

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПУТЕЙ СООБЩЕНИЯ (МИИТ)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

А. А. ЧЕБОТАРЕВА

ИНФОРМАЦИОННОЕ ПРАВО

Учебное пособие

МОСКВА — 2014

УДК 340 (075)
ББК 67.401.114я7
Ч—343
ISBN 5-7876-0072-X

Чеботарева, А. А. Информационное право : учеб. пособие /
А. А. Чеботарева. — М. : Юридический институт МИИТа, 2014. —
160 с.

В предлагаемом учебном пособии изложены основные темы учебной дисциплины «Информационное право». Учебное пособие подготовлено на базе действующего законодательства.

При работе с учебным пособием использовалась Справочная правовая система КонсультантПлюс.

Предназначается для студентов, изучающих «Информационное право», а также для слушателей и преподавателей, интересующихся вопросами информационного права.

© Чеботарева А. А., 2014

© Юридический институт МИИТа, 2014

Изд. заказ 26	Бумага офсетная	Тираж 40 экз.
Подписано в печать 07.08.2014	Печать трафаретная	Цена договорная
Усл. печ. л. 10,5	Уч.-изд. л. 7,4	Формат 60×90 ¹ / ₁₆

127994, Москва, ул. Образцова, д. 9, стр. 9.

ОГЛАВЛЕНИЕ

Предисловие	6
Введение	8
Глава 1. Информационное общество. Государственная политика в области информации	10
1.1. Понятие информации	10
1.2. Понятие и признаки информационного общества	13
1.3. Государственная информационная политика: цели, задачи, особенности реализации	15
<i>Вопросы и задания для самоконтроля</i>	<i>20</i>
<i>Нормативные правовые акты.....</i>	<i>20</i>
Глава 2. Информационное право как отрасль российского права	21
2.1. Понятие информационного права, его предмет и метод. Принципы информационного права	21
2.2. Система и источники информационного права	31
2.3. Информационное право в системе российского права. Информационное право как наука	36
<i>Вопросы и задания для самоконтроля</i>	<i>39</i>
<i>Нормативные правовые акты.....</i>	<i>39</i>
Глава 3. Информационные правоотношения. Информационно-правовые нормы	40
3.1. Информационные правоотношения: понятие, содержание, субъекты. Условия возникновения, изменения и прекращения информационных правоотношений	40
3.2. Понятие и признаки информационно-правовых норм	43
<i>Вопросы и задания для самоконтроля</i>	<i>46</i>
<i>Нормативные правовые акты.....</i>	<i>46</i>
Глава 4. Право на информацию как институт информационного права	47
4.1. Общая характеристика права на информацию	47
4.2. Доступ к информации о деятельности государственных органов и органов местного самоуправления	50
<i>Вопросы и задания для самоконтроля</i>	<i>52</i>
<i>Нормативные правовые акты.....</i>	<i>53</i>

Глава 5. Институт правового режима информационных ресурсов	53
5.1. Понятие информационного ресурса	53
5.2. Основные категории информационных ресурсов.	
Общедоступная информация и информация ограниченного доступа	56
<i>Вопросы и задания для самоконтроля</i>	<i>59</i>
<i>Нормативные правовые акты.....</i>	<i>59</i>
 Глава 6. Институт электронного документооборота	 60
6.1. Значение электронного документооборота в современных условиях развития электронного государства. Электронная подпись.....	60
6.2. Понятие электронного документооборота. Электронный документ ...	66
<i>Вопросы и задания для самоконтроля</i>	<i>70</i>
<i>Нормативные правовые акты.....</i>	<i>70</i>
 Глава 7. Глобальные информационные системы. Интернет. Средства массовой информации. Интернет-СМИ	 72
7.1. Правовая природа Интернета и Интернет-отношений	72
7.2. Понятие средств массовой информации. Конституционные гарантии свободы массовой информации	78
7.3. Средства массовой информации, функционирующие в сети Интернет	80
7.4. Интернет-диффамация: вопросы юридической ответственности	87
<i>Вопросы и задания для самоконтроля</i>	<i>94</i>
<i>Нормативные правовые акты.....</i>	<i>94</i>
 Глава 8. Электронное государство как институт информационного права и его реализация в триаде ветвей власти	 96
8.1. Понятие электронного государства. Электронный парламент и электронное голосование	96
8.2. Электронное правительство. Вопросы предоставления государственных и муниципальных услуг в электронном виде	101
8.3. Электронное правосудие как форма реализации судебной власти в электронном государстве	108
<i>Вопросы и задания для самоконтроля</i>	<i>111</i>
<i>Нормативные правовые акты.....</i>	<i>111</i>
 Глава 9. Персональные данные как институт информационного права	 113
9.1. Основные подходы к регулированию правоотношений по поводу персональных данных в зарубежных странах	113
9.2. Федеральный закон «О персональных данных» — основа действующего законодательства в сфере защиты персональных данных.....	118

<i>Вопросы и задания для самоконтроля</i>	125
<i>Нормативные правовые акты</i>	126

Глава 10. Значение и проблематика информационной

безопасности	127
10.1. Подходы к определению понятия «информационная безопасность».	
Задачи и гарантии обеспечения информационной безопасности	127
10.2. Информационная безопасность личности как приоритетная	
задача электронной России	137
<i>Вопросы и задания для самоконтроля</i>	146
<i>Нормативные правовые акты</i>	146
Список рекомендуемой литературы	148
Словарь-справочник	152

ПРЕДИСЛОВИЕ

Информационное право — одна из наиболее динамично развивающихся отраслей российского права, в основе которой — правовое регулирование общественных отношений, возникающих в процессе поиска, получения, передачи, производства и распространения информации, а также связанных с ними отношений.

Основное назначение учебного пособия — помочь студентам в короткие сроки качественно усвоить основные положения информационного права, получить представление о его основных институтах, а также подготовиться к сдаче зачета/экзамена. Используя учебное пособие, студенты могут систематизировать и конкретизировать свои знания по предмету, повторить основные понятия, сформулировать примерный план ответа.

Учебное пособие предназначается для студентов, изучающих «Информационное право», а также для слушателей и преподавателей, интересующихся вопросами информационного права. В результате изучения названной дисциплины студент должен:

знать

- основные закономерности создания и функционирования информационных процессов в правовой сфере;
- основы государственной политики в области информатики;
- методы и средства поиска, систематизации и обработки правовой информации;

уметь применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации;

владеть навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.

В результате изучения дисциплины студент должен ***обладать следующими общекультурными компетенциями (ОК):***

- понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования

информационной безопасности, в том числе защиты государственной тайны (ОК-10);

— работать с информацией в глобальных компьютерных сетях (ОК-12).

Каждая из глав предлагаемого учебного пособия начинается перечнем основных рассматриваемых вопросов и перечнем нормативно-правовых актов. Усвоить предмет, закрепить полученные знания поможет содержащееся в пособии приложение — Словарь-справочник.

Для самостоятельной работы студентов над темами курса и подготовки к семинарским занятиям к каждой из глав учебного пособия предлагаются вопросы для самоконтроля.

Учебное пособие подготовлено с учетом последних существенных изменений в информационном законодательстве.

ВВЕДЕНИЕ

Актуальность курса «Информационное право» и необходимость его преподавания в юридических вузах объясняется тем, что информационное право является правовым фундаментом экономических и политических преобразований, происходящих в России в последние годы.

Важную роль при подготовке учебного пособия сыграли существующие научные разработки, посвященные изучению различных вопросов информационного права. Среди ученых, специалистов в области информационного права, к трудам которых обращался автор, следует назвать И.Л. Бачило, П.У. Кузнецова, Т.А. Полякову, В.Н. Лопатина, А.В. Морозова, М.М. Рассолова, В.А. Копылова и др.

В структурном отношении учебное пособие состоит из десяти глав. Первая посвящена анализу информационной системы РФ, рассмотрению специфики государственной информационной политики. Во второй главе идет речь об информационном праве как отрасли права. В этой связи определены основные принципы информационного права, рассмотрены вопросы его предмета, метода правового регулирования информационных правоотношений, системы и источников информационного права, выделены актуальные проблемы науки информационного права на современном этапе развития Российской Федерации как электронного государства.

Третья глава учебного пособия охватывает вопросы особенностей информационно-правовых норм и информационных правоотношений. В четвертой главе рассмотрены проблемы, связанные с реализацией права на информацию, в пятой — анализируется понятие информационного ресурса, характеризуются основные категории информационных ресурсов. Шестая глава посвящена институту электронного документооборота, седьмая — правовой природе Интернета и Интернет-отношений, а также средствам массовой информации, при этом акцентируется внимание на специфике Интернет-СМИ.

Восьмая глава охватывает раскрытие таких актуальнейших институтов современной России, как электронное государство, электронный парламент, электронная демократия, электронное правительство, электронное правосудие. В девятой главе приводятся основные подходы к регулированию правоотношений по поводу персо-

нальных данных. Завершает пособие глава, посвященная проблемам обеспечения информационной безопасности.

Учебное пособие «Информационное право» в первую очередь адресовано студентам, изучающим данную дисциплину, магистрантам, аспирантам, всем тем, кто интересуется вопросами информационного права.

Глава 1. ИНФОРМАЦИОННОЕ ОБЩЕСТВО. ГОСУДАРСТВЕННАЯ ПОЛИТИКА В ОБЛАСТИ ИНФОРМАЦИИ

Понятие информации. Роль информации в жизни личности, общества, государства. Понятие, признаки информационного общества. Государственная программа «Информационное общество (2011—2020 годы)». Цели и задачи государственной информационной политики.

1.1. Понятие информации

Термин «информация» имеет латинские корни и произошел от слова *information* — разъяснение, осведомление, изложение¹.

В общем смысле информация представляет собой сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком; сообщения, осведомляющие о положении дел, о состоянии чего-либо². Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» *информация* — это сведения (сообщения, данные) независимо от формы их представления.

И.Л. Бачило в одном из своих учебников упоминает, что наука об информации — информатика — стала формироваться несколько веков назад. Ее упрощенно трактуют как научную дисциплину, изучающую закономерности получения, отбора, хранения, передачи, преобразования и применения информации (знаний) в самых разных областях общественной деятельности...Разрешение правовых про-

¹ См.: Википедия (Электронный ресурс): свободная интернет-энциклопедия. М.: WIKIPEDIA.RU, 2001-2014. Режим доступа: World Wide Web. URL: <http://ru.wikipedia.org>.

² Информационная безопасность и защита информации : учеб. пособие. Томск : ТПУ, 2009. С. 40.

блем информатики можно рассматривать как сферу информационного права¹.

Информация является основным объектом, по поводу которого возникают общественные отношения между различными субъектами в информационной сфере. Являясь разновидностью правовых отношений, информационные отношения регулируются информационно-правовыми актами, которые устанавливают порядок распространения информации, доступа к ней, ограничения, защиты и т.п.

В настоящее время для регулирования информационных отношений действует значительное количество норм, регламентирующих технические и правовые аспекты информационного обмена, информационных технологий и обеспечения информационной безопасности как на уровне нормативных правовых актов, так и на уровне различных ведомственных нормативных и ненормативных актов.

Реализация права на осуществление, поиск, получение и передачу информации (право на доступ к информации или право знать) является важнейшим определяющим институтом информационного права. Юридический фундамент этого института составляют информационно-правовые нормы Конституции РФ. Право на доступ к информации содержится в ст. 29 Конституции: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

Основу российского законодательства об информации составляет Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В ст. 2 этого Закона дается определение *информации*, согласно которому она представляет собой сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

И.Л. Бачило определяет *информацию* как воспринимаемую и понимаемую человеком характеристику окружающего мира во всем его разнообразии, которая возникает в процессе познания последнего и позволяет на основе свойств предметов, процессов, фактов и отражения их в различных формах восприятия отличать их признаки, зна-

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 28.

чения и устанавливать связи и зависимости всего многообразия проявления материального, духовного, идеологического мира — формировать мировую систему знаний¹.

К числу признаков, свойств информации можно отнести:

а) ее системность. Информация, как и любой другой объект реальности, обладает системной структурой. Совокупность информации о чем-либо формирует понятие «знание»;

б) неисчерпаемость информации;

в) материальность информации (информация — это нечто, что может объективно существовать (к примеру, на материальном носителе), кроме того, она отражает многообразие материального мира;

г) объективность информации: информация — отражение внешнего объективного мира;

д) идеальность информации — часто информацию мы воспринимаем с помощью технических средств.

Существует множество критериев классификации информации.

1) по степени организованности (упорядоченности) выделяют документированную и иную информацию; информационные ресурсы и свободную информацию, не находящуюся в информационных системах; систематизированную информацию (каталоги, энциклопедии, рубрикаторы и т.п.) и несистематизированную;

2) по виду носителя (форме закрепления) — на бумажном носителе, видео- и звуковая, компьютерная информация, в объемно-пространственной форме, устная, энергетическая (биологическая) при энергоинформационном обмене;

3) по степени доступа — информация с ограниченным доступом, информация без права ограничения доступа, объекты интеллектуальной собственности, «вредная информация» с ограничением по распространению, иная общедоступная информация;

4) по функциональному предназначению (по сфере применения) — массовая информация, распространяемая через СМИ, и отраслевая, профессиональная (по интересам) информация и т.д.

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 28.

1.2. Понятие и признаки информационного общества

Информационное общество — это термин, применяемый для обозначения современного состояния индустриально развитых стран, связанного с новой ролью информации во всех сторонах их жизнедеятельности, качественно новым уровнем производства, переработки и распространения информации.

Своим названием термин «информационное общество» обязан профессору Токийского технологического института Ю. Хаяши, чей термин был использован в появившихся практически одновременно — в Японии и США — в работах Ф. Махлупа (1962) и Т. Умесао (1963). Теория «информационного общества» была развита такими известными авторами, как М. Порат, Й. Массуда, Т. Стоунер, Р. Карц и др¹.

Как отмечает В.А. Копылов², в соответствии с концепцией З. Бжезинского, Д. Белла, О. Тоффлера, поддерживаемой и другими зарубежными учеными, информационное общество — разновидность постиндустриального общества. Рассматривая общественное развитие как «смену стадий», сторонники этой концепции информационного общества связывают его становление с доминированием «четвертого», информационного сектора экономики, следующего за тремя известными секторами — сельским хозяйством, промышленностью и экономикой услуг. При этом они утверждают, что капитал и труд, как основа индустриального общества, уступают место информации и знаниям в информационном обществе.

К признакам информационного общества можно отнести:

- 1) высокий уровень развития информационных технологий и их интенсивное использование гражданами, бизнесом и органами государственной власти;
- 2) получение гражданами и организациями преимуществ от применения информационных технологий за счет:
 - а) обеспечения равного доступа к информационным ресурсам;
 - б) развития цифрового контента;

¹ См.: Википедия (Электронный ресурс): свободная интернет-энциклопедия. М.: WIKIPEDIA.RU, 2001-2014. Режим доступа: World Wide Web. URL: <http://ru.wikipedia.org>.

² Копылов В. А. Информационное право : учеб. пособие. М. : Юристъ, 1999. С. 21.

в) применения инновационных технологий и радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе.

И.Л. Бачило акцентирует внимание на вопросе синтеза информационного и гражданского, а, следовательно, и правового общества¹.

И.М. Рассолов² видит структуру информационного общества двухуровневой, включающей:

— интересы и ценности;

— индивиды, территория и социальные структуры.

При этом важным фактором формирования информационного общества являются общественные связи или информационные отношения. Схематично это выглядит следующим образом:

Интересы + ценности

И + Т + СС

Итого: информационные отношения.

Охарактеризуем основные элементы представленной структуры информационного общества.

Интересы — это причины действий или поступков, а также выражение значимости объектов окружающего мира для человека.

Ценности — это установки и оценки, императивы и запреты, цели и проекты, выраженные в форме нормативных представлений, т.е. «ориентиры деятельности человека».

Индивид является основным элементом любого общества, в том числе и информационного, а территория является основой социального информационного пространства.

Под социальными структурами понимаются устойчивые социальные образования, социальные общности и социальные институты. К примеру, приобретший сегодня особенную популярность твиттер.

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 317.

² Рассолов И.М. Информационное право : учебник. М. : Юрайт, 2011. С. 24—26.

1.3. Государственная информационная политика: цели, задачи, особенности реализации

Государственную информационную политику определяют как совокупность целей, отражающих национальные интересы в информационной сфере, стратегии, тактики управленческих решений и методов их реализации, разрабатываемых и реализуемых государственной властью для регулирования и совершенствования, как непосредственно процессов информационного взаимодействия во всех сферах жизнедеятельности общества и государства, так и процессов технологического (в широком смысле) обеспечения такого взаимодействия¹.

В деятельности органов власти по разработке и реализации государственной политики в области развития информационного общества в России можно выделить несколько этапов.

1 этап (1991—1994 гг.) — формирование основ в сфере информатизации;

2 этап (1994—1998 гг.) — смена приоритетов от информатизации к выработке информационной политики;

3 этап (с 1998 г. и по настоящее время).— формирование политики в сфере построения информационного общества.

В соответствии со Стратегией развития информационного общества в Российской Федерации², целями формирования и развития информационного общества в Российской Федерации являются повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

При этом цели государственной политики определяют необходимость решения задач не только в сфере информационных технологий, но и в других отраслях экономики, науке и технике, социальной сфере и государственном управлении.

¹ Нисневич Ю. А. Информационная политика России: проблемы и перспективы. М., 1999. С. 4.

² Российская газета. 2009. 16 февр. № 34.

Государственная программа «Информационное общество (2011—2020 годы)» определяет конкретные задачи в процессе построения информационного общества современной России.

Повышение качества жизни граждан и улучшение условий развития бизнеса в информационном обществе предусматривает:

- развитие сервисов для упрощения процедур взаимодействия общества и государства с использованием информационных технологий;

- перевод государственных и муниципальных услуг в электронный вид;

- развитие инфраструктуры доступа к сервисам электронного государства;

- повышение открытости деятельности органов государственной власти;

- создание и развитие электронных сервисов в области здравоохранения, а также в областях жилищно-коммунального хозяйства, образования и науки, культуры и спорта.

Построение электронного правительства и повышение эффективности государственного управления предусматривает:

- формирование единого пространства электронного взаимодействия;

- создание и развитие государственных межведомственных информационных систем, предназначенных для принятия решений в реальном времени;

- создание справочников и классификаторов, используемых в государственных и муниципальных информационных системах;

- повышение эффективности внедрения информационных технологий на уровне субъектов РФ и муниципальных образований;

- создание инфраструктуры пространственных данных РФ;

- развитие системы учета результатов научно-исследовательских и опытно-конструкторских работ, выполненных в рамках государственного заказа;

- обеспечение перевода в электронный вид государственной учетной деятельности;

- создание и развитие специальных информационных и информационно-технологических систем обеспечения деятельности органов государственной власти, в том числе защищенного сегмента

сети Интернет и системы межведомственного электронного документооборота.

Развитие российского рынка информационных технологий, обеспечение перехода к экономике, осуществляемой с помощью информационных технологий, предусматривает:

- стимулирование отечественных разработок в сфере информационных технологий;

- подготовку квалифицированных кадров в сфере информационных технологий;

- развитие экономики и финансовой сферы на основе использования информационных технологий;

- формирование социально-экономической статистики развития информационного общества;

- развитие технопарков в сфере высоких технологий.

Преодоление высокого уровня различия в использовании информационных технологий регионами, различными слоями общества и создание базовой инфраструктуры информационного общества предусматривает:

- развитие телерадиовещания;

- развитие базовой инфраструктуры информационного общества;

- популяризацию возможностей и преимуществ информационного общества;

- повышение готовности населения и бизнеса к возможностям информационного общества, в том числе обучение использованию современных информационных технологий.

Обеспечение безопасности в информационном обществе предусматривает:

- противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам Российской Федерации;

- обеспечение технологической независимости Российской Федерации в отрасли информационных технологий;

- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасность информации ограниченного доступа;

— обеспечение развития законодательства РФ и совершенствование правоприменительной практики в сфере информационных технологий.

— Развитие цифрового контента и сохранение культурного наследия предусматривает:

— оцифровку объектов культурного наследия, включая архивные фонды;

— развитие средств обработки и предоставления удаленного доступа к цифровому контенту.

Итоговым результатом Программы станет наличие широкого спектра возможностей использования информационных технологий в производственных, научных, образовательных и социальных целях. Эти возможности будут доступны для любого гражданина вне зависимости от его возраста, состояния здоровья, региона проживания и любых других характеристик. Возможности использования информационных технологий обеспечиваются за счет создания соответствующей инфраструктуры, обеспечения цифрового контента и подготовки пользователей.

Совершенствование системы государственных гарантий конституционных прав человека и гражданина в информационной сфере будет обеспечиваться постоянным мониторингом законодательства РФ, актуализацией нормативных правовых актов, приведением их в соответствие с требованиями текущих потребностей информационного общества и международными нормами права.

Значимым результатом Программы должно стать повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг, а также снижение стоимости обеспечения государственного управления.

Эффекты, возникающие при использовании информационных технологий в различных сферах деятельности, в конечном итоге повлияют на повышение качества жизни граждан вне зависимости от их возраста, состояния здоровья и региона проживания, а также на повышение производительности труда и конкурентоспособности российских товаров.

В результате выполнения мероприятий Программы любому гражданину, например:

- для того чтобы получить государственную услугу, достаточно будет один раз дистанционно заполнить форму запроса, а через определенное время получить необходимый документ в свой почтовый ящик или проверить наличие изменений о своей персоне в соответствующей базе данных;

- для того чтобы выразить свое мнение по тому или иному вопросу или сформировать группу единомышленников для воплощения какой-либо инициативы, достаточно будет зайти на соответствующий сайт в сети Интернет;

- для того чтобы собрать ученика в школу, достаточно будет скачать информацию из комплекта учебников и сопутствующих материалов с регионального образовательного портала и сохранить их в электронной книге;

- для того чтобы сдать налоговую отчетность, не нужно будет посещать налоговую инспекцию;

- для того чтобы получить консультацию специалиста, пациенту не нужно будет ехать в медицинский центр, а достаточно будет оставить свои документы на портале и в назначенное время выйти на связь с профильным врачом;

- для того чтобы получить помощь в чрезвычайной ситуации, достаточно будет воспользоваться единым номером экстренных служб по таксофону связи, расположенному в шаговой доступности;

- для того чтобы подобрать литературу по интересующей тематике, достаточно будет воспользоваться электронным каталогом любой библиотеки на всей территории страны;

- для того чтобы приступить к выполнению отдельных видов профессиональной деятельности, не нужно будет тратить время на дорогу, достаточно будет включить компьютер и войти в корпоративную сеть;

- для того чтобы заключить договор с партнером из другого региона, не нужно будет командировать к нему своего представителя, достаточно будет удостоверить документы электронной цифровой подписью и т.п.

Вопросы и задания для самоконтроля

1. Определите соотношение понятий: «информация», «информационные ресурсы», «информатизация», «информационные технологии».
2. Какие признаки присущи информации?
3. Охарактеризуйте информационную деятельность государства и органов местного самоуправления.
4. Какими нормами Конституции РФ закреплены основы информационной деятельности государства и муниципальных образований?
5. В чем заключается особенность информационной политики государства? Назовите, какие специальные органы государственного управления созданы для выполнения соответствующих функций.
6. Дайте характеристику основных положений Государственной программы «Информационное общество (2011—2020 годы)».

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Стратегия развития информационного общества в Российской Федерации : утв. Президентом РФ от 7 февраля 2008 г. № Пр-212.

Государственная программа «Информационное общество (2011—2020 годы)» : распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р.

Глава 2. ИНФОРМАЦИОННОЕ ПРАВО КАК ОТРАСЛЬ РОССИЙСКОГО ПРАВА

Понятие информационного права, его предмет и метод. Принципы информационного права. Система информационного права. Информационное право в системе российского права. Связь информационного права с другими отраслями права. Основные информационно-правовые институты. Источники информационного права. Информационное законодательство и подзаконные акты, регулирующие информационные правоотношения. Информационное право как наука. Актуальные проблемы науки информационного права на этапе развития Российской Федерации как электронного государства.

2.1. Понятие информационного права, его предмет и метод. Принципы информационного права

Информационное право — это отрасль российского права, нормы которой регулируют общественные отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

К определению информационного права как отрасли права, его содержанию современные специалисты подходят неоднозначно. Информационное право можно рассматривать: 1) как отрасль права; 2) как науку; 3) как учебную дисциплину.

Своеобразной точкой отсчета в развитии информационного законодательства в России исследователи признают 1992 г., когда были приняты законы о правовой охране программ для ЭВМ и баз данных, о правовой охране технологий интегральных микросхем.

В.А. Копылов в первом и втором изданиях учебника «Информационное право» (1997 и 2002 гг.) определял информационное право как «новую, только лишь формирующуюся отрасль права». В 2000 г. информационное право было официально введено в структуру юридических дисциплин, как отрасль науки оно было включено в специальность «12.00.14: Административное право. Финансовое право. Информационное право».

Приказом Минобрнауки России от 10 января 2012 г. № 5 «О внесении изменений в Номенклатуру специальностей научных работников, утвержденную приказом Министерства образования и науки

РФ от 25 февраля 2009 года» (документ зарегистрирован в Минюсте РФ 1 февраля 2012 за номером 23091), информационное право выделено в отдельную научную специальность: 12.00.13 — информационное право.

Этим шагом поставлена последняя точка в многочисленных дискуссиях и сегодня, спустя более 20 лет можно с уверенностью говорить о свершившемся становлении данной отрасли, и обоснованно определять информационное право как самостоятельную отрасль российского права с четко определенными предметом и методом правового регулирования.

И.Л. Бачило подчеркивает, что отрасль информационного права отличается от других отраслей права тем, что имеет свой ярко выраженный предмет отношений. В состав предмета она включает отношения, воплощенные:

- 1) в информации при разнообразии форм ее проявления и формируемых на этой основе информационных ресурсах;
- 2) средствах и технологиях работы с информацией (информационных технологиях);
- 3) средствах и технологиях передачи информации по сетям связи¹.

Таким образом, подводя итог, можно определить *предмет информационного права* как общественные отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Предмет и метод правового регулирования органически связаны между собой. Если *предмет отрасли права* отвечает на вопрос «что?», то сущность *метода правового регулирования* соответствует вопросам «как?», «каким образом происходит правовое регулирование отношений, складывающихся между их участниками?».

По общему правилу методом правового регулирования называется совокупность приемов и способов, с помощью которых осуществляется воздействие на участников правовых отношений. Метод правового регулирования можно определить как специфический способ, при помощи которого государство на основе данной совокупности

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 25.

юридических норм обеспечивает нужное ему поведение людей как участников правоотношения.

Метод правового регулирования влияет на выбор способов установления прав и обязанностей субъектов, степень свободы действий субъектов в рамках правоотношения, их правовое положение по отношению друг к другу, а также на возможность использования тех или иных средств защиты субъективных прав участников правоотношения. Эффект подобного влияния достигается с помощью двух приемов правового регулирования: императивного и диспозитивного¹.

В теории права встречаются различные наименования базовых методов правового регулирования: императивный (авторитарный, метод централизации, или субординации, административно-правовой, метод властных предписаний, метод власти и подчинения) и диспозитивный (автономный, метод децентрализации или координации, гражданско-правовой, метод равенства сторон). Определим различия между ними.

При императивном регулировании правовое положение участников правоотношения строится на началах неравенства. Один из участников всегда наделяется властными полномочиями по отношению к другому. Как правило субъект, наделенный властными полномочиями, является государственным органом либо органом, уполномоченным государством на совершение определенных действий и наделенным правом издания односторонне-властных предписаний, адресованных другому участнику. Права и обязанности субъектов правоотношения, построенного на принципах власти-подчинения, подлежат жесткой регламентации со стороны государства, и объем правомочий не может быть изменен участниками самостоятельно.

При диспозитивном регулировании правоотношений участники находятся в равном, равноправном положении, наделяются правом выстраивать свои взаимоотношения на взаимовыгодных условиях или отказаться от участия в подобных отношениях. Государство предоставляет возможность участникам диспозитивных отношений выбирать для себя наиболее приемлемый вариант поведения, ограничивая этот выбор лишь соображениями законности. Отношения между

¹ Рукавишникова И.В. Метод финансового права. М. : Юрист, 2006. С. 79.

субъектами строятся не на основе односторонне-властных предписаний, а на базе свободного договора.

Теория разделения методов правового регулирования на диспозитивные и императивные тесно связана с разделением всего правового массива на частное и публичное право. Императивное регулирование традиционно присуще публично-правовым отраслям права, соответственно диспозитивное — отраслям, относящимся к разряду частноправовых.

Трансформируясь из базовых методов правового регулирования в отраслевые, каждый из методов приобретает специфическую окраску, уникальный набор приемов и способов правового регулирования, свойственный только данной отрасли права.

Отрасль информационного права обладает методом правового регулирования, сочетающим в себе элементы императивного и диспозитивного начал.

Проиллюстрируем сказанное на примере норм Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Диспозитивное регулирование, к примеру, установлено в ст. 6 данного закона, согласно которой оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. При этом лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

Императивное регулирование установлено в достаточно большом числе норм указанного закона. Например, согласно, ст. 14 право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- 1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Таким образом, специфика метода информационного права отражается в уникальном сочетании способов правового регулирования, определенном основными направлениями и принципами государственной информационной политики.

Находясь на этапе своего становления, информационное законодательство нуждается в серьезной методологической «подпитке», разработке основ теории информационного права. На сегодняшний день действующие нормативные акты не представляют собой систему информационного законодательства, в полной мере обеспечивающую регулирование складывающихся правоотношений в информационной сфере.

Одним из важнейших аспектов методологии является вопрос правовых принципов, в которых заложена суть правовых норм. Под принципами права понимаются выраженные в праве исходные нормативно-руководящие начала, характеризующие его создание, его основы, закреплённые в нем закономерности общественной жизни¹.

¹ Алексеев С. С. Право. Опыт комплексного исследования. М., 1999. С. 183.

Существующая система принципов, установленных в федеральных актах информационного законодательства, не позволяет говорить о целостности механизма правового регулирования информационных отношений в обществе.

Решение задачи определения основополагающих принципов сегодня наиболее актуально для одного из десяти выделяемых блоков проблем информационного законодательства¹: информационная деятельность, информационные отношения (формирование и использование информационных ресурсов, информационных систем; специализация организаций на информационной деятельности; обеспечение информационных потребностей граждан, юридических лиц; регулирование рынка информации и услуг и т. д.).

Поскольку принципы — это основополагающие идеи (требования), определяющие в своей совокупности идеальную конструкцию (модель) регулирования конкретной области общественных отношений, вопросу их детальной регламентации необходимо самое пристальное внимание. При этом необходим учет всех существенных признаков понятия «принципы права», разработанных философами и юристами, таких как:

а) закреплённость принципа в нормативном правовом акте, т.е. конкретном источнике информационного права;

б) предметная определенность. Она означает, что объективным критерием для определения принципа служит специфика предмета правового регулирования, т.е. особенности информационных правоотношений, регулируемых нормами права. Другими словами, принцип должен выражать сущность совокупности каких-то норм с точки зрения того, что они регулируют;

в) целевая направленность. Этот принципообразующий признак даёт возможность выделить принципы правовой защиты по направлениям и желаемым результатам в области правового регулирования информационных правоотношений. Признак целенаправленности означает, что принцип должен выражать сущность определенной совокупности норм права не только в статике, но и в динамике, в направлении достижения целей;

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 124—126.

г) нормативность. Как признак, она, в конечном счете, сводится к указанию того, что в общем случае может человек как субъект права и что обязаны и не могут государство, общество и другие люди по отношению к нему как субъекту права. Нормативность означает, что принципы права не только выражают ее существенные свойства, но также выступают и в качестве общего правила поведения субъектов общественных отношений, что, будучи закрепленными в правовых нормах, они приобретают значение общих правил поведения, имеющих регулятивный характер, и что, кроме того, они являются нормами прямого действия;

д) выражение внутреннего единства совокупности правовых норм института правовой защиты. Принципы права вносят единообразие во всю систему юридических норм правового института и придают глубокое единство правовому регулированию общественных отношений, цементируют все элементы механизма правовой защиты данных отношений, когда ими пронизываются не какие-либо отдельные, а все ее нормы;

е) стабильность. Этот признак означает, что принцип права действует в течение определенного, относительно длинного времени. Отражая качественное состояние системы права, он не может быть изменчив в такой же мере, как правовые нормы. При этом устойчивость не означает неподвижность. Напротив, устойчиво то, что способно к изменениям, к развитию;

ж) универсальность. Данный признак является ведущим при выделении принципа из норм права. Это важнейшее свойство, которое отличает его от правовой нормы. Универсальность принципа базируется на его общезначимости, общеобязательности, высшей императивности и прямом действии;

з) истинность. Принципом может быть только такое положение, которое не противоречит иным принципам права и правовой защиты, опыту и юридической практике;

и) взаимосвязь и взаимообусловленность принципов правовой защиты. Взаимосвязь принципов предполагает их взаимное воздействие. Характер связи может быть различным: содержание, причина, следствие, прямая, косвенная, непосредственная связь принципов определяется единой целью;

к) стабильные нормативно-руководящие положения должны быть присущи правовой действительности, формируются под воздействием экономических и социально-политических факторов и определяющей качественные особенности правового регулирования специфической группы общественных отношений;

л) сложившиеся на базе социально-политических и экономических явлений стабильные нормативно-руководящие начала выступают основой практической деятельности правотворческих органов, субъектов права;

м) принципы права олицетворяют собой объективные закономерности развития общественных отношений и служат правильным ориентиром отражения и использования указанных закономерностей, воплощая в себя функцию единства правового регулирования.

Восемь базовых принципов регулирования информационных отношений сформулировано в базовом Федеральном законе «Об информации, информационных технологиях и о защите информации» — это:

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

2) установление ограничений доступа к информации только федеральными законами;

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

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

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

6) достоверность информации и своевременность ее предоставления;

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

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных

технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Как известно, имея общеобязательный характер, принципы права способствуют укреплению внутреннего единства и взаимодействия различных его отраслей и институтов, правовых норм и правовых отношений.

Проанализируем, например, внутриотраслевые принципы формирующегося института предоставления государственных и муниципальных услуг, в том числе, в электронной форме, института, в котором в большей мере проявляется публично-правовой аспект информационных правоотношений.

Не вызывает сомнений, что основным характеризующим признаком совокупности норм, определяющих правовое обеспечение формирования и использования информационных ресурсов, является ее комплексность. Правовое регулирование общественных отношений в рассматриваемой области человеческой деятельности осуществляется нормами и методами конституционного, административного, государственного и гражданского права, а также иных отраслей права. Институт предоставления государственных и муниципальных услуг — не исключение, к нему в полной мере присущ признак комплексности.

Согласно ст. 1 Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» анализируемый институт охватывает отношения, возникающие в связи с предоставлением государственных и муниципальных услуг соответственно федеральными органами исполнительной власти, органами государственных внебюджетных фондов, исполнительными органами государственной власти субъектов РФ, а также органами местного самоуправления.

Первый принцип — правомерности предоставления государственных и муниципальных услуг органами, предоставляющими государственные услуги, и органами, предоставляющими муниципальные услуги, а также предоставления услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг и предоставляются организациями, участвующими в предоставлении государственных и муниципальных услуг.

Данный принцип корреспондирует к принципу обеспечения строгого соблюдения законности в информационных отношениях, predetermined, прежде всего, нормами Конституции РФ.

Второй принцип определяет заявительный порядок обращения за предоставлением государственных и муниципальных услуг. Этот принцип проявляет себя в нормах закона, определяющих правомочия заявителей при получении государственной и муниципальной услуги в электронной форме.

Третий принцип — правомерности взимания с заявителей государственной пошлины за предоставление государственных и муниципальных услуг, платы за предоставление государственных и муниципальных услуг, платы за предоставление услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг и предоставляются организациями, участвующими в предоставлении государственных и муниципальных услуг. Перечни платных услуг будут устанавливаться Правительством РФ, высшими исполнительными органами государственной власти субъектов РФ, главами местных администраций.

Четвертый принцип касается открытости деятельности органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, а также организаций, участвующих в предоставлении государственных и муниципальных услуг. Данный принцип относится к числу основополагающих и закреплён в ст. 3 Федерального закона «Об информации, информационных технологиях и о защите информации».

Принцип пятый — доступность обращения за предоставлением государственных и муниципальных услуг и предоставления государственных и муниципальных услуг, в том числе для лиц с ограниченными возможностями здоровья — ещё раз подчеркивает гарантии, установленные Указом Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию». Также данный принцип обусловлен и нормами Федерального закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Развивает принцип доступности и государственная программа РФ от 20 октября 2010 г. № 1815-р «Информационное общество

(2011—2020 годы)», которая направлена на получение гражданами и организациями преимуществ от применения информационных и телекоммуникационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий, радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе.

Принцип шестой — возможность получения государственных и муниципальных услуг в электронной форме, если это не запрещено законом, а также в иных формах, предусмотренных законодательством РФ, по выбору заявителя. В идеале система порталов государственных услуг призвана обеспечить возможность дистанционного получения государственных услуг по принципу «одного окна».

2.2. Система и источники информационного права

Информационное право, являясь отраслью права, состоит из множества отдельных информационно-правовых норм, совокупность которых выражается в сложной целостной системе. Внутри этой единой системы информационно-правовые нормы в определенной последовательности и взаимосвязи группируются в различные институты и более крупные подразделения.

Система информационного права — это объективно обусловленное системой общественных информационных отношений внутреннее строение, объединение и расположение информационно-правовых норм в определенной последовательности.

В системе информационного права выделяются части, разделы, институты. Наиболее крупные подразделения информационного права — это его общая и особенная части.

К *Общей части* относятся нормы информационного права, которые закрепляют основные принципы, формы и методы информационной деятельности граждан, государства, государственных органов, органов местного самоуправления.

Нормы *Общей части* информационного права конкретизируются в его *Особенной части*. *Особенная часть* состоит из нескольких разделов, включающих соответствующие информационно-правовые институты. Каждое из этих подразделений представляет собой сово-

купность информационно-правовых норм, регулирующих группу однородных информационных отношений. Информационно-правовой институт объединяет правовые нормы, регулирующие узкую и близкую по содержанию группу информационных отношений.

Особенную часть информационного права составляют разделы, в которых сгруппированы нормы, регулирующие отношения в области:

- реализации основных информационных прав и свобод, например, права на информацию;
- организации и деятельности средств массовой информации;
- обработки персональных данных;
- электронного документооборота;
- обеспечения информационной безопасности и др.

Остановимся на вопросе понятия института информационного права. Признаками правового института являются:

- а) юридическое единство правовых норм, определяемое предметной средой отношений;
- б) возможность обеспечить полноту регулирования совокупности однородных отношений;
- в) возможность обособить нормы, образующие институт в одном акте или существенно связанных между собой нескольких нормативных правовых актов.

Итак, институт информационного права — это относительно устойчивая группа информационно-правовых норм, регулирующая определенную группу информационных отношений. Так, институтами информационного права будут являться: институт правового режима информационных ресурсов, институт права на информацию, институт средств массовой информации и т.д.

В настоящее время авторским коллективом сектора информационного права ИГП РАН под руководством И.Л. Бачило разработана и представлена для обсуждения концепция Информационного кодекса РФ. При этом особенная часть кодекса представлена тремя супер-институтами¹:

¹ Концепция Информационного кодекса Российской Федерации / под ред. И. Л. Бачило. М., 2014. С. 151—156.

- 1) правовой режим информации, информационных ресурсов, информационных технологий и коммуникаций;
- 2) право на информацию;
- 3) правовое обеспечение информационной безопасности.

Нормы информационного права РФ содержатся в большом числе разнообразных правовых нормативных актов или источниках.

Источники информационного права — это правовые акты представительных и исполнительных органов государственной власти и местного самоуправления, в которых содержатся нормы информационного права.

Немаловажную роль в регулировании информационных правоотношений играют международно-правовые акты, среди которых основополагающее значение имеет Окинавская хартия глобального информационного общества от 22 июля 2000 г. Согласно положениям хартии «все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей».

Актуален как никогда вывод профессора В.А. Копылова, сделанный в одном из докладов еще в 2000 г. о том, что поскольку в информационном обществе практически отсутствуют географические и геополитические границы и даже временные рамки и часовые пояса, а также, как правило, не действуют национальные законодательства, то информационное право как правовое отображение такого общества должно строиться главным образом на нормах международного права, регулирующих основные группы информационных отношений на межгосударственном уровне. Так, посредством норм международного права государствами должны быть приняты определенные обязательства в области защиты информационных прав и свобод, в регламентации таких глобальных вопросов, как трансграничная передача персональных данных, когда главной целью становится адекватная защита прав субъектов данных.

Главный источник информационного права в национальном законодательстве — Конституция РФ. Она включает основные принци-

пиальные положения информационного права, поэтому нормы Конституции имеют высшую силу.

Источниками информационного права являются также многочисленные федеральные законы, регулирующие различные виды информационных отношений.

Это, прежде всего, федеральные конституционные законы, например, Федеральный конституционный закон от 17 декабря 1997 г. № 2-ФКЗ «О Правительстве Российской Федерации».

Разнообразные информационно-правовые отношения регулируются большим числом федеральных законов, к числу которых относятся: Федеральный закон «Об организации предоставления государственных и муниципальных услуг», Федеральный закон «О персональных данных») и др.

Необходимо отметить, что какого-либо единого источника по этой отрасли права в целом, типа кодекса, не имеется. Однако сегодня уже появились авторские концепции кодифицированного источника по информационному праву. В числе наиболее значимых среди них — концепция Информационного кодекса РФ, разработанная под руководством ведущего специалиста — И.Л. Бачило.

Особое значение для регулирования информационных отношений имеют указы Президента РФ. Сегодня Указы Президента в сфере информации носят организационный характер, т.е. содержат поручения органам государственной власти по разработке тех или иных нормативных актов, определяют порядок их разработки или основные направления деятельности этих органов в сфере информации, например, Указ Президента РФ от 2 апреля 2014 г. № 198 «О порядке опубликования законов и иных правовых актов субъектов Российской Федерации на “Официальном интернет-портале правовой информации” (www.pravo.gov.ru)».

Нормы информационного права содержатся также в соответствующих постановлениях и распоряжениях Правительства РФ. В их числе можно назвать: постановление Правительства РФ от 26 августа 2013 г. № 735 «О Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности», распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р «О государствен-

ной программе Российской Федерации “Информационное общество (2011—2020 годы)”».

Нормы информационного права содержатся также в большом количестве ведомственных актов, приказах, инструкциях, письмах. Например, приказ Роскомнадзора от 9 августа 2013 г. № 906 «Об утверждении формы заявления правообладателя о принятии мер по ограничению доступа к информационным ресурсам, распространяющим с нарушением исключительных прав фильма, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей».

В последние годы, в связи с внедрением элементов электронного государства в целом, электронного правительства усиливается роль актов, принимаемых органами государственной власти субъектов РФ, содержащих информационно-правовые нормы. При регулировании информационных отношений регионального уровня соответствующие законодательные и исполнительные органы власти могут использовать три метода правотворчества:

- а) дублирование норм федеральных законов;
- б) расширение содержания норм федеральных законов, осуществление их детализации;
- в) установление новых норм права.

При этом нормативные правовые акты субъектов РФ не должны создавать коллизии с нормами федеральных законов, поскольку действующее законодательство РФ является основополагающим.

В качестве примеров: Закон г. Москвы от 12 марта 2014 г. № 9 «Об обеспечении открытости информации и общественном контроле в сферах благоустройства, жилищных и коммунальных услуг», постановление Правительства Москвы от 15 апреля 2014 г. № 182-ПП «Об автоматизированной информационной системе «Узнай Москву».

Сегодня, в условиях серьезнейшего реформирования на пути построения информационного общества возрастает значимость актов органов местного самоуправления. Органы местного самоуправления, являясь публичной властью на своей территории, в целях осуществления информационной деятельности, наделены правом издавать информационные нормативные правовые и правоприменительные акты.

Например: Распоряжение администрации г. Кемерово от 3 мая 2011 г. № 1913 «О создании комиссии по развитию информационного общества и формированию элементов электронного правительства».

Информационно-правовые нормы могут содержаться также в локальных актах, принимаемых администрацией или иными органами предприятий, организаций, учреждений (например, положение о персональных данных).

Необходимо помнить, что информационное право и информационное законодательство — не тождественные понятия: последнему свойственна комплексность, так как помимо информационно-правовых оно содержит нормы и других отраслей права, и прежде всего — административного права.

Сегодня идет активный процесс формирования информационного права соответственно современным условиям жизни общества. Вопросы системы этой отрасли права и систематизации информационного законодательства приобрели высокую степень актуальности. К тому же далеко не все сферы информационной деятельности получили необходимое правовое регулирование.

2.3. Информационное право в системе российского права. **Информационное право как наука**

Каждая из отраслей российского права распространяется на свой, особый вид общественных отношений, требующих соответствующих предметов и методов правового регулирования. Определим место информационного права в системе российского права путем его сопоставления и отграничения от других отраслей права.

В юридической науке должен быть внимательно рассмотрен вопрос о месте информационного права в системе российского права на современном этапе.

Подчеркнем особенности информационного права, рассмотрев вопрос его связи с другими отраслями права и отграничения от них. В связи с тем, что информационное право распространяется на одну из областей деятельности государства, оно тесно соприкасается с конституционным и административным правом.

Конституционное право, являясь ведущей отраслью в системе права, закрепляет основы общественного строя РФ, правовое поло-

жение личности, систему и принципы организации и деятельности государственных органов и органов местного самоуправления. Как и все отрасли, информационное право базируется и развивается на этих нормах. Конституционное право содержит также нормы, непосредственно относящиеся к информационному праву. Так, право на информацию — это гарантированная Конституцией РФ возможность граждан получать достоверные сведения о деятельности государственных органов и организаций, общественных объединений и должностных лиц. Конституция РФ в ч. 4 ст. 29 закрепляет право каждого человека свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Сходство информационного права с административным проявляется в использовании сходных методов правового регулирования, главным образом метода властных предписаний. Неслучайно долгое время эти отрасли входила в одну научную специальность — 12.00.14. Основное разграничение этих отраслей права — по предмету правового регулирования. В предмет информационного права входят отношения, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Предмет административного права составляют общественные отношения в сфере управленческой деятельности государственных органов и должностных лиц по исполнению публичных функций государства и муниципальных образований. Сегодня, в условиях развития электронного правительства, механизмов предоставления государственных и муниципальных услуг в электронном виде связь информационного права с административным является особенно тесной. В этой связи просматривается связь информационного права и с муниципальным правом.

В вопросе ответственности за правонарушения в информационной сфере информационное право связано с уголовным правом.

Обозначая место информационного права в системе российского права, И.Л. Бачило подчеркивает два существенных момента: с одной стороны — его системообразующую роль для всех норм, связанных с проблемой информации и информатизации, и с другой — его системоорганизующую роль... Это как бы обратная связь особой социальной сферы через ее отрасль права со всеми остальными

структурами права...например, создание новых норм об ответственности за правонарушения в области информации, связи, информатизации, защиты информации и прав субъектов в этой области (УК РФ, КоАП РФ).

В условиях формирования информационного общества обнаруживается тесная связь информационного права как самостоятельной отрасли права как с базовыми отраслями российского права (конституционным, гражданским, уголовным), так и с другими, причем среди «смежных» с информационной отраслью права особенно явно проявляются имеющие ярко выраженный социальный аспект. Это трудовое право — в вопросе права на информацию субъектов трудового права, защиты персональных данных работника, муниципальное право — в контексте реализации права на доступ к информации о деятельности органов местного самоуправления, право социального обеспечения — в аспекте предоставления качественных государственных и муниципальных услуг.

Информационное право, ставшее в настоящее время одной из наиболее современных и актуальных отраслей отечественного права, отличается интенсивностью формирования своего нового содержания, масштабностью перемен, интенсивностью развития информационного законодательства. Наука информационного права еще молода, и многие проблемы информационного права еще не получили должной научной оценки.

Необходимо подчеркнуть, что правовая основа информационных отношений недостаточно разработана, нестабильна: в информационное законодательство постоянно вносятся многочисленные изменения и дополнения, что затрудняет его применение, а также и изучение. Важную роль в продолжающемся процессе формирования информационного права призвана выполнить наука информационного права.

В числе наиболее актуальных проблем науки информационного права — исследование вопросов предмета и системы информационного права, принципов информационно-правового регулирования.

Приобретают высокую степень актуальности и вопросы систематизации информационного законодательства, и, прежде всего, его

кодификации. Как справедливо отмечает П.У. Кузнецов¹, важнейшей предпосылкой кодификации информационного законодательства является создание полноценного и устоявшегося терминологического аппарата, который является главным стержневым юридикотехническим началом любого системообразующего закона.

Таким системообразующим законом в будущем может стать Информационный кодекс РФ.

Вопросы и задания для самоконтроля

1. Сформулируйте определение понятия «информационное право». Охарактеризуйте предмет информационного права.
2. В чем выражается специфика метода правового регулирования информационного права?
3. Какие принципы лежат в основе информационного права? Каково их значение?
4. Что понимается под системой информационного права? Каково содержание Общей части информационного права РФ? Каково содержание Особенной части информационного права РФ?
5. Что понимают под источниками информационного права?

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Стратегия развития информационного общества в Российской Федерации : утв. Президентом РФ от 7 февраля 2008 г. № Пр-212.

Государственная программа «Информационное общество (2011—2020 годы)» : распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р.

¹ Кузнецов П.У. Проблемы формирования источников нормативного обеспечения информационной среды // Информационное общество: проблемы развития законодательства : сб. науч. работ. М., 2012. С. 38.

Глава 3. ИНФОРМАЦИОННЫЕ ПРАВООТНОШЕНИЯ. ИНФОРМАЦИОННО-ПРАВОВЫЕ НОРМЫ

Понятие и структура информационного правоотношения. Юридические факты как основания возникновения, изменения и прекращения информационных правоотношений. Субъекты, объекты и содержание информационного правоотношения. Классификация информационных правоотношений. Права и обязанности субъектов информационных правоотношений. Информационно-правовая норма: понятие, признаки, структура.

3.1. Информационные правоотношения: понятие, содержание, субъекты. Условия возникновения, изменения и прекращения информационных правоотношений

В результате воздействия информационно-правовых норм на информационные отношения последние приобретают форму правоотношения. Правоотношения — это общественные отношения, урегулированные нормами права.

Информационные правоотношения — это общественные отношения, урегулированные нормами информационного права, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Прежде всего, информационное право как отдельная отрасль права регулирует однородную группу общественных отношений. Специфику данных отношений можно определить следующими признаками:

1) они возникают, изменяются и прекращаются в информационной сфере при обращении информации;

2) складываются по поводу обладающих определенной спецификой объектов, к которым относятся информация, информационные объекты, информационные технологии. И такие объекты в силу их особенностей невозможно поставить в один ряд с другими объектами правового регулирования.

Информационные правоотношения имеют характерное внутреннее строение (структуру). Структура показывает, из каких элементов состоит правоотношение и как эти элементы взаимосвязаны друг с другом. Правоотношение (в том числе и информационное) состоит из трех элементов: объект, субъект, содержание.

Важнейший элемент правоотношения — субъекты. Субъектами информационного права выступают участники (стороны) регулируемых нормами информационного права общественных отношений. К ним относятся человек, физическое лицо (включая граждан, лиц без гражданства и иностранных граждан), общество, юридическое лицо, государство, орган государственной власти, орган местного самоуправления.

Субъект информационного правоотношения должен обладать информационной правосубъектностью. Понятие «информационная правосубъектность» включает в себя понятие «информационная правоспособность» и «информационная дееспособность».

Информационная правоспособность рассматривается как проявление общей правоспособности, под которой понимается установленная и охраняемая государством возможность или способность данного субъекта вступать в правовые отношения. В этом случае субъект приобретает юридические права, обязанности, а также обязанность нести ответственность за реализацию таких прав и обязанностей. В таком понимании правоспособность является предпосылкой возникновения правовых отношений с участием этого субъекта.

Предпосылкой для возникновения информационных правоотношений является информационная правоспособность, которая выражается в определяемой информационно-правовыми нормами возможности данного субъекта приобретать информационные права и обязанности (права и обязанности в информационной сфере) и нести юридическую ответственность за их практическую реализацию. Каждый, кто нормами информационного права наделен правами и обязанностями в информационной сфере, может рассматриваться в качестве субъекта информационного права.

Однако субъект информационного права может стать субъектом информационных правоотношений тогда, когда он обладает вторым элементом информационной правосубъектности — информационной дееспособностью. Информационная дееспособность подразумевает способность субъекта своими действиями приобретать права, создавать для себя юридические обязанности, а также нести ответственность за свои действия в информационной сфере. В нашем случае речь идет о практической способности субъекта реализовывать свою информационную правоспособность в условиях конкретных информационных правоотношений.

При этом «гражданин, физическое лицо, вне зависимости от его трудовых и иных аналогичных контактов, всегда является членом социального коллектива, единицей в геополитических, административно-территориальных, культурологических, духовных структурах, деятельность которых регулируется либо морально-нравственными нормами, либо нормами законодательства. И все они связаны с информационным фоном потребностей этого лица в информации и являются активными приемниками информации, идущей от гражданина. Чем определеннее развиты различные институты демократии, тем прочнее связи гражданина с государством, государственной организацией»¹.

Рассматриваемая область общественных отношений, т.е. отношений, складывающихся в процессе реализации электронным государством своих функций, безусловно, обладает определенной спецификой, при этом упоминаемые И.Л. Бачило связи гражданина с этим государством становятся еще более тесными — с одной стороны, и более прозрачными и открытыми — с другой.

Объект правоотношения представляет собой то, на что воздействуют правоотношения. Это все те материальные, духовные и иные социальные блага, явления и процессы, по поводу которых субъекты информационного права вступают в информационно-правовые отношения. К примеру, объектом информационных правоотношений будут выступать государственные и муниципальные услуги в электронном виде.

Содержание, как третий элемент правоотношений, образует юридические права и обязанности участников (субъектов) информационных правоотношений. В нашем примере — это права и обязанности получателей услуг (заявителей) и тех, кто их предоставляет (федеральный орган исполнительной власти, орган государственного внебюджетного фонда, исполнительный орган государственной власти субъекта РФ, орган местного самоуправления).

Информационные правоотношения возникают, изменяются и прекращаются на основании юридических фактов. Юридические факты — это конкретные жизненные обстоятельства, с которыми связывается возникновение, изменение или прекращение правоотношений. Их можно подразделить на события и действия.

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт ; ИД Юрайт, 2011. С. 61.

События — это юридические факты, которые не связаны с волей людей (стихийные бедствия, смерть человека, достижение совершеннолетия и т.д.). Как пример события можно привести ситуацию аппаратного или программного сбоя.

Действия — это юридические факты, наступление которых связано с волей и сознанием участников правоотношений (в свою очередь подразделяются на правомерные и неправомерные). Правомерным действием, к примеру, будет являться соответствующее нормам закона предоставление (получение) государственной (муниципальной) услуги в электронном виде. Примером неправомерного действия будет уголовно наказуемое деяние — неправомерный доступ к компьютерной информации.

3.2. Понятие и признаки информационно-правовых норм

Информационно-правовые нормы, также как и иные нормы права, представляют собой установленные (в законах, указах Президента РФ, постановлениях Правительства РФ и других нормативных актах) и охраняемые государством (в лице своих правоохранительных органов) правила поведения участников общественных отношений, выраженные в их юридических правах и обязанностях.

Информационно-правовая норма — это установленное государством и обеспеченное мерами государственного принуждения правило поведения в общественных информационных отношениях, возникающих в процессе поиска, получения, передачи, производства и распространения информации, а также связанных с ними отношений.

Классификацию информационно-правовых норм можно провести по нескольким основаниям.

В зависимости от способа воздействия на участников информационных отношений, информационно-правовые нормы подразделяются:

— *на обязывающие информационно-правовые нормы* — это нормы, содержащие требования на совершение каких-либо действий. К примеру, в соответствии со ст. 6 Федерального закона «Об организации предоставления государственных и муниципальных услуг» органы, предоставляющие государственные и муниципальные услуги, обязаны:

1) предоставлять государственные или муниципальные услуги в соответствии с административными регламентами;

2) обеспечивать возможность получения заявителем государственной или муниципальной услуги в электронной форме, если это не запрещено законом, а также в иных формах, предусмотренных законодательством РФ, по выбору заявителя;

3) предоставлять в иные государственные органы, органы местного самоуправления, организации документы и информацию, необходимые для предоставления государственных и муниципальных услуг, а также получать от иных государственных органов, органов местного самоуправления, организаций такие документы и информацию;

4) исполнять иные обязанности в соответствии с требованиями настоящего Федерального закона, административных регламентов и иных нормативных правовых актов, регулирующих отношения, возникающие в связи с предоставлением государственных и муниципальных услуг);

— *запрещающие информационно-правовые нормы* — это нормы, содержащие запрет на совершение каких-либо действий. На примере указанного выше Федерального закона от 27 июля 2010 г. № 210-ФЗ проиллюстрируем сказанное: согласно ст. 7 органы, предоставляющие государственные или муниципальные услуги, не вправе требовать от заявителя:

1) предоставления документов и информации или осуществления действий, предоставление или осуществление которых не предусмотрено нормативными правовыми актами, регулирующими отношения, возникающие в связи с предоставлением государственной или муниципальной услуги;

2) предоставления документов и информации, которые находятся в распоряжении органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, иных государственных органов, органов местного самоуправления, организаций, в соответствии с нормативными правовыми актами РФ, нормативными правовыми актами субъектов РФ, муниципальными правовыми актами;

3) осуществления действий, в том числе согласований, необходимых для получения государственных и муниципальных услуг и

связанных с обращением в иные государственные органы, органы местного самоуправления, организации, за исключением получения услуг, включенных в перечни, указанные в части 1 статьи 9 Федерального закона;

— *уполномочивающие информационно-правовые нормы* — они устанавливают права участников правоотношений на совершение каких-либо определенных действий. К примеру, в вопросе предоставления государственных и муниципальных услуг многофункциональные центры, исходя из содержания ст. 16 Федерального закона от 27 июля 2010 г. № 210-ФЗ вправе запрашивать документы и информацию, необходимые для предоставления государственных и муниципальных услуг, в органах, предоставляющих государственные услуги, органах, предоставляющих муниципальные услуги, организациях, участвующих в предоставлении государственных и муниципальных услуг, а также получать от органов, предоставляющих государственные услуги, органов, предоставляющих муниципальные услуги, организаций, участвующих в предоставлении государственных и муниципальных услуг, такие документы и информацию.

В зависимости от своего содержания информационно-правовые нормы можно подразделить на два вида: 1) материальные; 2) процессуальные.

Материальные информационно-правовые нормы закрепляют материальное информационно-правовое содержание прав и обязанностей участников информационных отношений.

Процессуальные (процедурные) нормы информационного права порядок и действие норм материального права, например, порядок предоставления государственных и муниципальных услуг в электронном виде.

Структура нормы права поясняет, из каких структурных частей (элементов) состоит норма права и как эти части между собой взаимосвязаны. Как и норма всякой другой отрасли права информационно-правовая норма состоит из трех элементов: 1) гипотезы, 2) диспозиции, 3) санкции.

1. Гипотеза — это элемент информационно-правовой нормы, который указывает на условия действия информационно-правовой нормы. Определяет обстоятельства, при которых могут возникнуть

информационные правоотношения, и указывает на субъектов — участников этих правоотношений.

2. Диспозиция — это элемент информационно-правовой нормы, который устанавливает содержание самого правила поведения, т.е. определяет содержание прав и обязанностей участников информационных отношений.

3. Санкция — это элемент информационно-правовой нормы, который указывает на меры воздействия за нарушение информационно-правовой нормы. К примеру, согласно ст. 272 Уголовного кодекса РФ неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Вопросы и задания для самоконтроля

1. Сформулируйте понятие «информационно-правовая норма». Какие признаки отличают информационно-правовые нормы от других норм права?

2. Какие виды информационно-правовых норм выделяются в зависимости от способа воздействия на участников информационных отношений?

3. Из каких структурных элементов состоит информационно-правовая норма? Охарактеризуйте каждый из этих элементов.

4. Что понимается под информационными правоотношениями? Какие особенности им свойственны?

5. Определите понятие «субъект информационного правоотношения».

6. Охарактеризуйте субъектный состав информационных правоотношений.

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Стратегия развития информационного общества в Российской Федерации : утв. Президентом РФ 07 февраля 2008 № Пр-212.

Государственная программа «Информационное общество (2011—2020 годы)» : распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р.

Глава 4. ПРАВО НА ИНФОРМАЦИЮ КАК ИНСТИТУТ ИНФОРМАЦИОННОГО ПРАВА

Право на информацию как институт информационного права. Содержание права на информацию. Понятие цифрового неравенства. Основные подходы к обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления.

4.1. Общая характеристика права на информацию

Основополагающий институт информационного права — это институт права на информацию.

Под данным институтом понимается совокупность правовых актов и отдельных норм, определяющих порядок реализации прав субъектов информационного права в области производства (создания) информации, поиска и получения (доступа) информации, сбора, хранения, передачи, использования, распространения информации в целях, не противоречащих свободам, правам и интересам человека, государства, общества и обеспечивающих создание информационных ресурсов, необходимых для реализации других прав и обязанностей субъектов права, предусмотренных и гарантированных законодательством РФ и нормами международного права.

При этом доступ к информации должен подразумевать и доступ к открытой информации, общедоступной информации, и доступ к информации, являющейся общественным достоянием, информации особой социальной значимости, и доступ к информации в сфере средств массовой информации.

Несомненно, в условиях развития «электронного государства» можно говорить о расширении правоспособности человека как участника информационных правоотношений. И речь уже идет о правоспособности, основанной на транспарентности и открытости государственного управления.

Транспарентность можно определить как состояние информированности (наличие полного, достаточного и достоверного знания) о той или иной деятельности (ее объектах или результатах) любого заинтересованного в этом субъекта.

Состояние информированности возникает вследствие получения соответствующей информации, которое возможно посредством доступа к информации, под которым следует понимать ознакомление с информацией либо предоставление ее для ознакомления, т.е. анализируемому состоянию предшествует информационный процесс, состоящий в совершении действий по доступу к информации. Субъектами такого информационного процесса выступают две стороны: сторона, обладающая информацией, и сторона, заинтересованная в ее получении.

Так, субъектами информационного процесса «электронного государства» выступают, с одной стороны — человек, с другой — государственные органы, составляющие «электронное правительство». И государство должно обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения органов государственной власти. Сегодня возможно лишь констатировать недостаточный уровень информированности общества в целом и каждого человека в отдельности.

Второй немаловажный аспект — это обеспечение равного доступа к информационным технологиям.

Термины «цифровое неравенство» или «цифровой разрыв» (в англоязычной литературе *digital divide*) трактуются по-разному. Чаще всего под цифровым неравенством понимается неравный доступ к информационным технологиям, разделение на тех, кому эти технологии доступны, а кому нет, деление на «информационно богатых» и «информационно бедных».

ЮНЕСКО считает проявлением цифрового неравенства наличие на карте мира стран, где информационные технологии развиты и доступны гражданам, и стран, или даже целых регионов, где уровень развития информационных технологий низок и большинство населения не имеет к ним доступа.

Другие исследователи считают, что цифровое неравенство, это социально-экономический феномен, являющийся следствием разницы в уровне дохода, грамотности и образования, степени развития определенных навыков, различия в сфере бизнеса, культуры, законодательства.

Принято рассматривать цифровое неравенство как сложное социально-экономическое явление, имеющее множество форм:

1. Региональное или территориальное неравенство. Оно выражается в разделении мира на регионы, где информационные технологии доступны большинству населения и где нет. Границы информационно богатых и информационно бедных регионов практически совпадают с границами индустриально развитых регионов (Северная Америка, Западная Европа, развитые страны Юго-Восточной Азии) и стран «третьего мира» (Африка, Азия, Южная Америка).

Другим проявлением регионального неравенства является разная степень информатизации отдельных регионов внутри страны, деление ее на «информационно богатые» индустриальные регионы и «информационно бедные» сельские, малонаселенные или труднодоступные территории.

2. Социальное неравенство. Выражается в одновременном присутствии в обществе социальных групп, которые активно используют информационные технологии, и групп, которые не могут себе этого позволить по причине низкого дохода, недостатка образования и культуры, отсутствия необходимых навыков, ограниченных физических возможностей, в силу преклонного возраста и т.д.

Итак, для обеспечения цифрового равенства и цифрового единства граждан необходимыми условиям и являются:

- равенство в доступности технических средств;
- равенство в навыках использования ИКТ;
- равенство в способах и целях использования ИКТ.

Согласно «Стратегии развития информационного общества в Российской Федерации», к 2015 г. не менее 80% населенных пунктов должны получить доступ к открытым государственным ресурсам.

Сегодня же в рейтинговой оценке российских регионов по их готовности к информационному обществу индекс лидера в 22 раза превышает показатель региона-аутсайдера.

По аналогии, «как социальное государство обеспечивает социальное равенство, так электронное государство берет на себя обязанность обеспечить цифровое равенство... Проблема «цифрового равенства» по своей природе тесно связана с социальным равенством. Ее решение зависит от того, как государство решает вопрос выравнивания социального положения населения. Любое социальное неравен-

ство способно существенно дестабилизировать нормальное функционирование общественного процесса и государственного управления...

Принцип «цифрового равенства» должен не только получить законодательное воплощение, но пронизать собой все законодательство. Этот принцип исходит из того, чтобы лицо выбирало, в какой форме получать информацию — в традиционной бумажной или электронной».

4.2. Доступ к информации о деятельности государственных органов и органов местного самоуправления

Вступивший с 1 января 2010 г. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» определяет, что доступ к информации о деятельности государственных органов и органов местного самоуправления может обеспечиваться следующими способами:

1) обнародование (опубликование) государственными органами и органами местного самоуправления информации о своей деятельности в средствах массовой информации;

2) размещение государственными органами и органами местного самоуправления информации о своей деятельности в сети Интернет;

3) размещение государственными органами и органами местного самоуправления информации о своей деятельности в помещениях, занимаемых указанными органами, и в иных отведенных для этих целей местах;

4) ознакомление пользователей информацией с информацией о деятельности государственных органов и органов местного самоуправления в помещениях, занимаемых указанными органами, а также через библиотечные и архивные фонды;

5) присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, государственных органов и органов местного самоуправления, на заседаниях коллегиальных государственных органов и коллегиальных органов местного самоуправления, а также на заседаниях коллегиальных органов государственных органов и коллегиальных органов местного самоуправления;

6) предоставление пользователям информацией по их запросу информации о деятельности государственных органов и органов местного самоуправления;

7) другими способами, предусмотренными законами и (или) иными нормативными правовыми актами, а в отношении доступа к информации о деятельности органов местного самоуправления — также муниципальными правовыми актами.

И все эти способы в полной мере должны быть реализованы целенаправленными и обоснованными действиями чиновников всех уровней государственной власти.

Интернет впервые в истории человечества предоставляет техническую возможность для массового открытия информации. Но все не определяет необходимость делать это.

В настоящее время необходимым является изменение характера информационного взаимодействия общества и государства, выражающееся в расширении прав граждан путем не только предоставления доступа к разнообразной информации, но и увеличении возможностей людей участвовать в процессе принятия решений. Центральной фигурой в процессах информатизации органов государственной власти должен быть человек как источник, потребитель информации и субъект гражданского общества, его интересы и потребности. И это должно как никогда осознаваться государственными служащими.

Размещение в свободном доступе информации о деятельности органов исполнительной власти и органов местного самоуправления, а также формируемых ими информационных ресурсах позволяет сделать деятельность указанных органов более понятной и предсказуемой для граждан и организаций, а также уменьшить нагрузку на указанные выше органы за счет снижения количества поступающих обращений.

Согласно Концепции снижения административных барьеров и повышения доступности государственных и муниципальных услуг на 2011—2013 гг. в указанной сфере планомерно велась работа по обеспечению свободного доступа через сеть Интернет к содержимому основных федеральных государственных информационных ресурсов и систем, за исключением сведений, которые составляют охраняемую законом тайну, исключив случаи установления платы за предоставление информации из государственных информационных ресурсов в соответствии с ведомственными актами.

Необходимо отметить, что с 1 июля 2010 г. введена административная ответственность за нарушение законодательства об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления. Право граждан на ознакомление с документами и материалами органов государственной власти и органов местного самоуправления, непосредственно затрагивающими их права и свободы гарантировано ст. 24 Конституции РФ. Данному правонарушению посвящена ст. 5.39 КоАП РФ — отказ в предоставлении информации. Объективная сторона данного правонарушения заключается в неправомерном отказе в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременном ее предоставлении либо предоставлении заведомо недостоверной информации. Законом установлена административная ответственность за нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети «Интернет» (ст. 13.27 КоАП РФ) в виде наложения штрафа на должностных лиц.

В случае нарушения порядка предоставления информации о деятельности государственных органов и органов местного самоуправления, содержащей сведения, относящиеся к информации ограниченного доступа, а также незаконное взимание платы за предоставление информации о деятельности государственных органов и органов местного самоуправления либо нарушение порядка взимания платы за предоставление информации о деятельности государственных органов и органов местного самоуправления в случаях, если федеральным законом такая плата установлена (ст. 13.28 КоАП РФ), предусмотрена административная ответственность в виде штрафа на должностных лиц.

Рассмотрение данной категории дел отнесено к компетенции судей, а возбуждение дел осуществляется прокурором в порядке, предусмотренном ст. 28.4 КоАП РФ.

Вопросы и задания для самоконтроля

1. Каково содержание права на информацию?
2. Раскройте понятие цифрового неравенства, определите уровень доступности информационных технологий для граждан современной России.

3. Назовите и охарактеризуйте формы цифрового неравенства.
4. Определите основные направления нормативно-правового обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления.

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный конституционный закон от 17 декабря 1997 г. № 2-ФКЗ «О Правительстве Российской Федерации».

Федеральный закон Российской Федерации от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом РФ от 7 февраля 2008 г. № Пр-212.

О дополнительных гарантиях прав граждан на информацию : Указ Президента РФ от 31 декабря 1993 г. № 2334.

Государственная программа «Информационное общество (2011—2020 годы)» : распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р

Глава 5. ИНСТИТУТ ПРАВОВОГО РЕЖИМА ИНФОРМАЦИОННЫХ РЕСУРСОВ

Понятие информационного ресурса, правового режима информационных ресурсов. Категории информационных ресурсов по критерию доступа к ним. Общедоступные ресурсы и ресурсы с ограниченным доступом. Понятие государственной тайны. Конфиденциальность информации.

5.1. Понятие информационного ресурса

Информационный ресурс — это массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения (информацию), сформированные по определенному признаку или критерию.

Проиллюстрируем понятие информационного ресурса на примере информационных ресурсов таможенных органов. Информация постоянно циркулирует в системе таможенных органов, формируя тем самым информационные ресурсы таможенных органов. Информационные ресурсы таможенных органов составляет документированная информация (сведения), имеющаяся (имеющиеся) в распоряжении таможенных органов, в том числе:

1) представляемая лицами при совершении таможенных операций;

2) представляемая федеральными органами исполнительной власти в соответствии с межведомственными соглашениями об обмене информацией;

3) направляемая ведомствами иностранных государств по запросу федерального органа исполнительной власти, уполномоченного в области таможенного дела¹.

Таможенный кодекс Таможенного союза (далее — ТК ТС) дает следующее определение информационных ресурсов таможенных органов — это организованная совокупность документированной информации, включающая в себя базы данных, создаваемые, обрабатываемые и накапливаемые в информационных системах таможенных органов². В свою очередь под информационной системой таможенных органов понимается автоматизированная система управления процессами таможенной деятельности или Единая автоматизированная информационная система таможенных органов³.

Данные информационные ресурсы формируются на базе документов и сведений, представляемых при совершении таможенных операций, а также документов, необходимых для их совершения, и имеют ограниченный доступ. К открытым же информационным ресурсам таможенных органов относится информация, касающаяся таможенного законодательства Таможенного союза. Важно отметить, что в силу данного определения, информационные ресурсы таможенных органов являются федеральной собственностью. Порядок их

¹ См.: Федеральный закон от 27 ноября 2010 г. № 311-ФЗ «О таможенном регулировании в Российской Федерации».

² См.: Таможенный кодекс Таможенного союза : принят Решением Межгосударственного Совета ЕврАзЭС от 27 ноября 2009 г.

³ См.: приказ ФТС России от 17 июня 2010 г. № 1154.

формирования и использования, требования к документированию информации устанавливаются Федеральной таможенной службой (ФТС России).

Таможенная информация используется таможенными органами исключительно для таможенных целей, в том числе для предупреждения и пресечения административных правонарушений и преступлений. Такая информация может содержать конфиденциальные сведения о внешнеэкономической деятельности, составлять государственную, коммерческую, банковскую, налоговую или иную охраняемую законом тайну. Поэтому информация подобного рода нуждается в специальной защите и выделении финансовых средств на ее обеспечение.

Информация, которой обладают таможенные органы, относится к различным категориям и правовым режимам. Большая ее часть из соображений безопасности относится к информации ограниченного доступа, подразделяющейся на конфиденциальную и составляющую государственную тайну. Следовательно, разглашение или утечка подобной информации приводят к нарушению ее конфиденциальности, что может существенно подорвать экономическое положение государства.

Информация в системе таможенных органов характеризуется высокой интенсивностью потока и разнообразием типа документов. Основной объем таможенной информации приходится именно на документированную информацию, большую часть которой составляют декларации на товары, а также документы по ведению баз данных нормативно-справочной информации, документы таможенного транзита, международных перевозок и деклараций таможенной стоимости. Документированная информация — это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать¹.

¹ См.: Информационное обеспечение в таможенных органах : учебник / П. Н. Афонин. СПб : СПб филиал РТА им. В.Б. Бобкова, 2006. С. 23.

5.2. Основные категории информационных ресурсов.

Общедоступная информация и информация ограниченного доступа

Можно выделить ряд классификаций информационных ресурсов по различным основаниям.

Например, исходя из вопроса предмета ведения, информационные ресурсы, которые являются собственностью государства, могут находиться в ведении Российской Федерации, ее субъектов и соответствующих органов государственной власти. Согласно п. «и» ст. 71 Конституции РФ в ведении Российской Федерации находятся федеральная информация и средства связи. Объекты информационных ресурсов могут находиться и в совместном ведении Российской Федерации и ее субъектов.

Основной подход к классификации информационных ресурсов — это критерий доступа к ним пользователей. Итак, по категории доступа информационные ресурсы могут быть *открытыми (общедоступными)* или *с ограниченным доступом*.

Общедоступная информация предоставляется свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных, предоставленных законом прав.

В свою очередь, документированная информация с ограниченным доступом подразделяется на отнесенную к государственной тайне и конфиденциальную. Данное разграничение, в частности, отмечено в п. 4 ст. 29 Конституции: «Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

В соответствии со ст. 2 Закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» под *государственной тайной* понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

К сведениям, составляющим государственную тайну, относятся четыре составляющие:

- 1) сведения в военной области (к примеру, сведения о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящих-

ся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения);

2) сведения в области экономики, науки и техники (например, 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 объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов);

3) сведения в области внешней политики и экономики (к примеру, о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства);

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму (например, о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения; о методах и средствах защиты секретной информации).

Конфиденциальной является такая информация, доступ к которой ограничивается в соответствии с законодательством РФ. Перечень такой информации утвержден Указом Президента РФ от 6 марта 1996 г. № 188.

К таким сведениям относятся:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной

защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами РФ;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

В соответствии с Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»:

— *коммерческая тайна* — это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

— *информация, составляющая коммерческую тайну (секрет производства)* — сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Согласно ст. 10 вышеназванного Закона меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Вопросы и задания для самоконтроля

1. Раскройте понятие информационного ресурса.
2. Определите категории информационных ресурсов.
3. Определите признаки информации ограниченного доступа.
4. Какие сведения составляют государственную тайну?
5. Определите понятие конфиденциальной информации, охарактеризуйте ее виды.

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Гражданский кодекс РФ (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ.

Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 6 марта 1997 г. № 188.

О базовых государственных информационных ресурсах : постановление Правительства РФ от 14 сентября 2012 г. № 928.

Глава 6. ИНСТИТУТ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Значение электронного документооборота в условиях развития электронного государства. Значение межведомственного электронного документооборота. Проблемы электронного документооборота. Понятие, признаки и значение электронного документа. Понятие и значение электронной подписи. Юридическая значимость электронных документов.

6.1. Значение электронного документооборота в современных условиях развития электронного государства. Электронная подпись

Немаловажное значение в вопросе полноценного функционирования электронного правительства приобретает электронный документооборот (ЭДО), который можно определить как «систему ведения документации, при которой массив создаваемых электронных документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сеть, дающую возможность формирования и ведения распределенной базы данных»¹.

В утвержденной постановлением Правительства РФ программе «Электронная Россия»², говорилось о том, что совершенствование взаимодействия органов государственной власти и органов местного самоуправления с различными юридическими лицами предусматривает «перевод в электронную цифровую форму большей части документооборота, осуществляемого между хозяйствующими субъектами, органами государственной власти и органами местного самоуправления».

¹ Рассолов И. М. Информационное право : учебник. М. : Юрайт, 2011. С. 179.

² См. распоряжение Правительства РФ от 12 февраля 2001 г. № 207-р.

В августе 2006 г. была принята новая редакция программы. В ней фактически подтверждалось, что за четыре года решить эту задачу не удалось: лишь в незначительном количестве органов государственной власти развернуты и используются комплексные системы электронного документооборота. Получение населением и организациями государственных услуг, а также информации, связанной с деятельностью органов государственной власти, в большинстве случаев требует их личного обращения в органы государственной власти, а также предоставления запросов и другой необходимой информации в бумажном виде».

Еще через два года, в мае 2008 г., Правительство РФ одобрило концепцию формирования в Российской Федерации электронного правительства до 2010 г. Тогда оно вновь констатировало, что вопрос электронного документооборота решить так и не удалось: до настоящего времени не сформирована единая инфраструктура межведомственного обмена данными в электронной форме.

В 2009 г. премьер-министр В. Путин подписал положение о системе межведомственного электронного документооборота. Данное положение, утвержденное Постановлением Правительства РФ от 22 сентября 2009 г. № 754, определяет межведомственный электронный документооборот как взаимодействие информационных систем электронного документооборота федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и иных государственных органов (далее соответственно — информационные системы электронного документооборота, участники межведомственного электронного документооборота).

Сюда относят обмен электронными сообщениями и ведение служебной переписки в электронной форме между участниками межведомственного электронного документооборота — федеральными органами государственной власти, администрацией президента и аппаратом правительства. При этом допускается обмен и общедоступной информацией, и сведениями, составляющими служебную тайну.

При этом надо понимать, что в любом случае перенос в новую среду взаимодействия между государственным органом и гражданином или между госорганами и бизнесом возможен до известных пределов. Даже проект электронного правительства более продвинутых в этом отношении США предполагает детальную проработку вопросов

оптимального соотношения он-лайна и оф-лайна, и рациональное распределение ресурсов на развитие обеих процедур. Можно сделать удобный интерфейс для решения в он-лайне, например, задач налогообложения, но сколько у нас «электронных» физических или юридических лиц? И позволяет ли уровень самих технологий добиться необходимого уровня доверия при взаимодействии, основанном на платежных транзакциях? Здесь пока больше вопросов, чем ответов, и главный вопрос — урегулирование юридических процедур. Пройдет еще много времени, прежде чем электронному документу будут доверять так же, как бумажке с печатью. Вообще нормативная база — один из ключевых факторов в процессе становления электронного правительства. Оно должно быть столь же легитимным, как и традиционное государство, не менее легитимным, чем «электронное» физическое или юридическое лицо¹.

По словам В. Минина, руководителя рабочей группы по ЭДО Института современного развития, сопредседателя Комитета по информационной безопасности Российского Союза ИТ-директоров «в качестве одного из контрольных значений показателей развития информационного общества в Российской Федерации на период до 2015 г. Стратегия устанавливает долю ЭДО между органами государственной власти в общем объеме документооборота, которая должна достигнуть 70%. Внимание к развитию в стране ЭДО оправдано, ведь он создает необходимую базу для формирования технологий «электронного правительства», позволяет снизить стоимость предоставляемых услуг, в том числе государственных, и повысить их оперативность, в целом повысить эффективность управления, а также способствовать прозрачности информационного взаимодействия и противодействию коррупции.

Тем не менее проблемы, связанные с введением электронного документооборота, очевидны. В числе таких проблем можно назвать:

- 1) доказывание права авторства на информацию;
- 2) обнаружение и доказывание факта распространения контрафактных экземпляров;
- 3) идентификация содержания электронного документа с его творцом;

¹ <http://www.garant.ru/company/about/press/smi/10033/>

- 4) утверждение факта и даты ввода в Интернет документа;
- 5) определение и фиксация понятия электронного документа.¹

Необходимы комплексные решения в сфере безопасного электронного документооборота. Сегодня общественность России заинтересована в предоставлении услуг «электронного правительства» при условии конфиденциальности и секретности при взаимодействии с государственной службой (при прозрачности для финансовых органов), гарантиях против мошенничества или взлома компьютеров.

В то же время в опубликованных сегодня документах по построению электронного правительства вопросы информационной безопасности учтены не в полной мере. На стадии реализации проекта это может привести к таким инцидентам, как нарушение прав граждан на получение услуг, нарушение конфиденциальности, подмена сайтов или документов в электронном виде при выполнении государственными органами своих функций и оказании услуг. В случае даже единичного взлома, ставшего достоянием широкой общественности, доверие граждан и предприятий к электронному правительству может быть подорвано, что увеличит период перевода государственных услуг в электронную форму.

В настоящее время система электронного документооборота развита главным образом в банковской сфере, а также при взаимодействии хозяйствующих субъектов и контролирующих органов (например, при подаче налоговых деклараций).

В большинстве случаев организации и граждане обращаются в государственные органы для регистрации и подтверждения своих прав, для защиты своих интересов и т.д. Совершение этих действий сопровождается огромным количеством документов, и их конечным результатом также чаще всего является документ. Чтобы граждане и организации согласились общаться через интернет с государством, они должны быть уверены, что все их права будут документированы в электронном виде не менее надежно, чем на бумаге. Сами государственные органы должны быть уверены в целостности и аутентичности представленных гражданами и организациями электронных документов.

¹ Долинская В. В. Информационные отношения в гражданском обороте // Законы России. 2010. № 4. С. 12.

Действительно, автоматизация процессов обмена данными между отдельными ведомственными информационными системами, а также обеспечение доступа к ним других органов государственной власти требует создания интеграционной информационно-технологической и коммуникационной инфраструктуры для обработки и маршрутизации межведомственных информационных потоков с учетом требований по информационной безопасности¹.

Распоряжением Правительства РФ от 12 февраля 2011 г. № 176-р утвержден план мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности.

Положительно на системе электронного документооборота должно сказаться принятие 6 апреля 2011 г. Федерального закона № 63-ФЗ «Об электронной подписи». Этот Закон расширяет сферу использования и допустимые виды электронной подписи. Прежний закон разрешал применять только сертифицированные средства электронной подписи, а область ее использования ограничивалась гражданско-правовыми отношениями.

Законом установлены принципы использования электронной подписи:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической

¹ Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ... докт. юрид. наук. М., 2008.

силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Согласно закону выделяются два вида электронной подписи: простая и усиленная. Последняя может быть квалифицированной либо неквалифицированной. При этом простая электронная подпись подтверждает, что данное электронное сообщение отправлено конкретным лицом, а усиленная неквалифицированная электронная подпись позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

- 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- 2) позволяет определить лицо, подписавшее электронный документ;
- 3) позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- 4) создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- 1) ключ проверки электронной подписи указан в квалифицированном сертификате;
- 2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным указанным Законом.

Законом подчеркнуто, что сообщение с простой или неквалифицированной электронной подписью может быть приравнено к бумажному документу, подписанному собственноручно, если стороны заранее об этом договорились, а также в специально предусмотренных законом случаях.

Усиленная квалифицированная электронная подпись дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром. Сообщение с такой электронной подписью во всех случаях приравнивается к бумажному документу с собственноручной подписью.

По-настоящему эффективность электронного правительства может быть использована только тогда, когда будет создана законодательная основа для создания и использования электронных документов.

Необходимо отметить, что современная Россия переживает один из наиболее сложных этапов информатизации — процесс адаптации и коренной перестройки государства на пути к его «электронной версии». И в этом процессе далеко не последняя роль должна отводиться полноценному обеспечению прав и свобод человека. К сожалению, действительно, «во всех подходах к понятию электронного государства прослеживается его негативная черта — ориентация на общеуниверсальное представление о личности и человеке, отсутствие индивидуальных особенностей при совершении каких-либо юридических действий. Кроме того, развитые информационно-коммуникационные технологии могут явиться мощным инструментом подавления населения и стать предпосылкой возникновения антидемократического режима. Поэтому законодательство становящегося электронного государства должно содержать гарантии пресечения противоправного вмешательства в жизнь и сознание людей в определенных интересах, а также быть готово к информационным изменениям и отражать основные вопросы его функционирования»¹.

6.2. Понятие электронного документооборота. Электронный документ

Итак, под электронным документооборотом понимают систему ведения документации, при которой массив создаваемых электронных документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в

¹ Васькова М. Г. Электронное государство : проблемы правового регулирования // Информационное право. 2009. № 4. С. 24

сеть, дающую возможность формирования и ведения распределенной базы данных¹.

В соответствии с Федеральным законом Российской Федерации от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» под *документом* понимается материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения.

В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» *документированная информация* — это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

В свою очередь *электронный документ* — это документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронный документ состоит из двух частей:

— реквизитной, содержащей идентифицирующие атрибуты (имя, время и место создания, данные об авторе и т.д.) и электронную подпись;

— содержательной, включающей в себя текстовую, числовую и/или графическую информацию, которая обрабатывается в качестве единого целого.

Характеризуя основные проблемные области в сфере электронного документооборота, С.И. Семилетов отмечает: юридическая сила как официальных документов, так и прочих индивидуальных актов, обеспечивается их соответствием требованиям, установленным законом и наличием вытекающих из них необходимых реквизитов. Одним из обязательных и важных реквизитов документа, обеспечивающим

¹ Рассолов И. М. Информационное право : учебник. М. : Юрайт, 2011. С. 179.

юридическую силу документа, является собственноручная подпись физического или должностного лица, составившего документ, отображающая волю и согласие подписавшего лица по отношению к содержанию документа. По реквизиту (подпись) идентифицируется подписавшее документ лицо, оцениваются его полномочия. Такая же функция электронной подписи и в электронном документе¹.

В статье 6 Федерального закона «Об электронной подписи» названы условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи.

3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подпи-

¹ Законодательная база электронного документооборота в Российской Федерации // Информационное право. 2011. № 3. С. 11.

сью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

Безусловно, нормативно-правовое обеспечение юридической значимости электронных документов должно осуществляться с учетом правового режима электронного документа и его функционального назначения. В целях законодательного определения правового статуса электронных документов, по мнению Е.В. Семизоровой¹, необходимо:

- установить правовые критерии признания электронного документа юридически значимым;

- предусмотреть ответственность за умышленное уничтожение электронных документов или их реквизитов, обеспечивающих качество юридической значимости электронного документа;

- определить и стандартизировать основные типы файлов, используемых для обработки, хранения и передачи документированной электронной информации, в целях обеспечения их адекватного отображения у всех участников электронного документооборота и взаимного обмена документированной информацией в рамках деятельности электронного правительства. Данный перечень должен носить открытый характер;

¹ Семизорова Е. В. Правовой режим электронного документа : проблемы правового регулирования // Юрист. 2011. № 15. С. 33.

— предусмотреть меры, направленные на обеспечение доступности к информации в случае исключения каких-либо файловых типов из данного перечня;

— разработать и закрепить законодательно порядок осуществления третьей независимой стороной процедур перевода документов из традиционной формы в электронную и наоборот, в том числе в случаях, когда документ изначально был создан и существовал до момента перевода исключительно в электронной форме.

Вопрос правовой регламентации правоотношений в сфере электронного документооборота является одним из наиболее актуальных, требующих скорого решения. Согласимся с И.Л. Бачило¹, что для упорядочения и регламентирования электронных административных процедур имеется необходимость принятия федерального закона, в котором все базовые понятия «документ», «электронный документ», «носитель документа», «запись», «файл», «база данных» были бы учтены, сведены к единой системе понятий и нормативно закреплены. Таким актом мог бы быть и должен стать Федеральный закон «Об электронном документе» или «Об общих правилах организации электронного оборота документов в Российской Федерации».

Вопросы и задания для самоконтроля

1. Охарактеризуйте роль электронного документооборота на современном этапе развития электронной России.
2. Дайте характеристику электронному документообороту.
3. В чем специфика электронного документа? Каковы его реквизиты?
4. Определите понятие и признаки электронной подписи.
5. Охарактеризуйте виды электронной подписи.

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Об электронной цифровой подписи : Модельный закон : принят в Санкт-Петербурге 09 декабря 2000 г. Постановлением № 16-10 на 16-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ.

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт, 2011. С. 194.

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов».

Распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р «Государственная программа «Информационное общество (2011—2020 годы)».

Распоряжение Правительства РФ от 12 февраля 2011 г. № 176-р «Об утверждении плана мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности».

Постановление Правительства РФ от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

Постановление Правительства РФ от 22 сентября 2009 г. № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

Постановление Правительства РФ от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия».

Постановление Правительства РФ от 06 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти».

Глава 7. ГЛОБАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ. ИНТЕРНЕТ. СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ. ИНТЕРНЕТ-СМИ

Основные подходы к определению Интернета. Правовое регулирование интернет — отношений. Проблема идентификации субъектов интернет — отношений. Понятие средства массовой информации. Признаки средства массовой информации. Специфика Интернет-СМИ. Понятие сетевого издания. Понятие Интернет-диффамации.

7.1. Правовая природа Интернета и Интернет-отношений

Интернет (от англ. *Internet*) — это всемирная система объединённых компьютерных сетей, построенная на базе протокола IP и маршрутизации IP-пакетов. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (*World Wide Web, WWW*) и множества других систем (протоколов) передачи данных. Интернет представляет собой сеть взаимосвязанных компьютерных систем и ряда различных компьютерных служб.¹

При этом Интернет — глобальная информационная система, части которой логически взаимосвязаны друг с другом посредством единого адресного пространства. Интернет состоит из множества взаимосвязанных компьютерных сетей и обеспечивает удаленный доступ к компьютерам, электронной почте, доскам объявлений, базам данных и дискуссионным группам.

Русскоязычную часть всемирной сети Интернет принято именовать Рунетом. Более узкое определение гласит, что Рунет — это часть Всемирной паутины, принадлежащая к национальным доменам .su, .lu и .rf. 1987—1994 гг. стали ключевыми в зарождении русскоязычного Интернета. 28 августа 1990 г профессиональная научная сеть, выросшая в недрах Института атомной энергии им. И. В. Курчатова и ИПК Минавтопрома и объединившая учёных-физиков и программистов, соединилась с мировой сетью Интернет, положив начало современным российским сетям. 19 сентября 1990 г.

¹ Интернет-энциклопедия. СПб. : ЗАО «ПитерБук», 2008. С. 528.

был зарегистрирован домен первого уровня .su в базе данных Международного информационного центра InterNIC. В результате этого Советский Союз стал доступен через Интернет. 7 апреля 1994 г. в InterNIC был зарегистрирован российский домен .ru.

Домен «.рф», позволяющий использовать в адресе URL кириллические символы, делегирован в корневой зоне DNS 12 мая 2010 г.

Не прекращаются дискуссии по поводу главного вопроса: что есть Интернет? Объект права? Или, может быть, субъект?

Одна из точек зрения относит Интернет к средствам массовой информации. Эта точка зрения основана на положениях Закона «О средствах массовой информации», согласно которому:

— под *массовой информацией* понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы;

— под *средством массовой информации* понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием);

под *сетевым изданием* понимается сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с законом.

Второй подход основан на признании Интернета субъектом права, однако субъект права должен обладать рядом существенных признаков, например, правосубъектностью, которыми сеть в полной мере не обладает.

Третья точка зрения более обоснована, и заключается она в признании Интернета объектом права. Действительно, Интернет как инфраструктура информационного общества, скорее всего, очевидно, будет выступать в качестве объекта правового регулирования, причем даже не специального, а самого обычного¹.

Существует немало подходов к определению понятия Интернета. В России термин «Интернет» используется в многочисленных нормативных правовых актах, однако легальное определение Интернета отсутствует.

¹ Рассолов И. М. Информационное право : учебник. М. : Юрайт, 2011. С. 234.

Например, в соответствии со ст. 57 Федерального закона «О связи» в Российской Федерации гарантируется оказание универсальных услуг связи.

К универсальным услугам связи относятся:

- услуги телефонной связи с использованием таксофонов;
- услуги по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети «Интернет» с использованием пунктов коллективного доступа.

По мнению И.Л. Бачило¹, Интернет — это сфера непрерывного информационно-коммуникационного процесса, обеспечивающего обращение информации (сведений) в цифровой форме в неограниченном пространстве через связанные между собой сети связи, и реализации обмена информационным ресурсом любых субъектов (потребителей) в целях получения, накопления знаний или осуществления электронных операций субъектов в разных областях реализации их интересов, прав и обязанностей.

Специфика Интернета предопределена особенностями кибернетического пространства, к числу которых, по мнению И.М. Рассолова², относится:

- 1) отсутствие географических границ;
- 2) анонимность в киберпространстве;
- 3) возможность ускользать от контроля (пользователи Сети могут «выйти» из режима, определенного национальным законом, чтобы избежать выявления совершенных ими правонарушений...Субъекты преступлений стараются осуществлять свою преступную деятельность в наиболее свободных зонах Интернета, т.е. вне судебной юрисдикции собственного государства (например, в зонах .com, .net, .org, .ag, .sc)
- 4) иерархия и структурные зоны (Интернет представляет пространственную структуру, включающую иерархию различных участников: учреждений регистрации доменных имен и множества посредников, распределенных ассиметричным способом (интернет-провайдеры, торговые информационные посредники и др. Все они

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт, 2011. С. 335.

² Рассолов И. М. Информационное право : учебник. М. : Юрайт, 2011. С. 250—255.

обеспечивают возможность доступа потребителям информации к информационным разделам и наполнениям Сети);

5) растущее взаимодействие, интерактивность и динамизм;

6) наличие интерактивных информационных связей (Интернет характеризуется огромным числом электронных соединений, коммуникаций. Одним из характерных элементов этой среды является сетевой договор).

В юридической литературе выделяют *четыре* регулятора правоотношений в сети Интернет (поведения участников сети). Поведение в данной сфере может быть урегулировано следующими типами регуляторов:

- напрямую законом;
- социальными (корпоративными) нормами;
- законами рынка и конкуренции;
- техническими нормами¹.

В виду того, что сеть Интернет и отношения в рамках сети Интернет развиваются гораздо быстрее, чем законодатель успевает создавать соответствующие законные конструкции и формулы, в настоящее время регулирование большей части отношений строится на деловых обыкновениях, «Интернет-обычаях».

Безусловно, начинать правовое урегулирование сети Интернет необходимо с норм *международных* — единых для всех цивилизованных государств. Правоотношения, складывающиеся в сети Интернет, не могут регулироваться только нормами национального законодательства.

В настоящее время продолжают дискуссии по поводу целесообразности принятия в России отдельного закона об Интернет, и обусловлено это, в первую очередь, определенной спецификой интернет — отношений.

В числе их особенностей:

1. Особый субъектный состав. Интернет-отношения могут возникать между особыми субъектами (операторы связи, провайдеры, разработчики сетей, международные организации, отвечающие за развитие протоколов Интернета и т.д.).

¹ Рассолов И. М. Интернет и право. М. : Закон и право, 2008. С. 36.

2. Субъекты интернет-отношений могут находиться в разных странах, а их деятельность регулироваться законодательствами разных стран.

3. Интернет-отношения невозможны без использования информационно-коммуникационных технологий и сетей. Они имеют информационное наполнение, т.е. складываются по поводу информации в Интернете. Объектом этих отношений является не всякая информация, а только обрабатываемая в киберпространстве.

4. Интернет-отношения выделяются на современном этапе развития общества, государства и технологий... для целей автоматизации управления различными информационными системами, в нашем случае сложной кибернетической системы — Интернета¹.

В.А. Копылов важной особенностью глобального информационного пространства называл отсутствие географических и геополитических границ государств-участников, в результате чего происходит «столкновение» и «ломка» национальных законодательств стран в этих сетях. Интернет — по замечанию В.А. Копылова — по сути дела, представляет собой новую среду обитания человечества, новую среду деятельности личности, общества, государства. Эту среду нередко называют виртуальной, имея в виду тот факт, что информация — основной объект этой среды — физически, «на ощупь», не ощутима².

Приведем ряд статистических данных.

К концу 2013 г. число пользователей сети Интернет превысило 2,7 млрд. человек (все население планеты — 7 млрд. чел.).

Аудитория интернета в России составляет 66,5 миллиона человек — столько россиян старше 18 лет пользуются интернетом хотя бы раз в месяц (по данным ФОМ на осень 2013 г.). 80% пользователей — или 53 миллиона человек — выходят в сеть ежедневно³.

Особенность современности — это то, что сегодня наблюдается большой рост интереса к интернету со стороны пожилого населения.

¹ Рассолов И.М. Информационное право : учебник. М. : Юрайт, 2011. С. 237.

² Копылов В. А. Информационное право : учеб. пособие. М. : Юристъ, 1999. С. 235.

³ Информационный бюллетень по данным сервисов Яндекс.Метрика, Яндекс.Новости, Яндекс.Справочник и Яндекс.Каталог, а также Фонда «Общественное мнение» (ФОМ), исследовательской группы TNS и Технического Центра Интернет. Весна 2014.

«Взросление» веб-аудитории отмечается не только в России. По данным Roiworld американская молодежь массово покидает социальную сеть Facebook. Тинейджеров не устраивает, что услугами популярного портала теперь всё чаще пользуются их родители.

Очевидно, что Интернет сегодня прочно вошел в современную жизнь практически каждого человека. Однако нерешенных проблем в этой области еще достаточно. Остановимся на некоторых из них.

Прежде всего, по замечанию И.Л. Бачило¹, для развития правового регулирования встает задача найти стимулирующие средства включения ресурса Интернета в те сферы общежития граждан, которые наиболее действенны для поднятия уровня жизни, обучения пользованию новыми технологиями и способствуют повышению уровня образования и знаний.

Безусловно, в числе проблем современной России — проблема цифрового равенства. И здесь будет полезен опыт зарубежных государств, в которых работают специализированные программы соответствующей подготовки.

Проблема номер один сегодня — защита персональных данных в сети Интернет.

Анонимность интернет — отношений предопределяет и наличие проблемы установления личности субъекта Интернет-отношений, т.е. проблема идентификации.

Для вступления в некоторые коммуникационные интернет-отношения субъекты должны быть определенным образом идентифицированы². Многие интернет-ресурсы и сервисы предлагают или требуют для использования их пройти процедуру регистрации. Можно сказать, что для деятельности в виртуальном пространстве Интернета человек создает свой виртуальный образ или виртуальное лицо. По аналогии с реальным человеком виртуальное лицо будет иметь свое «имя», под которым действует (имя пользователя) и аналог фотографии и подписи в удостоверении личности — пароль.

¹ Бачило И. Л. Информационное право : учебник. 2-е изд., перераб. и доп. М. : Юрайт, 2011. С. 348.

² Андрищенко Е. С. Проблема идентификации субъектов интернет-отношений. Виртуальное лицо // Информационное общество : проблемы развития законодательства : сб. науч. работ. М., 2012. С. 81.

Поскольку субъект виртуальных отношений определяется только этими двумя параметрами, то виртуальные лица и реальные люди не соотносятся между собой как один к одному: один пользователь может иметь несколько виртуальных лиц, и за одним виртуальным лицом может стоять несколько людей. Основная возникающая в этом случае проблема: сложно установить реального человека, стоящего за виртуальным лицом, еще сложнее эту связь процессуально доказать. В механизме электронной подписи также не предусмотрено наличие идентифицирующего признака, непосредственно связанного с человеком, неотчуждаемого от него.

7.2. Понятие средств массовой информации.

Конституционные гарантии свободы массовой информации

Основной нормативный акт, регулирующий отношения, складывающиеся в сфере массовой информации, с участием средств массовой информации — это Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

Под массовой информацией, согласно данному закону, понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Распространение продукции средства массовой информации включает: продажу, подписку, доставку, раздачу периодического печатного издания, аудио- или видеозаписи программы, вещание телеканала, радиоканала (телевизионное вещание, радиовещание), вещание телепрограммы, радиопрограммы в составе соответственно телеканала, радиоканала, демонстрацию кинохроникальной программы, предоставление доступа к сетевому изданию, иные способы распространения.

В ст. 1 Закона РФ «О средствах массовой информации» четко определено, что в Российской Федерации поиск, получение, производство и распространение массовой информации, учреждение

средств массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации, не подлежат ограничениям, за исключением предусмотренных законодательством РФ о средствах массовой информации.

Основные гарантии в сфере массовой информации определены в Конституции РФ. Так, ч. 4 ст. 29 Конституции РФ закреплено право каждого на свободные поиск, получение, передачу, производство и распространение информации любым законным способом. Этот комплекс прав образует основу правового института свободы информации.

В ч. 5 ст. 29 Конституции РФ закреплена основополагающая конституционная гарантия свободы поиска, получения, передачи, производства, и распространения массовой информации, выраженная в форме обязанности государства гарантировать (своей деятельностью) свободу массовой информации — «Гарантируется свобода массовой информации. Цензура запрещается».

Исходя из содержания ст. 58 Закона РФ «О средствах массовой информации» ущемление свободы массовой информации, т.е. воспрепятствование в какой бы то ни было форме со стороны граждан, должностных лиц государственных органов и организаций, общественных объединений законной деятельности учредителей, редакций, издателей и распространителей продукции средства массовой информации, а также журналистов, в том числе посредством:

- осуществления цензуры;
- вмешательства в деятельность и нарушения профессиональной самостоятельности редакции;
- незаконного прекращения либо приостановления деятельности средства массовой информации;
- нарушения права редакции на запрос и получение информации;
- незаконного изъятия, а равно уничтожения тиража или его части;
- принуждения журналиста к распространению или отказу от распространения информации;

— установления ограничений на контакты с журналистом и передачу ему информации, за исключением сведений, составляющих государственную, коммерческую или иную специально охраняемую законом тайну;

— нарушения прав журналиста, установленных законом, влечет уголовную, административную, дисциплинарную или иную ответственность в соответствии с законодательством РФ.

Законодательством установлены и определенные ограничения в сфере массовой информации. Так, ч. 2 ст. 29 Конституции РФ установлены запреты, касающиеся информации, в том числе массовой, определенной направленности, распространение которой нарушает либо угрожает интересам личности, общества и государства, а именно — не допускается (запрещена) пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду, а также пропаганда социального, расового, национального, религиозного или языкового превосходства.

Основополагающий принцип правового регулирования деятельности СМИ, провозглашенный Конституцией РФ — это принцип свободы массовой информации. В то же время, в ст. 29 изложены два конституционных основания ограничения свободы массовой информации: ч. 2 ст. 29 устанавливает запрет распространения информации, являющейся пропагандой или агитацией, возбуждающей социальную, расовую, национальную или религиозную ненависть и вражду, ч. 4 ст. 29 устанавливает основание ограничения обращения сведений, составляющих государственную тайну.

7.3. Средства массовой информации, функционирующие в сети Интернет

Реалии развития Интернет-отношений позволяют с уверенностью утверждать: справедливо считать свершившимся появление нового средства массовой информации, объединяющего в себе черты теле- и радионовостей (оперативность обновления) с газетными и журнальными публикациями (объем предоставляемой информации).¹

¹ Кемрадж А. С., Головеров Д. Правовые аспекты использования интернет-технологий. М. : Книжный мир, 2002. С. 19.

Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает сегодня один из самых активных этапов своего развития.

Развитие единого информационного пространства Российской Федерации является одной из важнейших задач, стоящей перед государством, которое должно решать вопросы не только своего развития и как следствие — развития информационного пространства, но и обеспечения информационной безопасности.

Источником распространения массовой информации в сети является любой общедоступный и открытый информационный ресурс. Это может быть Интернет-страница или сайт, on-line конференция, электронная почтовая рассылка и т.д.

Безусловно, новые технологии заставили нас изменить традиционное представление о средствах массовых коммуникаций. Традиционные формы коммуникаций — телевидение и радио — с приходом глобальных компьютерных сетей и применением цифровых технологий обработки вещательного сигнала дали качественно новые возможности. А главное — увеличилась пропускная способность радио- и телеканалов и, в конечном счете, значительно увеличились возможности ресурса распространения электронных СМИ¹.

Свобода Интернета от коммерческих и политических ограничений вместе с его доступностью и интерактивностью придает электронным средствам коммуникаций громадный демократизирующий потенциал, поскольку позволяет избегать цензуры и регламентации. Однако, с другой стороны, эти возможности являются основой существующих угроз информационной безопасности, а также нелегальной деятельности хозяйствующих субъектов, бесконтрольного распространения рекламы, в том числе рекламы криминального характера.

Проанализируем средства массовой информации, функционирующие в сети Интернет, определим их правовой режим, акцентируя внимание на возможности применения норм действующего законодательства для регулирования правоотношений с участием таких СМИ.

¹ Какие опасности таит в себе Интернет? // Юридический консультант. 2006. № 10. С. 46.

Мы наблюдаем всплеск активности анализируемых СМИ в масштабах всей страны (что особенно наглядно в период предвыборных агитаций). Нельзя не принимать во внимание и предсказаний ежегодного удвоения «населения» русской Сети.

Говоря о регулировании средств массовой информации, функционирующих в Интернет, возникает вопрос: *насколько правомерно считать средствами массовой информации такие издания вообще?*

Активное развитие средств массовой информации в Сети очевидно. Тем не менее, до сих пор не выработано единого представления о содержании и формах деятельности таких СМИ, единого подхода к терминологии.

Прежде всего, необходимо отметить многовариантность правовых ответов на терминологическое выражение смыслового наполнения Интернета. Нет единого подхода и у специалистов, занимающихся проблемами правового урегулирования интернет-отношений.

Средства массовой информации в сети Интернет закон «О средствах массовой информации» определяет как сетевые издания. Под *сетевым изданием* согласно «букве закона» понимается сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с законом.

Средства массовой информации, функционирующие в Интернет, разнообразны по характеру своей деятельности, по тематике и т.д. В связи с этим представляется необходимым проанализировать возможность их классификации. Проанализируем уже имеющиеся подходы.

И. Давыдов еще в 2000 г. осуществил попытку охарактеризовать масс-медиа российского Интернета и предложил варианты классификации медийных ресурсов, представленных в русском Интернете¹. Им были выделены собственно сетевые издания (т.е. те, которые выходят только в Интернете и сетевые версии традиционных СМИ).

Кроме того, сетевые СМИ могут быть подразделены по типу представленного в них контента. Здесь возможны две классификации:

1) новостные; комментарийные; смешанные;

¹ Давыдов И. Масс-медиа российского Интернета. Основные тенденции развития и анализ текущей ситуации // www.russ.ru/politiks/20000928_davydov.html

2) авторские; редакционные; смешанные.

Возможны также классификации по тематике: монотематические (внутри этой группы деление может стать почти бесконечным ввиду обилия вариантов представленных монотематических ресурсов); политематические;

и классификация по принадлежности: принадлежащие государству; принадлежащие медийным группам; политическим группам; бизнес — группам; независимые.

Кроме того, существенно деление, которое, несмотря на используемую терминологию, относится не столько к географическому положению редакций конкретных ресурсов, сколько к аудитории, на которую данные ресурсы ориентированы в первую очередь: общероссийские ресурсы, региональные ресурсы (к данному типу могут быть отнесены также зарубежные русскоязычные ресурсы, ориентированные на относительно узкие диаспоры).

Необходимо отметить, что в последнее время появилось много новых информационных объектов: домашняя интернет-страница, сайт, портал, электронная библиотека, он-лайн конференция, чаты, службы мгновенного сообщения типа ICQ и MSN, электронная почтовая рассылка в популярном формате RSS или столь модный сегодня блог ¹.

Такие СМИ представляют собой информационные объекты, содержанием которых являются размещаемые на них и периодически обновляемые сведения, сообщения и материалы, по общему правилу предназначенные для неопределенного круга лиц. Иными словами эти объекты распространяют не что-нибудь, а именно «массовую ин-

¹ Блог — от англ. *weblog* — «сетевой дневник». Термин введен в 1997 г. американским писателем и специалистом по искусственному интеллекту Йорном Баргером. Это информационные объекты, содержание которых составляют регулярно добавляемые их посетителями статьи, записи, иные материалы и комментарии. Блоги приемлют практически все — собственное жизнеописание, прямой репортаж с какого-либо интересного мероприятия, впечатления об увиденном в путешествии и т.д. Значительнейшая часть блогонакопительства — результат своеобразного веб-серфинга, т. е. хождения по разным сайтам. Заприметил человек в Сети что-то интересное, написал об этом в своем блоге и дал ссылку. Кто-то сходил по этому адресу, а, вернувшись, оставил свой комментарий. Тем самым блог приобретает качества публичности, когда его ведением занимается уже не один человек, а все зарегистрированные посетители.

формацию» в понимании нормы ст. 2 Закона РФ «О средствах массовой информации».

Отмечая роль и оценивая влияние средств массовой информации в сети Интернет на российское общество в целом, исследователи подчеркивают, что «если на Западе в блогах больше речь идет о том, например, «как я провел лето» или «как я купил себе новый макинтош», то в России блоги совершенно особенная вещь — здесь проявляется наш особый путь. Политическая дискуссия, пропавшая со страниц газет, из ТВ и радио, она вся сейчас там. Люди интеллектуального труда пользуются Livejournal, и у них нет ощущения, что в стране отсутствует политическая дискуссия — она есть, просто она не в том месте, где была раньше»¹.

Известно, что «для сетевых информационных процессов характерны широта охвата аудитории, высокая оперативность, многообразие форм информационного воздействия при наличии обратных связей пользователя с поставщиком информации. Такое сочетание приводит к тому, что глобальные компьютерные сети становятся мощным инструментом выражения и формирования общественного мнения. В этом качестве они приближаются по своим возможностям к традиционным средствам массовой информации, а в некоторых случаях и превосходят их. Нередко электронные газеты сообщают о произошедших событиях раньше, чем традиционные СМИ»².

По мнению А.Г. Рихтера³, «между Интернетом и средствами массовой информации нельзя ставить знак равенства: признаки информации, распространяемой по телекоммуникационным сетям, не совпадают с признаками традиционной массовой информации». Прежде всего, для Интернет-страниц не подходит формула «форма периодического распространения массовой информации», характеризующая традиционные средства массовой информации.

¹ См. Самарина А. Выборы-2008 под знаком Интернета. // Независимая газета. 2005. 26 авг.

² Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Международные опыт. М. : Норма, 2004. С. 33.

³ Рихтер А. Г. Правовые основы журналистики. М. : Изд-во МГУ, 2002.

Как представляется, наиболее логичную и обоснованную позицию по данной проблеме предложил В. Наумов¹. В логике его подхода, — любой сайт — *источник массовой информации*, но отнюдь не любой сайт — *средство массовой информации*. Поскольку, как правильно отмечает В. Наумов, переход в правовое положение СМИ с неизбежностью сопряжен с соответствующими обременениями (новый баланс прав и обязанностей), то это серьезное и юридически значимое действие должно проводиться собственниками и менеджментом тех или иных сетевых ресурсов осознанно и добровольно.

Размышляя о *статусе СМИ*, В. Наумов метафорично интерпретирует его в качестве своеобразных «погон» или «униформы» для СМИ. А за красивые «погоны и униформу», дающие определенные права и преференции, как, впрочем, и за все в жизни, «надо платить». В частности, — повышенной юридической ответственностью за то, чем отзовется виртуальное слово и/или изображение.

В настоящее время в мире имеют место различные подходы к определению отношения государства к Интернет-СМИ. Например, китайский вариант, в той или иной степени распространённый в ряде государств Юго-Восточной Азии и Ближнего Востока. Суть его в строгом (сама степень строгости определяется исключительно мнениями руководства государства со ссылкой на национальные традиции) контроле за деятельностью в Интернете, или цензуре. Государство контролирует большую часть информации, циркулирующей в сети, а само существование Интернет-СМИ в ряде случаев невозможно.

Другой вариант (характерен для государств Западной Европы и Северной Америки) подразумевает государственный контроль, сводящийся к пресечению преступной деятельности в Интернете. Однако такой вариант не охватывает всего многообразия общественных отношений.

В настоящий момент трудно судить, какой вариант будет избран для России в качестве наиболее оптимального. Согласно Конституции, в нашей стране необходим баланс интересов с одной стороны общества и Интернет-СМИ, имеющих право на информацию, и

¹ Наумов В. Б. Право и Интернет : Очерки теории и практики. М. : Книжный Дом Университет, 2002. С. 68—95.

государства, призванного защищать общество от преступности, насилия и других негативных явлений. Формирование такого баланса зависит от позиции не только государственных ведомств, юристов и журналистов, но и рядовых граждан-пользователей Интернета.

В числе последних изменений законодательства — Федеральный закон № 97-ФЗ, принятый 5 мая 2014 г. приравнивает популярных блогеров, чьи сайты или страницы в соцсетях посещает более 3000 человек, к СМИ.

Согласно ст. 10.2 анализируемого Закона владелец сайта и (или) страницы сайта в сети «Интернет», на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети «Интернет» (блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данных сайте или странице сайта иными пользователями сети «Интернет», обязан обеспечивать соблюдение законодательства РФ, в частности:

1) не допускать использование сайта или страницы сайта в сети «Интернет» в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;

3) не допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства;

4) соблюдать запреты и ограничения, предусмотренные законодательством РФ о референдуме и законодательством РФ о выборах;

5) соблюдать требования законодательства РФ, регулирующие порядок распространения массовой информации;

6) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

Нарушение закона влечет за собой штраф в размере от 10 до 30 тыс. рублей для физических лиц, от 50 до 300 тыс. рублей — для юридических лиц. Повторное нарушение требований в течение года карается штрафом для граждан от 30 до 50 тыс. рублей, для юридических лиц — от 300 до 500 тыс. рублей или административным приостановлением деятельности на срок до 30 суток.

7.4. Интернет-диффамация: вопросы юридической ответственности

Среди специалистов уже несколько лет развивается дискуссия о природе юридической ответственности в Интернет-праве. Под системой юридической ответственности понимают совокупность и взаимодействие норм и институтов права, соблюдение которых обеспечивает правопорядок, а применение их при совершении правонарушения восстанавливает правопорядок¹. Юридическая ответственность выражается, прежде всего, в ответственном отношении к своим обязанностям самих участников общественных отношений и добросовестной реализации имеющихся прав и возложенных на них обязанностей.

Исследователями подчеркивается, что отсутствие отлаженных правовых механизмов влияния на представляемую информацию позволяет размещать в Интернете противоправные материалы откровенно националистического, фашистского, расистского содержания, различного рода дезинформацию, анонимные клеветнические публикации и т.д.².

В свете этой полемики актуальной и своевременной представляется проблема цивилизованного правового регулирования деятельности средств массовой информации в сети, в частности, их ответственности за оглашение каких-либо фактов, не соответствующих действительности, и сведений, порочащих честь, достоинство, репутацию и доброе имя.

¹ Мацкевич А. В. Функции юридической ответственности в современном обществе : понятие, система, тенденции развития // Российский следователь. 2006. № 12. С. 63.

² Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Международным опытом. М. : Норма, 2004. С. 33.

В соответствии с Доктриной информационной безопасности РФ информационная безопасность личности определяется как состояние защищенности ее интересов в информационной сфере. Эти интересы заключаются главным образом в реализации конституционных прав на доступ к информации, ее правомерном использовании и в защите информации, обеспечивающей личную безопасность¹.

Согласно ст. 5.61. КоАП *оскорбление*, т.е. унижение чести и достоинства другого лица, выраженное в неприличной форме, влечет наложение административного штрафа на граждан в размере от одной до трех тысяч рублей; на должностных лиц — от десяти до тридцати тысяч рублей; на юридических лиц — от пятидесяти до ста тысяч рублей.

Оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, влечет наложение административного штрафа на граждан в размере от трех до пяти тысяч рублей; на должностных лиц — от тридцати до пятидесяти тысяч рублей; на юридических лиц — от ста до пятисот тысяч рублей.

Непринятие мер к недопущению оскорбления в публично демонстрирующемся произведении или средствах массовой информации влечет наложение административного штрафа на должностных и юридических лиц.

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Единое мировое информационное пространство, создавая условия безграничной свободы и отсутствия должного правового регулирования, ставит под сомнение ряд закрепленных основным законом государства прав и свобод.

Нельзя не согласиться с А.А. Фатьяновым² — сложившаяся ситуация одновременно вдохновляет и настораживает. Вдохновляет потому, что человек может свободно самовыражаться, формируя и представляя на всеобщее обозрение информацию о себе самом (и не только). Настораживает потому, что свобода обмена информацией в Сети

¹ Горшенков Г. Г. Компенсация морального вреда как мера обеспечения информационной безопасности личности // Информационное право. 2005. № 3. С. 24.

² Правовое обеспечение безопасности информации в Российской Федерации : учеб. пособие. М.: Юрист, 2001. С. 34.

в ряде случаев реализуется как вседозволенность. В реалиях эдакой свободы слова без границ соблюдение конституционных прав и свобод человека и гражданина — второстепенно.

Развиваясь и совершенствуясь, «сетевое государство» пока еще не успевает установить конкретные юридические механизмы и процедуры защиты общепризнанных прав.

Изменения в законодательстве обусловили разные подходы специалистов к проблеме ответственности в Интернет-праве. Так, ряд исследователей определяют эту проблему не только как юридическую, но в том числе и как морально-этическую¹. Итак, институт интернет-диффамации, в связи с бурным развитием информационного законодательства в последние годы, приобретает новое содержание.

По оценкам специалистов, в общей системе мирового права диффамационное право занимает весьма скромное место. Однако если смотреть на него с точки зрения приоритетов, защищаемых правом вообще, где на первом месте находятся права, свободы и законные интересы конкретного индивида, то диффамационное право приобретает весьма важное значение в системе права, поскольку на основе его регулятивных и охранительных норм строятся отношения между личностью и средствами массовой информации. Еще большее значение диффамационное право будет приобретать в реалиях сегодняшнего развития виртуального пространства.

Масштабы распространения диффамационных материалов в Сети обусловлены особенностями Интернета, среди которых особо следует отметить: широкую аудиторию пользователей и возможность ее неограниченного расширения; трансграничное распространение информации; высокую скорость и оперативность предоставления информации; практически неограниченный выбор источников и видов информации; практическое отсутствие предварительного контроля содержания информации (цензуры); возможность обсуждения возникающих вопросов в режиме реального времени; возможность одновременного представления информации в различной форме (текст, графика, звук, анимация и др.)².

¹ Рассолов И. М. Право и интернет. Теоретические проблемы. М. : Норма, 2003. С. 197.

² Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики) : учеб. пособие / под ред. М. М. Рассолова. М. : Контракт, 2004. С. 220.

Диффамация вообще — это правонарушение в виде распространения (произнесения слов или публикации) не соответствующих действительности фактических сведений, порочащих честь, достоинство, деловую репутацию, доброе имя потерпевшего. Этот термин образован от латинского «diffamatio» — порочить.

Нормы диффамационного права на сегодня имеются в странах как романо-германского, так и англо-американского права. Например, в Великобритании действует Закон о диффамации 1996 года (Defamation Act, 1996).

Попытки законодателя решить ряд важных вопросов все же есть. В числе таковых — постановление Пленума Верховного Суда РФ от 24 февраля 2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц».

Постановлением подчеркивается, что, в соответствии с Конвенцией о защите прав человека и основных свобод, осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями. Перечисленные условия должны быть предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка в целях предотвращения беспорядков или преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

Под распространением сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, следует понимать опубликование таких сведений в печати, трансляцию по радио и телевидению, демонстрацию в кинохроникальных программах и других средствах массовой информации, *распространение в сети Интернет*, а также с использованием иных средств телекоммуникационной связи, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение в той или иной, в том числе устной, форме хотя бы одному лицу.

Прежде всего, Пленум Верховного Суда РФ разъясняет, что используемое Европейским Судом по правам человека в его постановлениях понятие *диффамации* тождественно понятию распространения не соответствующих действительности порочащих сведений, содержащемуся в ст. 152 ГК РФ.

Диффамация, или опозорение в печати, известна буржуазному уголовному законодательству как преступление, близкое к клевете, но отличающееся от нее двумя признаками:

1. Диффамация есть оглашение каких-либо позорящих фактов в печати, тогда как клевета может быть совершена на словах или в письме;

2. В Диффамации преступный момент заключается в самом оглашении в печати позорящих сведений, независимо от их правильности, клевета же всегда рассматривается как сообщение заведомо ложных сведений. Поэтому против обвинения в клевете можно защищаться, доказывая правильность сообщенных сведений, а против диффамации указанием на это защищаться нельзя.

Диффамация была известна законодательству дореволюционной России как «оглашение в печати о частном или должностном лице, обществе или установлении такого обстоятельства, которое может повредить их чести, достоинству или доброму имени». В таком виде диффамация являлась средством ограничения свободы печати не только против вторжения последней в частную жизнь граждан, но и против разоблачения в прессе неправильных действий должностных лиц. В отношении должностных лиц допускалась защита против обвинения в диффамации указанием на истинность оглашенного в печати позорящего обстоятельства, касающегося служебной деятельности опозоренного лица. Однако обвиняемый мог защищаться только путем представления письменных доказательств, что практически представлялось почти невозможным

Интернет-диффамация, кибер-диффамация, диффамация в Сети — можно по-разному определить обозначенное явление, главная опасность которого — в реальной угрозе задекларированных конституционных принципов общества и государства. До настоящего времени нет единого понимания, что такое Интернет-диффамация и каковы механизмы ее урегулирования правовыми мерами.

Интернет-диффамацию можно определить как распространение посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, деловую репутацию, доброе имя.

Неотъемлемый атрибут диффамационного деликта — признак порочности. Если распространенные сведения не носят порочащего характера, даже при условии, что они не соответствуют действительности, то не будет и состава диффамационного деликта.

Суть любого диффамационного спора — в разрешении коллизии между правом на защиту чести и достоинства, с одной стороны, и правом на свободу слова и массовой информации, — с другой.

Постулируя незыблемость прав и свобод человека, мировое общество, тем не менее, прекрасно осознает, что свобода не может быть безгранична. Она в любом случае будет ограничена аналогичной свободой других лиц. Отметим, что международные акты о правах человека разрешают государствам при определенных условиях вводить ограничения некоторых прав. Однако подобные меры должны приниматься только в той степени, в какой это необходимо государству в интересах безопасности его граждан и его собственной безопасности. Нормы, позволяющие ограничить действие некоторых прав человека, вводятся с целью установления равновесия между правами отдельных лиц и интересами общества и государства в целом, а также в том случае, когда между ними могут возникать противоречия¹. Проблема — в поиске ответа о соразмерности таких ограничений.

Итак, в связи с бурным развитием интернет-отношений представляется важным обращение к проблемам диффамационного права. Неслучайно сегодня неведомый большинству практикующих российских юристов термин «диффамация» все чаще используется не только в научных публикациях, но и в решениях Европейского Суда по правам человека.

Обязанность доказывать соответствие действительности распространенных в Интернете сведений лежит на ответчике. Истец же обязан доказать факт распространения сведений лицом, к которому

¹ Опалева С. А. Права человека и конституционно-правовое регулирование их допустимого ограничения // Гражданин и право. 2006. № 3. С. 25.

предъявлен иск, а также порочащий характер этих сведений. Гражданское законодательство (ст. 151, 152 ГК РФ) предусматривает возможность требования истцом прекращения распространения информации в Сети, ее опровержения, а также компенсации морального вреда.

В числе нерешенных вопросов — возможность обеспечения доказательств. Как доказать факт размещения клеветнической информации в Интернете? Практика показывает, что предъявить обоснованные претензии собственнику сайта очень сложно, практически невозможным представляется и требование об опубликовании опровержения. Неслучайно в условиях анонимного присутствия в Сети, так популярны интерактивные «гостевые книги», предоставляющие посетителям безграничные возможности реализации права на свободу слова. Как следствие, честь, достоинство и доброе имя граждан нередко выступают объектами посягательств в Интернете.

Затруднительность применения к средствам массовой информации, функционирующим с сети Интернет, обоснованных санкций превращает виртуальное пространство в привлекательное поле для диффамационных утверждений.

Дискуссионность вопроса о природе средств массовой информации, функционирующих в сети Интернет, определяет отсутствие правовых механизмов контроля их деятельности в виртуальном пространстве. Речь о цивилизованном правовом регулировании деятельности «иных средств массовой информации». Пока же российское законодательство в отношении средств массовой информации, функционирующих в сети Интернет, не обеспечивает соблюдение конституционных прав и свобод человека и гражданина.

Итак, *интернет-диффамация* — это распространение посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя. Честь, достоинство, репутация, доброе имя в случае распространения диффамационных материалов выступают специфичным объектом анализируемого правоотношения.

Возможность анонимного присутствия в Сети позволяет скрыть подлинные имена автора, источника и лица, разместившего информацию. В связи с отсутствием соответствующего законодательства, четко определенного перечня субъектов деятельности в Интернете и их

правового статуса реальная судебная защита прав личности, нарушаемых в Сети, в настоящее время не может быть обеспечена в полном объеме.

Проблема заключается в том, что для доказанности в суде факта распространения порочащих сведений конкретными лицами требуется проведение достаточно сложных процедур: просмотр протоколов доступа, проверка учетных записей провайдеров доступа, определение телефонных номеров и их владельцев, просмотр содержимого серверов, установление владельцев серверов, зачастую находящихся в разных странах, что связано с исполнением международных поручений, и т.д.

Сложность и в том, что географический размах связей в Интернете способен породить принципиальные вопросы, которые могут заставить пересмотреть само понятие «репутация». Что означает чья-то репутация в глобальном сообществе, и кого можно считать «разумным и благонамеренным представителем общества как целого», чьими критериями и стандартами, как предполагается, должен руководствоваться суд?

Подводя итог, отметим, что только тщательная проработка юридического механизма реализации конституционных гарантий прав, свобод и иных нематериальных благ в контексте функционирования в сети Интернет средств массовой информации позволит обеспечить эффективную и всестороннюю защиту прав и свобод граждан.

Вопросы и задания для самоконтроля

1. В чем специфика Интернета, интернет — отношений?
2. Охарактеризуйте основные подходы к определению Интернета.
3. Назовите основные проблемы правового регулирования интернет-отношений.
4. В чем проблематичность взаимоотношений человека с сетью Интернет?
5. Раскройте понятия «массовая информация», «средство массовой информации», «сетевое издание». Соотнесите их между собой.
6. Осветите конституционные гарантии свободы массовой информации.
7. В чем специфика средств массовой информации, функционирующих в сети Интернет?
8. Каковы основные подходы к определению отношения государств к Интернет-СМИ?

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

Федеральный закон от 5 мая 2014 г. № 97-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей».

Стратегия развития информационного общества в Российской Федерации : утв. Президентом РФ 7 февраля 2008 г. № Пр-212.

Государственная программа «Информационное общество (2011—2020 годы) : распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р.

Глава 8. ЭЛЕКТРОННОЕ ГОСУДАРСТВО КАК ИНСТИТУТ ИНФОРМАЦИОННОГО ПРАВА И ЕГО РЕАЛИЗАЦИЯ В ТРИАДЕ ВЕТВЕЙ ВЛАСТИ

Понятие электронного государства. Электронное правительство. Предоставление государственных и муниципальных услуг в электронном виде. Электронный парламент. Создание единой системы электронной демократии. Основные элементы электронного правосудия.

8.1. Понятие электронного государства. Электронный парламент и электронное голосование

Наряду с построением правового, конституционного, социального государства провозглашаемая сегодня задача — построение государства электронного.

В определении понятия «электронное государство» принципиальным вопросом является вопрос — или скорее немалая проблема — соответствующей терминологии. Особого внимания и поддержки заслуживает мнение П. У. Кузнецова о том, что «без научного осмысления в обиход «вбрасываются» такие новые словосочетания, как «электронное правительство», «электронное государство», «сервисное государство», «электронное правосудие», «электронный нотариат», «электронный сервис» и др., которые затем вписываются в документы официальной государственной политики. Казалось бы, это нормальный процесс создания терминологического поля, без которого невозможно выстраивать государственную политику в области формирования и развития информационного общества. Однако концептуальные рабочие термины не переходят в разряд нормативных правовых, где они должны наполняться праворегулирующим либо правообеспечивающим содержанием»¹.

Как соотносятся между собой понятия «электронное правительство» и «электронное государство»? В российской правовой литературе английский термин E-Government получил несколько переводов. Чаще он переводится как «электронное правительство». Такой пере-

¹ Кузнецов П. У. Социальная миссия электронного государства : ценности и терминологические проблемы // Информационное общество и социальное государство : сб. науч. работ. М., 2011. С. 16—17.

вод допустим, но он сужает понятие, по существу сводя вопрос только к исполнительной власти. Термин «электронное государство» не только больше соответствует английскому эквиваленту, но и подчеркивает, что речь идет о всех трех ветвях власти — законодательной, исполнительной и судебной¹.

Предполагается, что «электронное государство» в своей основе является и конституционным, и правовым, и социальным. При этом пример России, где в силу исторических особенностей поступательное развитие конституционного государства не сложилось, показывает трудность одновременного построения и конституционного, и правового, и социального, и «электронного государства». Отсутствие предшествующего социального опыта и проработанной модели конституционного государства затрудняет и тормозит развитие электронного государства, для которого необходимы не только развитая система ИКТ, но и высокий уровень правового развития. Усложнение социальных отношений (как следствие развития ИКТ) требует их дальнейшей юридизации, однако именно правовая основа электронного государства вырабатывается с наибольшим трудом².

Основой формирования электронного государства является информационное общество — качественно новое состояние элементарных ячеек социума, отдельного государства и человечества в целом, обусловленное развитием информационных технологий, коммуникационных систем, отражающее новый уровень развития научного знания, представляющее собой новый тип организации общества, общества нового века. Народ как субъект демократии в теории электронного государства имеет специфические черты.

Ученые ведут речь о возникновении «народа-избирателя» как единого субъекта демократии, а также о его качественном преобразовании — приобретении свойств диджитальной публики. Диджитальная публика, по мнению С. Московичи, представляет собой рассредоточенную массу избирателей, состоящих из индивидов-избирателей, которые ведут постоянный диалог между собой. Это самоорганизованная система, способная к выработке независимых решений. В.Н. Руденко утверждает, что способность такой публики к взаимодействию

¹ Право на доступ к информации. Доступ к открытой информации / отв. ред. И. Ю. Богдановская. М. : ЗАО «Юстицинформ», 2009. С. 222.

² Там же. С. 225.

вию и самоорганизации есть переход из сообщества «управляемых» к сообществу «управляющих», которое составит альтернативу правительствам и парламентам. Вопросы о том, существует ли информационное общество в России и обладает ли население России свойствами диджитальной публики, являются неоднозначными¹.

В качестве подпрограмм в долгосрочной целевой программе «Информационное общество» на 2011—2020 годы определены: «электронное государство и эффективность госуправления», «российский рынок информационных и телекоммуникационных технологий», «базовая инфраструктура информационного общества», «безопасность в информационном обществе».

Соответственно, субъектами информационного процесса «электронного государства» выступают, с одной стороны — человек, с другой — государственные органы, составляющие «электронное правительство». И государство должно обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения органов государственной власти. Сегодня возможно лишь констатировать недостаточный уровень информированности общества, конкретного человека.

Электронное государство — прежде всего, социальное государство, в свою очередь социальное государство — и эта позиция И.Л. Бачило² вызывает уважение — в определенной части является сервисным государством. При этом нужно иметь в виду, что только сервисные задачи и работа в этом направлении не исчерпывают функций государственных и муниципальных органов в области социальной сферы. Это, пожалуй, конечный итог каждой социальной функции — предоставить условия для граждан и организаций реализовать свои социальные и иные права. Для этого необходимо неуклонное выполнение базовых государственных функций. Конституционной основой социальности Российского государства является глава вторая Конституции РФ о правах и обязанностях человека и гражданина, где содер-

¹ Васькова М. Г. Электронное государство : проблемы правового регулирования // Информационное право. 2009. № 4. С. 23.

² Бачило И. Л. Государство социальное или сервисное? (информационно-правовой аспект) // Право. Журнал высшей школы экономики. 2010. № 1. С. 7.

жится основной перечень социальных прав каждого, находящегося под юрисдикцией России. Социальность государства обеспечивается, прежде всего, федеральными законами, актами Президента и Правительства, деятельностью федеральных и региональных органов исполнительной власти, актами органов местного самоуправления.

В числе проблем первым номером необходимо отметить реализацию федеральными органами исполнительной власти распоряжения Правительства РФ от 2 сентября 2010 г. № 1433-р, которым утвержден план мероприятий, необходимых для реализации Федерального закона «Об организации предоставления государственных и муниципальных услуг». Данным распоряжением предусмотрено принятие более 40 подзаконных нормативных актов, касающихся организации деятельности многофункциональных центров, межведомственного информационного взаимодействия, внедрения универсальных электронных карт.

Вместе с тем до настоящего времени большая их часть остается не принятыми, несмотря на то, что сроки их принятия неоднократно переносились. Отсутствие данных актов лишает возможности органы государственной власти всех регионов обеспечить полноценное решение вопросов реализации Федерального закона «Об организации предоставления государственных и муниципальных услуг» на региональном уровне.

Необходимо отметить, что современная Россия переживает один из наиболее сложных этапов информатизации — процесс адаптации и коренной перестройки государства на пути к его «электронной версии». И в этом процессе далеко не последняя роль должна отводиться полноценному обеспечению прав и свобод человека. Действительно, «во всех подходах к понятию электронного государства прослеживается его негативная черта — ориентация на общеуниверсальное представление о личности и человеке, отсутствие индивидуальных особенностей при совершении каких-либо юридических действий. Развитые информационно-коммуникационные технологии могут явиться мощным инструментом подавления населения и стать предпосылкой возникновения антидемократического режима. Поэтому законодательство становящегося электронного государства должно содержать гарантии пресечения противоправного вмешательства в жизнь и сознание людей в определенных интересах, а также быть го-

тово к информационным изменениям и отражать основные вопросы его функционирования»¹.

Речь идет о развитии в России электронной демократии. Именно сегодня «наряду с тем, что в большинстве сфер деятельности государства происходят позитивные изменения в реализации реформ, развитие информационной организации государства объективно переживает сложный период. В результате информационная сфера, ее ресурсы, в том числе и их защищенность, отстают в развитии от других институтов современного российского общества. Данное обстоятельство негативно сказывается не только на информационной организации государства, но и на состоянии информационной безопасности России, информационной безопасности личности и всего общества в целом»². Не вызывает сомнений, что процесс внедрения инструментов электронной демократии в реалии современной России необратим.

Под *электронной демократией* понимается такая форма организации общественно-политической деятельности граждан, которая обеспечивает за счет широкого применения информационно-коммуникационных технологий качественно новый уровень взаимодействия граждан друг с другом, с органами государственной власти, органами местного самоуправления, общественными организациями и коммерческими структурами.

Безусловно, «самым активным и часто уязвимым субъектом в эпоху перемен, а информатизация, цифровизация и сетевая жизнь информационной среды — это не что иное, как революция в развитии социума, остается человек, индивид, гражданин. И понять, что изменяется под воздействием информационно-технологических факторов чрезвычайно важно»³.

К вопросу о механизмах электронного голосования. Понятие «электронного голосования» отечественный законодатель определил в Федеральном законе от 12 июня 2002 г. № 67-ФЗ «Об основных га-

¹ Васькова М. Г. Электронное государство : проблемы правового регулирования // Информационное право. 2009. № 4. С. 24.

² Мазитов Р. Р. Информационная безопасность Российской Федерации на современном этапе // Российская юстиция. 2009. № 11. С. 4.

³ Бачило И. Л. Правовые вопросы социальных и демократических процессов в информационном обществе России // Информационное общество : проблемы развития законодательства : сб. науч. работ. М., 2012. С. 11.

рантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». Это голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса средств автоматизации ГАС «Выборы». В свою очередь, под электронным бюллетенем понимается бюллетень, подготовленный программно-техническими средствами в электронном виде, применяемый при проведении электронного голосования.

Безусловно, «плюсов» в применяемых технологиях электронного голосования больше, чем достаточно. Тем не менее возможных проблем тоже предостаточно. Так, электронные технологии могут быть использованы и в качестве средств фальсификации результатов голосования; кроме того, не исключены серьезные сбои в функционировании автоматизированных комплексов, обеспечивающих электронное голосование. Поэтому крайне важно в рамках внедрения электронного голосования разрабатывать не только процедуры голосования, подсчета голосов, но и процедуры контроля данных процессов, а также процедуры верификации результатов голосования. И, безусловно, важнейшей проблемой электронного голосования продолжает оставаться проблема цифровой идентификации граждан, являющихся пользователями систем электронной демократии. Во многом данная проблема является главным препятствием на пути повсеместного внедрения механизмов электронного голосования на уровне выборов субъектов государственной и муниципальной власти.

Эта проблема — не только проблема электронного голосования: идентификация гражданина при общении с органами власти — одна из наиболее сложных, требующих своего четкого решения проблема e-government¹.

8.2. Электронное правительство. Вопросы предоставления государственных и муниципальных услуг в электронном виде

Процессы формирования информационного общества и электронного правительства в России динамично развиваются. Информационное общество, т.е. общество, в котором информационные про-

¹ См. об этом: Чеботарева А. А. Человек и электронное государство. Право на информационную безопасность. Чита : ЧитГУ, 2011. С. 27.

цессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития.

Сегодня происходит ценностная переориентация в отношении власти и человека. Если на предшествующих этапах развития отсчет шел от государства к человеку, то теперь обозначился новый подход: истинным моментом становится человек. В этом контексте, информационные права — особый и специфический вид прав человека.¹ В системе этих прав человека электронного государства на одно из ведущих мест выходит право на предоставление государственных и муниципальных услуг в электронной форме.

Федеральный закон «Об организации предоставления государственных и муниципальных услуг»² действительно призван совершить революцию во взаимоотношениях государства и человека.

Правительственное веб-присутствие (согласно классификации Европейской комиссии) характеризуется последовательным прохождением пяти этапов:

1. Информационный (Information) — означает 20%-ное веб-присутствие и предполагает создание регулярно обновляемых правительственных веб-сайтов с публикацией на них основной правительственной информации (нормативные акты, распоряжения, постановления и пр.), ссылок на министерства и государственные департаменты (образования, здравоохранения, финансов и т.п.).

2. Интерактивный односторонний (One way interaction) — предполагает 40%-ное веб-присутствие и заключается в организации пассивного взаимодействия между клиентами и правительством. Он подразумевает, например, предоставление доступа в электронной форме к различным формулярам документов, которые требуются гражданам и бизнесу для взаимодействия с государством. Нужную форму можно распечатать, но отправлять ее придется традиционным образом, а не через Интернет. Или, например, поиск вакансий в госу-

¹ Устинович Е. С. Информационная деятельность как функция федеральных органов исполнительной власти Российской Федерации // Российская юстиция. 2010. № 4. С. 9.

² Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

дарственных организациях на основе заданных пользователем критериев.

3. Интерактивный двусторонний (Two way interaction) — означает 60%-ное веб-присутствие и реализуется посредством интерактивного двустороннего взаимодействия. На этой стадии онлайн-сервисы приобретают интерактивность и появляется возможность запрашивать информацию по тем или иным выступлениям и обсуждениям, обращаться к госчиновникам по электронной почте, участвовать в онлайн-дискуссиях или оставлять комментарии на досках сообщений и т.п.

4. Транзакционный (Transaction) — предполагает 80%-ное веб-присутствие и характеризуется транзакционным взаимодействием, благодаря чему возможно предоставление услуг, выполнимых в онлайн на всех стадиях. Примером может служить подача заявок в электронной форме на получение лицензий на ведение профессиональной деятельности, подача налоговых деклараций, заявлений на обмен документов и т.п.

5. Проактивный (Targetisation) — означает 100%-ное веб-присутствие и отличается тем, что правительство не только предоставляет гражданам и коммерческим структурам сервисные услуги, но и привлекает граждан к принятию решений и двустороннему диалогу на базе интерактивных сервисов.

Проанализировав данную классификацию, можно утверждать, что сегодня для России характерен переход от первого, информационного этапа, ко второму, интерактивному одностороннему. Согласно Федеральному закону «Об организации предоставления государственных и муниципальных услуг» сформирована основа для четвертого, транзакционного этапа правительственного вэб-присутствия.

Предлагая электронные услуги, государство должно сделать доступным онлайн-публичный сектор информации, чтобы большая часть административных процедур (оптимально — все) была доступна электронным способом. Государство обязано обеспечить универсальные услуги. Сеть «Интернет» должна быть доступна всем гражданам, включена в универсальные услуги и предлагаться пользователю по допустимой цене.

Федеральный закон «Об организации предоставления государственных и муниципальных услуг» предусматривает, что все органы

государственной власти — федеральные, региональные и муниципальные, а также государственные внебюджетные фонды — должны дать гражданам возможность получить ту или иную услугу в электронной форме. Так называемые «онлайн-транзакции» — обеспечивают предоставление услуг государственных и муниципальных учреждений через Интернет — оплату коммунальных платежей, заполнение налоговых деклараций и сбор налогов, регистрацию общественных объединений, а в перспективе — предпринимателей без образования юридического лица, предприятий малого бизнеса и др. На этой стадии формируется «информационная экономика», которая представляет собой новую ступень с точки зрения экономического эффекта, получаемого в результате постоянного интерактивного функционирования государственных порталов¹.

Законом предусмотрено также, что орган власти может делегировать предоставление государственных и муниципальных услуг так называемым многофункциональным центрам (МФЦ). Сегодня во многих городах России такие многофункциональные центры созданы и функционируют. Согласно ст. 15 Федерального закона предоставление государственных и муниципальных услуг в многофункциональных центрах осуществляется по принципу «одного окна». Это означает, что предоставление государственной или муниципальной услуги осуществляется после однократного обращения заявителя с соответствующим запросом, а взаимодействие с органами, предоставляющими государственные услуги, или органами, предоставляющими муниципальные услуги, осуществляется многофункциональным центром без участия заявителя в соответствии с нормативными правовыми актами и соглашением о взаимодействии, т.е. заявитель должен обратиться туда с запросом всего один раз. И даже если для получения запрошенной услуги требуются, условно говоря, несколько дополнительных справок из разных органов власти, то многофункциональный центр должен сделать все дополнительные запросы сам и выдать заявителю готовую информацию.

Многофункциональные центры в соответствии с соглашениями о взаимодействии осуществляют:

¹ Василенко Л. А. Интернет в информатизации государственной службы России. М. : РАГС, 2000. С. 24.

1) прием запросов заявителей о предоставлении государственных или муниципальных услуг;

2) представление интересов заявителей при взаимодействии с органами, предоставляющими государственные услуги, и органами, предоставляющими муниципальные услуги, а также с организациями, участвующими в предоставлении предусмотренных государственных и муниципальных услуг;

3) представление интересов органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, при взаимодействии с заявителями;

4) информирование заявителей о порядке предоставления государственных и муниципальных услуг в многофункциональных центрах, о ходе выполнения запросов о предоставлении государственных и муниципальных услуг, а также по иным вопросам, связанным с предоставлением государственных и муниципальных услуг;

5) взаимодействие с государственными органами и органами местного самоуправления по вопросам предоставления государственных и муниципальных услуг, а также с организациями, участвующими в предоставлении государственных и муниципальных услуг;

6) выдачу заявителям документов органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, по результатам предоставления государственных и муниципальных услуг, если иное не предусмотрено законодательством РФ;

7) прием, обработку информации из информационных систем органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, и выдачу заявителям на основании такой информации документов, если это предусмотрено соглашением о взаимодействии и иное не предусмотрено федеральным законом;

8) иные функции, указанные в соглашении о взаимодействии. Создан единый портал государственных и муниципальных услуг — государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием сети Интернет и размещенным в государственных и

муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг.

Законом предусмотрено право органов государственной власти субъектов РФ создавать региональные порталы государственных и муниципальных услуг, являющиеся государственными информационными системами субъектов РФ, обеспечивающими предоставление государственных услуг субъектов РФ и муниципальных услуг.

Единый портал государственных и муниципальных услуг призван обеспечить:

1) доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием сети Интернет и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров соответственно государственных и муниципальных услуг;

2) доступность для копирования и заполнения в электронной форме запроса и иных документов, необходимых для получения государственной или муниципальной услуги;

3) возможность подачи заявителем с использованием информационно-телекоммуникационных технологий запроса о предоставлении государственной или муниципальной услуги и иных документов, необходимых для получения государственной или муниципальной услуги;

4) возможность получения заявителем сведений о ходе выполнения запроса о предоставлении государственной или муниципальной услуги либо услуги;

5) возможность получения заявителем с использованием информационно-телекоммуникационных технологий результатов предоставления государственной или муниципальной услуги, за исключением случаев, когда такое получение запрещено федеральным законом;

6) возможность уплаты заявителем государственной пошлины за предоставление государственных и муниципальных услуг, осуществления заявителем платы за предоставление государственных и муниципальных услуг и услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, дистанционно в электронной форме.

Со временем через Интернет можно будет не только сделать запрос госуслуги, но и оплатить ее дистанционно в электронной форме. Для этого вводится в оборот универсальная электронная карта.

Эта пластиковая карта будет содержать в визуальной и электронной формах информацию о пользователе картой и позволит с ее помощью получать самые разные государственные и другие услуги. В том числе финансовые, медицинские, транспортные услуги.

Согласно ст. 22 Федерального закона «Об организации предоставления государственных и муниципальных услуг» универсальная электронная карта представляет собой материальный носитель, содержащий зафиксированную на нем в визуальной (графической) и электронной (машиночитываемой) формах информацию о пользователе картой и обеспечивающий доступ к информации о пользователе картой, используемой для удостоверения прав пользователя картой на получение государственных и муниципальных услуг, а также иных услуг, оказание которых осуществляется с учетом положений закона, в том числе для совершения в случаях, предусмотренных законодательством РФ, юридически значимых действий в электронной форме.

Пользователем универсальной электронной картой может быть гражданин Российской Федерации, а также в случаях, предусмотренных федеральными законами, иностранный гражданин либо лицо без гражданства.

Имея универсальную электронную карту и несколько электронных приложений к ней, гражданин сможет запросить, получить и оплатить ею все мыслимые услуги. В частности, федеральное электронное приложение обеспечит получение государственных услуг и услуг иных организаций на всей территории страны, региональное приложение даст возможность воспользоваться государственными услугами, предоставляемыми региональной властью, и т.д.

Под электронным приложением универсальной электронной карты понимается уникальная последовательность символов, записанная на электронном носителе универсальной электронной карты и предназначенная для авторизованного доступа пользователя такой картой к получению финансовой, транспортной или иной услуги, в том числе государственной или муниципальной услуги. Универсальная электронная карта может иметь несколько независимо функционирующих электронных приложений. Законом предусматриваются

федеральные электронные приложения, региональные электронные приложения и муниципальные электронные приложения. Также предусматривается функционирование электронного банковского приложения. Банк, осуществивший подключение электронного банковского приложения, обеспечивает функционирование электронного банковского приложения в соответствии с законодательством о банках и банковской деятельности.

Переход на предоставление государственных и муниципальных услуг в электронной форме соответственно федеральными органами исполнительной власти, исполнительными органами государственной власти субъектов РФ, органами местного самоуправления, организациями, участвующими в предоставлении государственных и муниципальных услуг, планируется поэтапным в соответствии с планами-графиками перехода на предоставление государственных и муниципальных услуг в электронной форме, утверждаемыми Правительством РФ, высшим исполнительным органом государственной власти субъекта РФ, органом местного самоуправления.

8.3. Электронное правосудие как форма реализации судебной власти в электронном государстве

В числе приоритетных направлений развития электронной России — вопросы построения электронного правосудия. В числе решаемых сегодня задач — вопросы реализации Федеральной целевой программы «Развитие судебной системы России на 2013—2020 гг.», утвержденной постановлением Правительства РФ от 27 декабря 2012 г. № 1406, проблемы реализации вступившего в силу с 1 июля 2010 г. Федерального закона от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Основополагающими целями судебной реформы были определены: доступность правосудия, быстрое и качественное рассмотрение дел, максимальное исключение какого-либо воздействия на судей извне.

На современном этапе развития науки и техники особое значение приобретает интеграция информационных технологий в те сферы жизни, от которых напрямую зависит стабильное существование об-

щества и его граждан. Если говорить о праве как об основном социальном регуляторе, то внедрение технологий, позволяющих наиболее эффективно кодифицировать, анализировать, применять и исполнять правовые нормы, является необходимым условием совершенствования правовой системы как в России, так и за рубежом.

Сущность концепции электронного правосудия заключается в осуществлении судами РФ своей деятельности в рамках электронного документооборота с использованием электронных банков данных.

Нельзя не согласиться с утверждением: «открытость суда общественному наблюдению и контролю является условием справедливости процесса. Если суд выступает как элемент гражданского общества, призванный служить пространством диалога на языке права между государством и личностью, он, по определению, открыт общественному контролю и заинтересован в информировании народа о своей деятельности»¹. Как правильно утверждал русский правовед П.И. Люблинский: «Суд есть явление, связанное только с правом»².

Мало того чтобы правосудие свершилось, люди должны быть уверены, что это произошло в действительности. Поэтому информационная открытость судов является гарантией провозглашенной в ст. 19 Международного пакта, ст. 10 Европейской конвенции свободы каждого «получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей»³.

Судопроизводство в России широко начало использовать современные достижения информационных технологий во всех органах судебной власти в субъектах РФ, включая и мировую юстицию. Сегодня актуальны вопросы обеспечения информационной открытости деятельности судов, проблемы организации работы сайтов судов, публикации судебных актов в системе Интернет, технологии аудио-записи, технологии применения видеоконференцсвязи, вопросы автоматизации систем судебного делопроизводства, проблемы электронного документооборота, применяемого в судах, подача исковых заявлений и жалоб в электронной форме.

¹ Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М. : ЗАО «Юстицинформ», 2009. С. 265.

² Люблинский П.И. Суд и права личности // Судебная реформа. Т. 2. М., 1915. С. 1.

³ Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. М. : ЗАО «Юстицинформ», 2009. С. 267.

Федеральные целевые программы «Развитие судебной системы России» положили начало рождению Государственной автоматизированной системы «Правосудие» (ГАС «Правосудие»), создание которой началось в 2004 г.

Государственная автоматизированная система (ГАС) «Правосудие» — это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и управлений (отделов) Судебного департамента при Верховном суде РФ.

Еще одним из элементов «электронного правосудия» является использование систем видеоконференцсвязи, предоставляющей участникам процесса возможность дистанционного участия в судебном заседании. Система видеоконференцсвязи в практике судов применяется уже достаточно широко, причем сегодня эта система начнет работать и в гражданском процессе. Федеральным законом от 26 апреля 13 № 66-ФЗ установлены особенности и порядок применения систем видеоконференцсвязи в гражданском процессе.

Беспристрастному и объективному освещению деятельности судов, а также формированию положительного отношения к правосудию, поддержанию авторитета судебной власти способствует также создание и поддержание судами собственных Интернет-сайтов.

Сегодня для судопроизводства актуальны как никогда: открытость и доступность; формирование информационных ресурсов, включая ход судебных заседаний; организация оперативного доступа к информационным ресурсам в рамках формирования единого информационного пространства арбитражных судов, федеральных судов общей юрисдикции и мировых судей; реализация новых требований судебного законодательства; оперативная организация мониторингов и аналитической работы на больших массивах консолидированной информации от всех участников информационного пространства.

Согласимся, что государство, внедряя информационные технологии в арбитражный процесс, а в перспективе и в гражданское судопроизводство, реализуя модели электронного правосудия в целом, должно ставить в качестве стратегической задачи изменение взаимоотношений между государством и обществом, между судом как ветвью государственной власти и остальными гражданами. Все это тре-

бует глубокого теоретического исследования проблемы внедрения электронных технологий в гражданское и арбитражное судопроизводство для выработки научных рекомендаций по совершенствованию процессуального законодательства, по повышению эффективности правоприменительной практики¹.

Как справедливо полагает И.А. Приходько, «идея правого и справедливого суда является одной из немногих, объединяющих все слои общества»². Высокий профессионализм, независимость, беспристрастность, справедливость, законность, открытость, доступность, эффективность, легитимность — это те требования, которые предъявляются к системе правосудия со стороны гражданского общества.

Назначение и современные возможности сервисов и систем электронного правосудия в судах, без сомнения, будут расширяться.

Вопросы и задания для самоконтроля

1. В чем особенности формирующегося электронного государства? Назовите основные нормативные акты, направленные на развитие основ электронного государства.

2. Дайте характеристику проекту Концепции развития в Российской Федерации механизмов электронной демократии до 2020 г.

3. Охарактеризуйте порядок предоставления государственных и муниципальных услуг в электронном виде.

4. В чем состоит назначение многофункциональных центров?

5. Каковы основные направления развития электронного правосудия в России?

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

¹ Решетняк В. И. К вопросу об электронном правосудии в арбитражном и гражданском судопроизводстве // <http://justicemaker.ru/>

² Приходько И. А. Доступность правосудия в арбитражном и гражданском процессе. СПб., 2005. С. 9.

«Стратегия развития информационного общества в Российской Федерации» : утв. Президентом РФ 7 февраля 2008 г. № Пр-212.

Указ Президента РФ от 30 июня 2012 г. № 918 «Об Управлении Президента Российской Федерации по применению информационных технологий и развитию электронной демократии».

Постановление Правительства РФ от 7 июля 2011 г. № 553 «О порядке оформления и представления заявлений и иных документов, необходимых для предоставления государственных и (или) муниципальных услуг, в форме электронных документов».

Постановление Правительства РФ от 22 декабря 2012 г. № 1376 «Об утверждении правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг».

Постановление Правительства РФ от 25 апреля 2011 г. № 321 «Об утверждении Правил выпуска универсальной электронной карты».

Постановление Правительства РФ от 24 апреля 2011 г. № 208 «О технических требованиях к универсальной электронной карте и федеральным электронным приложениям».

Постановление Правительства РФ от 3 октября 2009 г. № 796 «О некоторых мерах по повышению качества предоставления государственных (муниципальных) услуг на базе многофункциональных центров предоставления государственных (муниципальных) услуг».

Распоряжение Правительства РФ от 20 октября 2010 № 1815-р «Государственная программа «Информационное общество (2011-2020 годы)» // СЗ РФ. 2010. № 46. — Ст. 6026.

Распоряжение Правительства РФ от 2 сентября 2010 г. № 1433-р «О плане мероприятий, необходимых для реализации Федерального закона “Об организации предоставления государственных и муниципальных услуг”».

Распоряжение Правительства РФ от 31 апреля 2011 г. № 539-р «Об определении ОАО “Универсальная электронная карта” эмитентом федерального электронного приложения».

Глава 9. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ИНСТИТУТ ИНФОРМАЦИОННОГО ПРАВА

Понятие персональных данных. Содержание понятия «обработка персональных данных». Понятие оператора обработки персональных данных. Принципы защиты персональных данных. Особенности обработки специальных категорий персональных данных. Права субъекта персональных данных. Обязанности оператора при обработке персональных данных.

9.1. Основные подходы к регулированию правоотношений по поводу персональных данных в зарубежных странах

Защита персональных данных — условный термин, применяемый для обозначения права индивида на доступ к своему персональному досье, имеющемуся в распоряжении государственных или частных «пользователей информации», с целью обеспечения точности, своевременности и соотносимое имеющейся информации с целями, для которых она хранится, и проверки того, не может ли получить доступ к информации лицо, не обладающее соответствующими полномочиями. Таким образом, защита персональных данных связана также с личным характером информации.

В 60-х и 70-х гг. XX в. с приходом информационных технологий стал возрастать интерес к приватности. Возможность использования мощных компьютеров для слежки и контроля означала необходимость принятия особых правил, регулирующих сбор и обработку персональных данных. Во многих странах новые конституции отразили, это право. Процесс обновления законодательства в данной области можно проследить со времени появления первого закона о защите данных, изданного в Германии в земле Гессен в 1970 г. После этого были приняты законы в Швеции (1973), Соединенных Штатах (1974), Германии (1977) и Франции (1978).

Из этих законов «выросли» два важных международных документа. Первый — Конвенция Совета Европы о защите прав личности в связи с автоматической обработкой персональных данных. Второй — Руководящие принципы Организации по экономическому сотрудничеству и развитию о защите приватности в связи с трансграничной передачей персональных данных. Эти положения определяют персо-

нальную информацию как данные, которые нуждаются в защите на каждом этапе от сбора до хранения и распространения. Право граждан на доступ к своим данным и внесение в них изменений стало главной составляющей этих правил.

В разных законах и правилах по-разному определяются условия защиты данных. Повсеместно принято считать, что персональная информация должна быть:

- получена честным и законным путем;
- использована только для заранее определенных целей;
- соответствовать задаче, ради которой она собиралась;
- точной и свежей;
- обрабатываться только с согласия субъектов ее получения;
- доступна субъекту данных;
- защищена от несанкционированного доступа;
- уничтожена после того, как цель достигнута.

Два упомянутых соглашения сильно повлияли на развитие законодательства во всем мире. Почти 30 стран признали Конвенцию Совета Европы и еще несколько государств собираются сделать это в ближайшем будущем. Руководящие принципы Организации по экономическому сотрудничеству и развитию также широко используются законодателями разных стран, в том числе и не входящих в эту международную структуру.

Мировой опыт позволяет назвать три главные причины для принятия специальных законов о защите приватности и персональных данных:

1) приведение законодательства значительного числа стран к общемировым цивилизованным стандартам, отражающим высокий уровень защиты прав человека. Многие государства, особенно в Центральной и Восточной Европе (включая Россию), Южной Африке и Южной Америке, приняли соответствующие законы, чтобы исправить последствия нарушений прав человека при тоталитарных режимах прошлых лет;

2) создание благоприятных условий для развития электронного бизнеса. Многие страны, особенно в Азии, уже приняли (или разрабатывают) законы, направленные на развитие электронной коммерции. Правительства понимают, что в современном мире, насыщенном высокотехнологичными коммуникациями, персональные данные потре-

бителей находятся под угрозой — особенно когда они пересылаются по Интернету. Поэтому в законах об электронном бизнесе появляются гарантии приватности;

3) приведение национального законодательства в соответствие с европейскими соглашениями. Большинство стран Центральной и Восточной Европы принимает законы, основываясь на Конвенции Совета Европы 1981 г. и Директиве Европейского Союза о защите данных. Многие из этих стран в ближайшем будущем надеются стать членами ЕС. В других регионах мира государства приводят свои законы в соответствие требованиям ЕС просто потому, что иначе могут пострадать их торговые отношения с членами Евросоюза.

В имеющих сейчас базовое значение документах, регулирующих работу с персональными данными в мире, сформулированы основные принципы работы с персональными данными:

- персональные данные должны собираться и обрабатываться (храниться, использоваться, раскрываться, стираться и т.д.) только в соответствии с законом и наделенными соответствующими полномочиями органами;

- персональные данные должны быть адекватными заранее определенным целям и распоряжение ими должно ограничиваться по срокам, соответствующим указанным целям;

- персональные данные должны быть точны;

- персональные данные должны обрабатываться только с согласия субъектов этих данных;

- персональные данные должны быть доступны субъектам этих данных, в том числе и для внесения уточнения в эти данные;

- персональные данные должны быть должным образом защищены.

В международном праве существует большое число законов, отраслевых стандартов для финансовых институтов, телекоммуникационных компаний, учреждений здравоохранения и обязательных и рекомендательных документов, затрагивающих защиту информации от внутренних угроз и управление операционными рисками:

Стандарт Банка России СТО БР ИББС-1.0-2008 — стандарт для российских банков, исполнение положений которого пока носит рекомендательный характер. В стандарте в частности затронута необходимость защиты от действий инсайдеров, в том числе необходи-

мость контроля использования Интернета и корпоративной почты, а также ведения архива электронной почты.

Кодекс корпоративного поведения ФСФР России — свод правил и рекомендации ФСФР России для компаний — участников рынков ценных бумаг России. Основная цель Кодекса — обеспечение равенства прав акционеров и защита их интересов, а одна из важнейших глав кодекса — контроль финансово-хозяйственной деятельностью общества. В Кодексе корпоративного поведения регламентируется создание прозрачной системы менеджмента и построение системы управления операционными рисками, а также необходимость создания условия для независимой оценки любой финансово-хозяйственной операции.

PCI DSS — обязательный стандарт для операторов данных платежных карт систем VISA, MasterCard, American Express, JCB, Discover. Во-первых, в стандарте регламентируется необходимость шифрования носителей информации, содержащих данные платежных карт, и надежной защиты ключей шифрования. Также в PCI DSS определена необходимость генерации стойкого ключа и разделение криптографического ключа между несколькими лицами. Во-вторых, согласно стандарту операторы платежных карт должны защищать информацию от утечек по различным каналам, жестко регламентировав использование внешних устройств и перемещение конфиденциальных данных. В-третьих, в PCI DSS определена необходимость использования двухфакторной аутентификации для доступа к данным.

Basel II — довольно давно и успешно применяющийся в Евросоюзе, Северной Америке и Японии нормативный акт, регламентирующий банковскую деятельность. В частности в стандарте описана необходимость ведения архива конфиденциальной информации и создания системы управления операционными рисками.

SOX — Sarbanes-Oxley Act of 2002 является обязательным для всех публичных компаний, акции которых котируются на фондовых биржах США. За несоблюдение закона топ-менеджеры компании несут персональную финансовую (штраф до 25 млн долларов) и уголовную ответственность (до 20 лет лишения свободы). Секция 404 закона регламентирует необходимость внедрения системы внутреннего контроля для предотвращения и защиты информационных активов компании от утечек и несанкционированного использования.

SEC Rule 17a-4 и NASD 3010/3110 — своды правил для компаний, акции которых котируются на биржах США. В правилах регламентируется создание архива электронной корреспонденции и переписки через службы мгновенных сообщений. Требования NASD 3010/3110 еще более жесткие — требуется архивировать не только корреспонденцию участников системы, но и все транзакции брокеров, трейдеров и лиц, действующих от их имени.

Combined code on corporate governance — Кодекс корпоративного управления Великобритании пока не является обязательным для всех организаций, однако уже давно де-факто является стандартом для корпораций, чьи акции представлены на Лондонской фондовой бирже. Combined code регламентирует создание и поддержку системы внутреннего контроля и необходимость как минимум один раз в год проводить независимый аудит такой системы. Также в Кодексе говорится о необходимости постоянного мониторинга самой системы внутреннего контроля, а в случае возникновения какого-либо инцидента ИБ, высшее руководство компании должно быть немедленно информировано.

Американский закон HIPAA — затрагивает учреждения здравоохранения, страховые компании и посредников, хранящих, обрабатывающих и передающих конфиденциальные данные. Закон конкретизирует правила HIPAA, The Security Rule, в которых в частности регламентируется необходимость создания системы внутреннего контроля, написания правил использования рабочих компьютеров и внешних устройств и организации системы контроля доступа к информации.

GBLA & FACTA — защита непубличной информации клиентов финансовых корпораций регламентируется законами Gramm-Leach-Bliley Act of 1999 и Fair and Accurate Credit Transactions Act of 2003. Стандарт «Interagency Guidelines Establishing Information Security Standards» вносит дополнительные уточнения в приведенные законы и требует от финансовых институтов США защищать непубличные данные граждан в процессе хранения, использования, пересылки и утилизации от всех прогнозируемых рисков информационной безопасности, а также обеспечивать надежный контроль доступа к этой информации.

Архивирование информации (*data retain*) является распространенным требованием многих стандартов и законов, касающихся информационной безопасности. Сохранение переписки сотрудников, отправленных через Интернет данных, записанных на периферийные устройства файлов и копий распечатанных на принтерах документов является важной задачей как с точки зрения внутреннего контроля и управления операционными рисками, так и как самостоятельная задача. Очевидно, что часто для различных целей требуется провести ретроспективный анализ использованной и перемещенной за пределы корпоративной сети информации.

Несоблюдение требований архивирования информации в большинстве нормативных документов в большинстве случаев является прямым нарушением законодательства страны, за что предусматриваются солидные штрафы для компаний, а топ-менеджмент несет персональную уголовную и финансовую ответственность. Часто из-за невозможности предоставить электронные копии документов в суд компании проигрывают процессы и теряют огромные суммы. Одним из наиболее известных дел, показывающих необходимость архивирования информации, является процесс с участием Morgan Stanley. Первоначально присяжные приняли решение о взыскании с компании Morgan Stanley 1,5 млрд долларов за невозможность предоставления копий электронных писем, затребованных адвокатами другой стороны. Позже эта цифра была сокращена в сто раз и составила 15 млн. долл.

9.2. Федеральный закон «О персональных данных» — основа действующего законодательства в сфере защиты персональных данных

Федеральный закон «О персональных данных», претерпевший множество редакций, регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или

без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Согласно ст. 3 Закона под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

В свою очередь, под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка персональных данных включает:

- их распространение, предоставление, доступ;
- блокирование;
- уничтожение;
- обезличивание.

Распространение персональных данных — это действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных — это действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Под блокированием понимается временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных), а под их уничтожением — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — это действия, в результате которых становится невозможным без использования

дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Организует и (или) осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными оператор (государственный орган, муниципальный орган, юридическое или физическое лицо). При этом оператор обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Законом определены основополагающие принципы обработки персональных данных:

1) обработка персональных данных должна осуществляться на законной и справедливой основе;

2) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

3) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4) обработке подлежат только персональные данные, которые отвечают целям их обработки;

5) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

6) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

7) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект

персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Следует отметить, что принятию этого закона предшествовала ратификация Российской Федерацией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных¹.

В законе подчеркнуто:

1) Российская Федерация заявляет, что не будет применять Конвенцию к персональным данным:

¹ Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

а) обрабатываемым физическими лицами исключительно для личных и семейных нужд;

б) отнесенным к государственной тайне в порядке, установленном законодательством РФ о государственной тайне;

2) Российская Федерация заявляет, что ... будет применять Конвенцию к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации;

3) Российская Федерация заявляет, что ... оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Согласно Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации¹ обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Также следует отметить, что согласно Указу Президента РФ от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» руководителям государственных органов предписано:

— обеспечить защиту персональных данных государственных гражданских служащих Российской Федерации, содержащихся в их

¹ Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

личных делах, от неправомерного их использования или утраты за счет средств государственных органов в порядке, установленном федеральными законами;

— определить лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных государственных гражданских служащих Российской Федерации в государственном органе и несущих ответственность в соответствии с законодательством РФ за нарушение режима защиты этих персональных данных.

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации установлены постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные (далее — оператор), или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных

или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со ст. 8 Федерального закона «О персональных данных».

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)¹.

Вопросы и задания для самоконтроля

1. Раскройте понятия «персональные данные», «обработка персональных данных», «оператор обработки персональных данных».

¹ Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

2. Охарактеризуйте законодательство в сфере защиты персональных данных.
3. Назовите и раскройте принципы защиты персональных данных.
4. Раскройте особенности обработки специальных категорий персональных данных, а также биометрических персональных данных.
5. Какими правами обладает субъект персональных данных?
6. В чем состоят обязанности оператора при обработке персональных данных?

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

Указ Президента РФ от 29 декабря 2012 г. № 1709 «О паспорте гражданина Российской Федерации, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем на электронном носителе информации дополнительные биометрические персональные данные его владельца».

Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

Глава 10. ЗНАЧЕНИЕ И ПРОБЛЕМАТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность государства. Информационная безопасность человека и общества. Основные подходы к решению проблем информационной безопасности на современном этапе развития «Электронной России».

10.1. Подходы к определению понятия «информационная безопасность». Задачи и гарантии обеспечения информационной безопасности

Понятие «информационной безопасности» сегодня — одно из базовых понятий информационного права. Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития. А значит, актуально все, что связано с понятием безопасности в информационном обществе и в условиях формирования электронного правительства.

Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько основных этапов¹:

1 этап — до 1816 г. — характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

2 этап — начиная с 1816 г. — связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а имен-

¹ Безопасность информационных технологий. Системный подход : учеб. пособие. К. : ООО ТИД Диа Софт, 2004. С. 23.

но применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

3 этап — начиная с 1935 г. — связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на приемные устройства маскирующими и пассивными имитирующими радиоэлектронными помехами.

4 этап — начиная с 1946 г. — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

5 этап — начиная с 1965 г. — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединенных в локальную сеть путем администрирования и управления доступом к сетевым ресурсам.

6 этап — начиная с 1973 г. — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Для ее обеспечения в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

7 этап — начиная с 1985 г. — связан с созданием и развитием информационно-коммуникационных сетей с использованием космических средств обеспечения. Данный этап продолжается и по сегодняшний день. Характеризуется широким использованием сверхмо-

бильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов¹.

Понятие безопасности является очень широким и сужается в зависимости от контекста. Существует безопасность государства, личности, предприятия, общества в целом, а также пожарная безопасность, промышленная безопасность, радиационная и так далее — все они формируют общую систему национальной безопасности государства. В общем, под безопасностью следует понимать отсутствие недопустимого риска, связанного с возможностью нанесения ущерба. Национальная безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Центральным направлением в обеспечении национальной безопасности является формирование безопасной среды для реализации прав и свобод человека и гражданина².

Национальная безопасность включает в себя: государственную безопасность, общественную, техногенную, экологическую и защиту от угроз стихийных бедствий, экономическую безопасность, энергетическую, информационную, безопасность личности³.

Информационная безопасность является неотъемлемой частью национальной безопасности. Это связано с тем, что информация во все времена играла ключевую роль в обеспечении стабильности и безопасности любого государства. В свете бурного развития информационных технологий информационный ресурс превратился в важнейший актив государства, который нуждается в надежной защите.

В этой связи взаимосвязаны термины «информационная безопасность» и «защита информации».

¹ Информационная безопасность России : человек, общество, государство / В. Н. Лопатин. СПб. : Фонд Университет, 2000. С. 19.

² Правовые основы обеспечения национальной безопасности : учеб. пособие / В. Д. Самойлов. М. : МИЭМП, 2008. С. 37.

³ См.: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности¹. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

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

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации².

Под защитой информации может подразумеваться:

- программно-аппаратная защита (установка антивирусного программного обеспечения, межсетевых экранов, аппаратных модулей защиты);

- техническая защита информации;

- инженерная защита информации (создание инженерных и коммуникационных средств защиты);

- правовая защита информации;

- криптографическая защита информации;

- организационная защита информации³.

Данные способы защиты информации представляют собой комплексную деятельность организации, направленную на сохранение информационных ресурсов, представляющих ценность для организации.

Под информационной безопасностью в широком смысле понимается деятельность, направленная на обеспечение защищенного состояния объекта. В качестве такого объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизиро-

¹ Информационная безопасность : учеб. пособие / У. М. Шереметьева. Томск : Изд-во ТГПУ, 2009. С. 8.

² См.: Федеральный закон «Об информации, информационных технологиях и о защите информации».

³ Информационная безопасность : учеб. пособие. Ч. 1 / А. М. Блинов. СПб. : Изд-во СПбГУЭФ, 2010. С. 20.

ванная система, информационная система предприятия, общества, государства¹.

В учебном пособии У.М. Шереметьева дается такое определение информационной безопасности — защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры².

Необходимость защиты информации сформировалась под влиянием угроз информационной безопасности. В результате возникновения таких угроз возникает проблема эффективного обеспечения информационной безопасности, для создания которой требуется создание развитого методологического базиса, позволяющего решить следующие комплексные задачи:

- создать систему органов, ответственных за безопасность информации;

- разработать теоретико-методологические основы обеспечения безопасности информации;

- решить проблему управления защитой информации и ее автоматизации;

- создать нормативно-правовую базу, регламентирующую решение всех задач обеспечения безопасности информации;

- наладить производство средств защиты информации;

- организовать подготовку специалистов по защите информации;

- подготовить нормативно-методическую базу для проведения работ по обеспечению информационными технологиями³.

Стандартная модель безопасности, в том числе информационной, состоит в обеспечении доступности, целостности и конфиденци-

¹ См.: Википедия (Электронный ресурс): свободная интернет-энциклопедия. М.: WIKIPEDIA.RU, 2001—2012. Режим доступа: World Wide Web. URL: <http://ru.wikipedia.org>.

² Информационная безопасность : учеб. пособие / У. М. Шереметьева. Томск : Изд-во ТГПУ, 2009. С. 8.

³ Безопасность информационных технологий. Системный подход : учеб. пособие / В. В. Домарев. К. : ООО ТИД Диа Софт, 2004. С. 50.

альности информационных ресурсов и поддерживающей инфраструктуры¹. Это три важнейших базовых принципа, которые должны обеспечивать информационную безопасность.

Доступность информационных ресурсов является важнейшим элементом информационной безопасности и представляет собой гарантию получения требуемой информации или информационной услуги пользователем за определенное время. Информационные системы создаются и приобретаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это наносит ущерб всем субъектам информационных отношений.

Целостность подразумевает собой актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность — это гарантия доступности конкретной информации только кругу лиц, для которых она предназначена.

При обеспечении информационной безопасности участники информационных систем должны стремиться к реализации именно данных понятий, так как они составляют основу защиты информации².

В современной отечественной науке определение актуальных проблем информационной безопасности стало предметом комплексных исследований, проведенных И.А. Лазаревым, В.Н. Лопатиным, Ю.С. Уфимцевым, Е.А. Ерофеевым и др.

В последующем проблемы обеспечения информационной безопасности нашли отражение в трудах Б.В. Вербенко, А.А. Николаева, Э.М. Брандмана, Т.А. Поляковой и многих других.

Появление и научное закрепление дефиниции «информационная безопасность» непосредственно связано с осмыслением феномена информатизации и изучением содержания процесса формирования информационного общества. Данной проблеме посвящены работы зарубежных теоретиков Д. Белла, Э. Тоффлера, Т. Стоуньера, А. Турена, У. Дайзарда, М. Кастельса, К. Кояма, Е. Масуда.

¹ Информационная безопасность : конспект лекций / У. М. Шереметьева. Томск : Издательство ТГПУ, 2009. С. 87.

² Информационная безопасность: учеб. пособие. Ч. 1 / А. М. Блинов. СПб : Изд-во СПбГУЭФ, 2010. С. 15.

Представляет интерес вопрос анализа, наряду с правовым аспектом, подходов философов, политологов, социологов, исследователей технических наук к определению понятия «информационная безопасность». Остановимся на некоторых из них.

Подход философов¹ основывается на выделении трех составляющих информационной безопасности:

- удовлетворение информационных потребностей субъектов;
- обеспечение безопасности информации;
- обеспечение защиты субъектов.

Таким образом, в сущностном плане информационная безопасность, согласно философскому подходу, есть такое состояние объекта, при котором состояние информационной среды, в которой он находится, позволяет ему сохранять способность и возможность принимать и реализовывать решения сообразно своим целям, направленным на прогрессивное развитие. Это означает, что информационная безопасность может достигаться как в результате проведения мероприятий, направленных на поддержание информационной среды в безопасном для объекта состоянии, защиту объекта от деструктивного воздействия, так и путем укрепления иммунитета и развития способности объекта уклоняться от деструктивного информационного воздействия (в том числе за счет предвидения их возможности).

Следовательно, задача обеспечения информационной безопасности государства состоит в том, чтобы создать такие условия функционирования информационной инфраструктуры (главным элементом которой является не компьютер, а человек), при которых отдельные граждане, коллективы, органы власти могли бы принимать управленческие решения и добиваться их реализации сообразно целям, направленным на прогрессивное развитие всего общества.

Политический анализ проблематики информационной безопасности — сегодня один из наиболее активных и указывает, прежде всего, на растущую необходимость объединения усилий частного сектора, политических институтов и правоохранительных структур, экспертно-аналитических сообществ в поиске способов противостоя-

¹ Атаманов Г. А. Информационная безопасность : сущность и содержание // Бизнес и безопасность в России. 2007. № 47. С. 108.

ния многообразным угрозам в данной области. Политологами, в частности, высказывается мнение¹, согласно которому Россия всё ещё стоит на перепутье, и задача государственной политики в области безопасности РФ состоит не только в том, чтобы защитить граждан и общество от этих угроз, но и реализовать эту политику в таких формах и методах, которые, в свою очередь, не поставили бы под угрозу выбранный демократический вектор развития. Адекватная запросам времени политика в области безопасности должна опираться на приоритеты взаимовыгодного сотрудничества и развития гражданской инициативы при руководящей и направляющей роли государства. Сегодня сложились все предпосылки к тому, чтобы стратегии социального партнерства и гражданского участия заняли достойное место в процессах выработки и реализации комплексной политики информационной безопасности.

Характерной чертой политической науки стало признание необходимости привлечения к обеспечению информационной безопасности не только институтов федеральной государственной власти, но и структур государственного управления субъектов РФ².

Технический подход основывается, прежде всего, на проблеме разработки требований безопасности сайтов, включающих защиту серверов, лицензирование, сертификацию и аттестацию объектов информатизации, применение криптографических механизмов при передаче данных по каналам связи, использование методов идентификации и аутентификации пользователей на сайте³. Кроме того, подчеркивается, что системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные

¹ Ковалева Е. В. Обеспечение прозрачности органов местного самоуправления современной России в процессе информатизации политического управления : автореф. дис. ...канд. полит. наук. Саратов, 2010.

² Кафтанчиков Д. П. Информационная безопасность Российской Федерации : современное состояние и приоритеты обеспечения : автореф. дис. ...канд. полит. наук. Орел, 2009.

³ Проценко Е. А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации : автореф. дис. ...канд. тех. наук. СПб., 2008.

на укрепление международной информационной безопасности и вместе с тем максимально учитывались национальные интересы¹.

Социологи развивают понятие информационной безопасности в рамках одного из направлений социологии — социологии информатики, тем самым взаимосвязывая социологический и информационный подходы².

Среди юристов также пока не выработано единого подхода к определению понятия «информационной безопасности».

«Информационная безопасность является важнейшей составляющей национальной безопасности в целом... В структуре информационного права проблема обеспечения информационной безопасности является одним из институтов. Суть этого института информационного права состоит в осуществлении правовых, организационных, технических мер, обеспечивающих безопасное состояние всех составляющих информационно-коммуникационного комплекса государства, отдельных организаций и каждого человека»³.

По мнению В.Н. Лопатина⁴ объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Выделяя отдельно информационно-психологическую безопасность, В.Н. Лопатин трактует ее как «состояние защищенности жизненно важных интересов личности, общества и государства от воздействия вредной информации»⁵.

¹ Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации : автореф. дис. ...канд. юрид. наук. М., 2007.

² Шемякин В. П. Информационная безопасность в современных российских условиях : Социолого-управленческие аспекты : автореф. дис. ...канд. социол. наук. М., 2004.

³ Бачило И. Л. Информационное право : учебник для вузов. — М. : Высшее образование ; Юрайт-Издат, 2009. С. 398.

⁴ Лопатин В. Н. Информационная безопасность России : Человек, общество, государство. Серия: Безопасность человека и общества. СПб. : Фонд Университет, 2000.

⁵ Лопатин В. Н. Информационное право : учебник. СПб.: Юридический центр Пресс, 2005. С. 474.

А.А. Стрельцов понятие «обеспечение информационной безопасности» раскрывает как «сложное явление, включающее объект безопасности, образуемый совокупностью информационных потребностей государства и его деятельности по удовлетворению этих потребностей, угроз объекту безопасности, деятельности государства по противодействию угрозам, а также субъектов этого противодействия»¹.

Полякова Т.А. информационную безопасность рассматривает как состояние защищенности национальных интересов Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что, соответствует принципу обеспечения национальной безопасности в информационной сфере, определенному в Стратегии развития информационного общества в Российской Федерации.²

В целом государственная политика в области обеспечения безопасности, согласно ст. 4 Федерального закона «О безопасности» является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Сегодня только Доктрина информационной безопасности определяет исследуемую дефиницию: информационная безопасность — это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства³.

Однако необходимо согласиться с высказываемыми мнениями о необходимости уточнения и пояснения данного понятия. Так, действительно, требуют разграничения понятия «информационная безо-

¹ Стрельцов А. А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. 2001. Вып. 4. С. 16.

² Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ...докт. юрид. наук. М., 2008.

³ Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895).

пасность» и «информационная безопасность Российской Федерации». Состояние достижения информационной безопасности может рассматриваться как потребность не только государства, но и других субъектов информационных отношений: граждан, юридических лиц, а также технологических механизмов, систем, информационно-коммуникационных технологий — объектов информационной безопасности¹.

Представленные взгляды ученых на понятие и проблему информационной безопасности обнаруживают как наличие общих взглядов, так и специфику каждого из подходов. Ясно одно: решение проблем информационной безопасности возможно только за счет скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

10.2. Информационная безопасность личности как приоритетная задача электронной России

Сегодня, наряду с такими понятиями, как «безопасность», «национальная безопасность», «информационная безопасность» как никогда актуализируется понятие «информационной безопасности личности». В современных условиях эта проблема выдвигается на уровень общенациональной. Решение проблем обеспечения информационной безопасности личности сегодня — это и актуально, и своевременно, поскольку Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом РФ 7 февраля 2008 г. № Пр-212, подчеркивается, что в настоящее время в Российской Федерации сформировались необходимые условия для перехода к информационному обществу, одним из важнейших проявлений которого является обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации.

¹ Куняев Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. М. : Логос, 2010. С. 258.

Анализ основных правомочий человека электронного государства позволяет сделать вывод о приоритетности решения вопроса информационной безопасности личности.

Неслучайно Модельный информационный кодекс для государств-участников СНГ в ст. 1 в числе основных целей информационного законодательства называет в том числе — обеспечение и защиту конституционных прав и свобод человека в информационной сфере; обеспечение информационной безопасности человека, общества и государства; создание правовых условий для эффективного информационного обеспечения физических и юридических лиц, органов государственной власти и органов местного самоуправления.

При этом информатизация общества и проблема информационной безопасности личности тесно взаимосвязаны. К сожалению, в свете проблем «информационной безопасности государства», «информационной безопасности госструктур», «информационной безопасности бизнеса» и т.п. предмет нашего исследования остается как бы «в тени», за рамками внимания как законодателя, так и многих исследователей. Однако можно с уверенностью утверждать, что постепенно эта проблема выйдет на первый план и будет требовать скорейшего решения.

Формирующееся глобальное информационное пространство, в котором циркулируют информационные потоки, создаваемые всей человеческой цивилизацией, ставит в повестку дня решение не только технических, но и нравственных проблем, порождаемых самим фактом существования этого пространства. Активизация и глобализация информационных взаимодействий в современном обществе предъявляют все более высокие требования к обеспечению информационной безопасности личности.

Поскольку сегодня человек — хочет он этого или нет — начинает жить в электронной России, необходим целый комплекс специальных мер для обеспечения допустимого уровня безопасности жизни и деятельности человека в таком государстве. Данный комплекс должен включать мониторинг всех аспектов электронного государства, осуществляемый в режиме реального времени с целью своевременного выявления существующих и возникающих в нем информационных угроз, их предотвращения и нейтрализации, а также ликвидации негативных последствий этих угроз. Такой мониторинг станет возмож-

ным, если основная масса субъектов электронного государства станет сознательно в нем участвовать и возьмет на себя долю ответственности за безопасность этого государства. Это означает, что должна быть соответствующая этика — этика электронного государства, которой будут следовать субъекты данного государства и без которой безопасность человека в информационном обществе будет практически недостижима.

При этом, безусловно, должен соблюдаться определенный баланс интересов личности, интересов общества в целом и интересов самого электронного государства.

Застрахованы ли граждане, получив универсальную электронную карту, от мошенничества? Насколько обеспечена будет защита персональных данных?

Для сравнения. Во многих странах, преуспевающих в сфере информационных технологий, нет унифицированной электронной карты. Так, в Германии нет такой карты — это законодательно запрещено по соображениям безопасности граждан. В Англии для безопасности граждан в 2010 г. законодательно упразднен Регистр идентификации и уничтожены базы данных. В Южной Корее создали электронное правительство, но из-за высокого уровня электронного мошенничества население отказалось пользоваться этими услугами.

Какой сценарий развития событий ждет Россию? С выводами спешить не стоит. Оценить адекватность правового регулирования складывающихся в электронном государстве правоотношений можно будет не раньше 2015—2020 гг.

Формирование электронной России как электронного государства по-новому расставляет акценты в вопросе реализации прав субъектов информационных отношений, и, прежде всего, человека как основного, первичного их участника.

А какой он — этот участник современных информационных правоотношений? И какое влияние оказывает на него Сеть? И.Л. Бачило в одной из своих работ особенно акцентирует внимание на социальных сетях (блог, твиттер, сети типа «одноклассники», «вконтакте», «мой мир», «фэйсбук»...) и приводит пример, как в фильме Дэвида Финчера «Социальная сеть» через конкретный сюжет обнаруживается ее влияние на формирование личности. Структура формируемого человека под ее влиянием описана следующим образом:

«лицо...должно быть именно таким: глуповатым, трусоватым, вместе с тем нагловатым, а главное, аутичным, не способным выражать адекватную реакцию на слова собеседника»¹. Это образное представление субъекта социальной сети сопровождается и сообщением о миллиардных доходах лиц, создающих определенные сегменты в этом пространстве².

Что происходит сегодня? Скандал с сайтом «русликс».., еще один подобный, когда в результате перехода Пенсионного фонда на электронную систему документооборота в Интернет попали личные данные граждан. Конфиденциальная информация о клиентах Пенсионного фонда России по Твери и Тверской области оказались в свободном доступе в интернете³. И это еще только начало. Проблема безопасности в таких условиях более чем актуальна.

Вывод: гарантии прав и интересов в информационной сфере приобретают далеко не маловажное значение. И эта проблема требует своего решения как никогда. К примеру, Модельный информационный кодекс для государств-участников СНГ в качестве таковых гарантий называет следующее:

1. Обеспечение информационных прав и свобод человека в информационной сфере, обеспечение информационной безопасности является важнейшей функцией государства.

2. Обеспечение права каждого человека на свободу поиска, получения, использования, создания, распространения и хранения информации любыми законными способами и средствами возлагается на органы государственной власти и местного самоуправления.

3. Органы государственной власти и органы местного самоуправления, юридические лица обязаны предоставлять информацию по запросу субъектов информационных отношений и информационно-инфраструктурных отношений, за исключением информации, доступ к которой ограничен законом⁴.

¹ Маслова Л. Кого за сетью посылать. Удачный случай социопатии в «Социальной сети» // Коммерсантъ. 2010. 27 окт.

² Бачило И. Л. Методологические проблемы идентификации и правовой поддержки развития социальных сетей // Информационное общество и социальное государство : сб. науч. работ. М. : ИГП РАН, ИПО «У Никитских ворот», 2011. С. 33.

³ <http://www.newsland.ru/news/detail/id/820130/>

⁴ Модельный информационный кодекс для государств — участников СНГ. Часть первая (Санкт-Петербург, 3 апреля 2008 г.).

Сегодня, в условиях формирующегося электронного государства задача полноценного обеспечения информационных прав и свобод человека не только не теряет своей актуальности, а, напротив, становится все более значимой.

Государственная программа Российской Федерации № 1815-р «Информационное общество (2011—2020 годы)» констатирует наличие проблем в области защиты прав и свобод человека в информационном обществе российского государства и подчеркивает, что в настоящее время наблюдается неконтролируемый рост объемов информации о гражданах, об организациях и объектах хозяйственного оборота, содержащейся в государственных информационных системах, что в условиях отсутствия эффективных механизмов контроля ее использования создает также угрозу нарушения прав граждан; сохраняется высокий уровень различия в использовании информационных технологий...различными слоями общества, и недостаточно развита базовая инфраструктура информационного общества.

Механизм предоставления государственных и муниципальных услуг, заложенный в Федеральном законе от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», система введения универсальных электронных карт, многофункциональных центров выводит на одно из первых мест задачу обеспечения информационной безопасности личности, прежде всего, задачу обеспечения защиты персональных данных.

Проблем больше, чем достаточно. Не вызывает сомнений одно: развивающееся законодательство в сфере регулирования информационных правоотношений должно быть ориентировано прежде всего на человека как основного, первичного их участника. Этот самый «главный» участник — человек электронного государства, человек информационного общества — не должен остаться в стороне, и его права и свободы, которые в условиях развития электронного государства актуализируются как никогда, законодателем в полной мере должны быть обеспечены. Понятия «права человека», «законность» должны стать лидирующим ядром в ряду институциональных признаков «электронного государства».

Принцип правовой защищенности человека и гражданина, как основополагающий принцип правового государства, должен лечь в основу решения проблемы «человек в информационном обществе»,

«человек и общество «Электронной России». И это должно найти отражение, как в федеральном, так и региональном законодательстве.

Важным событием 2013 г. стало внимание законодателя к сфере неприкосновенности частной жизни граждан: 1 октября вступил в силу Федеральный закон от 2 июля 2013 г. № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации», новая статья которого — 152.2 ГК РФ — устанавливает запрет без согласия гражданина на сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни.

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Право на неприкосновенность частной жизни имеет прямое отношение к понятию «информационная безопасность личности», которая, согласно положениям Доктрины информационной безопасности РФ, определяется как состояние защищенности ее интересов в информационной сфере.

Дела о защите чести, достоинства и деловой репутации граждан в нашем обществе имеют тенденцию к увеличению. Прежде всего, в последние годы новое звучание приобрела проблема интернет-диффамации, т.е. распространения в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя.

Право на неприкосновенность частной жизни относится к числу основных прав человека и защищено Всеобщей декларацией прав человека и Конституцией РФ.

Соблюдение конституционных прав и свобод человека и гражданина — задача любого государства, позиционирующего себя в мировом сообществе как демократическое. Перечень и содержание основных прав и свобод человека закреплены во Всеобщей декларации прав человека, которую называют совестью мира, нравственным эталоном человечества. В этом историческом документе, как и в Уставе ООН, подтверждена истина: все люди рождаются свободными и равными в своем человеческом достоинстве и основных, естественных правах. Во всеобщей декларации утверждается право каждого чело-

века на жизнь без нужды и страха на личную неприкосновенность, свободу слова и убеждений.

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Единое мировое информационное пространство, создавая условия безграничной свободы и отсутствия должного правового регулирования, ставит под сомнение ряд закрепленных основным законом государства прав и свобод.

Исторической вехой в решении вопроса защиты чести, достоинства и деловой репутации в случае распространения ложной или оскорбляющей информации в Интернете стало Постановление Конституционного Суда РФ от 9 июля 2013 г. № 18-П. Данным Постановлением некоторые положения ст. 152 Гражданского кодекса РФ признаны соответствующими требованиям Конституции, в частности, что сведения, порочащие честь и достоинство гражданина, опубликованные в сети интернет на сайтах, не являющихся средствами массовой информации, нарушают конституционные права гражданина. Однако, владелец данного сайта или лицо, отвечающее за его администрирование, не могут нести никакой ответственности за их публикацию.

В то же время некоторые положения ст. 152 ГК РФ названным Постановлением КС РФ были признаны не соответствующими нормам Основного закона. Речь, прежде всего, о том, что статья не обязывает владельца или администратора такого интернет-ресурса удалять сведения, опубликованные третьими лицами и признанные по решению суда ложными или оскорбляющими честь и достоинство гражданина.

Информационное общество, т.е. общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, информационные ресурсы доступны всем слоям населения, при этом полноценно решена проблема признания, реализации и защиты прав и свобод субъектов информационных правоотношений, переживает сегодня один из самых активных этапов своего развития. В процессе формирования информационного общества вступившие в силу изменения ГК РФ — очередной значимый шаг.

Согласно п. 4 ст. 152.2 ГК РФ в случаях, когда информация о частной жизни гражданина, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно.

При этом нужно иметь в виду, что формулировка введенной в ГК РФ ст. 152.2 предполагает открытый характер списка информации, относящейся к понятию частной жизни. Таким образом, понятие частной жизни включает и образ мыслей, и политическое, и социальное мировоззрение, увлечения, творчество, целый ряд профессиональных тайн (например, врачебная тайна, адвокатская тайна и т.д.), перечень иных сведений, которые, по мнению человека, должны остаться в тайне.

Фактически именно гражданин решает, какие именно сведения относятся к его частной жизни и подлежат защите, что неизбежно вызовет увеличение судебных споров по этому вопросу. Конечно, суд может с ним не согласиться и отказать отнести какие-либо сведения к частной жизни.

Законодателем подчеркивается, что не являются неправомерными сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, а также в случаях, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле. И если с распространением информации по воле самого гражданина все понятно, то с вопросом, какие именно государственные, общественные или иные публичные интересы будут оправдывать вмешательство в частную жизнь гражданина, дело обстоит гораздо сложнее.

Помимо того, что гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъя-

тия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно закон не исключает и дополнительные гражданско-правовые способы защиты права на неприкосновенность частной жизни. К таковым закон относит возможность компенсации морального вреда и другие способы гражданских прав, предусмотренные ст.12 ГК РФ.

В скором времени появится возможность проанализировать складывающуюся практику правоприменения новелл ГК РФ в части охраны частной жизни гражданина, однако механизм реализации Федерального закона «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации» нельзя признать полностью понятным, как в части самого процесса удаления неправомерно распространенной ложной или оскорбляющей честь и достоинство гражданина информации, так и в части точного определения информации, относящейся к понятию частной жизни, а также в вопросе правомерности сбора, хранения, распространения и использования информации о частной жизни гражданина в государственных, общественных или иных публичных интересах. Последнее — тем более актуально в условиях, когда в решении вопроса охраны частной жизни заинтересовано мировое сообщество.

На повестке дня вопрос: право каждого гражданина на частную жизнь и возможность ограничения этого права. В отношении судебной практики по вопросу применения норм вступившего в силу Федерального закона «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации» правоприменителю необходимо будет учитывать правовую позицию Конституционного Суда РФ, высказанную в Постановлении Конституционного Суда РФ от 30 октября 2003 г. № 15-П:

а) ограничения конституционных прав должны быть необходимыми и соразмерными конституционно признаваемым целям таких ограничений;

б) при допустимости ограничения того или иного права в соответствии с конституционно одобряемыми целями государство, обеспечивая баланс конституционно защищаемых ценностей и интересов,

должно использовать не чрезмерные, а только необходимые и строго обусловленные этими целями;

в) публичные интересы, перечисленные в ст. 55 (ч. 3) Конституции РФ, могут оправдать правовые ограничения прав и свобод, только если такие ограничения отвечают требованиям справедливости, являются адекватными, пропорциональными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе прав и законных интересов других лиц, не имеют обратной силы и не затрагивают само существо конституционного права с тем, чтобы исключить возможность несоразмерного ограничения прав и свобод человека и гражданина в конкретной правоприменительной ситуации.

Вопросы и задания для самоконтроля

1. Дайте характеристику Доктрине информационной безопасности РФ.

2. Раскройте понятия «информационная безопасность», «информационная безопасность личности», «информационная безопасность общества», «информационная безопасность государства».

3. Какова роль международно-правовых актов в решении вопросов информационной безопасности?

Нормативные правовые акты

Конституция Российской Федерации : принята всенародным голосованием 25 декабря 1993 г.

Окинавская хартия глобального информационного общества : принята на о. Окинава 22 июля 2000 г.

Всеобщая декларация прав человека : принята Генеральной Ассамблеей ООН 10 декабря 1948 г.

Декларация о правах человека и верховенстве права в информационном обществе / Российский комитет программы ЮНЕСКО «Информация для всех», Национальный фонд подготовки кадров, Фонд гражданских инициатив в политике Интернет. Публикация № 050512/d/1.

Доктрина информационной безопасности Российской Федерации : утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895).

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ г. «О безопасности».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Стратегия развития информационного общества в Российской Федерации : утверждена Президентом РФ 7 февраля 2008 г. № Пр-212.

Распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р «Государственная программа «Информационное общество (2011—2020 годы)».

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

- Бачило, И. Л. Информационное право : учебник / И. Л. Бачило. — М. : Юрайт, 2013.
- Городов, О. А. Информационное право : учебник для бакалавров. — М. : Проспект, 2014.
- Лопатин, В. Н. Информационное право : учебник / В. Н. Лопатин. — СПб. : Юридический центр Пресс, 2005.
- Рассолов, И. М. Информационное право : учебник / И. М. Рассолов. — М. : Юрайт, 2011.

Дополнительная литература

- Атаманов, Г. А. Информационная безопасность : сущность и содержание / Г. А. Атаманов. // Бизнес и безопасность в России. — 2007. — № 47.
- Бачило, И. Л. Государство социальное или сервисное? (информационно-правовой аспект) / И. Л. Бачило. // Право. Журнал высшей школы экономики. — 2010. — № 1.
- Брандман, Э. М. Глобализация и информационная безопасность общества / Э.М. Брандман. — М. : Изд-во ГПИБ России, 2007.
- Василенко, Л. А. Интернет в информатизации государственной службы России / Л.А. Василенко. — М. : РАГС, 2000.
- Васильева, А. Ф. Теория правоотношений, складывающихся в сфере предоставления публичных услуг / А. Ф. Васильева. // Государство и право. — 2010. — № 7.
- Васькова, М. Г. Электронное государство : проблемы правового регулирования / М. Г. Васькова. // Информационное право. — 2009. — № 4.
- Вербенко, Б. В. Информационная безопасность России в контексте современного политического процесса : сущность, проблемы обеспечения : автореф. дис. ... канд. полит. наук / Б. В. Вербенко. — М., 2004.
- Волчинская, Е. К. Некоторые приоритеты национальной безопасности в информационной сфере и проблемы их законодательного обеспечения / Е. К. Волчинская. // Информационное право. — 2009. — № 4.
- Гунин, Д. И. Транспарентность и тайна информации : теоретико-правовой аспект : автореф. дис. ...канд. юрид. наук / Д. И. Гунин. — Екатеринбург, 2008.
- Дашян, М. Правовое регулирование в сфере Интернета на уровне субъектов РФ / М. Дашян. // Право и экономика. — 2004. — № 12.
- Долинская, В. В. Информационные отношения в гражданском обороте / В. В. Долинская. // Законы России. — 2010. — № 4.

Информационная безопасность : учеб. пособие. Часть 1. / А. М. Блинов. — СПб. : СПбГУЭФ, 2010.

Информационная безопасность и защита информации : учеб. пособие / Э. Н. Камышев. — Томск : ТПУ, 2009.

Информационное общество : проблемы развития законодательства : сб. науч. трудов. — М. : ИГП РАН, ЮРКОМПНИ, 2012.

Кастель, М. Информационная эпоха. Экономика, общество и культура : пер. с англ. / М. Кастель. — М. : ГУ-ВШЭ, 2000.

Ковалева, Е. В. Обеспечение транспарентности органов местного самоуправления современной России в процессе информатизации политического управления : автореф. дис. ...канд. полит. Наук : 23.00.02 / Е. В. Ковалева. — Саратов, 2010.

Копылов, В. А. Информационное право : учеб. пособие / В. А. Копылов. — М. : Юрист, 1999.

Крылов, Г. О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации : автореф. дис. ...канд. юрид. наук : 05.13.19 / Г. О. Крылов. — М., 2007.

Кузнецов, П. У. Социальная миссия электронного государства : ценности и терминологические проблемы // Информационное общество и социальное государство : сб. науч. работ / П. У. Кузнецов. — М. : ИГП РАН, 2011.

Куликова, С. А. Практика реализации права граждан на доступ к информации о деятельности государственных органов: на примере Саратовской области // Информационное общество и социальное государство : сб. науч. работ / С. А. Куликова. — М. : ИГП РАН, 2011.

Лазарев, И. А. Информация и безопасность. Композиционная технология / И. А. Лазарев. — М. : Изд-во Московского ЦНТИ, 2002.

Лопатин, В. Н. Информационная безопасность России : Человек. Общество. Государство / В. Н. Лопатин. — СПб. : Фонд Университет, 2000.

Маслова, Н. Р. Состояние и проблемы формирования правовой основы реализации «Стратегии развития информационного общества в России» на федеральном и региональном уровне / Н. Р. Маслова. // Информационное право. — 2009. — № 2.

Морозов, А. В. Организационно-правовое обеспечение информационное безопасности : монография / А. В. Морозов, Т. А. Полякова. — М. : РПА Минюста России, 2013.

Морозов, А. В. Этапы и проблемы формирования единого информационно-правового пространства России / А. В. Морозов, Т. А. Полякова, Л. В. Филатова. // Информационное право. — 2012. — № 1 (28).

Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. ... докт. юрид. наук / Т. А. Полякова. — М., 2008.

Полякова, Т. А. Информационная безопасность в условиях построения информационного общества в России / Т.А. Полякова. — М. : РПА Минюста России, 2007.

Право на доступ к информации. Доступ к открытой информации / отв. ред. И. Ю. Богдановская. — М. : ЗАО «Юстицинформ», 2009. — 344 с.

Рассолов, М. М. Информационное право : учеб. пособие / М. М. Рассолов. — М. : Юрайт, 2013.

Сергиенко, Л. А. История формирования информационного права в СССР и Российской Федерации 1960-2000 гг. : монография / Л. А. Сергиенко. — М. : ЮРКОМПАНИ, 2013.

Стрельцов, А. А. Содержание понятия «обеспечение информационной безопасности» / А. А. Стрельцов. // Информационное общество. — 2001. — Вып. 4.

Устинович, Е. С. Понятие информационной политики государства / Е. С. Устинович. // Информационное право. — 2012. — № 1 (28).

Уэбстер, Ф. Теории информационного общества / Ф. Уэбстер. — М. : Аспект-пресс, 2004.

Филатова, Л. В. Актуальные вопросы правового регулирования предоставления государственных услуг в электронной форме // Условия реализации прав граждан и организаций на основе информационных технологий / Л. В. Филатова. — М. : ИГП РАН, 2010.

Чеботарева, А. А. Право на защиту чести, достоинства и деловой репутации в информационном обществе / А. А. Чеботарева. // Вестник УрФО. Безопасность в информационной сфере. — 2013. — № 3 (9).

Чеботарева, А. А. Сравнительное исследование научных подходов к сущности и содержанию понятия «Информационная безопасность» / А. А. Чеботарева. // Информационное право. — 2011. — № 1.

Чеботарева, А. А. Человек и электронное государство. Право на информационную безопасность : монография / А. А. Чеботарева. — Чита : ЧитГУ, 2011.

Чеботарева, А. А. Электронный документооборот электронного правительства : к вопросу о проблемах обеспечения прав и свобод субъектов информационного общества // Юридический мир. — 2014. — № 2.

Червяковский, А. В. Регулирование доступа граждан к правовой информации, размещенной на официальных сайтах федеральных органов исполнительной власти А. В. Червяковский. // Законы России : опыт, анализ, практика. — 2010. — № 4.

Якимец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учеб. пособие. — 2-е изд., доп. и перераб. / Е. Н. Якимец. — М. : Юрлитинформ, 2014.

Сетевые электронные ресурсы

Интернет в цифрах [Электронный ресурс]. — Режим доступа: <http://www.in-numbers.ru/>

Официальный сайт ОАО «Универсальная электронная карта» [Электронный ресурс]. — Режим доступа: <http://www.uecard.ru/>

Портал государственных услуг Российской Федерации [Электронный ресурс]. — Режим доступа: <http://www.gosuslugi.ru/>

Портал «Молодежное Информационное Равенство» [Электронный ресурс]. — Режим доступа: <http://www.mir4you.ru/node/14349>

СЛОВАРЬ-СПРАВОЧНИК

Биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Государственная автоматизированная система (ГАС) «Правосудие» — это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и управлений (отделов) Судебного департамента при Верховном суде РФ.

Государственная информационная политика — это совокупность целей, отражающих национальные интересы в информационной сфере, стратегии, тактики управленческих решений и методов их реализации, разрабатываемых и реализуемых государственной властью для регулирования и совершенствования как непосредственно процессов информационного взаимодействия во всех сферах жизнедеятельности общества и государства, так и процессов технологического (в широком смысле) обеспечения такого взаимодействия.

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Государственная услуга — деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта РФ, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов РФ, которая осуществляется по запросам заявителей в пределах установленных нормативными правовыми актами РФ и нормативными правовыми актами субъектов РФ полномочий органов, предоставляющих государственные услуги.

Документ — материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и

(или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

Доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет».

Единый портал государственных и муниципальных услуг — государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием сети Интернет и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг.

Защита информации — комплекс мероприятий, направленных на обеспечение информационной безопасности.

Институт информационного права — это относительно устойчивая группа информационно-правовых норм, регулирующая определенную группу информационных отношений.

Источники информационного права — правовые акты представительных и исполнительных органов государственной власти и местного самоуправления, в которых содержатся нормы информационного права.

Интернет — сфера непрерывного информационно-коммуникационного процесса, обеспечивающего обращение информации (сведений) в цифровой форме в неограниченном пространстве через связанные между собой сети связи, и реализации обмена информационным ресурсом любых субъектов (потребителей) в целях получения, накопления знаний или осуществления электронных операций субъектов в разных областях реализации их интересов, прав и обязанностей.

Интернет-диффамация — распространение посредством средств массовой информации в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, деловую репутацию, доброе имя.

Информационное право — отрасль российского права, нормы которой регулируют общественные отношения, возникающие в процессе

поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Информационные правоотношения — общественные отношения, урегулированные нормами информационного права, возникающие в процессе поиска, получения, передачи, производства и распространения информации, а также связанные с ними отношения.

Информационно-правовая норма — установленное государством и обеспеченное мерами государственного принуждения правило поведения в общественных информационных отношениях, возникающих в процессе поиска, получения, передачи, производства и распространения информации, а также связанных с ними отношений.

Информация — сведения (сообщения, данные) независимо от формы их представления; т.е. воспринимаемая и понимаемая человеком характеристика окружающего мира во всем его разнообразии, которая возникает в процессе познания последнего и позволяет на основе свойств предметов, процессов, фактов и отражения их в различных формах восприятия отличать их признаки, значения и устанавливать связи и зависимости всего многообразия проявления материального, духовного, идеологического мира — формировать мировую систему знаний.

Информация, составляющая коммерческую тайну (секрет производства) — сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Информационная безопасность — состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационное общество — термин, применяемый для обозначения современного состояния индустриально развитых стран, связанного с новой ролью информации во всех сторонах их жизнедеятельности, качественно новым уровнем производства, переработки и распространения информации.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационный ресурс — массив или отдельный документ, другой визуально воспринимаемый информационный объект, который аккумулирует сведения (информацию), сформированные по определенному признаку или критерию.

Квалифицированная электронная подпись — электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Конфиденциальная информация — такая информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Массовая информация — предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Межведомственное информационное взаимодействие — осуществляемое в целях предоставления государственных и муниципальных услуг взаимодействие по вопросам обмена документами и информацией, в том числе в электронной форме, между органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, подведомственными государственным органам или органам местного самоуправления организациями, участвующими в предоставлении государственных или муниципальных услуг, иными государственными

органами, органами местного самоуправления, многофункциональными центрами.

Многофункциональный центр предоставления государственных и муниципальных услуг — российская организация независимо от организационно-правовой формы (в том числе являющаяся автономным учреждением), отвечающая требованиям, установленным настоящим Федеральным законом, и уполномоченная на организацию предоставления государственных и муниципальных услуг, в том числе в электронной форме, по принципу «одного окна».

Муниципальная услуга — деятельность по реализации функций органа местного самоуправления, которая осуществляется по запросам заявителей в пределах полномочий органа, предоставляющего муниципальные услуги, по решению вопросов местного значения, установленных соответствующим законодательством.

Обезличивание персональных данных — это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступная информация — информация, предоставляемая свободно в силу прямого указания закона в случаях реализации гражданином своих конституционных и иных, предоставленных законом прав.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Оператор обработки персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, которое организует и (или) осуществляет обработку персональных данных, а

также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Портал государственных и муниципальных услуг — государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием информационно-телекоммуникационной сети «Интернет» и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг.

Право на информацию — это совокупность правовых актов и отдельных норм, определяющих порядок реализации прав субъектов информационного права в области производства (создания) информации, поиска и получения (доступа) информации, сбора, хранения, передачи, использования, распространения информации в целях, не противоречащих свободам, правам и интересам человека, государства, общества и обеспечивающих создание информационных ресурсов, необходимых для реализации других прав и обязанностей субъектов права, предусмотренных и гарантированных законодательством РФ и нормами международного права.

Предоставление государственных и муниципальных услуг в электронной форме — это предоставление государственных и муниципальных услуг с использованием информационно-телекоммуникационных технологий, включая использование единого портала государственных и муниципальных услуг и (или) региональных порталов государственных и муниципальных услуг, а также использование универсальной электронной карты, в том числе осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями. В целях предоставления государственных и муниципальных услуг в электронной форме могут использоваться другие средства информационно-телекоммуникационных технологий в случаях и порядке, которые определяются Правительством РФ.

Предоставление государственных и муниципальных услуг по принципу «одного окна» — это предоставление государственной или муници-

пальной услуги после однократного обращения заявителя с соответствующим запросом, при этом взаимодействие с органами, предоставляющими государственные услуги, или органами, предоставляющими муниципальные услуги, осуществляется многофункциональным центром без участия заявителя в соответствии с нормативными правовыми актами и соглашением о взаимодействии.

Предоставление персональных данных — это действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет».

Простая электронная подпись — электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Распространение персональных данных — это действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет».

Сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.

Система информационного права — это объективно обусловленное системой общественных информационных отношений внутреннее его строение, объединение и расположение информационно-правовых норм в определенной последовательности.

Специальные категории персональных данных — это данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Средство массовой информации — периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Сетевое издание — сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с законом.

Транспарентность — состояние информированности (наличие полного, достаточного и достоверного знания) о той или иной деятельности (ее объектах или результатах) любого заинтересованного в этом субъекта.

Универсальная электронная карта — материальный носитель, содержащий зафиксированную на нем в визуальной (графической) и электронной (машиночитываемой) формах информацию о пользователе картой и обеспечивающий доступ к информации о пользователе картой, используемой для удостоверения прав пользователя картой на получение государственных и муниципальных услуг, а также иных услуг, оказание которых осуществляется с учетом положений закона, в том числе для совершения в случаях, предусмотренных законодательством РФ, юридически значимых действий в электронной форме.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Цифровое неравенство — неравный доступ к информационным технологиям, разделение на тех, кому эти технологии доступны, а кому — нет, деление на «информационно богатых» и «информационно бедных».

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронный бюллетень — бюллетень, подготовленный программно-техническими средствами в электронном виде, применяемый при проведении электронного голосования.

Электронное голосование — голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса средств автоматизации ГАС «Выборы».

Электронная демократия — такая форма организации общественно-политической деятельности граждан, которая обеспечивает за счет широкого применения информационно-коммуникационных технологий

качественно новый уровень взаимодействия граждан друг с другом, с органами государственной власти, органами местного самоуправления, общественными организациями и коммерческими структурами.

Электронное приложение универсальной электронной карты — уникальная последовательность символов, записанная на электронном носителе универсальной электронной карты и предназначенная для авторизованного доступа пользователя такой картой к получению финансовой, транспортной или иной услуги, в том числе государственной или муниципальной услуги.

Электронный документ — документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронный документооборот (ЭДО) — система ведения документации, при которой массив создаваемых электронных документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сеть, дающую возможность формирования и ведения распределенной базы данных.