закон «Об участии в международном информационном обмене» предусматривает норму о пополнении государственных информационных ресурсов путем международного информационного обмена. Согласно ст. 11 названного Закона, порядок определения состава документированной информации, ввозимой на территорию РФ для пополнения государственных информационных ресурсов РФ (в том числе закупаемой документированной информации), порядок ее при-

¹ САПП РФ. 1994. № 42. Ст. 878; СЗ РФ. 1996. № 15. Ст. 1575; 1998. № 49. Ст. 6007.

ббретения (в том числе закупки), порядок ее использования устанавливаются Правительством РФ.

Важное значение для формирования государственных информационных ресурсов и обеспечения их полноты играет Федеральный закон «Об обязательном экземпляре документов», которым определяется политика государства в области формирования обязательного экземпляра документов как ресурсной базы комплектования полного национального библиотечно-информационного фонда документов РФ.

3. Пункт 3 комментируемой статьи предусматривает финансирование из федерального бюджета и бюджетов субъектов РФ деятельности органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов РФ. Данная норма должна применяться с учетом правил, закрепленных в Бюджетном кодексе Российской Федерации¹, который устанавливает общие принципы бюджетного законодательства РФ, правовые основы функционирования бюджетной системы РФ, включая федеральный бюджет, бюджеты субъектов РФ и муниципальных образований. Все иные правовые акты, регулирующие бюджетные отношения, в том числе акты федеральных органов власти, а также субъектов РФ и органов местного самоуправления, не могут противоречить Бюджетному кодексу РФ.

Статья 8. Обязательное представление документированной информации для формирования государственных информационных ресурсов

1. Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

¹СЗРФ. 1998. №31. Ст. 3823.

Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство Российской Федерации.

2. Порядок и условия обязательного представления документированной информации доводятся до сведения граждан и организаций.

Порядок обязательного представления (получения) информации, отнесенной к государственной тайне и конфиденциальной информации, устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.

3. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).

Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов с адресами их представления, привлекаются к дисциплинарной ответственности вплоть до снятия с должности.

4. Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

1. Комментируемая статья закрепляет обязанность граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений по представлению документированной информации органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

Действующее законодательство не детализирует порядок исполнения закрепленной комментируемым законом обязан-

ности граждан по представлению уполномоченным органам и организациям документированной информации. Исключение составляют отдельные нормативно-правовые акты целевого характера, регламентирующие отношения по предоставлению информации гражданами, занимающимися предпринимательской деятельностью. Как правило, указанные нормативно-правовые акты возлагают аналогичную обязанность и на иных хозяйствующих субъектов. К числу этих нормативно-правовых актов относятся, в частности:

- Постановление Правительства РФ от 6 сентября 2002 г. № 663 «О формировании и использовании государственных информационных ресурсов топливно-энергетического комплекса Российской Федерации»¹;
- Постановление Правительства РФ от 17 апреля 2002 г. № 245 «Об утверждении Положения о предоставлении информации в Комитет Российской Федерации по финансовому мониторингу организациями, осуществляющими операции с денежными средствами или иным имуществом»²;
- Правила о порядке представления и рассмотрения органом регулирования естественных монополий в области связи и на транспорте ходатайств и уведомлений в соответствии с требованиями ст. 7 Федерального закона «О естественных монополиях», утвержденные приказом Министерства РФ по антимонопольной политике и поддержке предпринимательства от 3 августа 2001 г. № 908³;
- Положение о порядке представления статистической информации, необходимой для проведения государственных статистических наблюдений, утвержденное постановлением Государственного комитета РФ по статистике от 15 июля 2002 г. № 154⁴;

¹ Российская газета. 2002. 29 октября.

² СЗ РФ. 2002. № 16. Ст. 1572.

³ Российская газета. 2002. 15 января.

⁴ Российская газета. 2002. 4 сентября.

- Инструкция о представлении в Комитет Российской Федерации по финансовому мониторингу информации, предусмотренной Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем», утвержденная приказом Комитета РФ по финансовому мониторингу от 3 сентября 2002 г. № 62'.

Сфера отношений, возникающих по поводу деятельности производителей и получателей обязательного экземпляра документов, включая организации, распространяющие обязательный экземпляр, регламентирована Федеральным законом «Об обязательном экземпляре документов»².

Согласно ст. 1 указанного Закона, под обязательным экземпляром документов понимаются экземпляры различных видов тиражированных документов, подлежащие передаче производителями в соответствующие организации в порядке и количестве, установленных федеральным законом.

В основу данного термина положены понятия документа и экземпляра, которые для целей Федерального закона «Об обязательном экземпляре документов» отличаются от аналогичных понятий, используемых в иных законодательных актах. В данном случае законодатель рассматривает документ в качестве материального носителя с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, предназначенного для передачи во времени и пространстве в целях общественного использования и хранения. Под экземпляром понимается образец тиражированного документа, идентичный оригиналу.

Обязательные экземпляры документов могут быть платными и бесплатными.

Платные экземпляры документов подлежат передаче за плату их производителями в соответствующие организации. Для

¹ Российская газета. 2002. 22 октября.

² СЗ РФ. 1995. № 1. Ст. 1; Российская газета. 2002. 14 февраля.

бесплатных экземпляров характерна безвозмездная их передача производителями.

В зависимости от территориально-административного признака места изготовления экземпляра различаются: обязательные бесплатные федеральные экземпляры документов, обязательные экземпляры документов субъекта Российской Федерации, обязательные бесплатные экземпляры документов муниципального образования. Обязательные бесплатные федеральные экземпляры представляют собой экземпляры различных видов документов, изготовленных на территории Российской Федерации, за ее пределами по заказу организаций и отдельных лиц, находящихся в ведении Российской Федерации, а также документов, импортируемых для общественного распространения на территории России.

Обязательные экземпляры документов субъекта Российской Федерации — это экземпляры различных видов документов, изготовленных на территориях субъектов Российской Федерации, которые подлежат передаче их производителями в соответствующие организации.

Фигура производителя документов занимает важное место в системе формирования обязательного экземпляра документов. Поэтому действующее законодательство весьма детально регламентирует круг отношений, субъектом которых являются лица, так либо иначе вовлеченные в процесс производства документированной информации.

В соответствии со ст. 1 Федерального закона «Об обязательном экземпляре документов», производитель документов — это юридическое лицо, независимо от его организационно-правовой формы и формы собственности, или физическое лицо, осуществляющее предпринимательскую деятельность без образования юридического лица, осуществляющее подготовку, публикацию (выпуск) и рассылку (передачу, доставку) обязательного экземпляра (издатель, редакция средства массовой информации, производитель фонограммы, производитель аудиовизуальной продукции, организация по производ-

- соблюдение получателями обязательного бесплатного экземпляра прав производителей в соответствии с законодательством РФ об интеллектуальной собственности;
- письменное подтверждение доставки обязательного экземпляра.

Основной обязанностью производителя документов является доставка обязательного бесплатного экземпляра тех либо иных разновидностей документов. Согласно п.1 ст. 6 Федерального закона «Об обязательном экземпляре документов», производители документов обязаны передавать обязательный бесплатный экземпляр получателям документов безвозмездно. Затраты на подготовку, публикацию (выпуск) и рассылку (передачу, доставку) обязательных бесплатных экземпляров производители документов должны относить на себестоимость документов, входящих в состав обязательного бесплатного экземпляра.

При этом дефектные экземпляры по запросу получателей должны быть заменены в месячный срок. Недопоставленные производителями документов обязательные экземпляры могут закупаться получателями за счет производителей.

Обязанность производителя документов по доставке обязательного бесплатного экземпляра дифференцируется законодателем применительно к конкретному виду документа, входящего в состав обязательного экземпляра, подлежащего доставке. В рамках названной дифференциации получают развитие вопросы, связанные со сроками доставки, количеством экземпляров, подлежащих доставке, адресатом доставки и т. п. Рассмотрим это подробнее.

Обязанности производителя по доставке обязательного бесплатного экземпляра изданий определены в ст. 7, 8, 9 Федерального закона «Об обязательном экземпляре документов»¹. В соответствии с названной статьей, производители документов доставляют через полиграфические организации в федеральный орган исполнительной власти по вопросам печати, телерадиове-

¹ См. также: Постановление Правительства РФ от 3 декабря 2002 г. № 859// Российская газета 2002 г. 17 декабря.

щения и средств массовых коммуникаций по одному обязательному бесплатному федеральному экземпляру всех видов печатных изданий в день выхода в свет первой партии тиража.

В целях последующего распределения изданий между библиотечно-информационными организациями, производители обязаны доставлять в день выхода в свет первой партии тиража печатных изданий в Российскую книжную палату:

- шестнадцать обязательных бесплатных экземпляров книг и брошюр, журналов и продолжающихся изданий на русском языке;
- семь обязательных бесплатных экземпляров изоизданий, нотных изданий, географических карт и атласов на русском языке;
- девять обязательных бесплатных экземпляров центральных газет и газет субъектов РФ на русском языке;
- три обязательных бесплатных экземпляра многотиражных газет муниципальных образований и рекламных изданий на русском языке;
- четыре обязательных бесплатных экземпляра книг и брошюр, журналов и продолжающихся изданий, изоизданий, географических карт и атласов на языках народов РФ (за исключением русского) и на иностранных языках;
- три обязательных бесплатных экземпляра газет на языках народов РФ и иностранных языках;
- четыре обязательных бесплатных экземпляра текстовых листовых изданий;
- девять обязательных бесплатных экземпляров авторефератов диссертации и диссертаций в виде научных докладов;
- десять обязательных бесплатных экземпляров стандартов.

Кроме того, производители документов доставляют через полиграфические организации по три обязательных бес-

платных экземпляра документов субъекта РФ всех видов печатных изданий в соответствующие республиканские (национальные) книжные палаты или сектора государственной библиографии национальных библиотек в день выхода в свет первой партии тиража, а также по два обязательных бесплатных экземпляра документов муниципальных образований всех видов печатных изданий, выпущенных в городе или районе, в соответствующие краевые, областные, городские, районные универсальные научные библиотеки в день выхода в свет первой партии тиража.

В интересах развития единого информационного пространства государств — участников СНГ, на основе соответствующих договоров осуществляется поставка в национальные фондохранилища этих государств обязательного экземпляра отечественных изданий.

В Российскую государственную библиотеку для слепых производители документов обязаны направлять по два обязательных бесплатных экземпляра изданий для слепых и слабовидящих в течение двух дней после выхода в свет первой партии тиража.

Обязанности производителя по доставке обязательного бесплатного экземпляра неопубликованных и официальных документов очерчены законодателем в ст. 10 и 11 Федерального закона «Об обязательном экземпляре документов».

В зависимости от вида неопубликованного документа, его экземпляры полагается доставлять в соответствующие органы научно-технической информации и библиотеки.

Производители документов обязаны в тридцатидневный срок доставлять во Всероссийский научно-технический информационный центр федерального органа исполнительной власти по вопросам промышленности, науки и технологий обязательные бесплатные экземпляры следующих видов неопубликованных документов:

- а) отчетов о научно-исследовательских и опытно-конструкторских работах — со дня их утверждения;

- б) алгоритмов и программ — со дня окончания их разработки;
- в) диссертаций — со дня их защиты и присуждения ученой степени.

В тридцатидневный же срок доставляются бесплатные экземпляры диссертаций по всем отраслям знаний (за исключением медицины и фармацевтики) в Российскую государственную библиотеку. Бесплатные экземпляры диссертаций по медицине и фармацевтике доставляются в этот же срок в Государственную центральную научную медицинскую библиотеку.

Обязательные бесплатные экземпляры депонированных научных работ по общественным наукам, после вынесения решения о депонировании соответствующими учеными или редакционно-издательскими советами, в десятидневный срок доставляются в Институт научной информации по общественным наукам Российской академии наук.

Бесплатные экземпляры депонированных научных работ по естественным, точным наукам и технике в том же порядке и сроки доставляются во Всероссийский институт научной и технической информации Российской академии наук.

Обязательные бесплатные экземпляры официальных документов доставляются органами государственной власти РФ и органами государственной власти субъектов РФ в Парламентскую библиотеку Российской Федерации. Эти экземпляры, в количестве двух, включаются в списки рассылки документов несекретного характера и направляются в указанную библиотеку после утверждения и регистрации (постановки регистрационного номера и гербовой печати) соответствующего документа.

Обязанности производителей по доставке обязательных бесплатных экземпляров аудиовизуальной продукции и электронных изданий определены в ст. 12 и 13 Федерального закона «Об обязательном экземпляре документов».

На производителей аудиовизуальной продукции возлагается обязанность по ее доставке пяти адресатам:

- в Российскую книжную палату — по три обязательных бесплатных экземпляра фонограмм в день их выхода в свет и видеофильмов в день окончания их копирования.
- в Государственный фонд телевизионных и радиопрограмм — по два обязательных бесплатных экземпляра фонопродукции, кинопродукции в виде позитивных копий, а также по два экземпляра видеопродукции, аудиовизуальной продукции на электронных носителях, созданной для телевидения и радиовещания, не позднее чем через месяц со дня ее выхода в эфир;
- в Государственный фонд кинофильмов Российской Федерации — по одному обязательному бесплатному экземпляру игровых, анимационных, научно-популярных фильмов в виде позитивной копии не позднее чем через месяц со дня окончания их монтажа или дубляжа; по одному экземпляру игровых, анимационных и научно-популярных видеофильмов в виде копии на оригинальных носителях любых видов;
- в Российский государственный архив кинофотодокументов — по одному обязательному бесплатному экземпляру документальных фильмов и киножурналов в виде позитивной копии не позднее чем через месяц со дня окончания их монтажа или дубляжа; по одному, обязательному экземпляру документальных видеофильмов в виде копии на оригинальных носителях любых видов; по два обязательных экземпляра фотодокументов;
- в Российский государственный архив фонодокументов — по два обязательных бесплатных экземпляра фонопродукции, созданной для телевидения и радиовещания.

Обязательные бесплатные экземпляры электронных изданий их производители обязаны доставлять в Межотраслевой научно-исследовательский институт «Интеграл». В данном

случае доставляется один экземпляр программ для электронных вычислительных машин, входящих в состав электронных изданий или являющихся самостоятельными изданиями. Кроме того, для целей последующего распределения электронных изданий между библиотечно-информационными организациями на производителей возлагается обязанность по доставке четырех обязательных экземпляров электронных изданий (за исключением электронных изданий для слепых и слабовидящих, программ для ЭВМ и баз данных, аудиовизуальных и патентных документов на электронных носителях) в Научно-технический центр «Информрегистр».

Обязанности производителя документов по доставке обязательного платного экземпляра изданий определены законодателем в ст. 14 Федерального закона «Об обязательном экземпляре документов»¹. Согласно названной статье, производители документов обязаны доставлять в Центральный коллектор научных библиотек из первой партии тиража обязательный платный экземпляр изданий в количестве и порядке, определяемом Правительством РФ. Затраты на доставку обязательного платного экземпляра относятся на себестоимость издательской продукции.

Обязательный экземпляр, состоящий из совокупности документов, выполненных на различных носителях (печатных, аудиовизуальных, электронных), должен рассылаться получателям единым комплектом. Почтовая пересылка обязательного бесплатного экземпляра и обязательного платного экземпляра производится с 50% скидкой по тарифам, установленным для бюджетных организаций.

2. Пункт 2 комментируемой статьи устанавливает требование законодателя о соблюдении гласности порядка и условий обязательного представления документированной информации. При этом порядок обязательного представления (получения) инфор-

¹ См. также: Постановление Правительства РФ от 3 декабря 2002 г. № 860// Российская газета. 2002 г. 11 декабря.

мации, отнесенной к государственной тайне и конфиденциальной информации, устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.

Обращаясь к порядку обязательного представления (получения) информации, отнесенной к государственной тайне, следует подчеркнуть, что Закон РФ «О государственной тайне» в явном виде не устанавливает подобного порядка. По данному вопросу существует множество подзаконных актов, которые регулируют особенности представления (получения) закрытой информации в отдельных отраслях экономики. Так, согласно Правилам организации системы государственного учета и контроля ядерных материалов, утвержденным постановлением Правительства РФ от 10 июля 1998 г. № 746\ представление информации о государственном учете и контроле ядерных материалов на ведомственном уровне в информационно-аналитические организации и центры сбора, обработки и передачи информации, обеспечивающие функционирование системы государственного учета и контроля ядерных материалов на федеральном уровне, обеспечивают федеральные органы исполнительной власти, осуществляющие государственное управление использованием атомной энергии, и Российская академия наук, имеющие подведомственные организации, деятельность которых связана с использованием ядерных материалов. При этом объем и порядок представления сведений в области учета и контроля ядерных материалов, не составляющих государственную тайну, организациям, в том числе общественным, и гражданам определяется законодательством РФ.

Отдельные нормы, регулирующие особенности представления конфиденциальной информации и информации, составляющей государственную тайну, содержатся в Федеральном законе «Об экспортном контроле»². Так, согласно ст. 13 названного закона, федеральные органы законодательной власти, а также федеральные органы исполнительной власти, осущест-

¹ СЗ РФ. 1998. № 29. Ст. 3559.

² СЗ РФ. 1999. № 30. Ст. 3774.

ствляющие полномочия в области экспертного контроля, имеют право запрашивать и получать документы и информацию, необходимую для целей экспортного контроля.

Указанная информация, в соответствии со ст. 15, используется исключительно в целях экспортного контроля. Информация, составляющая государственную, коммерческую и иную охраняемую законом тайну, а также конфиденциальная информация не должна разглашаться, использоваться должностными лицами в личных целях, передаваться третьим лицам, за исключением случаев, предусмотренных законодательством РФ. Подобные случаи в отношении сведений, составляющих государственную тайну, предусмотрены разделом V Закона РФ «О государственной тайне».

3. В пункте 3 комментируемой статьи содержатся нормы, устанавливающие обязанности регистрационных органов по обеспечению регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов. Сегодня отношения, возникающие в связи с государственной регистрацией юридических лиц при их создании, реорганизации и ликвидации, регулируются Федеральным законом «О государственной регистрации юридических лиц»¹. Согласно ст. 12 названного закона, при государственной регистрации создаваемого юридического лица в регистрирующий орган представляются:

- подписанное заявителем заявление о государственной регистрации по форме, утвержденной Правительством РФ;
- решение о создании юридического лица в виде протокола, договора или иного документа в соответствии с законодательством РФ;
- » учредительные документы юридического лица (подлинники или нотариально удостоверенные копии);

¹СЗ РФ. 2001. № 33. Ч. 1. Ст. 3431.

- * выписка из реестра иностранных юридических лиц соответствующей страны происхождения или иное равное по юридической силе доказательство юридического статуса иностранного юридического лица-учредителя;
- « документ об уплате государственной пошлины.

Перечень документов, представляемых при регистрации юридического лица, создаваемого путем реорганизации установлен ст. 14 Федерального закона «О государственной регистрации, юридических лиц», а ст. 17 и ст. 21 определяют, соответственно, перечни документов, представляемых для государственной регистрации изменений, вносимых в учредительные документы юридического лица и представляемых для государственной регистрации при ликвидации юридического лица.

В соответствии с постановлением Правительства РФ от 17 мая 2002 г. № 319 «Об уполномоченном федеральном органе исполнительной власти, осуществляющем государственную регистрацию юридических лиц»¹, начиная с 1 июля 2002 г. государственную регистрацию юридических лиц уполномочено осуществлять Министерство РФ по налогам и сборам.

Основаниями для отказа в государственной регистрации, согласно ст. 23 Федерального закона «О государственной регистрации юридических лиц», являются: непредоставление определенных законом и необходимых для регистрации документов; предоставление документов в ненадлежащий регистрирующий орган. При этом решение об отказе в государственной регистрации должно содержать основания отказа с обязательной ссылкой на нарушения и быть принятым не позднее чем через пять рабочих дней со дня представления документов в регистрирующий орган. Правила ведения Единого государственного реестра юридических лиц и предоставления содержащихся в нем сведений установлены

¹ Российская газета. 2002. 22 мая.

постановлением Правительства РФ от 19 июня 2002 г. № 438 «О Едином государственном реестре юридических лиц»¹.

Санкции за нарушение законодательства о государственной регистрации юридических лиц органами, осуществляющими государственную регистрацию, предусмотрены ст. 14.25 Кодекса Российской Федерации об административных правонарушениях. Так, несвоевременное или неточное внесение записей о юридическом лице в единый государственный реестр юридических лиц влечет наложение административного штрафа на должностных лиц органов, осуществляющих государственную регистрацию юридических лиц, в размере от десяти до двадцати минимальных размеров оплаты труда.

4. Комментируемый пункт содержит норму, которая предоставляет возможность физическим и юридическим лицам, при соблюдении установленных правил, включать принадлежащие им документы в состав государственных информационных ресурсов. Указанная возможность, например, предусмотрена ст. 18 Основ законодательства РФ об Архивном фонде РФ и архивах, согласно которой государственные архивы комплектуются архивными документами, образующимися в деятельности органов государственной власти, государственных учреждений, организаций, а также документами, переданными им негосударственными организациями и гражданами.

Статья 9. Отнесение информационных ресурсов к общероссийскому национальному достоянию

1. Отдельные объекты федеральных информационных ресурсов могут быть объявлены общероссийским национальным достоянием.

2. Отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому национальному достоянию и определение их правового режима устанавливаются федеральным законом.

¹ Российская газета. 2002. 26 июня.

1. Комментируемая статья содержит отсылочные нормы, регулирующие отношения по поводу отнесения информационных ресурсов к общероссийскому национальному достоянию. Правовой режим документированной информации как национального достояния является модифицированным вариантом режима свободного доступа к информации, который квалифицируется Конституцией РФ как основная гарантия прав человека и гражданина. Установление режима общероссийского национального достояния в отношении информации обусловлено необходимостью придания отдельным разновидностям документированных сведений качеств, общественно необходимых и полезных всем членам общества.

В режиме общероссийского национального достояния (в широком смысле общественного достояния) может находиться не любая общедоступная документированная информация, а лишь та, которая незаменима по своей природе и уникальна. К подобного рода документам относятся, например, уникальные рукописи, документы, архивы, редкие книги, фольклорные записи и т. п.

Режим национального достояния зиждется на определенных принципах, важнейшими из которых являются:

- общедоступность;
- равенство возможностей на доступ;
- обеспеченность документированной информации особой охраной со стороны государства.

2. Принцип общедоступности реализуется посредством создания условий для беспрепятственного ознакомления и (или) использования соответствующих сведений. Вместе с тем беспрепятственный доступ к документированной информации, отнесенной в разряд национального достояния, может быть осуществлен не при любых обстоятельствах.

Подобного рода ограничение сформулировано в п. 2 комментируемой статьи, согласно которому отнесение конкретных объектов федеральных информационных ресурсов к об-

щероссиискому национальному достоянию и определение их правового режима устанавливаются федеральным законом. Такой закон в настоящее время еще не принят.

3. Принцип равенства возможностей на доступ реализуется путем предоставления всем членам общества, при наличии оправданного к тому интереса, единообразных условий для ознакомления с документированной информацией, отнесенной к национальному достоянию, и ее получения. Очевидно, что не существует препятствий для установления государством оснований и порядка доступа к таким документам, и требований о возмещении расходов, связанных с хранением информации и доступом к ней. В данном случае важно, чтобы правила, определяющие порядок доступа, были одинаковыми для всех.

4. Принцип обеспеченности документированной информации особой охраной со стороны государства реализуется через комплекс организационно-обеспечительных мер, направленных на поиск и сохранность наиболее ценных и необходимых обществу информационных ресурсов.

Статья 10. Информационные ресурсы по категориям доступа

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

3. Запрещено относить к информации с ограниченным доступом:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию,

необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

4. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне».

5. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 настоящего Федерального закона.

1. В комментируемой статье содержатся общие положения классификации информационных ресурсов по категориям доступа. В основу данной классификации положено деление всех информационных ресурсов на две категории:

- общедоступные информационные ресурсы;
- информационные ресурсы ограниченного доступа.

В свою очередь информационные ресурсы ограниченного доступа дифференцируются по условиям их правового режима на:

- конфиденциальную документированную информацию;
- документированную информацию, отнесенную к государственной тайне.

Общедоступные информационные ресурсы дальнейшей классификации в комментируемой статье не подвергаются.

Систематическое толкование комментируемого Закона, а также иных законодательных актов, регулирующих отношения

в информационной сфере, позволяет сделать вывод о том, что общедоступные информационные ресурсы по условиям их правового режима следует дифференцировать на:

- документированную информацию, содержащую сведения об охраняемых результатах интеллектуальной деятельности;
- документированную информацию, отнесенную к национальному (общественному) достоянию;
- документированную информацию, продуцируемую средствами массовой информации.

2. Правовая модель закрытия каких-либо сведений от доступа к ним третьих лиц строится на применении для этих целей единственно возможного юридического механизма, обозначаемого понятием тайны. Данное понятие не подвергалось детальным исследованиям в рамках правовой науки, вследствие чего не выработано теоретически обоснованного подхода к нему. В результате многие нормативно-правовые акты, а равно и литературные источники изобилуют терминологическим разнобоем, ошибочными утверждениями и механическим переносом на отношения, возникающие по поводу скрываемых сведений, чуждых этим отношениям юридических моделей. Так, И. Б. Ткачук утверждает, что «исходным условием защиты коммерческой тайны является право собственности на нее, полученное хозяйствующим субъектом на основаниях, предусмотренных законом»¹.

Между тем законодатель достаточно часто оперирует термином «тайна» и семантически созвучными с ним терминами «конфиденциальный», «секретный» и т. п. По данным, приводимым в литературе, уже сегодня в законодательных и подзаконных нормативных актах фигурируют более сорока видов тайн, и их число продолжает расти².

¹ Ткачук И. Б. Коммерческая тайна: организация защиты, расследование посягательств. М., 1999. С. 9.

² Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право: Учебник/ Под ред. Б. Н. Топорнина. СПб., 2001. С. 483.

Используемый в текстах нормативно-правовых актов термин «тайна» с прилагательными типа «коммерческая, служебная, банковская, аудиторская, врачебная, государственная» и т. п. употребляется как синоним сведений, которые неизвестны либо должны быть неизвестны третьим лицам. Таким образом, тайна в легальной интерпретации — это информация, доступ к которой ограничен.

Чаще всего применяется формула «сведения, составляющие» ту либо иную разновидность тайны. Данная формула положена, в частности, в основу дефиниций коммерческой и служебной тайны (п. 1 ст. 139 ГК РФ), банковской тайны (п. 2 ст. 857 ГК РФ), аудиторской тайны (п. 3, ст. 8 Федерального закона «Об аудиторской деятельности»)¹.

Несколько иные формулировки используются в отношении, например, государственной тайны и тайны страхования. В первом случае — это защищаемые государством сведения (ст. 2 Закона РФ «О государственной тайне»), а во втором — сведения о страхователе, полученные страховщиком (ст. 946 ГК РФ).

В отношении других видов тайн применяются словосочетания «сведения» о чем-либо. Так, врачебной тайной являются, в частности, сведения о наличии у гражданина психического расстройства (ст. 9 Закона РФ «О психиатрической помощи и гарантиях прав граждан на ее оказание»)².

Приведенные примеры позволяют сделать вывод о том, что законодатель рассматривает тайну в широком смысле в качестве объективно существующих, но неизвестных третьим лицам сведений о чем-либо.

Информация, точнее сведения, посредством которых строится юридическая модель тайны, видимо, не единственный объективный эквивалент, которым может оперировать правовая наука, определяя существо тайны. Специфика отношений,

¹ СЗ РФ. 2001. № 33. Ст. 3422; Российская газета. 2002. 12 января.

² Ведомости СНД и ВС РФ. 1992. № 33. Ст. 2470.

которые складываются в обществе по поводу информации, лежащей в основе употребляемого законодателем термина «тайна», не может не отражать универсальных закономерностей, открытых в иных областях научных знаний, в частности, в теории информации.

Зададим в этой связи вопрос о том, устраняют ли у третьих лиц неизвестные им сведения неопределенность их представления о чем-либо? Строго говоря — не устраняют. Такие сведения являются информацией только для лиц, имеющих к ним доступ. Данное утверждение будет тем более справедливо, если рассматривать информацию как знание, как меру устранения неопределенности представления о чем-либо. Следовательно, неизвестность (незнание) — это не информация, а нечто ей противоположное. В теории информации (синтаксический аспект) это нечто обозначается как мера неопределенности сведений и именуется энтропией. Таким образом, логично предположить, что тайна выступает в качестве информации только для обладателя последней, но для третьих лиц, до момента получения соответствующих сведений, такая тайна будет выступать в качестве «энтропии». Говоря иначе, закрытая информация для ее обладателя — не тайна, но и для третьих лиц — не информация. В этом проявляется диалектика феномена тайны, ее двойственный, полярный характер, который обусловлен наличием механизма доступа к сведениям, основанного на запретах и позитивных обязываниях, устанавливаемых законодателем в отношении третьих лиц и обладателей закрытых сведений соответственно.

Отмеченное выше позволяет сделать вывод о том, что понятие тайны несводимо к информации. Тайна — это не информация, а правовой режим информации. Поэтому информация (сведения) не может составлять тайны, как это зафиксировано в ряде законодательных актов, в том числе и в ГК РФ, она может находиться в тайне, т. е. особом правовом режиме.

Информации, находящейся в тайне и относимой в разряд как конфиденциальной, так и государственной тайны, присущ ряд признаков, в числе которых выделяются:

- ценность скрываемых сведений, которая обусловлена спецификой их содержания и (или) фактором их неизвестности третьим лицам;
- отсутствие свободного доступа к сведениям на законных к тому основаниях;
- наличие превентивных мер, принимаемых обладателем сведений к охране их от доступа третьих лиц.

Обращаясь к первому из названных признаков, следует подчеркнуть его значимость для рассказывания закрытых сведений по видам тайн, в режимах которых эти сведения могут находиться. Ценностный фактор сведений проявляется в двух взаимно связанных аспектах. Первый аспект характеризует содержательную сторону информации, которая выступает предметом специфических интересов субъектов, не заинтересованных в ее преждевременном раскрытии, и которые не готовы или не имеют права это сделать под угрозой наступления неблагоприятных последствий. Примером подобного рода информации являются данные о секретных изобретениях. Второй аспект формально не связан с содержанием информации, ибо в этом случае ценность будет представлять не содержательная сторона сведений, хотя от нее и не уйти, а фактическая возможность доступа к ней в порядке и на условиях, продиктованных ее обладателем, который готов и имеет право это сделать.

Между обозначенными аспектами ценностного фактора информации существует тесная связь, и они не могут рассматриваться изолированно, поскольку это две стороны одной медали. В зависимости от характера и содержания информации, превалирует тот либо иной аспект, которому законодатель придает правовое значение. Так, сведения, чья ценность состоит в неизвестности их третьим лицам, а содержание может быть доведено до сведения их неограниченного круга без угрозы наступления неблагоприятных последствий, могут легально выступить в качестве товара и тем самым участвовать

в хозяйственном обороте наряду с другими благами, признаваемыми объектами гражданских прав.

Отсутствие доступа к информации, за исключением легальной возможности осуществления подобного действия, выступает вторым признаком информации, находящейся в тайне. Этот признак характеризует меру свободы получения сведений, обладатель которых притязает на их роль в качестве закрытых.

В этой связи следует различать санкционированную и не санкционированную разновидности доступа к информации.

Санкционированный доступ характеризуется законными основаниями получения закрытых сведений, например, путем знакомства с ними в силу прямых служебных обязанностей. Данный вид доступа не порочит конфиденциальности либо секретности сведений.

Несанкционированный доступ характеризуется противоправными действиями по сбору сведений, находящихся в тайне, например путем хищения документов, содержащих данные о потенциально патентоспособном техническом решении.

Третьим признаком информации, находящейся в тайне, выступают преднамеренные действия ее обладателя, свидетельствующие о принятии им мер, направленных на охрану конфиденциальности или секретности сведений и пресечении несанкционированного доступа к ним. Характер данных мер может быть самым различным. Это могут быть организационные, технические, режимные, правовые и т. п. меры. Главное требование, предъявляемое к ним, — превентивность.

Правовой режим сведений, находящихся в тайне, коренным образом отличается от правового режима, установленного в отношении охраняемых результатов интеллектуальной деятельности. Это отличие проявляется в следующем.

Во-первых, в особенностях объекта, в отношении которого устанавливается соответствующий правовой режим. Формально юридически информация, находящаяся в тайне,

не отнесена к числу объектов интеллектуальной собственности (ст. 138 ГК РФ), что в целом является верным решением законодателя, поскольку не информация является частью интеллектуальной продукции, а результаты интеллектуальной деятельности выступают одной из сторон проявления информации¹.

Во-вторых, в противоположной направленности интересов обладателя информации, содержащей сведения закрытого характера, и интересов обладателя информации, представляющей собой результат интеллектуальной деятельности. Первый из них заинтересован в принятии мер, препятствующих распространению соответствующих сведений, и обязан принимать эти меры, а второй — заинтересован в распространении интеллектуального продукта, а в ряде случаев и обязан это делать.

В-третьих, в различных юридических механизмах охраны прав и интересов обладателя результата интеллектуальной деятельности и обладателя сведений закрытого характера. В случае с информацией, содержанием которой выступают закрытые сведения, юридический механизм охраны интересов ее обладателя будет основываться не на запрете использования верифицированного результата интеллектуальной деятельности третьими лицами, а на запрете на доступ к не верифицированным сведениям третьих лиц, понимаемом как блокирование техническими и иными средствами действий по «снятию» информации, осуществляемое силами фактического ее обладателя. Здесь налицо альтернативный исключительному праву вариант механизма охраны информации от

¹ В литературе, посвященной вопросам служебной и коммерческой тайны, высказываются различные позиции, касающиеся соотношения информации, составляющей служебную и коммерческую тайну, и объектов исключительных прав. Представляются ошибочными взгляды сторонников отнесения служебной и коммерческой тайны к самостоятельной разновидности объектов интеллектуальной собственности, поскольку ими ставится знак равенства между монополией *de jure* (исключительным правом) и монополией *de facto* (самостоятельными превентивными мерами, основанными на общем дозволении это делать).

ее несанкционированного использования, именуемый обычно фактической монополией. Преднамеренно скрываемые сведения невозможно заключить в рамки исключительных прав, поскольку фактор их неизвестности не позволяет установить самого содержания информации в качестве объекта охраны, т. е. формализовать объективные границы тайны и идентифицировать ее без угрозы раскрытия. В данном случае нельзя, как это сделано в отношении результатов интеллектуальной деятельности, нормативно определить меру возможного поведения обладателя информации, кроме общего правила об установлении этой меры им самим либо специальных правил, определяющих последствия распространения закрытых сведений с точки зрения нанесения ущерба вследствие такого распространения.

Исключение от использования и исключение от доступа — внешне схожие термины, но эта схожесть не может служить основанием считать второй из них содержанием некоего исключительного права, поскольку у обладателя закрытой информации нет самого субъективного права, а имеется лишь общее дозволение либо позитивное обязывание на сокрытие от третьих лиц тех сведений, которые представляют для ее обладателя коммерческую или иную ценность либо угрозу его интересам и безопасности.

3. В действующем законодательстве России отсутствует единое понятие конфиденциальной информации, равно как и четкое определение ее структурного состава. Согласно ст. 2 комментируемого Закона и ст. 2 Федерального закона «Об участии в международном информационном обмене»¹, в качестве конфиденциальной признается документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Таможенный кодекс РФ определяет конфиденциальную информацию как информацию, не являющуюся общедоступной

¹ СЗ РФ. 1996. № 28. Ст. 3347.

и могущую нанести ущерб правам и охраняемым законом интересам представившего ее лица.

Что касается структуры относящихся к конфиденциальным сведений, то она также отличается разнообразием подходов законодателя. В комментируемом Законе предпринята попытка обозначения круга сведений конфиденциального характера, но прямо об этом сказано только в отношении персональных данных и опосредованно — в отношении информации о частной жизни, информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Большею упорядоченностью отличается перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 6 марта 1997 г. № 188¹. В этот перечень включены:

- персональные данные — сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральным законом случаях²;
- тайна следствия и судопроизводства;
- служебная тайна — служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами;
- профессиональная тайна — сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариаль-

¹СЗРФ. 1997. № 10. Ст. 1127.

² Более узкое значение понятию персональных данных придает Трудовой кодекс РФ. Согласно ст. 85 Трудового кодекса, персональные данные работника — информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника//Российская газета, 2002, 31 декабря.

ная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений);

- коммерческая тайна— сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Таким образом, специфику правового режима конфиденциальной информации следует искать в особенностях режимов отдельных блоков закрытых сведений, которые законодатель относит к тем либо иным разновидностям тайн.

4. Согласно п. 1 ст. 139 ГК РФ, информация составляет 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. Сведения, которые не могут составлять коммерческую тайну, определяются законом и иными правовыми актами.

Из этого определения вытекают юридически значимые признаки информации, наличие которых придает ей режим коммерческой тайны. Такими признаками выступают:

- неизвестность информации третьим лицам;
- недоступность информации третьим лицам.

Первый из названных признаков является фактором, который придает информации действительную или потенциальную коммерческую ценность, т. е. сообщает ей качество товара, способного выступать источником получения прибыли. Факт приобретения информации, равнозначный знакомству с субъективно новыми сведениями на предложенных их обладателем условиях, будет свидетельствовать о действительной (реальной) ценности этих сведений.

Потенциальной коммерческой ценностью информация будет обладать в случае ее невостребованности возможными приобретателями в данный период времени в силу, например, недостаточности усилий обладателя закрытых сведений, направленных на пропаганду эффекта от их применения. Будучи востребованной, информация из разряда потенциально ценной перейдет в действительно ценную. При этом важна лишь коммерческая сторона ценности информации, отражающая ее прагматическое свойство служить источником получения прибыли, а, скажем, не научная, которая в сфере товарно-денежных отношений не является или очень редко является надлежащим критерием ценности.

Второй из выделенных признаков информации — ее недоступность — характеризует меру свободы получения сведений. Мера свободы доступа к информации определяется ее обладателем путем установления соответствующих правил обращения к закрытым сведениям.

Перечень сведений, которые не могут находиться в режиме коммерческой тайны, установлен постановлением Правительства РСФСР от 5 декабря 1991 г. №35¹. Это сведения, которые содержатся в учредительных документах и уставах предприятий или учреждений; в документах, дающих право заниматься предпринимательской деятельностью; в документах о платежеспособности; в справках об уплате налогов и обязательных платежах; сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственный бюджет России; информация о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест; данные о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации про-

¹СПРФ. 1992. № 1-2. Ст. 7.

дукции, причиняющей вред здоровью населения, а также о других нарушениях законодательства и размерах причиненного при этом ущерба; сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Кроме того, государственным и муниципальным предприятиям до и в процессе приватизации запрещено относить к коммерческой тайне данные о размерах имущества предприятия и его денежных средствах; о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий; данные о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РФ и заключенных им договоров, о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

Приведенный перечень не является закрытым, более того, он может применяться в ограниченных случаях, определенных целями издания постановления Правительства РСФСР № 35, в качестве которых названы: обеспечение деятельности государственной налоговой службы, правоохранительных и контролирующих органов, а также предупреждение злоупотреблений в процессе приватизации.

В ряде федеральных законов имеются нормы, содержащие свои составы сведений, как относимых, так и не включаемых в число закрытых и находящихся в режиме коммерческой тайны. Так, согласно п. 4 ст. 10 Федерального закона «О бухгалтерском учете»¹, содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности является коммерческой тайной. В соответствии с п. 7 ст. 19 Федерального закона «О благотворительной деятельности и благотворительных организациях»², сведения о размерах и структуре доходов

¹СЗ РФ 1996. № 48. Ст. 5369.

²СЗ РФ 1995 № 33. Ст. 3340.

благотворительной организации, а также сведения о размерах ее имущества, ее расходах, численности работников, об оплате их труда и о привлечении добровольцев не могут составлять коммерческую тайну.

5. Категория служебной тайны по смыслу ст. 139 ГК РФ находится в одном ряду с коммерческой тайной и ей, соответственно, должны быть присущи все признаки режима последней. Однако подобный подход законодателя вряд ли может быть признан оптимальным, поскольку акцент на наличие действительной или потенциальной коммерческой, а не служебной ценности сведений, нивелирует самостоятельность института служебной тайны. Очевидно, что подобная самостоятельность должна конституироваться исходя из своеобразия служебных интересов организаций и учреждений по отношению к их коммерческим интересам. Соответственно, критерием разграничения сведений, находящихся в режиме коммерческой либо служебной тайны, должен быть характер интересов обладателя информации, охраняемых посредством ее закрытия. Если раскрытие информации повлечет за собой ущерб коммерческим интересам ее обладателя, налицо состав сведений, подлежащий установлению в отношении его режима коммерческой тайны. Если подобное раскрытие имеет следствием ущерб служебным интересам (интересам службы в широком смысле, включающем и служебные интересы коммерческих организаций), мы можем говорить о составе сведений, подлежащем установлению в отношении его режима служебной тайны.

В то же время признаки неизвестности информации и недоступности к ней третьих лиц должны выступать в качестве основополагающих при придании сведениям служебного характера режима служебной тайны. При этом неизвестность информации, если пользоваться аналогией режима коммерческой тайны, должна придавать служебным сведениям некую ценность, т. е. сообщать им качество полезности при исполнении служебных обязанностей и принятии управленческих ре-

шений, которого было бы невозможно достичь при общеизвестном характере этих сведений.

В отношении недоступности служебной информации третьим лицам, которая, как было показано выше, определяется мерой свободы доступа, оформляемой правилами обращения к закрытым сведениям, действующее законодательство не содержит ясно сформулированной позиции и, прежде всего, по вопросу о том, кто определяет порядок доступа к конфиденциальным сведениям служебного характера и кто, собственно, уполномочен закрывать их. По смыслу Указа Президента РФ от 6 марта 1997 г. № 188, доступ к служебным сведениям ограничивается органами государственной власти, а согласно ст. 139 ГК РФ, любым обладателем информации, «составляющей» служебную тайну. Представляется, что сведения служебного характера могут формироваться и циркулировать не только в органах государственной власти, но и в любых иных учреждениях и организациях, которые вправе самостоятельно диктовать в своих же интересах правила доступа к сведениям с целью сохранения их конфиденциальности и тем самым служебной ценности.

Действующим законодательством не установлен исчерпывающий состав сведений, требующих их закрытия в режиме служебной тайны. В отдельных федеральных законах между тем содержатся нормы, позволяющие говорить об имеющей место демаркации, осуществленной законодателем в отношении коммерческой и служебной тайны. Так, согласно п. 2 ст. 12 Федерального закона «Об основах государственной службы Российской Федерации»¹, поступающие в органы государственной налоговой службы сведения о полученных государственными служащими доходах и имуществе, принадлежащим им на праве собственности, составляют служебную тайну. Режим служебной тайны распространяется, согласно ст. 155 УК РФ, в отношении фактов усыновления (удочерения).

¹ СЗ РФ. 1995. № 31. Ст. 2990.

Перечень сведений, которые не могут быть отнесены к разряду служебной информации ограниченного распространения, определен в постановлении Правительства РФ от 3 ноября 1994 г. № 1233¹. В этот перечень включены: акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов; описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес; порядок рассмотрения и разрешения заявлений, в том числе юридических лиц: сведения об исполнении бюджета и использования других государственных ресурсов, о состоянии экономики и потребностей населения; документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организации, необходимые для реализации прав, свобод и обязанностей граждан.

6. Банковская тайна как режим сведений, не подлежащих разглашению их третьим лицам, представляет собой самостоятельный вид тайны. В отличие от сведений служебного или коммерческого характера, чья ценность определяется в первую очередь фактором их неизвестности, неизвестность сведений, находящихся в режиме банковской тайны, не является определяющим ее признаком, хотя он и должен присутствовать в качестве элемента, присущего любой из разновидностей тайн.

Статьей 857 ГК РФ установлено, что банк гарантирует тайну банковского счета и банковского вклада, операций по счету и

¹ Информационно-правовая система «Кодекс».

сведений о клиенте. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом. Аналогичное правило содержится и в ст. 26 Федерального закона «О банках и банковской деятельности»¹, которая расширила регулятивную сферу отношений ст. 857 ГК РФ, распространив обязанность гарантии тайны не только на банки, но и на иные кредитные (небанковские) организации. Кроме того, в режиме банковской тайны должны находиться сведения об операциях, счетах и вкладах не только клиентов, но корреспондентов.

Таким образом, законодатель очертил круг сведений, в отношении которых должен быть установлен режим конфиденциальности. Ценность этих сведений определяется, прежде всего, их содержанием, которое фиксируется специальными договорами, опосредующими расчетные и кредитные отношения, а также отражается в механизмах движения денежных ресурсов.

Информация, находящаяся в режиме банковской тайны, характеризуется, помимо ценностного аспекта содержания сведений, и мерой свободы их получения. Сегодня сфера санкционированного доступа к сведениям, находящимся в режиме банковской тайны, как, впрочем, и других тайн, значительно расширена. Это произошло вследствие принятия Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем»². Согласно ст. 9 названного закона, предоставление по запросу уполномоченного органа информации и документов органами государственной власти РФ, органами государственной власти субъектов

¹ ВС РСФСР. 1990. № 27. Ст. 357; СЗ РФ. 1996. № 6. Ст. 492; 1998. № 31. Ст. 3829; 1999. № 28. Ст. 3469; Российская газета. 2001. 23 июня.

² Российская газета. 2001. 9 августа.

РФ, органами местного самоуправления и Центральным банком РФ в целях и порядке, которые предусмотрены федеральным законом, не являются нарушением служебной, банковской, налоговой и коммерческой тайны. Данная норма получила развитие в ст. 3 Федерального закона «О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и терроризму"»¹, дополнившей ст. 26 Федерального закона «О банках и банковской деятельности» правилом, в соответствии с которым информация по операциям юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, и физических лиц, предоставляется кредитными организациями в уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем. Указанную информацию уполномоченный орган не вправе раскрывать третьим лицам.

7. Основополагающим элементом государственной тайны по действующему законодательству выступают защищаемые государством отдельные категории сведений, перечень которых сгруппирован в ст. 5 Закона РФ «О государственной тайне» по важнейшим направлениям деятельности государства. Понятие перечня сведений, составляющих государственную тайну, занимает исключительно важное место в процессе конституирования института информации, режим которой определяется как государственная тайна. Поэтому не случайно законодатель посвящает этому перечню специальный раздел Закона РФ «О государственной тайне».

Под перечнем сведений, составляющих государственную тайну, понимается совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установ-

¹ Российская газета. 2001. 9 августа.

ленных федеральным законодательством. Категории сведений связаны с конкретными областями деятельности государства. Так, в состав сведений в военной области (военная тайна) включены, в частности, сведения о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов; о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники; о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов; о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники; о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации; о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения.

К составу сведений в области экономики, науки и техники, подлежащих нахождению их в режиме государственной тайны, отнесены, в частности, сведения о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях Промышленности по изготовлению и ремонту вооружения и военной техники; об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства; об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции; о достижениях науки

и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства.

К сведениям в области внешней политики и экономики отнесены, в частности, сведения о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства; о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства.

К сведениям, составляющим государственную тайну в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в частности, отнесены: сведения о силах, средствах, об источниках, о методах, планах и результатах этих видов деятельности, а также данные о финансировании этой деятельности; о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность; о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения; о методах и средствах защиты секретной информации; о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Приведенный выше перечень сведений является весьма обобщенным, но он составляет ту основу, на фундаменте которой формируются более детальные составы сведений, от-

носимых в установленном порядке к информации, находящейся в режиме государственной тайны.

На основе базового перечня сведений, составляющих государственную тайну, сформулированного в ст. 5 Закона РФ «О государственной тайне» и в соответствии с п. 2. ст. 4 названного Закона, Президент РФ утверждает подробный Перечень сведений, отнесенных к государственной тайне, в котором помимо собственно сведений указываются государственные органы, наделенные полномочиями по их распоряжению¹. Данный Перечень периодически и по мере надобности пересматривается в соответствии с принципами отнесения сведений к государственной тайне и засекречивания этих сведений.

Указанные принципы нашли свое закрепление в ст. 6 Закона РФ «О государственной тайне». К ним отнесены принципы законности, обоснованности и своевременности.

Под законностью отнесения сведений к государственной тайне понимается соответствие засекречиваемых сведений законодательству РФ о государственной тайне и, в частности, перечню сведений, составляющих государственную тайну.

Обоснованность отнесения сведений к государственной тайне и их засекречивания заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивания состоит в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

¹ В настоящее время действует Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203 в ред. Указов Президента РФ от 24 января 1998 г. № 61, от 6 июня 2001 г. № 659, от 10 сентября 2001 г. № 1114 от 29 мая 2002 г. № 518 //СЗ РФ. 1995. № 49. Ст. 4775; 2001. № 24. Ст. 2418; 2001. № 38. Ст. 3724. 2002. № 22. Ст. 2714.

8. Пункт 3 комментируемой статьи определяет перечень документов, содержащих информацию, запрещено относить к категории ограниченно доступной. Аналогичный перечень содержится и Закон РФ «О государственной тайне».

В соответствии со ст. 7 названного Закона, не подлежат отнесению к государственной тайне и засекречиванию сведения о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности; о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, организациям; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах РФ; о состоянии здоровья высших должностных лиц РФ; о фактах нарушения законности органами государственной власти и их должностными лицами.

9. Пункт 4 комментируемой статьи содержит отсылочную норму к Закону РФ «О государственной тайне», разделом III которого установлены правила отнесения сведений к государственной тайне и их засекречивания.

10. Пункт 5 комментируемой статьи устанавливает правило, согласно которому отнесение информации к разряду конфиденциальной, устанавливается в порядке, предусмотренном законодательством РФ. Термин законодательство в данном случае следует толковать распространительно и включать в него не только федеральные законы, но также и подзаконные акты. Исключение сделано в отношении персональных данных, перечни которых подлежат закреплению на уровне федерального закона.

Статья 11. Информация о гражданах (персональные данные)

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов

субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.

Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании ст. 14 и 15 настоящего Федерального закона и законодательства о персональных данных.

1. В соответствии с п.1 комментируемой статьи, персональные данные отнесены к категории конфиденциальной информации, что обусловлено тесной связью сведений, относящихся к конкретному человеку, с его правом на неприкосновенность частной жизни, т. е. той особой сферы семейных, бытовых, личных и интимных отношений, которая не подлежит контролю со стороны государства. Это право не абсолютно и в случаях, установленных законом, может быть ограничено.

Подобное ограничение продиктовано вынужденной необходимостью, связанной с решением проблем борьбы с преступностью, защитой прав, здоровья граждан и т. п.

Таким образом, правовой режим персональных данных должен основываться на разрешении объективно существующего противоречия между неприкосновенностью частной жизни и вынужденной необходимостью сбора, хранения, использования и передачи определенных сведений об этой жизни. Составы этих сведений, оформленные соответствующими перечнями, в случае включения их в различного рода информационные ресурсы, должны быть закреплены на уровне федерального закона. Для всех видов юридически значимых действий с персональными данными должен быть присущ принцип единства их целевого назначения, который означает, что персональные данные хранятся, используются и передаются только для достижения тех целей, ради которых они собирались.

Правовое регулирование отношений на каждой из стадий работы с персональными данными имеет свою специфику.

На стадии сбора сведений, составляющих персональные данные, должно соблюдаться правило, согласно которому персональные данные, за исключением случаев, предусмотренных законодательством, должны быть получены от лица, к которому они относятся. Это правило нашло отражение, в частности, в п. 3 ст. 86 Трудового кодекса РФ, согласно которому все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и у него должно быть получено письменное согласие.

В ряде случаев действующее законодательство содержит запреты на сбор отдельных сведений. Так, в соответствии с п. 2 ст. 8 Федерального закона «Об основах государственной службы Российской Федерации», запрещается сбор и внесение в личные дела и реестры государственных служащих све-

дений об их политической и религиозной принадлежности, а также о частной жизни.

Хранение информации, носящей характер персональных данных, должно обеспечивать исключение возможности несанкционированного доступа к ней. Это достигается выбором соответствующей формы хранения, которая позволяет безошибочно идентифицировать конкретного субъекта в течение определенного периода его жизнедеятельности. Данный период, по общему правилу, не должен превышать срока, определяемого потребностями, для удовлетворения которых осуществлялся сбор персональных данных.

Важным вопросом, который необходимо решить при хранении персональных данных, является вопрос о доступе лиц к своим персональным данным и их корректировке в необходимых случаях. Наиболее последовательно указанный вопрос решен в ст. 89 Трудового кодекса РФ в отношении персональных данных, хранящихся у работодателя. Согласно нормам названной статьи, работники, в частности, имеют право на: полную информацию об их персональных данных и обработку этих данных; свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом; требование об исключении или исправлении неверных или неполных персональных данных.

Использование персональных данных должно осуществляться в пределах целей их сбора и объема потребностей применения. Это отвечает принципу единства целевого назначения сведений, составляющих персональные данные. В действующем законодательстве существуют правила, указывающие на необходимость использования персональных данных по целевому назначению. Согласно ст. 88 Трудового кодекса РФ, в обязанность работодателя входит предупреждение лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены,

и требование от этих лиц подтверждения того, что это правило соблюдено.

Передача персональных данных в настоящее время широко распространенное явление, и в этой связи проблема нормативного закрепления порядка распространения сведений персонального характера весьма актуальна. Здесь возникает достаточно широкий перечень вопросов, разрешение которых связано, прежде всего, с определением оснований передачи таких сведений, круга субъектов, которым передаются данные и которые их передают, видов персональных данных, подлежащих передаче, форм и условий передачи. Очевидно, что передача сведений персонального характера может допускаться лишь в случаях и порядке, установленных законодательством. Примером тому служит правило п. 1 ст. 6 Федерального закона «О государственной регистрации юридических лиц»¹, в соответствии с которым паспортные данные физических лиц и их идентификационные номера налогоплательщиков могут быть предоставлены исключительно по запросам органов государственной власти, в соответствии с их компетенцией².

В абз. 2 комментируемого пункта получили отражение конституционные положения, закрепленные в части второй ст. 23 и части первой ст. 24 Конституции РФ, которые провозглашают право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, т. е. сообщений, переданных с использованием доступных технических каналов связи, а равно налагают запрет на сбор, хранение, использование и распространение информации о частной жизни. Всякое ограничение названных тайн (режимов инфор-

¹СЗ РФ. 2001. № 33. Ст. 3431.

² По смыслу цитированной ст. 6 Федерального закона «О государственной регистрации юридических лиц», сведения об идентификационном номере налогоплательщика не являются открытыми и общедоступными, но они в то же время, согласно ст. 102 Налогового кодекса РФ, «не составляют» и налоговую тайну. В этой связи представляется целесообразным отнести указанные сведения в разряд персональных данных.

мации) в силу прямого указания Конституции РФ требует судебного решения.

2. В п. 2 комментируемой статьи законодатель делает акцент на запрет использования персональных данных, имеющего целью причинение имущественного и морального вреда, затруднения реализации прав и свобод граждан России. Пол вредом (в гражданском праве) чаще всего понимают умаление какого-либо имущественного либо личного блага. Имущественный вред — это потери, которые выражаются в уменьшении стоимости вещи, в производстве дополнительных расходов, в уменьшении ожидаемого дохода и т. п. Моральный вред — это нравственные или физические страдания гражданина, которые вызваны умалением его личных благ либо нарушением личных неимущественных прав.

Второе предложение п. 2 комментируемой статьи воспроизводит конституционную норму, запрещающую любые формы ограничения прав граждан по признакам социальной, расовой, национальной, языковой или религиозной принадлежности (ч. 2 ст. 19 Конституции РФ). Наличие у гражданина указанных признаков не должно служить основанием для какого-либо ущемления его прав и свобод. Более того, согласно ч. 1 ст. 282 УК РФ, пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, национальной или расовой принадлежности является уголовно наказуемым деянием и, если оно совершено публично или с использованием средств массовой информации, наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок от двух до четырех лет. Аналогичная норма за деяния, нарушающие равноправие граждан, содержится и в ст. 136 УК РФ.

3. В п. 3 комментируемой статьи формулируется правило, указывающее на необходимость применения мер юридиче-

ской ответственности за нарушение режима защиты, обработки и порядка использования информации о гражданах. Меры такого рода, ответственность установлены нормами УК РФ и КоАП РФ.

Так, согласно ч. 1 ст. 137 УК РФ, незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, — наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

Административно-правовые санкции предусмотрены, в частности, ст. 13.14 КоАП, в соответствии с которой, разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, — влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц — от сорока до пятидесяти минимальных размеров оплаты труда.

4. Пункт 4 комментируемой статьи дублирует положения Закона РФ «Об обжаловании в суд действий и решений, нарушающих права и свободы граждан»¹, согласно ст. 1 которого каждый гражданин вправе обратиться с жалобой в суд, если счи-

¹ Ведомости РФ. 1993. № 19. Ст. 685.

тает, что неправомерными действиями (решениями) государственных органов, органов местного самоуправления, организаций, общественных объединений или должностных лиц, государственных служащих нарушены его права и свободы.

В комментируемом пункте уточняется, что в судебном порядке могут быть обжалованы: отказ владельца информационных ресурсов субъекту в доступе к информации о нем (п. 4 ст. 14 комментируемого Закона) и действия владельца или собственника информационных ресурсов, влекущие нарушение режима обработки и правил предоставления информации пользователю (п. 1 ст. 15 комментируемого Закона).

Глава 3

ПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

Статья 12. Реализация права на доступ к информации из информационных ресурсов

1. Пользователи — граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения — обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению.

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов.

3. Порядок получения пользователем информации (указание места, времени, ответственных должностных лиц, необходимых процедур) определяет собственник или владелец информационных ресурсов с соблюдением требований, установленных настоящим Федеральным законом.

Перечни информации и услуг по информационному обеспечению, сведения о порядке и условиях доступа к информационным ресурсам владельцы информационных ресурсов и информационных систем предоставляют пользователям бесплатно.

4. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций.

5. Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенными вид и массивы информации, в соответствии с их компетенцией либо непосредственно ее собственником в соответствии с законодательством.

1. Комментируемая статья посвящена регулированию отношений, складывающихся по поводу реализации права на доступ к информации, содержащейся в информационных ресурсах.

Принято считать, и это подкрепляется нормативными предписаниями, что доступ к информации — это получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств¹. Представляется, что юридически обеспеченную возможность ознакомления с теми либо иными документами следует рассматривать как право на ознакомление, но не право на доступ. Без реализации права на доступ невозможно реализовать право на ознакомление. Кроме того, право на доступ должно устанавливаться в отношении не общедоступных сведений. Общедоступные сведения не нуждаются в специальном юридическом механизме доступа. Правом на ознакомление может быть наделено только физическое лицо.

Право на доступ к информации, продекларированное в комментируемом законе, базируется на положении части второй ст. 24 Конституции РФ, обязывающем органы государственной власти и органы местного самоуправления, их должностных лиц обеспечить каждому возможность ознаком-

¹ ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

ления с документами и материалами, непосредственно затрагивающими его права и свободы.

В п. 1 комментируемой статьи закреплена норма о равенстве прав на доступ к государственным информационным ресурсам граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений.

При реализации права на доступ к государственным информационным ресурсам (за исключением государственных информационных ресурсов, содержащих информацию с ограниченным доступом) пользователи не обязаны обосновывать необходимость получения запрашиваемой ими информации.

Доступ физических и юридических лиц к государственным информационным ресурсам рассматривается законодателем в качестве основы осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер жизнедеятельности¹.

2. Первое предложение п. 2 комментируемой статьи устанавливает две формы обеспечения пользователей (потребителей) информацией, содержащейся в информационных ресурсах: внедоговорную и договорную.

Внедоговорная форма обеспечения информацией обусловлена отношениями, возникающими по поводу предоставления информации, собираемой органами и организациями в силу предоставленных им полномочий и компетенции за счет соответствующих бюджетных средств. Примером внедоговорной формы обеспечения информацией может служить норма п.1 ст. 7 Федерального закона «О государственной регистрации прав на недвижимое имущество и сделок с ним»¹ согласно ко-

¹ См. Постановление Правительства РФ от 12 февраля 2003 г. № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и Федеральных органов исполнительной власти»//Российская газета. 2003. 15 февраля.

² СЗ РФ. 1997. № 30. Ст. 3594.

торой орган, осуществляющий государственную регистрацию прав, обязан предоставлять сведения, содержащиеся в Едином государственном реестре прав, о любом объекте недвижимости любому лицу, предъявившему удостоверение личности и заявление в письменной форме (юридическому лицу — документы, подтверждающие регистрацию данного юридического лица и полномочия его представителя).

Договорная форма обеспечения информацией лежит в плоскости частноправовых отношений. В рамках этих отношений с одной стороны выступают хозяйствующие субъекты, осуществляющие информационную деятельность на профессиональной основе, а с другой — пользователи. На практике возможно заключение множества различных видов договоров, предметом которых является передача определенной информации либо оказание услуг по информационному обеспечению. К последним, в частности, следует отнести договоры об оказании консалтинговых, инжиниринговых и маркетинговых услуг.

Комментируемым пунктом вводится понятие производной информации, под которой следует в данном случае понимать сведения, полученные путем переработки информации, полученной на законных основаниях из государственных информационных ресурсов. Степень переработки исходной (первичной) информации является юридически безразличным параметром. По существу, исходная информация может быть просто зафиксирована на другом носителе со ссылкой на источник и реализована путем коммерческого распространения. По мысли законодателя (абз. 3 комментируемого пункта) источником прибыли в этом случае является результат вложенных трудов (перезапись на другой носитель) и средств (сам носитель), но не исходная информация, полученная из государственных ресурсов. На практике дело обстоит несколько иначе, поскольку коммерческую ценность представляет не вложенный в создание производной информации труд и средства, но субъективная новизна реализуемой информации.

Особым спросом, например, пользуются брошюры, содержащие тексты только что принятых нормативно-правовых актов.

3. Порядок получения информации пользователем определяет собственник или владелец информационных ресурсов с указанием места, времени, ответственных должностных лиц, необходимых процедур. При этом условия получения информации не должны выходить за рамки требований, установленных комментируемым Законом. Перечни, характеризующие содержание информации и услуг по информационному обеспечению, а также сведения о порядке и условиях доступа к информационным ресурсам предоставляются пользователям бесплатно.

Очевидно, что пользователь, реализуя свое право на получение информации из государственных ресурсов, может требовать представления только тех сведений, которыми располагает владелец и собственник информационного ресурса.

4. В п. 4 содержится норма, закрепляющая обязанность органов государственной власти и организаций, ответственных за формирование и использование информационных ресурсов по обеспечению условий для оперативного и полного предоставления пользователям документированной информации. Данная обязанность должна соответствовать полномочиям органов и организаций, определенных их уставами или положениями о них.

Так, согласно п. 3 ст. 8 Федерального закона «О государственной регистрации прав на недвижимое имущество и сделок с ним», органы государственной власти субъектов РФ и органы местного самоуправления, организации по учету объектов недвижимого имущества, другие организации, имеющие сведения, необходимые для государственной регистрации прав на объекты недвижимого имущества, в срок не более чем десять дней с даты обращения обязаны предоставлять такие сведения правообладателям и учреждениям юстиции по регистрации прав на недвижимое имущество и сделок с ним бесплатно или за плату.

Аналогичная норма закреплена в ст. 6 Федерального закона «О государственной регистрации юридических лиц»¹, в соответствии с которой сведения, содержащиеся в государственном реестре, являются открытыми и общедоступными, за исключением паспортных данных физических лиц и их идентификационных номеров налогоплательщиков.

5. В п. 5 закрепляется правило, устанавливающее право органов государственной власти, ответственных за определенный вид и массивы информации, а равно собственника документированной информации, определять порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней. Наиболее детальную регламентацию сфера данных общественных отношений получила в Законе РФ «О государственной тайне». Так, в ст. 4 названного Закона установлены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты, в ст. 21 определены общие правила допуска должностных лиц и граждан к государственной тайне, в ст. 27 регламентированы вопросы допуска организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. В развитие названных статей Закона РФ «О государственной тайне» Правительством РФ и иными органами государственной власти принят ряд постановлений, конкретизирующих требования закона. Например, допуск должностных лиц и граждан РФ к государственной тайне осуществляется в порядке, установленном Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне; утвержденной постановлением Правительства РФ от 28 октября 1995 г. № 1050². Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к го-

¹ Российская газета. 2001. 10 августа.

² СЗ РФ. 1995. № 43. Ст. 4987.

сударственной тайне осуществляется в порядке, установленном специальным Положением, утвержденным постановлением Правительства РФ от 22 августа 1998 г. № 1003¹. Допуск организаций на проведение работ с использованием сведений, составляющих государственную тайну, определяется в порядке, установленном Инструкцией о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, утвержденной приказом ФСБ России от 23 августа 1995 г. № 28 и согласованной с Гостехкомиссией РФ и ФАПСИ².

Статья 13. Гарантии предоставления информации

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, представляющим общественный интерес.

2. Отказ в доступе к информационным ресурсам, предусмотренным в пункте 1 настоящей статьи, может быть обжалован в суд.

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистрацию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения права граждан на доступ к информации.

4. Перечень информационных услуг, предоставляемых пользователям из государственных информационных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги, устанавливает Правительство Российской Федерации.

Расходы на указанные услуги компенсируются из средств федерального бюджета и бюджетов субъектов Российской Федерации.

¹ СЗ РФ. 1998. № 35. Ст. 4407.

² Бюллетень Государственного комитета Российской Федерации по высшему образованию. 1995. № 11.

1, Комментируемая статья устанавливает гарантии предоставления информации пользователям путем возложения на органы государственной власти и органы местного самоуправления обязанностей по созданию доступных для каждого информационных ресурсов. Содержание таких ресурсов должна составлять информация, касающаяся деятельности этих органов и подведомственных им организаций. При этом массовое информационное обеспечение пользователей распространяется на вопросы, представляющие общественный интерес. В числе таких вопросов законодатель называет вопросы прав, свобод и обязанностей граждан, вопросы их безопасности.

Массовое информационное обеспечение осуществляется, как правило, через средства массовой информации, законодательство о которых содержит институт обязательных сообщений. Согласно ст. 35 Закона РФ «О средствах массовой информации»¹, редакция обязана опубликовать бесплатно и в предписанный срок:

- « вступившее в законную силу решение суда, содержащее требование об опубликовании такого решения через данное средство массовой информации;
- поступившее от органа, зарегистрировавшего данное средство массовой информации, сообщение, касающееся деятельности редакции.

Редакции средств массовой информации, учредителями (соучредителями) которых являются государственные органы, обязаны публиковать по требованию этих органов их официальные сообщения в порядке, регулируемом уставом редакции или заменяющим его договором, а равно иные материалы, публикация которых в данных средствах массовой информации предусмотрена законодательством РФ.

¹ Ведомости РФ. 1992. №72. Ст. 300; СЗ РФ. 1996. №1. Ст. 4; 1998. №10. Ст. 1143; 2000. №26. Ст. 2737; №32. Ст. 3333.

Государственные средства массовой информации обязаны публиковать сообщения и материалы федеральных органов государственной власти и органов государственной власти субъектов РФ в порядке, установленном Федеральным законом «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»¹.

Общественный интерес представляет и так называемая потребительская информация. Обязанности по ее предоставлению установлены, в частности, ст. 8 и 9 Закона РФ «О защите прав потребителей»².

Очевидно, что информационная открытость органов государственной власти и органов местного самоуправления предполагает аналогичную открытость и руководства названных органов. В соответствии со ст. 39 Закона РФ «О средствах массовой информации», руководители государственных органов обязаны предоставлять запрашиваемые редакцией средства массовой информации сведения о деятельности соответствующих государственных органов. Отказ и отсрочка в предоставлении информации возможны лишь по основаниям, сформулированным в ст. 40 указанного Закона.

2. Пункт 2 комментируемой статьи содержит правило о возможности обжалования в судебном порядке действий органов государственной власти и местного самоуправления, выразившихся в отказе к доступу к информационным ресурсам, содержащим информацию, представляющую общественный интерес. Подобного рода отказы не раз были предметом разбирательств Судебной палаты по информационным спорам при Президенте РФ. Так, в решении № 1 от 17 февраля 1994 г. «О нарушении права журналистов радиостанции "Маяк" на получение общественно значимой информации», было сделано замечание директору Управления вкладов и расчетов Сбербан-

¹ СЗ РФ. 1995. №3. Ст. 170.

² Российская газета. 1996. 16 января.

ка, отказавшемуся прокомментировать опубликованный Указ Президента РФ от 24 декабря 1993 г. № 2297 «О единовременных компенсациях вкладчикам Сберегательного банка РФ, имевшим вклады на 1 января 1992 г.», поскольку последний представлял несомненный интерес для слушателей в связи с начинающейся 1 февраля 1994 г. компенсацией вкладов населения. Судебная палата указала на недопустимость нарушения права граждан на информацию и права прессы на получение информации, закрепленных в законодательстве РФ¹. В судах общей юрисдикции подобная практика отсутствует. Во многом это объясняется эффектом блокирования норм, обязывающих органы публичной власти обеспечивать информационную открытость, нормами законодательства об основах государственной (муниципальной) службы. Так, согласно подп. 6. п. 1 ст. 11 Федерального закона «Об основах государственной службы Российской Федерации»², государственный служащий не вправе использовать в неслужебных целях средства информационного обеспечения, другое государственное имущество и служебную информацию. Аналогичная норма сформулирована и в отношении муниципальных служащих.

3. Пункт 3 комментируемой статьи определяет орган, ответственный за организацию регистрации всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения прав граждан на доступ к информации.

Сегодня названная ответственность канализирована в область ведомственной компетенции, в сферы полномочий федеральных органов исполнительной власти, проводящих государственную политику и осуществляющих управление в соответствующих отраслях. Специальными полномочиями по

¹ Информационные споры; как в них победить? Решения, рекомендации, экспертные заключения Судебной палаты по информационным спорам при Президенте РФ/Под ред. А. К. Симонова. М., 2002. С. 39-40.

² СЗ РФ. 1995. № 31. Ст. 2990.

организации регистрации информационных ресурсов и систем наделено Министерство РФ по связи и информации¹.

При Президенте РФ образовано Информационное управление Президента РФ, являющееся самостоятельным подразделением Администрации Президента РФ. Положение об Информационном управлении утверждено Указом Президента РФ от 5 ноября 2001 г. № 1274². Основными функциями Управления являются: обеспечение деятельности Президента РФ в области государственной информационной политики в целях реализации главой государства своих конституционных полномочий; подготовка предложений Президенту РФ, касающихся формирования российского информационного пространства, а также участие по поручению Президента РФ в реализации указанных предложений.

4. Комментируемая статья определяет компетенцию Правительства РФ по установлению перечня информационных услуг, предоставляемых пользователям из государственных информационных ресурсов безвозмездно или на возмездной основе. Такого перечня сегодня не существует. Отдельные фрагменты из возможного перечня информационных услуг получают косвенное опосредование в нормативно-правовых актах Правительства РФ и ведомственных актах. Так, согласно п. 4 Правил распространения периодических печатных изданий по подписке, утвержденных постановлением Правительства РФ от 1 ноября 2001 г. № 759³, информация о периодическом печатном издании доводится до сведения подписчиков редакциями, издателями и распространителями путем издания каталогов периодических печатных изданий, через средства массовой информации, при помощи рекламы и другими способами.

Расходы на услуги, предоставляемые пользователям государственных информационных ресурсов, полагается, по

¹ СЗ РФ. 2000. № 14. Ст. 1498.

² СЗ РФ. 2001. № 46. Ст. 4344.

³ Российская газета. 2001. 6 ноября.

смыслу абз. 2 п. 4 комментируемой статьи, компенсировать из средств федерального бюджета и бюджетов субъектов РФ.

Статья 14. Доступ граждан и организаций к информации о них

1. Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.

2. Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации.

3. Субъекты, представляющие информацию о себе для комплектования информационных ресурсов на основании ст. 7 и 8 настоящего Федерального закона, имеют право бесплатно пользоваться этой информацией.

4. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

1. Пункт 1 комментируемой статьи в содержательном аспекте дублирует норму части 2 ст. 24 Конституции РФ, устанавливающую право доступа лиц к документированной информации о них, которую соответствующие органы государственной власти и органы местного самоуправления, располагающие этой информацией, обязаны предоставить гражданам и организациям. Целями подобного доступа являются обеспечение полноты и достоверности, имеющихся сведений о гражданах и организациях, а также знание о том, кто и в каких целях использует или использовал указанные сведения.

Существуют две основные возможности осуществления права на доступ к документированной информации о лицах.

Первая из них заключается в создании общедоступных реестров, в которых фиксируются и обнародуются те либо иные сведения об организациях и гражданах. Примерами подобного рода

реестров являются государственный реестр, содержащий сведения о создании, реорганизации и ликвидации юридических лиц, предусмотренный главой II Федерального закона «О государственной регистрации юридических лиц», федеральный реестр государственных служащих и реестры государственных служащих субъектов РФ, предусмотренные ст. 8 Федерального закона «Об основах государственной службы Российской Федерации».

В соответствии с п. 4 ст. 5 Федерального закона «О государственной регистрации юридических лиц» юридическое лицо в течение трех дней с момента изменения сведений о нем обязано сообщить об этом в регистрирующий орган по месту своего нахождения. Согласно п. 2 ст. 6 указанного Закона, содержащиеся в государственном реестре сведения о конкретном юридическом лице предоставляются в виде: выписки из государственного реестра; копии документа (документов), содержащегося в регистрационном деле; справки об отсутствии запрашиваемой информации.

В соответствии со ст. 8 Федерального закона «Об основах государственной службы Российской Федерации», сведения о государственных служащих, в том числе сведения о государственных служащих, включенных в резерв на выдвижение на вышестоящие государственные должности, вносятся в соответствующие реестры. Согласно подп. 7 п. 1 ст. 9 названного Закона, государственный служащий имеет право на ознакомление со всеми материалами своего личного дела, отзывами о своей деятельности и другими документами до внесения их в личное дело, приобщение к личному делу своих объяснений.

Вторая возможность осуществления права на доступ к документированной информации о лицах состоит в законодательно закрепленном праве лиц запрашивать соответствующие органы и организации о том, содержится ли у них относящаяся к данному лицу информация и каково ее содержание. Так, согласно ст. 20 Основ законодательства Российской Федерации об Архи-

вном фонде Российской Федерации и архивах¹, граждане, учреждения, организации и предприятия, а также общественные и религиозные объединения и организации имеют право получать заверенные копии из архивных документов и выписки из архивных документов, хранящихся в государственных архивах или архивах организаций, или самостоятельно изготавливать копии этих документов и делать выписки из них, если это не угрожает физической сохранности документов.

Ограничения права на доступ лиц к касающейся их² информации допустимо лишь по основаниям, предусмотренным федеральными законами. Не подлежит, в частности, предоставлению информация о частной жизни другого лица без его согласия (персональные данные), об осуществлении оперативно-розыскной и следственной деятельности, о судебном рассмотрении гражданских и уголовных дел в случаях, когда разглашение этих сведений запрещено законом либо может нарушить право гражданина на объективное судебное рассмотрение его дела, создать угрозу жизни или здоровью граждан.

2. Пункт 2 комментируемой статьи возлагает на владельца документированной информации о гражданах обязанность безвозмездного ее предоставления по требованию тех лиц, которых она касается. Так, согласно ст. 89 Трудового кодекса Российской Федерации, в целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника.

Ограничения на безвозмездное получение документированной информации о гражданах возможно лишь по основаниям, установленным законодательством РФ.

¹ Ведомости РФ. 1993. № 33. Ст. 1311.

² См., также постановление Правительства РФ от 10 марта 1999 г. № 266 «О порядке ведения единого государственного реестра налогоплательщиков»//СЗ рф. 1999. № 11. Ст. 1307.

3. В п. 3 комментируемой статьи очерчивается круг лиц, имеющих право безвозмездного пользования информацией. К ним относятся граждане и организации, участвовавшие или участвующие по своему желанию в формировании государственных информационных ресурсов (п. 2 ст. 7 комментируемого Закона), а также граждане и организации, обязанные в установленном порядке представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов (п. 1 ст. 8 комментируемого Закона).

4. Пунктом 4 предусматривается возможность обжалования действий владельца информационных ресурсов, отказавшего гражданину или организации в доступе к информации о них, в судебном порядке.

Статья 15. Обязанности и ответственность владельца информационных ресурсов

1. Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством Российской Федерации или собственником этих информационных ресурсов, в соответствии с законодательством.

2. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

1. Комментируемая статья устанавливает обязанность владельца информационных ресурсов и определяет характер его ответственности за нарушение правил работы с информацией.

Законодатель выделяет две группы обязанностей.

Первая включает в себя обязанности по обеспечению соблюдения режима обработки информации. Вторая — объемлет обязанности по обеспечению соблюдения правил предоставления информации пользователю, установленных законо-

дательством РФ или собственником информационных ресурсов, в соответствии с законодательством.

Режим обработки информации является одним из элементов порядка движения документов в организации¹. Выделяются несколько разновидностей обработки, в частности, экспедиционная обработка документов, поступающих в организацию, обработка исполненных документов, экспедиционная обработка отправляемых документов. Это стандартные виды обработки, которые должны осуществляться с соблюдением ГОСТ 6.10.4-84².

Свои особенности имеет обработка конфиденциальных документов. В отличие от открытых документов, к обработке конфиденциальных документов предъявляется ряд специфических требований, которые позволяют решить задачу обеспечения защиты носителей информации и самой информации от несанкционированного доступа. В литературе по документоведению выделяют, в частности, следующие требования, составляющие технологическую систему обработки конфиденциальных документов:

- централизация всех стадий, процедур и операций по обработке и хранению конфиденциальных документов;
- в операционный учет всех технологических действий, производимых с традиционными (бумажными) или электронными носителями (в том числе чистыми) и документами, учет каждого факта «жизненного цикла» документа;
- « учет всех без исключения конфиденциальных документов;
- в обязательный контроль правильности выполнения учетных операций;

¹ См.: Организация работы с документами: Учебник/Под ред. проф. В. А. Кудряева. М., 2002. С. 152-178; Типовая инструкция по делопроизводству в министерствах и ведомствах Российской Федерации. М., Росархив. 1995.

² ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. М.: Изд-во стандартов. 1985.

- 9 обязательная подпись руководителей, исполнителей и технического персонала при выполнении любых действий с документом в целях обеспечения персональной ответственности сотрудников фирмы за сохранность носителя и конфиденциальность информации;
- письменное фиксирование всех обращений персонала к документу при наличии письменной санкции руководителя;
 - систематические (периодические и разовые) проверки наличия документов у исполнителей, в делах, базах данных, на машинных носителях;
 - ежедневный контроль сохранности, комплектности, целостности и местонахождения каждого конфиденциального документа;
 - коллегиальность процедур уничтожения документов, дел и баз данных¹.

Технологические системы обработки конфиденциальной документированной информации могут быть традиционными, автоматизированными и смешанными.

Обращаясь к правилам представления информации пользователю, следует подчеркнуть, что в целом действующее законодательство весьма скупое регламентирует эту сферу общественных отношений. Наиболее детально данный вопрос урегулирован в законодательстве об архивах и библиотечном деле. Так, правила пользования библиотеками, согласно п. 2 ст. 13 Федерального закона «О библиотечном деле»², утверждаются библиотеками по согласованию с учредителями. При этом порядок доступа к фондам библиотек, перечень основных услуг и условия их предоставления устанавливаются в соответствии с уставами библиотек, законодательством об ох-

¹ Организация работы с документами: Учебник/Под ред. проф. В. А. Кудряева. М., 2002. С. 224-225.

² СЗРФ. 1995. №1. Ст. 2

ране государственной тайны и законодательством об обеспечении сохранности культурного достояния народов РФ.

В соответствии со ст. 20 Основ законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, порядок использования документов государственной части Архивного фонда РФ, находящихся на временном хранении в центральных органах исполнительной власти РФ, в государственных учреждениях, организациях и на предприятиях, определяется ими по согласованию с соответствующими органами и учреждениями системы Федеральной архивной службы России. Порядок использования архивных документов в государственных архивах определяется Федеральной архивной службой России¹.

2. Пункт 2 предусматривает несение владельцем информационных ресурсов юридической ответственности за нарушение правил работы с информацией.

При рассмотрении категории юридической ответственности возникает вопрос об определении содержания этого понятия, которое относится к числу общетеоретических и применяемых в различных отраслях права. Это понятие неоднозначное и в известной мере спорное для юридической науки. Современные интерпретации юридической ответственности полагают ее как одну из форм государственно-принудительного воздействия на нарушителей норм права.

Будучи одним из юридических средств, нейтрализующих последствия ненадлежащего поведения субъекта, нарушающего права и охраняемые законом интересы других лиц, юридическая ответственность выступает как реакция государства за совершенное правонарушение. Эта реакция имеет властный, принудительный характер, понуждающий правонарушителя претерпеть неблагоприятные для него последствия в виде лишения определенных благ. Исходя из этого, содержанием

¹ См.: Основные правила работы ведомственных архивов. М.: Главархив СССР. 1988; Правила работы пользователей в читальных залах государственных архивов Российской Федерации. М.: Росархив, 1998.

юридической ответственности будет выступать государственное властное принуждение, проявляющее себя в различных формах. Вместе с тем не всякое государственное принуждение следует считать ответственностью. Например, принудительное (судебное) воздействие, побуждающее владельца информационных ресурсов, нарушившего предусмотренный законодательством РФ порядок работы с информацией, к исполнению своих обязанностей, не является мерой ответственности, поскольку в данном случае отсутствует элемент дополнительных неблагоприятных последствий для нарушителя, т. е. тех самых лишений, которые выходят за рамки принудительно исполненной обязанности.

Государственное принуждение осуществляется путем применения различных мер воздействия на нарушителя, которые влекут для него различные последствия. От характера этих мер и характера последствий зависит отраслевая принадлежность юридической ответственности. Если неблагоприятные последствия носят имущественный характер и выражаются в возмещении убытков, уплате неустойки, возмещении вреда, имеет место гражданско-правовая ответственность. Если неблагоприятные последствия выражаются в санкциях, предусмотренных нормами административного или уголовного законодательства, имеет место административно-правовая или уголовная ответственность.

Глава 4

ИНФОРМАТИЗАЦИЯ. ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ТЕХНОЛОГИИ И СРЕДСТВА ИХ ОБЕСПЕЧЕНИЯ

Статья 16. Разработка и производство информационных систем, технологий и средств их обеспечения

1. Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

2. Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

3. Государство создает условия для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения.

Правительство Российской Федерации определяет приоритетные направления развития информатизации и устанавливает порядок их финансирования.

4. Разработка и эксплуатация федеральных информационных систем финансируются из средств федерального бюджета по статье расходов «Информатика» («Информационное обеспечение»).

5. Органы государственной статистики совместно с Комитетом при Президенте Российской Федерации по политике информатизации устанавливают правила учета и анализа состояния отрасли экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

1. Комментируемая статья устанавливает основы процесса информатизации в части разработки и производства инфор-

мационных систем и сетей, технологий и средств их обеспечения. Указанная часть объявляется специальной отраслью экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политической информатизации.

Государственная научно-техническая политика, согласно ст. 2 Федерального закона «О науке и государственной научно-технической политике»¹, представляет собой составную часть социально-экономической политики, которая выражает отношение государства к научной и научно-технической деятельности, определяет цели, направления, формы деятельности органов государственной власти РФ в области науки, техники и реализации достижений науки и техники.

Государственная научно-техническая политика в области информатизации, основные направления которой определены в ст. 3 комментируемого Закона, получила наиболее отчетливое выражение в Федеральной целевой программе «Электронная Россия (2002—2010 гг.)»². Реализация последней должна оказать существенное воздействие на все сферы общественной жизни и повысить темпы развития экономики.

Предполагается, в частности, что выполнение программных мероприятий:

- приведет к увеличению количества хозяйствующих субъектов и развитию конкуренции в области информационных и коммуникационных технологий, сокращению доли теневого рынка программного обеспечения, что позволит повысить доходы и увеличить налоговые поступления в бюджет;
- вызовет повышение спроса на продукцию информационных и коммуникационных технологий и обеспечит в период до 2005 г. прирост отечественного производства това-

¹ СЗ РФ. 1996. № 335. Ст. 4137.

² Российская газета. 2002. 12, 19, 27 февраля.

- ров и услуг в этой сфере и рост экспорта в размере 16—20% ежегодно;
- будет способствовать формированию более прогрессивной структуры экономики, создаст принципиально новые возможности для наращивания производства и экспорта отечественной высокотехнологичной продукции;
 - обеспечит кардинальное ускорение процессов информационного обмена в экономике и обществе в целом, в том числе между гражданами и органами государственной власти;
 - повысит эффективность государственного управления и местного самоуправления, создаст принципиально новые возможности для мониторинга процессов в экономике и обществе;
 - позволит сформировать единый порядок сбора, обработки, накопления, хранения, поиска и распространения информации, что существенно повысит возможность координации действий силовых структур и будет способствовать повышению безопасности и обороноспособности страны.

2. В п. 2 комментируемой статьи провозглашается равенство прав государственных и негосударственных организаций, а также граждан на разработку и производство информационных систем, технологий и средств их обеспечения. Это равенство достаточно условно, поскольку по ряду лицензируемых видов деятельности существуют позиции лицензионных требований, выполнение которых всяким и каждым недопустимо.

Так, одним из лицензионных требований при осуществлении деятельности по разработке и (или) производству средств защиты конфиденциальной информации, отнесенных к компетенции ФАПСИ, является наличие у руководителя лицензиата и (или) уполномоченного им лица высшего образования и (или) профессиональной подготовки в области защиты информации с квалификацией «специалист по защите информации»

и производственным стажем в области лицензируемой деятельности не менее 5 лет¹.

3. В п. 3 сформулирована норма, определяющая обязанность государства по созданию условий для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения. Очевидно, что и технологические работы в указанной области также являются предметом заботы государства.

Статья 8 Федерального закона «О науке и государственной научно-технической политике» определяет, что основной правовой формой отношений между научной организацией, заказчиком и иными потребителями научной и (или) научно-технической продукции, в том числе министерствами и иными федеральными органами исполнительной власти, являются договоры (контракты) на создание, передачу и использование научной или научно-технической продукции, оказание научных, научно-технических, инженерно-консультационных и иных услуг, а также другие договоры, в том числе договоры о совместной научной и (или) научно-технической деятельности и распределении прибыли.

На основе указанных договоров (контрактов) выполняются научные исследования и экспериментальные разработки для государственных нужд.

Акцент, сделанный законодателем на договорные отношения в сфере производства научной и научно-технической продукции, обусловлен отказом от планово-административных методов регулирования и переходом к товарно-денежным отношениям.

Научно-исследовательские, опытно-конструкторские и технологические работы могут носить как самостоятельный характер, так и выступать в качестве стадий инновационного

¹ См.: постановление Правительства РФ от 27 мая 2002 г. № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты информации»//Российская газета. 2002. 22 июня.

процесса, которые имеют общепринятое наименование, отражающее существо завершающего их результата¹.

Инновационный процесс начинается со стадии фундаментальных исследований, которые направлены на получение новых научных знаний в конкретной области, в данном случае в области разработки информационных систем, технологий и средств их обеспечения. Второй стадией инновационного процесса являются прикладные исследования. Целью их проведения служит нахождение путей практического применения, полученных на стадии фундаментальных исследований научных знаний. Третья стадия имеет своим содержанием проведение опытно-конструкторских работ. Целью данного вида работ является создание или усовершенствование на базе результатов прикладных исследований образцов новой техники, материалов, разработка новых технологических процессов. Освоение промышленного производства новых информационных систем, технологий и средств является четвертой стадией инновационного процесса. На этой стадии проводятся опытные и экспериментальные работы, имеющие своей целью отработку опытных образцов новой техники и новых технологических процессов. После этапа освоения начинается стадия промышленного производства. Данная стадия имеет своей целью доведение материализованных новых систем, технологий и средств до потребителя.

Инновационный процесс как последовательная цепь этапов, при завершении которых информационная система, технология и средство их обеспечения трансформируются от идеи до конкретного продукта или технологического процесса, может быть упорядочен в рамках отдельных стадий различными гражданско-правовыми договорами.

На стадиях фундаментальных и прикладных исследований отношения по поводу проведения соответствующих исследо-

¹ См.: Коммерческое право. В 2 ч.: Учебник / Под ред. В. Ф. Попондопуло, В. Ф. Яковлевой. М., 2002. Ч. 2. С. 181-211 (автор главы — О. А. Городов).

ваний опосредуются договорами на выполнение научно-исследовательских работ.

На стадии опытно-конструкторских работ отношения по поводу разработки образцов новых информационных систем и средств их обеспечения и конструкторской документации на них регулируются договорами на выполнение опытно-конструкторских и технологических работ.

На стадиях освоения промышленного производства новых или усовершенствованных информационных систем и средств их обеспечения и, собственно, их промышленного производства отношения по поводу производительной деятельности опосредуются договорами подряда.

Доведение новых информационных систем, технологий и средств их обеспечения до потребителей регламентируется различными разновидностями договорных обязательств по передаче имущества или договорами коммерческой концессии.

Все стадии инновационного процесса, за исключением, пожалуй, стадии промышленного производства, могут быть опосредованы широко использовавшимся с конца 80-х гг. прошлого столетия смешанным договором на создание (передачу) научно-технической продукции¹, но с учетом правил ст. 769-778 ГК РФ.

Создавая условия для проведения указанных работ, государство должно содействовать развитию сферы разработки и производства информационных систем, технологий и средств их обеспечения. Это содействие со стороны государства может осуществляться в различных формах. Первой и наиболее значимой формой содействия выступает государственное финансирование производства информационных систем, технологий и средств их обеспечения. Существенным элементом государственного содействия является стандартизация и сертификация систем, технологий и средств. Важную роль в создании условий для проведения научно-исследовательских и опыт-

¹ БНА. 1988. №5.

но-конструкторских работ играют косвенные формы государственного содействия.

Среди них видное место занимают предоставление различного рода льгот, в том числе налоговых, а также меры морального и материального стимулирования.

4. Норма, содержащаяся в п. 4 комментируемой статьи, предусматривает финансирование из средств федерального бюджета разработку и эксплуатацию федеральных информационных систем. Речь в данном случае может идти о финансировании, в частности, космических телекоммуникационных систем¹, Государственной автоматизированной системы «Выборы»², Общенациональной системы правовой информации³.

Специальное финансирование предусмотрено Федеральной целевой программой «Электронная Россия (2002—2010 гг.)»⁴. Указанное финансирование планируется осуществлять по девяти разделам программы с разбивкой объема финансирования по годам.

5. Пункт 5 комментируемой статьи определяет органы, ответственные за установление правил учета и анализа состояния производства информационных систем и сетей, технологий и средств их обеспечения. К этим органам отнесены Государственный комитет РФ по статистике и подведомственные ему организации, а также Министерство РФ по связи и информатизации.

Статья 17. Право собственности на информационные системы, технологии и средства их обеспечения

1. Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства.

¹ См.: Указ Президента РФ «О мерах по созданию космических телекоммуникационных систем Российской Федерации» // СЗ РФ. 1996. № 32. Ст. 3839.

² СЗ РФ. 1994. № 318. Ст. 2067; СЗ РФ. 1999. № 26. Ст. 3178. Российская газета. 2003. 15 января.

³ См.: Указ Президента РФ «О мерах по ускорению создания центров правовой информации» // САПП РФ. 1993. № 47. Ст. 1473.

⁴ Российская газета. 2002. 27 февраля.

2. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

3. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков.

Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

1. Комментируемая статья вводит в гражданский оборот новый для российской системы права объект права собственности, именуемый информационной технологией. На это прямо указывается в п. 1, согласно которому информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, а также государства. Муниципальные образования в число собственников названных объектов не включены.

В данном случае законодатель в очередной раз вышел за пределы применимости гражданско-правового института вещного права собственности, включив в число объектов этого права совокупность процессов (технологии), что само по себе является абсурдным шагом и не поддается рациональному объяснению.

Что касается информационных систем как объектов права собственности, то корректнее вести речь о праве собственности на имущество, входящее в состав комплекса средств, являющихся в свою очередь частью информационных систем.

Такого подхода придерживается законодатель в ст. 8 и 14 Федерального закона «О государственной автоматизированной системе Российской Федерации "Выборы"». Согласно п. 2 ст. 8 указанного Закона, в состав ГАС «Выборы» входят:

- комплекс средств автоматизации Центральной избирательной комиссии РФ;

- комплекс средств автоматизации избирательных комиссий субъектов РФ;
- комплексы средств автоматизации муниципальных, окружных, территориальных избирательных комиссий.

При этом в соответствии со ст. 14, имущество, входящее в состав комплексов средств автоматизации, созданное или приобретенное за счет средств федерального бюджета, является федеральной собственностью.

2. Пункт 2 комментируемой статьи должен применяться с учетом правил, закрепленных в гл. 32, 38 и гл. 61-65 ГК РФ.

3. Информационные системы, технологии и средства их обеспечения по аналогии с информационными ресурсами (см. комментарий к ст. 6) включаются в состав имущества собственника или владельца. При этом все они в совокупности либо в качестве самостоятельных объектов признаются товаром, т. е. продуктом труда, предназначенным для обмена.

При создании информационных систем, технологий и средств их обеспечения могут возникать проблемы, касающиеся прав заказчиков и исполнителей на результаты работ по созданию указанных объектов. Часто заказчики, т. е. лица, на средства которых в основном и создаются системы, технологии и средства обеспечения, настаивают на том, чтобы полученный охраноспособный результат автоматически передавался в качестве неотъемлемого элемента выполненной работы. Между тем подобная передача требует особого соглашения между исполнителем и заказчиком, которое может достигаться как в рамках отдельной договоренности, так и в самом договоре на выполнение НИР и ОКТР, например, в форме обязанности исполнителя об уступке им права на подачу заявки на предполагаемое изобретение заказчику. Статья 772 ГК РФ устанавливает на этот счет весьма нечеткие правила, предоставляя сторонам самостоятельно определять в договоре пределы и условия использования результатов работ. Представляется, что отношения между исполнителем и заказчиком могут

выстраиваться по модели отношений автор—работодатель, нашедшей свое закрепление в п. 2 ст. 8 Патентного закона РФ¹. При этом права и обязанности сторон должны быть детально отражены в договоре. В противном случае, к отношениям сторон будет применяться диспозитивная норма п. 2 ст. 772 ГК РФ, в соответствии с которой заказчик имеет право использовать переданные ему исполнителем результаты работ, в том числе охраноспособные, а исполнитель вправе использовать полученные им результаты лишь для собственных нужд.

Особые правила в отношении прав сторон на охраноспособные результаты НИР и ОКТР установлены в сфере исполнения государственных контрактов на выполнение НИР и ОКТР для федеральных государственных нужд. Согласно постановлению Правительства РФ от 2 сентября 1999 г. № 982 «Об использовании результатов научно-технической деятельности»², на государственных заказчиков НИР и ОКТР для федеральных государственных нужд возлагается обязанность по обеспечению закрепления за РФ прав на результаты научно-технической деятельности, полученные при реализации государственных контрактов, а также закрепляется полномочие по распоряжению этими правами от имени РФ в порядке, определяемом Правительством РФ.

Свою специфику имеет и решение проблемы распределения прав на охраняемые результаты интеллектуальной деятельности, полученные либо используемые в рамках договоров на выполнение НИР и ОКТР, одной из сторон которых выступает иностранный участник. Данная проблема нашла свое формальное разрешение в Руководстве по распределению интеллектуальной собственности в договорах на выполнение научно-исследовательских, опытно-конструкторских и технологических работ и в договорах о совместной научно-технической деятельности, заключаемых между российскими и ино-

¹ Ведомости РФ. 1992. № 42. Ст. 2319; Российская газета. 2003. 11 февраля.

² СЗ РФ. 1999. № 36. Ст. 4412.

странными организациями, утвержденном приказом Государственного комитета РФ по науке и технологиям от 29 января 1997 г. № 13¹. Руководством определено, в частности, что при заключении контрактов и соглашений на выполнение научно-технических работ каждая из сторон должна иметь право на использование «создаваемой интеллектуальной собственности». При этом минимальный объем прав должен состоять в праве каждой из договаривающихся сторон использовать «создаваемую интеллектуальную собственность» для собственных нужд.

Следует подчеркнуть, что комментируемая статья игнорирует требования законодательства об интеллектуальной собственности, допуская суперпозицию вещных и исключительных прав на один и тот же объект.

Абзац 2 п. 3 наделяет собственника информационной системы, технологии и средств их обеспечения правом определять условия их использования. Так, согласно ст. 20 Федерального закона «О Государственной автоматизированной системе российской Федерации "Выборы"», данная система и ее фрагменты могут использоваться для решения задач, не связанных с выборами и референдумом, в соответствии с федеральными законами, нормативными правовыми актами Центральной избирательной комиссии РФ. Порядок использования комплексов средств автоматизации, информационных ресурсов ГАС «Выборы», средств связи, других средств обеспечения органами государственной власти, государственными органами, органами местного самоуправления и другими организациями для решения задач, не связанных с выборами и референдумом, устанавливается федеральными законами, нормативными правовыми актами Центральной избирательной комиссии РФ.

¹ Информационно-правовая база «Консультант Плюс». Документ: «Приказ ГКНТ от 29.01.97 г. №13».

Статья 18. Право авторства и право собственности
на информационные системы, технологии
и средства их обеспечения

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам.

Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством Российской Федерации.

1. Комментируемая статья дублирует известное правило о независимости права авторства как личного неимущественного права от имущественных прав на использование полученного автором охраняемого результата интеллектуальной деятельности. Вместе с тем формулировку данного правила, содержащуюся в комментируемой статье, нельзя признать удачной. Здесь речь должна была бы идти по аналогии с п. 5 ст. 6 Закона РФ «Об авторском праве и смежных правах»¹ о том, что авторское право (но не только право авторства) на охраняемый результат интеллектуальной деятельности, содержащийся в информационной системе, технологии или средстве их обеспечения, не связано с правом собственности на информационную систему или средство ее обеспечения. При этом передача права собственности на информационную систему или средство ее обеспечения, а равно на средство обеспечения информационной технологии или права владения на них, сама по себе не влечет передачи каких-либо авторских прав (личных неимущественных и имущественных) на охраняемый результат, воплощенный в системе или средстве.

2. Абзац 2 комментируемой статьи лишен смысла, поскольку защита исключительных прав, в том числе авторских, является прерогативой обладателя этих прав, но не собственника материального объекта, в котором они воплощены, если, конечно, обладатель исключительных прав и собственник не совпадают в одном лице.

¹ Ведомости РФ. 1993. 332. Ст. 1242; СЗ РФ. 1995. №30. Ст. 2866.

Статья 19. Сертификация информационных систем, технологий, средств их обеспечения

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. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

1. Комментируемая статья устанавливает необходимость сертификации информационных систем, технологий, средств их обеспечения.

Базовым нормативно-правовым актом, регулирующим отношения в области сертификации, является Федеральный закон «О техническом регулировании»¹, пришедший на смену Закону РФ «О сертификации продукции и услуг»².

Согласно ст. 2 нового закона, сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Подтверждение соответствия может носить добровольный или обязательный характер.

Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

¹ Российская газета. 2002. 31 декабря

² Ведомости РФ. 1993. № 26. Ст. 966; СЗ РФ. 1996. № 1. Ст. 4; 1998. № 10. Ст. 1143; № 31. Ст. 3832.

Обязательное подтверждение соответствия осуществляется в формах:

- * принятия декларации о соответствии (декларирование соответствия);
- * обязательной сертификации.

Добровольное подтверждение соответствия осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации. Система добровольной сертификации может быть создана юридическим лицом и (или) индивидуальным предпринимателем или их группой.

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента. Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории РФ.

Декларирование соответствия осуществляется по одной из двух схем:

- » принятие декларации о соответствии на основании собственных доказательств;
- * принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра).

Обязательная сертификация осуществляется органом по сертификации, аккредитованным в порядке, установленном Правительством РФ, на основании договора с заявителем. Схемы сертификации, применяемые для сертификации информационных систем, баз и банков данных, предназначенных для информационного обслуживания граждан и организаций, устанавливаются соответствующим техническим регламентом.

2. Пункт 1 комментируемой статьи содержит отсылочную норму, определяющую порядок сертификации информаци-

онных систем, баз и банков данных, предназначенных для информационного обслуживания граждан и организаций. В общем виде указанный порядок установлен ст. 21, 24, 26 Федерального закона «О техническом регулировании».

3. Пункт 2 закрепляет правило, предусматривающее проведение обязательной сертификации информационных систем органов государственной власти РФ, органов государственной власти субъектов РФ, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом. Примером реализации указанного правила может служить действующая до принятия соответствующего технического регламента сертификация средств защиты информации.

Средства защиты информации, находящейся в режиме государственной тайны, должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. Согласно ст. 28 Закона РФ «О государственной тайне», организация сертификации средств защиты информации возлагается на Гостехкомиссию РФ, ФСБ РФ, ФАПСИ, Минобороны РФ в соответствии с функциями, возложенными на них законодательством РФ. Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ. В развитии Закона РФ «О государственной тайне» постановлением Правительства РФ от 26 июня 1995 г. № 608 утверждено Положение о сертификации средств защиты информации¹. Данное Положение устанавливает общий порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. Согласно Положению, средствами защиты информации являются технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства конт-

¹ СЗ РФ. 1995. № 27. Ст. 2579; 1996. № 18. Ст. 2142.

роля эффективности защиты информации. Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. Система сертификации представляет собой совокупность участников сертификации, осуществляющих ее по установленным правилам. Системы сертификации создаются Гостехкомиссией РФ, ФАПСИ, ФСБ РФ, Минобороны РФ, СВР РФ. В каждой системе сертификации разрабатываются и согласовываются с Межведомственной комиссией по защите государственной тайны положения об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Так, ФСБ РФ создана система обязательной сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ).

Основные цели создания, организационная структура системы сертификации СЗИ-ГТ, порядок проведения сертификации этих средств, порядок регистрации сертифицированных средств, а также порядок проведения инспекционного контроля за сертифицированными средствами установлены Положением о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, утвержденным приказом ФСБ РФ от 13 ноября 1999 г. №564¹.

Основными целями создания данной системы сертификации являются:

- обеспечение национальной безопасности в сфере информации;
- формирование и осуществление единой научно-технической и промышленной политики в сфере информатиза-

¹ См.: Сумин А. А. Комментарий к Закону РФ «О государственной тайне». М., 2001. С. 180-199.

ции с учетом требований системы защиты государственной тайны;

- содействие формированию рынка защищенных информационных технологий и средств их обеспечения;
- регулирование и контроль разработки, а также последующего производства средств защиты информации;
- содействие потребителям в компетентном выборе средств защиты информации;
- защита потребителя от недобросовестности изготовителя (продавца, исполнителя);
- подтверждение показателей качества продукции, заявленных изготовителями.

Органы по сертификации системы СЗИ-ГТ проводят обязательную сертификацию средств защиты информации, используемых при работе со сведениями, составляющими государственную тайну, в том числе иностранного производства. Номенклатура СЗИ-ГТ разрабатывается ФСБ РФ на основании видов средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ и утверждается по согласованию с Межведомственной комиссией по защите государственной тайны.

По инициативе разработчика, изготовителя или потребителя может проводиться добровольная сертификация средств защиты информации, не предназначенных для работы со сведениями, составляющими государственную тайну.

Сертификация СЗИ-ГТ осуществляется аккредитованными органами по сертификации, а испытания проводятся в аккредитованных испытательных центрах или лабораториях. Признание сертификатов соответствия на средства защиты информации, выданных другими системами сертификации, осуществляется в порядке, определяемом ФСБ РФ и Межведомственной комиссией по защите государственной тайны.

Организационную структуру данной системы сертификации образуют:

- ФСБ РФ (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации средств защиты информации);
- центральный орган системы сертификации (создается при необходимости);
- органы по сертификации СЗИ-ГТ;
- испытательные центры (лаборатории);
- учебно-методический центр;
- заявители (разработчики, изготовители, продавцы, потребители СЗИ-ГТ).

ФСБ РФ в пределах своей компетенции осуществляет, в частности, функции по:

- созданию системы сертификации и установлению правил проведения сертификации;
- представлению на государственную регистрацию в Госстандарт РФ системы сертификации СЗИ-ГТ и ее знаки соответствия;
- организации функционирования системы сертификации;
- определению номенклатуры СЗИ-ГТ;
- установлению правил аккредитации и выдачи лицензий на проведение работ по сертификации;
- утверждению нормативных документов, на соответствие которым проводится сертификация СЗИ-ГТ в системе сертификации и методические документы по проведению сертификационных испытаний;
- ведению государственного реестра сертифицированных средств защиты информации, аккредитованных в системе сертификации СЗИ-ГТ, органов по сертификации и испытательных центров (лабораторий), других участников сертификации, а также выданных и аннулированных сертификатов соответствия и лицензий на применение знака соответствия.

Органы по сертификации СЗИ-ГТ в пределах установленной области аккредитации, в частности:

- проводят идентификацию средств защиты информации;
- определяют схему сертификации конкретных средств защиты;
- разрабатывают предложения по номенклатуре СЗИ-ГТ;
- оформляют экспертное заключение по сертификации СЗИ-ГТ, сертификаты соответствия и лицензии на применение знака соответствия и представляют их в ФСБ РФ для регистрации в государственном реестре;
- выдают сертификаты соответствия и лицензии на применение знака соответствия;
- представляют заявителю перечень испытательных центров (лабораторий), в которых могут проводиться испытания конкретного СЗИ-ГТ;
- приостанавливают либо отменяют действие выданных сертификатов соответствия и лицензий на применение знака соответствия.

Испытательные центры (лаборатории) в пределах установленной области аккредитации, в частности:

- разрабатывают, утверждают программы и методики проведения сертификационных испытаний;
- осуществляют отбор образцов СЗИ-ГТ для проведения сертификационных испытаний;
- осуществляют сертификационные и инспекционные испытания СЗИ-ГТ, оформляют технические заключения и протоколы сертификационных испытаний;
- обеспечивают сохранность образцов СЗИ-ГТ и конфиденциальность информации.

Учебно-методический центр:

- осуществляет подготовку, переподготовку и повышение квалификации кадров;

- осуществляет подготовку и аттестацию экспертов;
- участвует в разработке и совершенствовании нормативных и методических документов в системы сертификации СЗИ-ГТ.

Заявители (разработчики, изготовители, продавцы) должны иметь лицензию на соответствующий вид деятельности и обязаны, в частности:

- применять сертификат и знак соответствия СЗИ-ГТ, руководствуясь правилами системы сертификации;
- указывать в сопроводительной технической документации сведения о сертификате на СЗИ-ГТ, обеспечивать доведение этой информации до потребителя;
- • принимать меры для обеспечения стабильности характеристик СЗИ-ГТ, определяющих безопасность информации;
- извещать орган по сертификации, проводивший сертификацию, обо всех изменениях в технологии, конструкции (составе) сертифицированного СЗИ-ГТ и технической документации на него для принятия решения о необходимости проведения повторной сертификации данного СЗИ-ГТ.

Органы по сертификации и испытательные центры (лаборатории) должны быть юридическими лицами, располагать подготовленными специалистами, необходимыми средствами измерений, испытательным оборудованием и методиками испытаний, нормативными документами для проведения всего комплекса работ по испытаниям СЗИ-ГТ в своей области аккредитации.

Проведению сертификации предшествует подача заявки на сертификацию, осуществляемая заявителем. Заявка с указанием схемы проведения сертификации государственных стандартов и иных нормативно-методических документов направляется в орган по сертификации, который обязан в десяти-

дневный срок передать копию заявки на проведение сертификации продукции в ФСБ РФ.

В месячный срок после получения заявки орган по сертификации СЗИ-ГТ направляет заявителю решение на проведение сертификации, в котором указывается перечень испытательных центров, область аккредитации которых позволяет проводить сертификационные испытания данного СЗИ-ГТ.

После получения решения заявитель представляет средство защиты в испытательный центр или (в отдельных случаях) в орган по сертификации. Сроки проведения испытаний могут быть установлены в договоре между заявителем и испытательным центром.

Результаты испытаний оформляются протоколами и техническим заключением, которые направляются органу по сертификации и заявителю.

Орган по сертификации проводит экспертизу результатов испытаний и готовит экспертное заключение. При соответствии результатов испытаний требованиям нормативных документов данный орган оформляет сертификат соответствия и лицензию на применение знака соответствия, которые вместе с копией экспертного заключения направляет в ФСБ РФ для регистрации в государственном реестре. Срок действия сертификата соответствия устанавливается не более чем на пять лет.

Заявителю сертификат соответствия и лицензия на применение знака соответствия выдаются после их регистрации в государственном реестре системы сертификации СЗИ-ГТ.

Инспекционный контроль за сертифицированными СЗИ-ГТ осуществляет орган по сертификации, проводивший сертификацию с привлечением в случае необходимости испытательного центра.

4. Пункт 3 комментируемой статьи возлагает на таможенные органы РФ обязанность по защите интересов потребителя информации при использовании импортной продукции в информационных системах. Данная норма получила содержатель-

ное подкрепление в ст. 17 Федерального закона «Об участии в международном информационном обмене»¹. Согласно названной статье, при ввозе информационных продуктов, информационных услуг в РФ импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию РФ информационных продуктов или услуг риск за использование данных продуктов и услуг лежит на импортере.

Средства международного информационного обмена (информационные системы, сети и сети связи, используемые при международном информационном обмене), которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации. При этом сертификация сетей связи производится в порядке, определяемом ст. 16 Федерального закона «О связи»².

¹ СЗ РФ. 1996. № 28. Ст. 3347

² СЗ РФ. 1995. № 8. Ст. 600.

Глава 5

ЗАЩИТА ИНФОРМАЦИИ И ПРАВ СУБЪЕКТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ИНФОРМАТИЗАЦИИ

Статья 20. Цели защиты

Целями защиты являются:

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, имеющих 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.

1. Данная статья открывает специальный раздел комментируемого Закона, посвященный регулированию отношений, складывающихся в связи с защитой информации и защитой прав субъектов в области информационных процессов и информатизации. Поэтому цели защиты, провозглашаемые комментируемой статьей, касаются двух различных объектов защиты, а именно: документированной информации и субъективных прав лиц, которые нарушены либо оспорены.

Стабильность прав и экономических интересов участников информационных отношений может быть гарантирована не только путем закрепления за ними соответствующего статуса (собственник, владелец, пользователь), но и посредством предоставления дополнительных юридических возможностей, которые состоят в применении правоохранительных мер, направленных на принудительное исполнение обязанностей в случае уклонения обязанного субъекта от должного поведения. И если правовая охрана отношений, складывающихся в области информационных процессов и информации, осуществляется с разной степенью интенсивности практически всеми отраслями права с применением норм, обеспечивающих нормальное и беспрепятственное функционирование информационной сферы, и отношений, его опосредующих, то правоохранительные меры применяются в связи с совершением против этих отношений действий, именуемых правонарушениями.

Данное обстоятельство применительно к охране отношений собственности было в свое время отмечено О. С. Иоффе, который выделял охрану отношений собственности всеми отраслями советского права в качестве охраны в широком смысле, а совокупность гражданско-правовых способов и средств, которые применяются в связи с совершением против отношений собственности правонарушений, именовал гражданско-правовой охраной в узком смысле¹.

Позднее понятие охраны, используемое в отмеченных выше смыслах, трансформировалось в две относительно самостоятельные категории, получившие большое количество разнообразных интерпретаций. Это категории «охраны» и «защиты». Таким образом, охрана информации есть установление ее общего правового режима, а защита информации — те меры, которые предпринимаются в случаях, когда субъективные права на информацию нарушены либо оспорены.

¹ Иоффе О. С. Советское гражданское право. М., 1967. С. 473.

Характер нарушения, подлежащего защите субъективного права, определяет порядок и пределы употребления конкретных способов защиты, которые могут быть применены посредством Исполнения комплекса внутренне согласованных организационных мероприятий по защите субъективных прав и охраняемых законом интересов, именуемых в юридической науке формами защиты. В настоящее время получила признание и распространение терминологическая градация форм защиты на две ее разновидности: юрисдикционную и неюрисдикционную¹. Их основное отличие состоит в том, что юрисдикционная форма защиты предполагает обращение лица, чьи права и охраняемые законом интересы нарушены, в компетентные органы, которые уполномочены на рассмотрение юридических дел и на вынесение по ним юридически обязательных решений. Неюрисдикционная форма защиты предполагает защиту нарушенного права или охраняемого законом интереса посредством самостоятельных действий уполномоченного лица, совершаемых им с применением дозволенных законом средств без обращения в компетентные органы. В рамках юрисдикционной формы защиты выделяют общий и специальный порядок защиты. Для общего порядка характерна реализация прав на защиту путем обращения уполномоченного лица в судебные органы. К специальному порядку защиты причисляют административный порядок, который надлежит использовать лишь в случаях, предусмотренных законом (п. 2. ст. 11 ГК РФ).

Действующее законодательство устанавливает внушительный перечень способов защиты прав, под которыми следует понимать установленные законом правоохранительные меры, применение которых направлено на восстановление (признание) нарушенного (оспариваемого) права и на оказание воздействия на нарушителя. Перечень способов защиты гражданских прав закреплен в ст. 12 ГК РФ. Выбор наиболее подходя-

¹ См., например: Гражданское право. Ч. 1. Учебник/Под ред. Ю. К. Толстого, А. П. Сергеева. М., 1996. С. 242-243 (автор главы — А. П. Сергеев).

щего из способов защиты и процессуальный порядок его применения будут зависеть от характера совершенного правонарушения и существа нарушенного (оспариваемого) права.

2. Комментируемая статья определяет цели защиты информации и прав субъектов в области информационных процессов и информатизации, которые могут быть достигнуты в рамках как юрисдикционной, так и неюрисдикционной формы защиты.

Так, предотвращение утечки, хищения, утраты, искажения, подделки информации, несанкционированных действий по уничтожению, кодификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы может быть достигнуто в рамках неюрисдикционной формы защиты, а именно путем самозащиты. Аналогичную форму защиты следует применять и для сохранения государственной тайны, конфиденциальности документированной информации.

Путем признания права достигается цель защиты конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных.

Путем восстановления положения, существовавшего до нарушения права, достигается цель обеспечения прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Статья 21. Защита информации

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

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.

2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

1. Комментируемая статья регулирует отношения, складывающиеся по поводу защиты информации. В данном случае защита рассматривается как деятельность по предотвраще-

нию незаконного вмешательства в информационный ресурс, которая лежит в плоскости неюрисдикционной формы защиты. защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Формулируя данную норму, законодатель не раскрывает содержание термина «неправомерное обращение», как, впрочем, и характер наносимого ущерба.

В ГОСТе Р 50922-96 «Защита информации. Основные термины и определения» дается ряд определений, характеризующих с содержательной стороны термин «неправомерное обращение», и показываются разновидности защиты информации в зависимости от характера угроз. Согласно названному документу:

- а) защита информации от непреднамеренного воздействия — деятельность по предотвращению воздействия на защищенную информацию от ошибок пользователей информации, сбоев технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- б) защита информации от несанкционированного воздействия — деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- в) защита информации от несанкционированного доступа — деятельность по предотвращению получения защищав-

- мой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или прав доступа к защищаемой информации;
- г) защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации, от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации (иностранцами) разведками;
- д) защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;
- е) защита информации от (иностранной) разведки — деятельность по предотвращению получения защищаемой информации (иностранной) разведкой;
- ж) защита информации от агентурной разведки — деятельность по предотвращению получения защищаемой информации агентурной разведкой;
- з) защита информации от (иностранной) технической разведки — деятельность по предотвращению получения защищаемой информации (иностранной) технической разведкой с помощью технических средств.

2. Комментируемая статья определяет способы установления режима защиты информации в зависимости от характера ее содержания.

В отношении сведений, отнесенных к государственной тайне, режим их защиты устанавливается уполномоченными органами на основании Закона РФ «О государственной тайне». В указанном Законе определен значительный комплекс мер, направленных на создание системы защиты сведений, находящихся в режиме государственной тайны. Закон РФ «О государственной тайне» рассматривает систему защиты государ-

ственной тайны как совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях. Перечень органов защиты государственной тайны установлен ст. 20 Закона РФ «О государственной тайне».

В отношении конфиденциальной документированной информации режим ее защиты устанавливается собственником информационных ресурсов или уполномоченным лицом на основании ст. 22 комментируемого Закона.

В отношении персональных данных — режим их защиты должен быть установлен федеральным законом.

3. Пункт 2 комментируемой статьи предписывает органам государственной власти и организациям, ответственным за формирование и использование информационных ресурсов, подлежащих защите, а также органам и организациям, разрабатывающим и применяющим информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствоваться в своей деятельности законодательством Российской Федерации.

4. Пункт 3 содержит важное правило, устанавливающее государственный контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также за обеспечением организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом, негосударственными организациями.

Государственный контроль за указанными сферами деятельности осуществляется посредством созданных в РФ систем лицензирования, стандартизации, сертификации и метрологии (см. комментарий к ст. 19).

5. Пункт 4 устанавливает обязанность организаций, обрабатывающих документированную информацию с ограничен-

ным доступом и являющуюся собственностью государства, создавать специальные службы, обеспечивающие защиту информации. Это могут быть как самостоятельные подразделения, так и подразделения, входящие в состав служб безопасности. Их главной задачей является обеспечение защищенного документооборота и обеспечение функционирования технологических систем обработки и хранения конфиденциальных документов.

6. В качестве дополнительной к государственному контролю меры по соблюдению требований к защите информации, п. 5 комментируемой статьи наделяет собственника информационных ресурсов правом на осуществление частного контроля за выполнением требований по защите информации. Реализуя данное право, собственник может запрещать или приостанавливать обработку документированной информации. Аналогичная возможность предоставляется и уполномоченному собственником лицу.

7. Пункт 6 комментируемой статьи закрепляет за собственником или владельцем документированной информации право на обращение в органы государственной власти с целью оценки последними правильности выполнения норм и требований по защите информации, принадлежащей собственнику.

Представляется, что данная норма не вполне точно расставляет акценты в решении существа вопроса и наделяет органы государственной власти несвойственными им функциями поставника.

Правильность выполнения действующих правил и требований по защите информации проверяют соответствующие государственные органы. В их функции не входит оказание помощи. Об этом, в частности, свидетельствуют нормы, содержащиеся в ст. 12 Федерального закона «О лицензировании отдельных видов деятельности», гл. 6 Федерального закона «О техническом регулировании».

Статья 22. Права и обязанности субъектов в области защиты информации

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

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 обо всех фактах нарушения режима защиты информации.

1. Комментируемая статья призвана установить права и обязанности собственника, а также владельца документированной информации и уполномоченных лиц в области ее защиты. Нормы данной статьи в значительной степени пересекаются с правилами п. 6 ст. 6, п. 3 ст. 12, ст. 15 комментируемого Закона. В статье, несмотря на ее название, отсутствует полный перечень прав и обязанностей упомянутых в ней субъектов.

2. Собственник документов, массива документов, информационных систем имеет право на обращение в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения

анализа достаточности мер защиты его ресурсов и систем и получения консультаций. Права и обязанности заявителя в области обязательного подтверждения соответствия детализированы в ст. 28 Федерального закона «О техническом регулировании». Согласно названной статье, заявитель вправе:

- выбирать форму и схему подтверждения соответствия, предусмотренные для определенных видов продукции соответствующим техническим регламентом;
- обращаться для осуществления обязательной сертификации в любой орган по сертификации, область аккредитации которого распространяется на продукцию, которую заявитель намеревается сертифицировать;
- обращаться в орган по аккредитации с жалобами на неправомерные действия органов по сертификации и аккредитованных испытательных лабораторий (центров).

Собственник документов, массивов документов, информационных систем или уполномоченные им лица обязаны устанавливать порядок предоставления информации пользователю. Данный порядок должен содержать указание места, времени, ответственных должностных лиц, а также необходимых процедур предоставления информации. Кроме того, собственник или уполномоченные им лица обеспечивают условия доступа пользователей к информации.

На собственнике несертифицированных информационных систем и средств их обеспечения лежит риск, связанный с их использованием.

3. На владельца документов, массива документов, информационных систем возлагаются обязанности по обеспечению уровня защиты информации и по оповещению собственника информационных ресурсов и (или) информационных систем обо всех фактах нарушения режима защиты информации. Владелец несертифицированных информационных систем и средств их обеспечения наряду с их собственником несет риск, связанный с использованием таких систем и средств.

4. Потребитель, получивший документированную информацию из несертифицированной информационной системы, несет риск, связанный с использованием этой информации.

Статья 23. Защита прав субъектов в сфере информационных процессов информатизации

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

1. Статья посвящена регулированию отношений, складывающихся по поводу защиты прав субъектов, которыми они обладают в сферах информационных процессов и информатизации.

Как уже отмечалось выше (см. комментарий кет. 20), под защитой понимаются те меры, которые предпринимаются управомоченным лицом в случае, когда нарушены или оспорены его права либо охраняемые законом интересы.

В качестве целей защиты прав субъектов п. 1 комментируемой статьи называет предупреждение правонарушений, пресечение неправомерных действий, восстановление нарушенных прав и возмещение причиненного ущерба. Указанные цели защиты прав не в полной мере совпадают с общими целями защиты, закрепленными в ст. 20 комментируемого Закона.

Кроме того, в качестве целей защиты законодатель, в данном случае, обозначил сами правоохранительные меры, что не может не внести путаницу в уже устоявшиеся понятия.

2. Пункт 2 комментируемой статьи определяет органы правосудия, в которых осуществляется защита прав в сферах формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения. В качестве таких органов называются суды общей юрисдикции, арбитражные суды и третейские суды.

Подведомственность гражданских дел судам общей юрисдикции закреплена в ст. 22 Гражданского процессуального кодекса Российской Федерации¹. Согласно названной статье, суды рассматривают и разрешают:

- исковые дела с участием граждан, организаций, органов государственной власти, органов местного самоуправления о защите нарушенных или оспариваемых прав, свобод и законных интересов, по спорам, возникающим из гражданских, семейных, трудовых, жилищных, земельных, экологических и иных правоотношений;
- дела по требованиям, разрешаемым в порядке приказного производства;

¹ Российская газета. 2002. 20 ноября.

- дела, возникающие из публичных правоотношений;
- дела особого производства;
- дела об оспаривании решений третейских судов и о выдаче исполнительных листов на принудительное исполнение решений третейских судов;
- дела о признании и приведении в исполнение решений иностранных судов и иностранных арбитражных решений.

Подведомственность дел арбитражному суду закреплена в ст. 27-33 Арбитражного процессуального кодекса Российской Федерации¹. Согласно указанным статьям, арбитражному суду подведомственны дела по экономическим спорам и другие дела, связанные с осуществлением предпринимательской и иной экономической деятельности.

Арбитражные суды рассматривают в порядке искового производства возникающие из гражданских правоотношений экономические споры и другие дела, связанные с осуществлением предпринимательской и иной экономической деятельности юридическими лицами и индивидуальными предпринимателями, а в случаях, предусмотренных федеральными законами, другими организациями и гражданами.

Арбитражные суды рассматривают в порядке административного судопроизводства возникающие из административных и иных публичных правоотношений экономические споры и иные дела, связанные с осуществлением организациями и гражданами предпринимательской и иной экономической деятельности; о выдаче исполнительных листов на принудительное исполнение решений третейских судов по спорам, возникающим при осуществлении предпринимательской и иной экономической деятельности.

Порядок образования и деятельности третейских судов, находящихся на территории РФ; регулируется Федеральным

¹ Российская газета. 2002. 27 июля.

законом «О третейских судах в Российской Федерации»¹. Согласно ст. 2 указанного Закона, третейский суд — постоянно действующий третейский суд или третейский суд, образованный сторонами для решения конкретного спора.

Компетенция третейского суда определена в ст. 17 Федерального закона «О третейских судах в Российской Федерации». В соответствии с названной статьей, третейский суд самостоятельно решает вопрос о наличии или об отсутствии у него компетенции рассматривать переданный на его разрешение спор, в том числе в случае, когда одна из сторон возражает против третейского разбирательства по мотиву отсутствия или недействительности третейского соглашения.

3. В п. 3 установлена необходимость привлечения к ответственности органов государственной власти, организаций и их должностных лиц за правонарушения, допущенные при работе с документированной информацией. Однако необходимость еще не означает возможность такого привлечения и в особенности органов государственной власти и их должностных лиц.

Определенная нормативная база в этом отношении все же существует. Ее основу составляет правило ст. 53 Конституции РФ, согласно которому каждый имеет право на возмещение вреда, причиненного незаконными действиями (или бездействием) органов государственной власти или их должностных лиц.

Гражданское законодательство (ст. 16 и 1069 ГК РФ) специально выделяет ответственность государственных органов и органов местного самоуправления за убытки (вред), причиненные гражданину или юридическому лицу в результате незаконных действий (бездействия) указанных органов или их должностных лиц, в том числе издания не соответствующего закону или иному правовому акту акта государственного органа или органа местного самоуправления.

¹ Российская газета. 2002. 27 июля.

Уголовная и административно-правовая ответственность установлены для отдельных видов преступлений и административных правонарушений.

Так, согласно ст. 292 УК РФ служебный подлог, т. е. внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности, — наказываются штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев.

В соответствии с п. 2 ст. 13.12 Кодекса РФ об административных правонарушениях использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), — влечет наложение административного штрафа на должностных лиц — от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц — от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

4. В п. 4 комментируемой статьи содержится правило об ответственности за нарушение международных норм и правил, которая возлагается на органы государственной власти, организации и граждан. Данное правило не имеет какого-либо юридического значения.

Речь, видимо, должна идти об ответственности по внешне-экономическим сделкам, поскольку в процессе осуществления торгово-экономических связей между организациями и фирмами различных государств могут заключаться контракты,

предметом которых являются информационные ресурсы, информационные системы, технологии и средства их обеспечения. Такие контракты имеют место, как правило, в области научно-технического сотрудничества. Стороны, участвующие в сделке, руководствуясь принципом *Lex voluntatis*, вправе своим соглашением выбрать законодательство того государства, которое и будет регулировать их отношения (см. ст. 1210 ГК РФ).

Статья 24. Защита права на доступ к информации

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

1. Статья развивает положения ст. 12—14 комментируемого Закона, касающиеся гарантий предоставления информации. Первое предложение п. 1 фактически воспроизводит п. 2 ст. 13; п. 4 ст. 14, дополняя их возможностью обжалования действий по предоставлению заведомо недостоверной информации. При этом законодатель не раскрывает содержание понятия заведомо недостоверной информации. Если пользоваться

аналогией закона (ст. 7 Федерального закона «О рекламе»¹ — недостоверная реклама), то под недостоверной информацией следует понимать информацию, содержащую не соответствующие действительности сведения о лицах, предметах, фактах, событиях, явлениях и процессах. Предоставление заведомо недостоверной информации — это действие, которое сознательно направлено на правонарушение, т. е. совершено с умыслом.

Абзац второй п. 1 содержит правило, которое касается компетенции арбитражных судов, а именно подведомственности дел арбитражному суду (§ 1 гл. 4 Арбитражного процессуального кодекса РФ). В этой связи правило не несет юридической нагрузки.

Лица, права которых на доступ к информации нарушены, а равно лица, получившие недостоверную информацию, вправе требовать возмещения понесенного ими ущерба. В данном случае возмещение убытков лицу, право которого нарушено, ограничено расходами данного лица, которые оно произвело или должно будет произвести для восстановления нарушенного права (п. 2 ст. 15 ГК РФ). Упущенная выгода, по смыслу абз. 3 комментируемого пункта, возмещению не подлежит. Поскольку нарушение прав, связанных с доступом к информации, является деликтом, суд должен применять к спорным правоотношениям общие положения ст. 1064-1083 ГК РФ.

2. Споры о необоснованном отнесении информации к категории ограниченного доступа подлежат рассмотрению в судебном порядке. Необоснованное отнесение в данном случае следует рассматривать как незаконное (осуществленное по основаниям, не предусмотренным действующими нормативно-правовыми актами, или противоречащее им). В таком значении необоснованное отнесение информации к категории конфиденциальной или информации, отнесенной к государственной тайне, не является сокрытием информации (ст. 14.13; 10.7; 19.9; 23.22; 8.5; 23.23; 23.33; 5.23 КоАП).

¹ СЗ РФ. 1995. № 30. Ст. 2864; Российская газета. 2001. 20 декабря.

3. Пункт 3 комментируемой статьи возлагает гражданско-правовую, административно-правовую и уголовную ответственность на руководителей и других служащих органов государственной власти организаций, виновных в незаконном ограничении доступа к информации и нарушении режима ее защиты. Данный пункт имеет отсылочный характер.

Статья 25. Вступление в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Предложить Президенту Российской Федерации привести в соответствие с настоящим Федеральным законом изданные им правовые акты.

3. Поручить Правительству Российской Федерации: привести в соответствие с настоящим Федеральным законом изданные им правовые акты;

подготовить и внести в Государственную Думу в трехмесячный срок в установленном порядке предложения о внесении изменений и дополнений в законодательство Российской Федерации в связи с принятием настоящего Федерального закона;

принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

1. Пунктом 1 установлено, что комментируемый Закон вступает в силу со дня его официального опубликования. Закон был официально опубликован в Российской газете 22 февраля 1995 г. С этого дня данный Закон и вступил в силу. Текст Закона опубликован в Собрании законодательства РФ в 1995 г. № 8. Ст. 609.

Изменения в Закон внесены Федеральным законом «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности"»¹.

2. Пунктом 2 Президенту РФ предложено привести изданные им правовые акты в соответствие с комментируемым За-

¹ Российская газета. 2003. 15 января.

коном. Согласно ст. 90 Конституции РФ, Президент РФ издает указы и распоряжения, обязательные для исполнения на всей территории РФ. Указы — это нормативные акты, относящиеся к неопределенному кругу лиц, органов публичной власти, должностных лиц, организаций. Распоряжения — это, как правило, акты, носящие индивидуальный характер.

3. В пункте 3 содержится ряд поручений, адресованных Правительству РФ, которое обязано привести в соответствие с комментируемым Законом изданные им правовые акты (нормативные, оперативно-распорядительные, индивидуальные, смешанные), подготовить и внести в Государственную Думу в установленном порядке предложения о внесении изменений и дополнений в законодательство РФ в связи с принятием закона, принять нормативные акты, обеспечивающие его реализацию.

ПРИЛОЖЕНИЯ

Приложение 1

Проект Федерального закона «О внесении изменений и дополнений в статьи 2, 11, 16 ФЗ "Об информации, информатизации и защите информации"»¹

Статья 1. Внести в Федеральный закон «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609) следующие изменения и дополнения:

1. Статью 2 дополнить абзацем следующего содержания: «Идентификация физического лица — отождествление физического лица с персональной информацией о нем и персональной информации с

соответствующим физическим лицом».

2. В ст. 11 п. 1 дополнить абзацем следующего содержания: «Основными факторами идентификации физического лица являются имя, фамилия, отчество физического лица, дата и место его рождения, место проживания. Применение иных идентифицирующих физическое лицо факторов допускается только в качестве дополнительных, в случаях, предусмотренных действующим законодательством».

3. Статью 16 дополнить пунктом «б» следующего содержания: «При разработке, производстве и использовании всех видов информационных систем и сетей, технологий и средств их обеспечения не допускается применение биоэлектронных и иных средств автоматической идентификации физических лиц, размещаемых в организме человека».

Статья 2. Правительству Российской Федерации привести свои нормативные акты в соответствие с настоящим Федеральным законом.

Статья 3. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент Российской Федерации

¹ Текст проекта находится в Интернете на сайте Государственной Думы.

Приложение 2

Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № ПР-1895

I. Информационная безопасность Российской Федерации (п. 1-4)

II. Методы обеспечения информационной безопасности (п. 5-7) Российской Федерации

III. Основные положения государственной политики (п. 8-9) обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

IV. Организационная основа системы обеспечения (п. 10-11) информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

- 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 информационной безопасности Российской Федерации.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

I. Информационная безопасность Российской Федерации

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструкту-

ры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

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

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
- обеспечить *конституционные права и свободы* человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных *федеральным законодательством* ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя 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.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя 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. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего, безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих *государственную тайну*;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2. Виды угроз информационной безопасности Российской Федерации.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы *конституционным правам и свободам* человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

-
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
 - противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
 - неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
 - неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
 - дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
 - нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
 - вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
 - девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
 - снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
 - манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуника-

ции и связи при создании и развитии российской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

3. Источники угроз информационной безопасности Российской Федерации.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне», *Основы законодательства* Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы «*Об информации, информатизации и защите информации*», «*Об участии в международном информационном обмене*», ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в *Конституции* Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских

информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий полити-

ческого и социально-экономического развития России и реальности угроз применения «информационного оружия»;

- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и, прежде всего, используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. Методы обеспечения информационной безопасности Российской Федерации

5. Общие методы обеспечения информационной безопасности Российской Федерации.

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка 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, регулирующие 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 Российская Федерация, 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 Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов Российской Федерации, 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;

- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников 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 Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- « создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального про—то обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-техни-

ческих методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

В сфере экономики. Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой,

биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и
- анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В сфере внутренней политики. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- конституционные права и свободы человека и гражданина;
- конституционный строй, *национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;*
- открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;
- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий рас-

пространения дезинформации о внутренней политике России.

В сфере внешней политики. К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;
- информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;
- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
- распространение за рубежом дезинформации о внешней политике Российской Федерации;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной

власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- создание российским представительством и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- « научно-технические кадры и система их подготовки;
- « системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;
- создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим репрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

- политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств — участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;
- » активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- ® сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;
- неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники — это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализа-

ции угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В сфере духовной жизни. Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;
- свобода массовой информации;
- * неприкосновенность частной жизни, личная и семейная тайна;
- * русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного обще-

ния народов государств — участников Содружества Независимых Государств;

- языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;
- объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

- деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;
- ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;
- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;
- использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;
- неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

- развитие в России основ гражданского общества;

- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;
- совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;
- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;,,
- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;
- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката

программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осу-

ществление контроля за функционированием информационных и телекоммуникационных систем;

- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- обеспечение информационной безопасности при подключении общегосударственных информационных и телеком-

муникационных систем к внешним информационным сетям, включая международные;

- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны. К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;
- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняю-

щих государственные оборонные заказы либо занимающихся оборонной проблематикой;

- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

- в все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- « деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах. К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;
- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в карточках и автоматизированных банках данных и используемой для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

- отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;
- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

- создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;
- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций. Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Соккрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс; к быстрому воз-

никновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;
- совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;
- повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;
- прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;
- разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности — неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях клю-

чевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами — участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие

России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение *Конституции* Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный по-

иск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

- формулирует и реализует государственную информационную политику России;
- ® организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

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 нормативных 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 Российской Федерации в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
- разработку нормативных 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, дисциплинар-

ной 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 Российской Федерации.

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.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости странУ в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;
- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;
- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных

и телекоммуникационных систем общего и специального назначения.

IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации

10. Основные функции системы обеспечения информационной безопасности Российской Федерации.

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Фе-

дерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов

Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятель-

ностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

Приложение 3

Постановление Правительства РФ от 28 января 2002 г. № 65
«О федеральной целевой программе "Электронная Россия (2002—2010 годы)"» (извлечение)

Правительство Российской Федерации постановляет:

1. Утвердить прилагаемую *федеральную целевую программу «Электронная Россия (2002-2010 годы)»*.

Министерству экономического развития и торговли Российской Федерации, Министерству финансов Российской Федерации и Министерству промышленности, науки и технологий Российской Федерации при формировании проектов федерального бюджета на 2002-2010 годы ежегодно уточнять размер выделяемых на реализацию Программы ассигнований с учетом возможностей федерального бюджета.

2. Образовать Межведомственную комиссию по координации деятельности заказчиков и исполнителей федеральной целевой программы «Электронная Россия (2002-2010 годы)» и координации вопросов финансирования других федеральных, ведомственных и региональных программ, содержащих задания по разработке и использованию информационно-коммуникационных технологий в Российской Федерации (далее именуется — Межведомственная комиссия).

Утвердить министра экономического развития и торговли Российской Федерации Грефа Г. О. председателем Межведомственной комиссии, министра Российской Федерации по связи и информатизации Реймана Л. Д. — заместителем председателя Межведомственной комиссии.

Министерству экономического развития и торговли Российской Федерации и Министерству Российской Федерации по связи и информатизации представить в 2-месячный срок в Правительство Российской Федерации проект положения о Межведомственной комиссии и предложения по ее составу.

3. Рекомендовать органам исполнительной власти субъектов Российской Федерации принять участие в реализации федеральной целевой программы «Электронная Россия (2002-2010 годы)».

4. Признать утратившим силу пункт 2 распоряжения Правительства Российской Федерации от 12 февраля 2001 г. № 207-р (Собрание законодательства Российской Федерации, 2001, № 8, ст. 770).

Председатель Правительства РФ

М. Касьянов

Федеральная целевая программа «Электронная Россия (2002—2010 годы)» (утв. постановлением Правительства РФ от 28 января 2002 г. № 65). Паспорт федеральной целевой программы «Электронная Россия (2002-2010 годы)»

1. Содержание проблемы и обоснование необходимости ее решения программными методами.
2. Цели, задачи, сроки и этапы реализации Программы.
3. Система программных мероприятий.
4. Ресурсное обеспечение Программы.
5. Механизм реализации Программы.
6. Управление и контроль реализации Программы.
7. Ожидаемые конечные результаты реализации Программы.
8. Приложение. Мероприятия федеральной целевой программы «Электронная Россия (2002-2010 годы)»

1. Паспорт федеральной целевой программы «Электронная Россия (2002-2010 годы)».

Наименование Программы — федеральная целевая программа «Электронная Россия (2002-2010 годы)».

Основание разработки Программы — распоряжение Правительства Российской Федерации от 12 февраля 2001 г. № 207-р.

Государственный заказчик (координатор Программы) — Министерство Российской Федерации по связи и информатизации.

Государственные заказчики Программы — Министерство экономического развития и торговли Российской Федерации, Министерство образования Российской Федерации, Министерство промышленности, науки и технологий Российской Федерации, Российское авиационно-космическое агентство, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Российское агентство по системам управления.

Основные исполнители Программы — организации, определяемые на конкурсной основе в порядке, установленном Федеральным законом «О конкурсах на размещение заказов на поставку товаров, выполнение работ, оказание услуг для государственных нужд».

Цель Программы — создание условий для развития демократии, повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения информационных и коммуникационных технологий, обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширения подготовки специалистов по информационным и коммуникационным технологиям и квалифицированных пользователей.

Задачи Программы — совершенствование законодательства и системы государственного регулирования в сфере информационных и коммуникационных технологий; обеспечение открытости в деятельности органов государственной власти и общедоступности государственных информационных ресурсов, создание условий для эффективного взаимодействия между органами государственной власти и гражданами на основе использования информационных и коммуникационных технологий; совершенствование деятельности органов государственной власти и органов местного самоуправления на основе использования информационных и коммуникационных технологий; совершенствование взаимодействия органов государственной власти и органов местного самоуправления с хозяйствующими субъектами и вне-

дрение информационных и коммуникационных технологий в реальный сектор экономики; развитие системы подготовки специалистов по информационным и коммуникационным технологиям и квалифицированных пользователей; содействие развитию независимых средств массовой информации посредством внедрения информационных и коммуникационных технологий; развитие телекоммуникационной инфраструктуры и создание пунктов подключения к открытым информационным системам; разработка и создание системы электронной торговли; формирование общественной поддержки выполнения мероприятий Программы.

Сроки и этапы реализации Программы — 2002-2010 годы:

I этап — 2002 год;

II этап — 2003-2004 годы;

III этап — 2005-2010 годы.

Объемы, источники финансирования и направления — всего на 2002-2010 годы — 77179,1 млн рублей, расходов в том числе:

за счет федерального бюджета — 39383 млн рублей,
из них:

научно-исследовательские и опытно-конструкторские работы — 3193 млн рублей;

инвестиции — 21418 млн рублей;

прочие нужды — 14772 млн рублей;

бюджеты субъектов Российской Федерации и местные бюджеты — 22610,1 млн рублей (предполагаемые данные);

внебюджетные источники — 15186 млн рублей.

Ожидаемые результаты — повышение эффективности реализации Программы государственного управления и развитие экономики за счет активизации внедрения и повышения результативности использования информационных и коммуникационных технологий; создание условий для ускоренного развития конкурентоспособного производства товаров и услуг в сфере информационных и коммуникационных технологий, ориентированного на внутренний и внешний рынки; активное вовлечение граждан и хозяйствующих субъектов в использование информационных и коммуникационных технологий за счет снижения тарифов на услуги связи и подключение к общедоступным информационным системам; повышение информационной открытости органов государственной власти и органов местного самоуправления, эффектив-

ности их взаимодействия с гражданами и организациями, качества оказываемых им услуг; повышение качества образования за счет использования информационных и коммуникационных технологий; развитие независимых средств массовой информации посредством внедрения информационных и коммуникационных технологий.

Контроль исполнения Программы — осуществляется Министерством Российской Федерации по связи и информатизации совместно с государственными заказчиками Программы в соответствии с законодательством Российской Федерации.

1. Содержание проблемы и обоснование необходимости ее решения программными методами.

Развитие и широкое применение информационных и коммуникационных технологий (далее именуются — ИКТ) является глобальной тенденцией мирового развития и научно-технической революции последних десятилетий. Применение ИКТ имеет решающее значение для повышения конкурентоспособности экономики, расширения возможностей ее интеграции в мировую систему хозяйства, повышения эффективности государственного управления и местного самоуправления.

Важным результатом распространения ИКТ и проникновения их во все сферы общественной жизни является создание правовых, организационных и технологических условий для развития демократии за счет реального обеспечения прав граждан на свободный поиск, получение, передачу, производство и распространение информации.

Несмотря на высокие темпы развития ИКТ в последнее десятилетие, Россия не смогла сократить отставание от промышленно развитых стран в уровне информатизации экономики и общества. Отчасти такое положение вызвано общеэкономическими причинами (длительный кризис в экономике, низкий уровень материального благосостояния большинства населения). Вместе с тем недостаточное развитие ИКТ в России усугубляется целым рядом факторов, создающих препятствия для широкого внедрения и эффективного использования ИКТ в экономике, развития производства в сфере ИКТ. К числу таких негативных факторов относятся:

- несовершенная нормативная правовая база, разрабатывавшаяся без учета возможностей современных ИКТ;

- недостаточное развитие ИКТ в области государственного управления, неготовность органов государственной власти к применению эффективных технологий управления и организации взаимодействия с гражданами и хозяйствующими субъектами;
- отсутствие целостной информационной инфраструктуры и эффективной информационной поддержки рынков товаров и услуг, в том числе в сфере электронной торговли;
- недостаточный уровень подготовки кадров в области создания и использования ИКТ;
- барьеры, возникающие из-за недостатков в регулировании экономической деятельности при выходе российских предприятий и других организаций сферы ИКТ на российский и мировой рынки;
- высокий уровень монополизации сетей связи, создающий барьеры на пути их использования и приводящий к перекосам в тарифной политике.

Процессы информатизации уже активно идут на всех уровнях, многие мероприятия, направленные на развитие ИКТ, реализуются или планируются к реализации в рамках федеральных, региональных и ведомственных программ.

Федеральная целевая программа «Электронная Россия (2002-2010 годы)» (далее именуется — Программа) должна обеспечить формирование нормативной правовой базы в сфере ИКТ, развитие информационной и телекоммуникационной инфраструктуры, сформировать условия для подключения к открытым информационным системам (в том числе посредством сети Интернет), а также обеспечить эффективное взаимодействие органов государственной власти и органов местного самоуправления с гражданами и хозяйствующими субъектами на основе широкого внедрения ИКТ. В процессе выполнения Программы будут определяться общие направления развития ИКТ (основные принципы, стандарты и типовые решения по реализации различных проектов) как одного из основных направлений социально-экономического развития страны.

2. Цели, задачи, сроки и этапы реализации Программы:

Первый этап реализации Программы (2002 год).

Второй этап реализации Программы (2003-2004 годы).

Третий этап реализации Программы (2005-2010 годы).

Основными целями Программы являются создание условий для развития демократии, повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения ИКТ, обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширения подготовки специалистов по ИКТ и квалифицированных пользователей.

Реализация Программы позволит:

- эффективно использовать интеллектуальный и кадровый потенциал России в сфере ИКТ;
- обеспечить гармоничное вхождение России в мировую экономику на основе кооперации и информационной открытости;
- преодолеть отставание России от развитых стран в уровне использования и развития ИКТ;
- обеспечить равноправное вхождение граждан России в глобальное информационное сообщество на основе соблюдения прав человека, в том числе права на свободный поиск, получение, передачу, производство и распространение информации, а также права на обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах.

Для достижения целей Программы необходимо решить следующие задачи:

- сформировать эффективную нормативную правовую базу в сфере ИКТ, регулирующую в том числе вопросы обеспечения информационной безопасности и реализации прав, гарантированных *Конституцией* Российской Федерации;
- повысить эффективность взаимодействия органов государственной власти и органов местного самоуправления как между собой, так и с хозяйствующими субъектами и гражданами на основе использования современных ИКТ;
- обеспечить условия для повышения эффективности и более широкого использования ИКТ в экономической и социальной сфере;

- повысить уровень подготовки и переподготовки кадров за счет совершенствования образования на базе ИКТ;
- содействовать развитию независимых средств массовой информации посредством стимулирования внедрения ИКТ в их деятельность;
- содействовать развитию телекоммуникационной инфраструктуры и возможностей подключения к открытым информационным системам для граждан и хозяйствующих субъектов, а также существенно повысить качество предоставляемых услуг в этой области;
- сформировать единую информационную и телекоммуникационную инфраструктуру, необходимую для совершенствования работы органов государственной власти и органов местного самоуправления, предприятий и других организаций;
- сформировать условия, необходимые для широкого использования на товарных рынках России механизмов электронной торговли, способствующих ускорению продвижения товаров (услуг), поддержанию стабильного воспроизводства, удовлетворению нужд потребителей и повышению эффективности управления поставками продукции для федеральных государственных нужд.

Цели и задачи Программы определены с учетом Стратегии социально-экономического развития России на период до 2010 года, основных положений Окинавской хартии глобально-информационного общества, принятой на совещании Группы восьми 22 июля 2000 г. на острове Окинава, Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов, Доктрины информационной безопасности Российской Федерации.

Первый этап реализации Программы (2002 год).

На первом этапе формируются предпосылки для реализации мероприятий Программы. Это предполагает проведение анализа нормативной правовой базы с целью выявления ключевых проблем, препятствующих широкому внедрению ИКТ, изучение уровня информатизации экономики, анализ эффективности расходования бюджетных средств, выделяемых на информатизацию,

проведение полного учета государственных информационных ресурсов, анализ зарубежного опыта реализации подобных программ, изучение опыта работы в сфере ИКТ различных организаций.

В ходе первого этапа должны быть сформированы системы мониторинга:

- мировых тенденций развития ИКТ и их использования в социально-экономической сфере;
- уровня распространения ИКТ в стране;
- эффективности расходования бюджетных средств в сфере информатизации;
- эффективности использования ИКТ, информационных ресурсов в органах государственной власти и бюджетных организациях, обеспеченности их техническими средствами обработки информации и средствами связи;
- эффективности действующей нормативной правовой базы, регулирующей использование ИКТ, в том числе в социально-экономической сфере.

Наряду с формированием предпосылок для реализации Программы на первом этапе будет подготовлен пакет законопроектов, направленных на решение проблем, связанных с созданием и распространением электронных документов, развитием электронной торговли, снижением административных барьеров, препятствующих выходу российских организаций на рынки ИКТ, гармонизацией законодательства Российской Федерации в сфере ИКТ с положениями международных конвенций и законодательством стран Европейского союза.

Начнут реализовываться опытные проекты по переходу к электронному документообороту в органах государственной власти и органах местного самоуправления, развитию телекоммуникационной инфраструктуры и подключению к компьютерным сетям органов государственной власти, органов местного самоуправления и бюджетных организаций, развитию системы электронной торговли и поддержки рынка товаров (услуг), развитию системы подготовки специалистов для сферы ИКТ и квалифицированных пользователей.

Будет осуществлена подготовительная работа и начато осуществление опытных проектов по подключению к компьютерным се-

тям органов государственной власти, органов местного самоуправления и бюджетных организаций, созданию общественных пунктов подключения к общедоступным информационным системам.

Начнется разработка и реализация программы подготовки и переподготовки кадров по ИКТ для государственной и муниципальной службы, и прежде всего из числа работников бюджетных организаций, представителей средств массовой информации, безработных и социально не защищенных граждан.

Второй этап реализации Программы (2003-2004 годы).

На втором этапе на основе проведенных исследований, разработанных концепций и сформированной нормативной правовой базы будут реализованы проекты, обеспечивающие взаимодействие органов государственной власти и органов местного самоуправления с гражданами и хозяйствующими субъектами в сфере налогообложения, по вопросам оформления таможенной документации, регистрации и ликвидации юридических лиц, выдачи лицензий и сертификатов, подготовки и представления отчетной документации, предусмотренной законодательством Российской Федерации об акционерных обществах, рынке ценных бумаг и поставках продукции для федеральных государственных нужд.

В рамках Программы намечена реализация комплекса мероприятий по внедрению ИКТ в организациях государственного сектора экономики с целью создания системы мониторинга их финансово-экономической деятельности, реализации опытных проектов по внедрению унифицированных информационных систем для предприятий оборонно-промышленного комплекса. Будут созданы предпосылки для обеспечения передачи находящихся в государственной собственности передовых ИКТ организациям гражданской сферы, созданы технопарки как центры развития инновационного предпринимательства в сфере ИКТ.

На этом этапе будет создана основа единой информационной и телекоммуникационной инфраструктуры для органов государственной власти и органов местного самоуправления, бюджетных и некоммерческих организаций, системы электронной торговли в сфере поставок продукции для федеральных государственных нужд и для общественных пунктов подключения к общедоступным информационным системам.

Будет создана современная материально-техническая база для подготовки в ведущих образовательных учреждениях страны специалистов в сфере ИКТ и существенно увеличено число их выпускников.

Продолжится совершенствование нормативной правовой базы в сфере ИКТ. Будет развернута деятельность по продвижению российских товаров и услуг в сфере ИКТ на мировом рынке.

Третий этап реализации Программы (2005 - 2010 годы).

На третьем этапе будут созданы предпосылки для массового распространения ИКТ во всех сферах общественной деятельности на основе единой информационной и телекоммуникационной инфраструктуры и использования системы электронной торговли.

Будет обеспечено комплексное внедрение системы электронной торговли в сфере поставок продукции для государственных нужд на федеральном уровне и уровне субъектов Российской Федерации, стандартизованного электронного документооборота и систем обеспечения информационной безопасности.

На этом этапе будет завершено формирование единой информационной и телекоммуникационной инфраструктуры для органов государственной власти и органов местного самоуправления, бюджетных и некоммерческих организаций, общественных пунктов подключения к общедоступным информационным системам.

В результате создания эффективной системы правового регулирования, функционирования единой информационной и телекоммуникационной инфраструктуры, совершенствования системы государственного управления и подготовки кадров в сфере ИКТ будут сформированы предпосылки для структурной перестройки экономики.

3. Система программных мероприятий:

- совершенствование законодательства и системы государственного регулирования в сфере ИКТ;
- обеспечение открытости в деятельности органов государственной власти и общедоступности государственных информационных ресурсов, создание условий для эффективного взаимодействия между органами государственной власти и гражданами на основе использования ИКТ;

- совершенствование деятельности органов государственной власти и органов местного самоуправления на основе использования ИКТ;
- совершенствование взаимодействия органов государственной власти и органов местного самоуправления с хозяйствующими субъектами и внедрение ИКТ в реальный сектор экономики;
- развитие системы подготовки специалистов по ИКТ и квалифицированных пользователей;
- содействие развитию независимых средств массовой информации посредством внедрения ИКТ;
- развитие телекоммуникационной инфраструктуры и создание пунктов подключения к открытым информационным системам;
- разработка и создание системы электронной торговли;
- формирование общественной поддержки выполнения мероприятий Программы.

В Программе предусматривается реализация мероприятий по девяти основным направлениям.

Совершенствование законодательства и системы государственного регулирования в сфере ИКТ.

Целью мероприятий этого направления является создание правовых предпосылок для широкого использования ИКТ во всех сферах общественной жизни, в экономике, во взаимоотношениях органов государственной власти и местного самоуправления с гражданами и организациями.

Основными задачами, реализуемыми в рамках данного направления, являются создание правовой базы для решения проблем, связанных с производством и распространением документов в электронной цифровой форме, снижением административных барьеров и ограничений, препятствующих выходу организаций России на рынки ИКТ, обеспечение равных прав на получение информации из всех общедоступных информационных систем, усиление контроля целесообразности любого расширения перечня требований к хозяйствующим субъектам со стороны государственных и местных органов исполнительной власти, применение средств криптографии в сфере гражданско-правовых отношений.

Правовое регулирование ИКТ будет основываться на следующих принципах:

- обеспечение единства информационного пространства на территории Российской Федерации, ликвидация региональных и ведомственных барьеров на пути распространения информации;
- обеспечение беспрепятственной интеграции Российской Федерации в международные системы информационного обмена;
- обеспечение права каждого на свободное получение информации из общедоступных информационных систем;
- гласность и открытость разработки регулирующих норм путем привлечения общественности и предпринимателей к подготовке и обсуждению их проектов;
- гласность и открытость при рассмотрении заявлений на получение лицензий и сертификатов, общественный контроль за обоснованностью их выдачи или отказа в выдаче;
- создание равных условий и устранение монополизма в сфере ИКТ;
- создание правовых условий для использования электронных документов в государственном управлении и гражданско-правовой сфере;
- правовое решение проблем, связанных с проведением оперативно-разыскной деятельности в компьютерных сетях;
- упрощение процедур экспорта высокотехнологичной продукции, производимой в сфере ИКТ;
- комплексный подход к совершенствованию законодательства Российской Федерации в сфере ИКТ и его гармонизация с положениями международных конвенций и законодательством государств — членов Европейского союза.

Обеспечение открытости в деятельности органов государственной власти и общедоступности государственных информационных ресурсов, создание условий для эффективного взаимодействия между органами государственной власти и гражданами на основе использования ИКТ.

Основными задачами этого направления являются расширение объема информации и перечня информационных услуг, пре-

доставляемых гражданам и хозяйствующим субъектам органами государственной власти и органами местного самоуправления, формирование механизма общественного контроля их деятельности.

Решение этих задач будет основано на следующих принципах:

- открытость деятельности органов государственной власти и общедоступность государственных информационных ресурсов;
- обеспечение оперативного информационного взаимодействия граждан и органов государственной власти, повышение доверия граждан к государству;
- открытость процедур, связанных с проведением конкурсов на размещение заказов на поставки товаров, выполнение работ и оказание услуг для федеральных государственных нужд.

Использование ИКТ в работе органов государственной власти позволит расширить объем открытой информации о деятельности этих органов и обеспечить гражданам возможность ее оперативно-го получения из информационных систем, в том числе по таким актуальным вопросам, как законопроектная деятельность, бюджетный процесс, закупки продукции для федеральных государственных нужд, управление государственной собственностью, конкурсное замещение вакантных должностей.

Совершенствование деятельности органов государственной власти и органов местного самоуправления на основе использования ИКТ.

Основной задачей мероприятий данного направления является повышение эффективности работы органов государственной власти и органов местного самоуправления путем обеспечения совместимости стандартов хранения информации и документооборота, подключения к компьютерным сетям органов государственной власти и органов местного самоуправления, бюджетных учреждений, реализации отраслевых программ информатизации, создания межведомственных и местных информационных систем и баз данных. Использование ИКТ позволит обеспечить реализацию прав граждан России на свободное получение открытой информации из информационных систем, а также на использование других услуг, предоставляемых этими системами.

Использование ИКТ в деятельности органов государственной власти и органов местного самоуправления будет осуществляться по следующим направлениям:

- развитие системы электронного документооборота, локальных информационных сетей, использование стандартов делопроизводства и документооборота;
- преимущественное использование алгоритмов и программ для ЭВМ, тексты которых открыты и общедоступны;
- развитие систем межведомственного электронного документооборота, обеспечивающих сокращение сроков обработки документов;
- повышение качества принимаемых управленческих решений путем распространения опыта, накопленного в социально-экономической сфере, консультирования и повышения квалификации.

Реализация работ должна сопровождаться комплексом организационных мероприятий, обеспечивающих координацию деятельности органов власти в сфере информатизации, разработку и внедрение стандартных решений, эффективное использование выделяемых на эти цели бюджетных средств.

Совершенствование взаимодействия органов государственной власти и органов местного самоуправления с хозяйствующими субъектами и внедрение ИКТ в реальный сектор экономики.

Мероприятия этого направления предусматривают перевод в электронную цифровую форму большей части документооборота, осуществляемого между хозяйствующими субъектами, органами государственной власти и органами местного самоуправления.

Для достижения данной задачи необходимо:

- обеспечить согласованность действий органов государственной власти и органов местного самоуправления в процессе информационного обмена;
- обеспечить совместимость стандартов обмена информацией, документооборота, принципов защиты информации, использования электронной цифровой подписи;

- определить последовательность перехода к электронному документообороту.

В сфере содействия внедрению ИКТ в реальный сектор экономики основными задачами являются:

- развитие рынка научно-технической продукции;
- обеспечение эффективной передачи ИКТ, находящихся в государственной собственности, организациям гражданского сектора экономики;
- развитие телекоммуникационной инфраструктуры и создание общественных пунктов подключения к открытым информационным системам;
- сокращение издержек для выхода на рынок ИКТ новых хозяйствующих субъектов, стимулирование выхода российских производителей на мировой рынок ИКТ;
- стимулирование хозяйствующих субъектов к повышению открытости их деятельности.

В рамках данного направления реализуются задачи применения ИКТ в организациях государственного сектора, в том числе оборонно-промышленного комплекса, одним из результатов чего должно стать развитие системы электронной торговли.

Важную роль в реализации данного направления будут играть технопарки, создаваемые как центры развития инновационного предпринимательства в сфере ИКТ.

В рамках данного направления предполагается разработка и реализация комплекса мер по содействию внешнеэкономической деятельности, включающего финансирование части издержек российских предпринимателей в сфере ИКТ при выходе на мировые рынки, содействие продвижению продукции российских предприятий и других организаций на эти рынки, проведение мероприятий, популяризирующих Российскую Федерацию как поставщика продукции и услуг в сфере ИКТ, участие Российской Федерации в международных мероприятиях и программах развития ИКТ и стандартизации в сфере ИКТ, поддержка проведения конференций, симпозиумов, семинаров и других общественных мероприятий по актуальным вопросам развития сферы ИКТ.

При разработке и реализации мер содействия внешнеэкономической деятельности предусматривается участие предприни-

мателей, деловых кругов и общественных организаций, входящих в сферу ИКТ.

Развитие системы подготовки специалистов по ИКТ и квалифицированных пользователей.

Мероприятия этого направления нацелены на совершенствование системы подготовки специалистов для работы с современными ИКТ, ее структурное изменение, обеспечение современного материально-технического оснащения учебного процесса. Мероприятия разработаны с учетом *федеральной целевой программы* «Развитие единой образовательной информационной среды (2001—2005 годы)».

Широкое развитие ИКТ и их проникновение во все сферы жизни общества требует подготовки не только соответствующих специалистов в рамках профессиональных образовательных программ, но и квалифицированных пользователей. При этом необходимо прогнозировать потребности общества в специалистах на 10—15 лет вперед и способствовать организации этой работы в настоящее время.

Основными задачами данного направления являются:

- создание в отобранных учреждениях высшего профессионального образования современной методической и материально-технической базы подготовки и переподготовки специалистов для сферы ИКТ;
- формирование необходимой кадровой, методической и материально-технической базы в образовательных учреждениях начального и среднего профессионального образования;
- создание нормативной правовой базы информатизации образования и развития системы дистанционного обучения;
- развитие информационной и телекоммуникационной инфраструктуры в учреждениях среднего и высшего профессионального образования;
- » развитие системы приема на работу и продвижения по службе на конкурсной основе с использованием ИКТ.

Начата разработка и реализация программ переподготовки кадров государственной и муниципальной службы, бюджетных организаций, развития среднего и высшего профессионального образования на базе ИКТ.

В результате реализации указанных мероприятий будут сформированы профессиональные образовательные программы, созданы необходимые для их реализации аппаратные и программные средства.

Содействие развитию независимых средств массовой информации посредством внедрения **ИКТ**.

Содействие развитию независимых средств массовой информации предполагается осуществлять посредством:

- обучения работников средств массовой информации методам работы с современными средствами ИКТ;
- обеспечения общедоступности российских и международных открытых информационных ресурсов с помощью сети Интернет;
- создания электронных версий российских средств массовой информации и архивов в сети Интернет.

Использование ИКТ в средствах массовой информации будет осуществляться на основе конкурса проектов. При принятии решений о выделении средств из федерального бюджета для реализации подобных проектов будут учитываться профессиональный уровень творческих коллективов, наличие обоснованного проекта использования ИКТ и участие редакции в финансировании проекта. Конкурсы предполагается проводить на федеральном и региональном уровнях. При этом будет обеспечено тесное взаимодействие со сложившимися в данной сфере профессиональными объединениями.

Развитие телекоммуникационной инфраструктуры и создание **пунктов** подключения к открытым информационным системам.

Одна из принципиальных проблем, которую необходимо решить при реализации Программы, — отсутствие в ряде районов России необходимой телекоммуникационной инфраструктуры и высокие тарифы на подключение к компьютерным сетям (в том числе к сети Интернет). Это делает открытые информационные системы недоступными для граждан с невысокими доходами, а также существенно ограничивает возможность их использования образовательными и научными учреждениями, учреждениями здравоохранения и культуры, бюджетными организациями, мест-

ными средствами массовой информации, органами государственной власти и органами местного самоуправления.

Для решения этих задач Программой предусматриваются мероприятия по двум направлениям:

- содействие развитию общей телекоммуникационной инфраструктуры страны;
- создание пунктов подключения к общедоступным информационным системам.

Реализация мероприятий первого направления будет обеспечиваться преимущественно путем снижения административных барьеров и снятия ограничений для предпринимательской деятельности, повышения конкуренции и создания благоприятных условий для притока иностранных инвестиций в сферу ИКТ.

Мероприятия второго направления планируется осуществлять путем финансирования (в том числе долевого) за счет средств федерального бюджета развития пунктов подключения к общедоступным информационным системам органов государственной власти, бюджетных и некоммерческих организаций.

За счет средств федерального бюджета предполагается финансировать подключение к компьютерным сетям и текущие расходы на их использование территориальными органами и подразделениями федеральных органов исполнительной власти и государственных учреждений федерального подчинения. На условиях долевого финансирования предусматривается реализовать проекты по подключению к компьютерным сетям и оплате текущих расходов государственных учреждений субъектов Российской Федерации и муниципальных учреждений, образовательных и научных учреждений, учреждений здравоохранения и культуры, местных средств массовой информации, общественных пунктов подключения к компьютерным сетям, а также технопарков, действующих и создаваемых при университетах и научно-производственных центрах.

Для обеспечения подключения к открытым информационным системам будет максимально использоваться действующая инфраструктура телекоммуникационных сетей России, в том числе сеть связи общего пользования, ведомственные сети связи, а также сети, созданные в системе образования и для научных целей.

Разработка и создание системы электронной торговли.

Мероприятия этого направления предусматривают создание системы электронной торговли, в том числе для осуществления закупок продукции для федеральных государственных нужд. Такая система существенно повысит эффективность использования средств федерального бюджета и бюджетов субъектов Российской Федерации при осуществлении государственных закупок, а также создаст предпосылки для широкого использования ИКТ в процессе взаимодействия органов государственной власти и хозяйствующих субъектов.

Для внедрения методов и технологий электронной торговли потребуется уточнить и дополнить существующую нормативную правовую базу с учетом международных норм и принятых Россией международных обязательств в сфере торговли.

Для достижения этих целей необходимо создать:

- единую информационную инфраструктуру электронной торговли, включающую общероссийскую систему информационно-маркетинговых центров;
- систему электронной торговли для осуществления закупок продукции для федеральных государственных нужд;
- единую базу данных товаров и услуг и систему ее поддержки.

Создание системы электронной торговли для осуществления закупок продукции для федеральных государственных нужд позволит автоматизировать эти процессы во всех федеральных органах исполнительной власти, значительно уменьшить издержки государственных заказчиков при проведении конкурсов, сократить потери и злоупотребления. При этом для государственных заказчиков будут созданы типовые комплексы аппаратных и программных средств, необходимые для проведения электронной торговли при осуществлении закупок продукции для федеральных государственных нужд. Ожидается, что экономия бюджетных средств после внедрения системы составит примерно 15 процентов.

Система информационно-маркетинговых центров создается для решения следующих задач:

- формирование единого информационного пространства, объединяющего данные о предложении и спросе по всей номенклатуре товаров и услуг;
- подготовка информационно-аналитических материалов по различным аспектам состояния предложения и спроса товаров и услуг по регионам и по стране в целом;
- формирование условий для значительного увеличения числа хозяйствующих субъектов — постоянных пользователей компьютерных сетей;
- обеспечение информационной и функциональной взаимосвязи всех элементов, входящих в систему электронной торговли.

Создание системы информационно-маркетинговых центров будет способствовать поддержке и актуализации разрабатываемой в рамках данного направления единой базы данных о продукции и услугах, которая через компьютерные сети будет доступна для всех граждан, хозяйствующих субъектов и органов государственной власти.

Формирование общественной поддержки выполнения мероприятий Программы.

В рамках данного направления планируется осуществить следующие мероприятия:

- организация научно-практических конференций по проблемам развития ИКТ и их использованию в экономике России и социально-экономической сфере. По их результатам будут составляться рекомендации по внедрению принятых международным сообществом решений в области развития ИКТ, определяться основные перспективы и проблемы развития ИКТ в России;
- реализация системы мониторинга эффективности использования ИКТ и информационных ресурсов в органах государственной власти и государственном секторе экономики, а также технической обеспеченности органов государственной власти, что позволит своевременно определять и устранять недостатки;
- внедрение системы для слежения за выполнением нормативных правовых документов в области ИКТ, что позволит

своевременно выявить их нарушение, будет содействовать демонаполизации и снижению административных барьеров в сфере ИКТ;

- организация обсуждения через сеть Интернет стандартов, необходимых для распространения ИКТ, анализ распространения различных стандартов ИКТ и их применения в деятельности независимых организаций, что даст возможность принимать оптимальные решения при выработке стандартов ИКТ, сочетающих международную совместимость программных и технических средств с национальными интересами государства, граждан и хозяйствующих субъектов;
- обеспечение широкого информационного сопровождения Программы для привлечения к ней общественного внимания, осуществления поддержки ее реализации со стороны органов государственной власти и органов местного самоуправления, предпринимательских кругов, организаций в сфере науки, культуры и образования. В сети Интернет будет создана электронная страница, освещающая ход реализации Программы;
- осуществление мониторинга и анализ освещения в средствах массовой информации мероприятий, проводимых в рамках Программы, регулярная публикация аналитических обзоров о ходе реализации Программы, отражающих в обобщенном виде реакцию на нее средств массовой информации;
- ежегодное проведение конкурсов «Лучшее высшее учебное заведение в сфере ИКТ», «Лучшая школа в сфере ИКТ», «Лучший регион в сфере ИКТ», «Лучшее государственное учреждение в сфере ИКТ» для стимулирования внедрения и развития ИКТ.

4. Ресурсное обеспечение Программы.

Общий объем финансовых ресурсов, необходимых для реализации Программы, составляет 77179,1 млн рублей (в ценах 2002 года), в том числе средства федерального бюджета — 39383 млн рублей, средства бюджетов субъектов Российской Федерации — 22610,1 млн рублей (предположительно), внебюджетные источники — 15186 млн рублей.

Объем финансирования реализации первого этапа Программы (2002 год) составит 2604,4 млн рублей, второго этапа (2003-2004 годы) — 25480,5 млн рублей, третьего этапа (2005-2010 годы) — 49094,2 млн рублей.

Для реализации первого этапа Программы за счет средств федерального бюджета будет выделено 350 млн рублей, что составляет 13,4 процента общего планируемого объема финансирования этого этапа. Предполагается, что из средств бюджетов субъектов Российской Федерации и местных бюджетов будет выделено 1259,7 млн рублей (или 48,4 процента) и из внебюджетных источников — 994,8 млн рублей (или 38,2 процента).

На первом этапе Программы инвестиции составят 50 млн рублей (или 14,3 процента), расходы на научно-исследовательские и опытно-конструкторские работы — 100 млн рублей (или 28,6 процента) и на прочие нужды — 200 млн рублей (или 57,2 процента).

По результатам реализации первого этапа Программы будут уточнены мероприятия второго этапа и объемы внебюджетных средств, средств бюджетов субъектов Российской Федерации и местных бюджетов.

Для реализации второго этапа Программы за счет средств федерального бюджета будет выделено 13973,8 млн рублей, что составляет 54,8 процента общего планируемого объема финансирования этого этапа. Предполагается, что из средств бюджетов субъектов Российской Федерации и местных бюджетов будет выделено 7501,9 млн рублей (или 29,4 процента) и из внебюджетных источников — 4004,8 млн. рублей (или 15,7 процента).

На втором этапе Программы инвестиции составят 7987,6 млн рублей (или 57,2 процента), расходы на научно-исследовательские и опытно-конструкторские работы — 1327,6 млн рублей (или 9,5 процента) и на прочие нужды — 4658,6 млн рублей (или 33,3 процента).

Для реализации третьего этапа Программы за счет средств федерального бюджета будет выделено 25059,3 млн рублей, что составляет 51 процент общего планируемого объема финансирования этого этапа. Предполагается, что из средств бюджетов субъектов Российской Федерации и местных бюджетов будет выделено 13848,5 млн рублей (или 28,2 процента) и из внебюджетных источников — 10186,4 млн рублей (или 20,7 процента).

На третьем этапе Программы инвестиции составят 13380,3 млн рублей (или 53,4 процента), расходы на научно-исследовательские и опытно-конструкторские работы — 1765,5 млн рублей (или 7 процентов) и на прочие нужды — 9913,45 млн рублей (или 39,6 процента).

5. Механизм реализации Программы.

Министерство Российской Федерации по связи и информатизации совместно с другими государственными заказчиками разрабатывает и направляет в Министерство финансов Российской Федерации сводную бюджетную заявку на финансирование мероприятий Программы за счет средств федерального бюджета на очередной финансовый год.

Министерство Российской Федерации по связи и информатизации совместно с другими государственными заказчиками Программы с учетом финансовых средств, выделяемых на реализацию Программы из всех источников, и предварительных результатов выполнения мероприятий Программы уточняет мероприятия, промежуточные сроки реализации и объемы их финансирования.

Выполнение мероприятий Программы осуществляется посредством заключения государственных контрактов между государственными заказчиками и исполнителями программных мероприятий. Организации для выполнения программных мероприятий определяются в соответствии с *Федеральным законом* «О конкурсах на размещение заказов на поставки товаров, выполнение работ, оказание услуг для государственных нужд». Объемы финансирования мероприятий Программы включены расходы на осуществление конкурсных процедур.

Одним из принципов реализации Программы является привлечение внебюджетных финансовых средств для выполнения тех мероприятий, которые могут иметь коммерческую направленность. Предполагается, что для реализации мероприятий Программы будут привлекаться также средства бюджетов субъектов Российской Федерации и местных бюджетов, средства Международного банка реконструкции и развития, российских и иностранных инвесторов, а также других заинтересованных организаций. Формы их участия в реализации мероприятий Программы определяются договорами (контрактами) между ними и государственными заказчиками Программы.

Средства федерального бюджета для реализации мероприятий Программы, представляющих непосредственный интерес для регионов, отраслей и ведомств, будут предоставляться на условиях долевого финансирования целевых расходов.

6. Управление и контроль реализации Программы.

Система организации и контроля реализации Программы определяется государственными заказчиками Программы в соответствии с законодательством Российской Федерации.

Для управления реализацией Программы Министерство Российской Федерации по связи и информатизации создает в установленном порядке дирекцию Программы.

Министерство Российской Федерации по связи и информатизации совместно с другими государственными заказчиками Программы в установленном порядке разрабатывает и направляет в Министерство финансов Российской Федерации сводную бюджетную заявку на финансирование мероприятий Программы за счёт средств федерального бюджета на очередной финансовый год, ежегодно организует подготовку доклада о ходе реализации Программы и представляет его до 1 марта в Министерство экономического развития и торговли Российской Федерации (по инвестициям), Министерство промышленности, науки и технологий Российской Федерации (по научно-исследовательским и опытно-конструкторским работам) и в Министерство финансов Российской Федерации (по расходованию средств федерального бюджета).

Для координации деятельности по реализации Программы и координации вопросов финансирования других федеральных, ведомственных и региональных программ, содержащих задания по разработке и использованию ИКТ в Российской Федерации, образуется межведомственная комиссия, в состав которой могут включаться руководители заинтересованных федеральных органов исполнительной власти и субъектов Российской Федерации. В рамках этой межведомственной комиссии образуется экспертный совет, в который включаются представители деловых кругов, высших учебных заведений, Российской академии наук, других научных и профессиональных организаций, Торгово-промышленной палаты Российской Федерации, заинтересованных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

Указанная межведомственная комиссия осуществляет мониторинг и оценку эффективности реализации Программы и других программ в сфере ИКТ, взаимодействует с государственными заказчиками и другими заинтересованными федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации, в том числе рассматривает доклады о ходе реализации Программы, дает рекомендации и при необходимости представляет соответствующие предложения в Правительство Российской Федерации.

У. Ожидаемые конечные результаты реализации Программы.

Реализация Программы окажет воздействие на все сферы общественной жизни. Совершенствование нормативной правовой базы в сфере ИКТ, направленное на упрощение порядка лицензирования и процедур сертификации, будет способствовать ускорению темпов развития этой области экономики.

Реализация программных мероприятий приведет к увеличению количества хозяйствующих субъектов и развитию конкуренции в области ИКТ. При этом существенно повысятся стимулы для точного и полного соблюдения всех правовых норм, регламентирующих деятельность в сфере ИКТ, и сократится доля теневого рынка программного обеспечения, что позволит повысить доходы в этой области и увеличить налоговые поступления в бюджет.

Повышение спроса на продукцию ИКТ, вызванное их широким использованием в деятельности органов государственной власти и органами местного самоуправления, обеспечит в период до 2005 г. прирост отечественного производства товаров и услуг в этой сфере и рост экспорта в размере 15-20 процентов ежегодно. Предполагается, что объем рынка информационных услуг и программного обеспечения возрастет к 2005 году в 2-3 раза и к 2010 г. — в 5-6 раз. Доля ИКТ в экономике увеличится в несколько раз и составит к 2010 г. не менее 2 процентов общего объема российского рынка.

Быстрое развитие ИКТ, расширение применения современных ИКТ во всех сферах общественной жизни будет способствовать формированию более прогрессивной структуры экономики, создаст принципиально новые возможности для наращивания производства и экспорта отечественной высокотехнологичной продукции.

Реализация мероприятий Программы в области подготовки кадров и создание нормативной правовой базы для внешнеэкономической деятельности в сфере ИКТ позволят многократно увеличить объем экспорта из России информационных продуктов и услуг, который с учетом конъюнктуры мирового рынка к 2005 году составит более 2 млрд долларов США.

Предусмотренные Программой меры по модернизации государственного управления и местного самоуправления обеспечат кардинальное ускорение процессов информационного обмена в экономике и обществе в целом, в том числе между гражданами и органами государственной власти, повышение эффективности государственного управления и местного самоуправления, создание принципиально новых возможностей для мониторинга процессов в экономике и обществе и принятия своевременных решений по регулированию этих процессов и, как следствие, рост числа граждан и организаций, использующих ИКТ во взаимоотношениях с органами государственной власти и органами местного самоуправления.

Использование современных ИКТ при осуществлении работы федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления позволит сократить издержки на управление, в том числе за счет высвобождения части технического персонала этих органов. Долю электронного документооборота в общем объеме документооборота в этих органах предполагается довести до 65 процентов внутри ведомств и до 40 процентов в межведомственном документообороте.

Создание системы электронной торговли для осуществления закупок продукции для федеральных государственных нужд позволит сэкономить от 20 до 40 процентов средств соответствующих бюджетов, выделяемых на подготовку и проведение торгов и организацию закупок.

Большое значение будет иметь интеграция государственных и муниципальных информационных ресурсов в единую информационную систему, что позволит сократить возможности для финансовых махинаций, нарушения законов, уклонения от уплаты налогов.

В результате реализации Программы фактически сформируется единый порядок сбора, обработки, накопления, хранения, по-

иска и распространения информации (информационный процесс), что существенно повысит возможности координации действий силовых структур и будет способствовать повышению безопасности и обороноспособности страны.

Предусматриваемые Программой меры по ускорению распространения современных способов передачи информации и внедрению электронного документооборота в сфере предпринимательства приведут к сокращению времени на заключение сделок, осуществление взаимодействия с органами государственной власти, органами местного самоуправления и, в конечном счете, к сокращению торговых издержек, повышению конкурентоспособности отечественной продукции.

Реализация Программы создаст необходимые условия для приведения стандартов России в сфере ИКТ в соответствие с мировой системой стандартов, будет способствовать расширению присутствия России в сети Интернет, увеличению количества направлений и масштабов участия России в международном разделении труда. Показателем эффективности Программы в этой области будут объемы произведенных в России информационных ресурсов в сети Интернет, их доля в общих мировых ресурсах, а также объемы внешнеэкономической деятельности в сфере ИКТ.

Большое значение будет иметь создание единого информационного пространства на всей территории страны. Развитие ИКТ создаст предпосылки для преодоления экономического отставания отдельных территорий, обеспечит гражданам и организациям независимо от мест проживания и расположения равную общедоступность всех отечественных и мировых открытых информационных ресурсов.

Вследствие особой географической протяженности и организационной централизации информационных ресурсов России во многих регионах особо важно наличие возможности подключения к удаленным информационным системам для обеспечения граждан и хозяйствующих субъектов необходимыми сведениями. Развитие ИКТ потенциально позволит всем гражданам получать медицинские, юридические и иные виды консультационных услуг, оказываемых высококвалифицированными специалистами, существенно увеличит возможности обучения и повышения квалификации с помощью системы дистанционного обучения, явится важным шагом на пути развития демократии и реального обеспе-

чения равных прав всех граждан в области информации. Показателем наличия таких потребностей может служить быстрый рост числа пользователей сети Интернет и объема получаемых с ее помощью услуг.

Реализация мероприятий Программы обеспечит опережающий рост числа пользователей компьютерных сетей и объемов передаваемой информации по сравнению с ростом числа компьютеров. Прогнозируется, что количество пользователей сети Интернет вырастет к 2005 году по сравнению с 2000 годом более чем в 8 раз. Важным условием распространения сети Интернет являются тарифы на подключение и использование этой сети. Ожидается, что расширение рынка услуг в сфере ИКТ позволит снизить эти тарифы к 2005 году на 40 процентов, к 2010 году примерно вдвое и довести месячный тариф за произвольное время подключения к сети Интернет до *3 минимальных размеров оплаты труда*.

На базе развития современных методов информационного взаимодействия органов государственной власти и органов местного самоуправления с гражданами и организациями появятся принципиально новые возможности для обеспечения открытости и гласности принятия решений, повышения уровня доверия и взаимодействия, сокращения затрат времени на реализацию гражданами России своих конституционных прав и обязанностей.

Значительное место в Программе уделено мероприятиям по развитию технологий обучения с использованием ИКТ и подготовке специалистов в сфере ИКТ, в результате чего повысится эффективность обучения, упростится получение гражданами образования путем широкого использования информационных ресурсов в области образовательных программ. Кроме того, в результате реализации мероприятий Программы в сфере образования будет обеспечено повышение общего уровня грамотности граждан в области современных методов работы с информацией, развитие системы подготовки специалистов для сферы ИКТ. Предусмотренные в Программе темпы распространения ИКТ резко увеличат потребность в специалистах в этой области. К 2005 году ежегодная потребность в специалистах со средним и высшим профессиональным образованием составит до 100 тыс. человек, а к концу срока действия Программы — более 130 тыс. человек. Программой предусмотрено обеспечить к 2005 году подготовку ежегодно не менее 25 тыс. специалистов в сфере ИКТ с высшим

профессиональным образованием и не менее 60 тыс. специалистов в этой области — с начальным и средним профессиональным образованием. Дальнейшее развитие кадрового потенциала будет определяться потребностями в указанных специалистах. С учетом реализации *федеральной целевой программы «Развитие единой образовательной информационной среды (2001-2005 годах)»* предполагается подключить к информационным системам (включая подключение к сети Интернет) к 2005 году все высшие учебные заведения, а к 2010 году — все средние специальные учебные заведения.

В целом реализация Программы позволит существенно повысить конкурентоспособность экономики страны за счет снижения издержек и повышения качества продукции и услуг, эффективности государственного управления и местного самоуправления, обеспечит рост качества жизни граждан, сократит отставание от развитых стран мира, позволит избежать информационной и экономической изоляции от мировой экономики и мирового сообщества, обеспечит развитие процессов международной интеграции.

Олег Александрович Городов
Комментарий к Федеральному закону
«Об информации, информатизации
и защите информации»

Главный редактор	<i>Е. Строганова</i>
Заведующий редакцией	<i>И. Андреева</i>
Руководитель проекта	<i>В. Зассеева</i>
Выпускающий редактор	<i>О. Морозова</i>
Художественный редактор	<i>Р. Яцко</i>
Редактор	<i>О. Кувакина</i>
Корректоры	<i>Л. Ванькаева, С. Шаханова</i>
Верстка	<i>М. Кеслер, О. Морозова</i>

ООО «Питер Принт». 196105, Санкт-Петербург, ул. Благодатная, д. 67в.
Лицензия ИД № 05784 от 07.09.01.
Налоговая льгота — общероссийский классификатор продукции ОК 005-93,
том 2; 95 3005 — литература учебная.
Подписано в печать IS.03.03. Формат 60 х 90/16. Усл. п. л. 17. Тираж 5000.
Заказ № 4.
Отпечатано с готовых диапозитивов в ООО «Типография Правда 1906».
191119, С.-Петербург, Социалистическая ул., 14.



О. А. Городов

**КОММЕНТАРИЙ
К ФЕДЕРАЛЬНОМУ ЗАКОНУ
ОБ ИНФОРМАЦИИ,
ИНФОРМАТИЗАЦИИ
И ЗАЩИТЕ ИНФОРМАЦИИ**

*В издательстве «Питер» вышли
и готовятся к выпуску:*

Налоговый кодекс Российской Федерации

Гражданский кодекс Российской Федерации (3 части)

Уголовно-процессуальный кодекс Российской Федерации

Трудовой кодекс Российской Федерации. Практический комментарий

*Комментарий Федерального закона
«Об оперативно-розыскной деятельности»*

*Комментарий Федерального закона
«Об исполнительном производстве»*

*Постатейный комментарий к Федеральному закону
«Об адвокатской деятельности и адвокатуре в Российской Федерации»*

Комментарий Уголовно-процессуального кодекса РФ

Комментарий Гражданско-процессуального кодекса РФ

Комментарий Арбитражно-процессуального кодекса РФ

Комментарий к Конституции РФ (постатейный)

Заказ наложенным платежом:

197198, С.-Петербург, а/я 619
e-mail: postbook@piter.com
для жителей России



61093, г. Харьков-93, а/я 9130, ООО «Питер»
e-mail: piter@tender.kharkov.ua
Тел.: (0572) 23-75-63,
28-20-05 (факс)
для жителей Украины

ПИТЕР
WWW.PITER.COM

Посетите наш web-магазин:

www.piter.com

ISBN 5-94723-539-0

