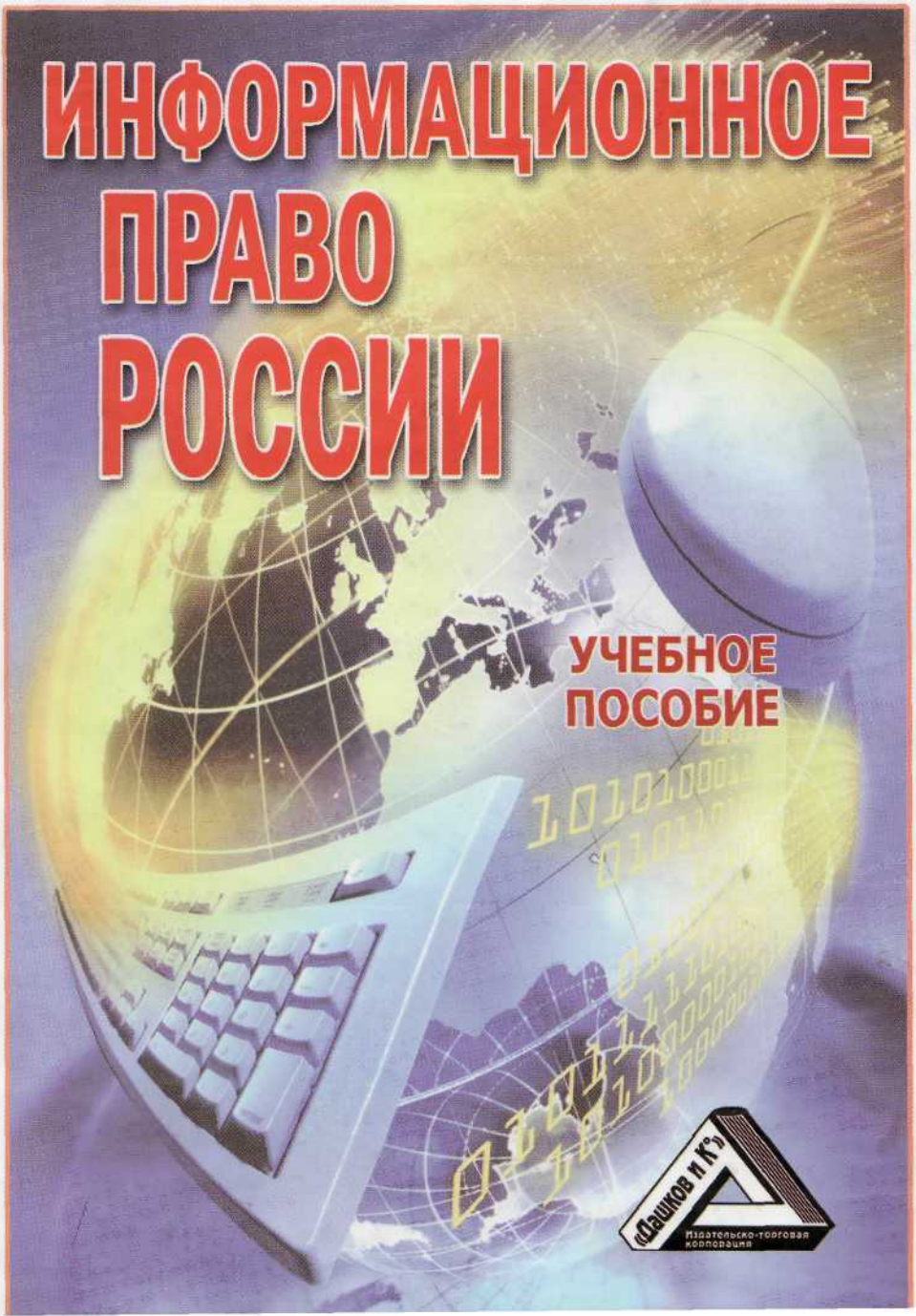
Н. Н. КОВАЛЕВА

ИНФОРМАЦИОННОЕ ПРАВО РОССИИ



УЧЕБНОЕ ПОСОБИЕ

«Дашков и К°»
Издательско-торговая корпорация

Издательско-торговая корпорация «Дашков и К°»

Н. Н. Ковалева

ИНФОРМАЦИОННОЕ ПРАВО РОССИИ

Учебное пособие

Москва, 2007

УДК 34
ББК67
К56

Ковалева Наталия Николаевна — кандидат юридических наук, доцент кафедры административного и муниципального права, декан факультета магистратуры, грант Президента РФ поддержки молодых кандидатов наук «Взаимодействие органов местного самоуправления» 2003—2004 гг., «Базовые категории в системе информационного права» ИГПРАН, февраль 2006 г. Соискатель степени доктора юридических наук (по теме «Информационное обеспечение системы органов власти»). Читаемые курсы: административное право, муниципальное право, информационное право.

К56 **Ковалева Н. Н. Информационное право России:** Учебное пособие. — М.: Издательско-торговая корпорация «Дашков и К°», 2007. — 360 с.

ISBN 5-91131-321-9

В учебном пособии раскрываются понятия информации, информационного права и информационных правоотношений в современном обществе, дается характеристика электронного документооборота, выявляются особенности правового регулирования Интернета.

Значительное внимание уделяется проблемам защиты конфиденциальной информации, информационной безопасности личности, общества и государства, а также вопросам правового регулирования прав интеллектуальной собственности на информационные продукты.

Для студентов, магистрантов, обучающихся по направлению «Юриспруденция», а также для всех интересующихся данной проблемой.

ПРАВООБЛАДАТЕЛЬ — ООО «АИ ПИ ЭР МЕДИА»

ISBN5-91131-321-9

Содержание

Сокращения **8**

Предисловие **9**

РАЗДЕЛ 1. ОБЩИЕ ПОЛОЖЕНИЯ **11**

Глава 1. Информационное право как отрасль права **11**

1. Понятие информации 11
2. Виды информации. Документированная и недокументированная информация 15
3. Предмет информационного права 20
4. Особенности формирования информационного права 22
5. Международный характер информационного права 25
6. Комплексный характер информационного права 28
7. Методы информационного права 30
8. Правовое регулирование информационных отношений за рубежом **31**

Глава 2. Информационно-правовые нормы и отношения. Система и источники информационного права 39

1. Информационная норма: понятие, особенности, виды 39
2. Информационно-правовые отношения: понятие, виды, соотношение с правовой нормой, структура и защита 40
3. Система информационного права 51
4. Виды источников информационного права 52
5. Принципы информационного права 53

Глава 3. Понятие и виды субъектов информационного права 56

1. Понятие субъектов информационного права (общая характеристика) 56
2. Российская Федерация, субъекты РФ и муниципальные образования как субъекты информационного права 58
3. Граждане и другие физические лица как субъекты информационного права 61
4. Правовой статус общественных объединений и коммерческих организаций как субъектов информационного права 63

РАЗДЕЛ 2. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ **65**

Глава 4. Система органов государственной власти, регулирующих информационную сферу 65
1. Государственное управление в информационной сфере 65
2. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации 69
3. Система и компетенция органов, обеспечивающих охрану государственной тайны 72
4. Компетенция органов государственной власти по обеспечению правовых режимов конфиденциальной информации 74
5. Взаимодействие органов местного самоуправления и органов государственной власти в условиях информатизации общества 74
6. Электронное государство 80

Глава 5. Правовые режимы информационных ресурсов 94
1. Понятие правового режима информационных ресурсов 94
2. Понятие и виды охраноспособной информации 95
3. Режимы защиты информации 98
4. Государственная тайна как предмет, изъятый из гражданского оборота 100
5. Служебная и профессиональная тайна 106
6. Тайна частной жизни 117
7. Коммерческая и банковская тайна 129

Глава 6. Правовое регулирование, создание и применение информационных технологий 135
1. Понятие и виды информационных технологий 135
2. Порядок создания информационных технологий 137
3. Применение информационных технологий государственными органами, юридическими лицами и физическими лицами 141
4. Нарушение порядка применения информационных технологий: информационная война, информационное оружие 145

Глава 7. Правовое регулирование информационных систем 156
1. Понятие и виды информационных систем 156
2. Порядок разработки и официальная регистрация программ для ЭВМ и баз данных **157**

Глава 8. Особенности правового регулирования Интернета 164
1. Общая характеристика Интернета как особой информационно-телекоммуникационной сети 164
2. Деятельность, осуществляемая посредством Интернета 168
3. Государственное регулирование Интернета в России и за рубежом 170

Глава 9. Правовое регулирование информационных ресурсов 175
1. Понятие и виды информационных ресурсов 175
2. Порядок формирования информационных ресурсов и предоставления информационных услуг 179
3. Государственные информационные ресурсы 180
4. Государственное регулирование библиотечного дела 183
5. Государственное регулирование архивного дела 191

Глава 10. Электронный документ 194
1. Понятие и структура электронного документа 194
2. Правовой статус электронной цифровой подписи 196

Глава 11. Права граждан в информационной сфере 204
1. Право на доступ к информации 204
2. Право интеллектуальной собственности 212

Глава 12. Правовое регулирование средств массовой информации 217
1. Понятие и виды средств массовой информации 217
2. Правовой статус средств массовой информации 220
3. Правовой статус журналиста 248

Глава 13. Информационный рынок 253
1. Понятие и структура информационного рынка 253
2. Тенденции развития информационного рынка 254

Раздел **3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** 257

Глава 14. Общая характеристика информационной безопасности 257
1. Понятие информационной безопасности 257
2. Национальные интересы РФ в информационной сфере и их обеспечение 258
3. Источники угроз информационной безопасности РФ 261
4. Государственная политика в сфере информационной безопасности 263
5. Обеспечение информационной безопасности 266

Глава 15. Информационная безопасность личности 268
1. Общая характеристика информационной безопасности личности 268
2. Информационно-психологическая безопасность 269
3. Информационно-идеологическая безопасность 272

Глава 16. Информационная безопасность общества 278
1. Общая характеристика информационной безопасности общества 278
2. Угрозы информационной безопасности общества 280

Глава 17. Информационная безопасность государства 281
1. Общая характеристика информационной безопасности государства 281
2. Угрозы безопасности государства в информационной сфере 282

Глава 18. Информационная безопасность в глобальном информационном пространстве 288
1. Понятие глобального информационного пространства 288
2. Структура глобального информационного пространства 289
3. Обеспечение безопасности в глобальном информационном пространстве 290

Раздел 4. ОТВЕТСТВЕННОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ ... 294

Глава 19. Ответственность в информационной сфере ... 294
1. Дисциплинарная и административная ответственность в информационной сфере ... 294
2. Уголовная ответственность ... 302
3. Гражданско-правовая ответственность ... 308

Глава 20. Ответственность в области массовой информации ... 309
1. Ответственность за распространение запрещенной рекламы ... 309
2. Ответственность за иные нарушения законодательства о средствах массовой информации ... 312
3. Основания освобождения от ответственности субъектов права массовой информации ... 314
4. Ответственность за ущемление свободы массовой информации ... 315
5. Приостановление выпуска СМИ как особый вид ответственности ... 316

Глава 21. Особенности ответственности в сети «Интернет» ... 318
1. Уголовная ответственность в Интернете ... 318
2. Административная ответственность в Интернете ... 320
3. Гражданская ответственность в Интернете ... 321
4. Ответственность провайдеров в Интернете ... 325

Приложения ... 329
Приложение 1. Программа курса «Информационное право» ... 329
Цели и задачи преподавания дисциплины ... 329
Структура и содержание дисциплины ... 332
Приложение 2. Словарь терминов ... 337
Приложение 3. Список рекомендуемой литературы ... 357

Сокращения

АПК РФ — Арбитражный процессуальный кодекс РФ

БК **РФ** — Бюджетный кодекс РФ

ГК РФ — Гражданский кодекс РФ

ГПК РФ — Гражданский процессуальный кодекс РФ

КоАП РФ — Кодекс РФ об административных правонарушениях

МРОТ — минимальный размер оплаты труда

РФ — Российская Федерация

СЗ **РФ** — Собрание законодательства РФ

ТК РФ — Трудовой кодекс РФ

ТмК РФ — Таможенный кодекс РФ

УИК РФ — Уголовно-исполнительный кодекс РФ

УК РФ — Уголовный кодекс РФ

УПК РФ — Уголовно-процессуальный кодекс РФ

ФЗ — Федеральный закон

ФКЗ — Федеральный конституционный закон

ПРЕДИСЛОВИЕ

Высокие информационные технологии буквально пронизывают наше общество. В условиях развития рыночной экономики они приобретают особое значение, так как позволяют осуществлять управление государством не административными методами, а социально ориентированными, они также призваны отражать баланс интересов, существующих в обществе.

Обязательными предпосылками построения правового государства, создания демократической и эффективной системы управления делами страны, формирования передовой социально ориентированной экономики, подъема нации, образования, культуры являются информационный потенциал, отвечающий самым строгим меркам научно-технического прогресса. Высокие интеллектуальные технологии в сфере информатизации превращаются в сильный фактор, активно влияющий на развитие человечества. Надлежащее состояние информационного дела повышает уровень правовой защищенности человека. Новые технологии способствуют расширению прямых и обратных связей между государством и гражданским обществом.

Сама по себе информатизация нейтральна, но она создает благоприятные условия для проведения структурных государственных реформ. Расширение сферы информационной деятельности, развитие информационных технологий обусловили появление такой отрасли законодательства, как информационное право. Во многих странах мира ученые заявляют о создании самостоятельной отрасли права — информационного права. Необходимо существенное улучшение состояния дел в сфере правовой информатизации. Состояние информационного права отражает роль и место информатизации в жизни страны, отношение к ней со стороны власти и всего общества. Будучи в значительной мере предопределено объемом, характером и назначением всего информационного дела, само информационное право, в свою очередь, воздействует на ход информационных процессов.

В информационном праве огромное количество теоретических и практических нерешенных проблем. Это связано

в первую очередь с недостатком специалистов в данной сфере. Углубленное изучение информационного права необходимо не только юристам, но и огромной армии государственных служащих. Современное государство активно распространяет использование новейших технологий, что позволяет приблизить государственный аппарат к конкретным людям.

Терминология информационного права до сих пор в значительной мере не отработана, хотя в последнее время учеными проделана большая работа в этом направлении. Расследование информационных правонарушений, их профилактика невозможны без унификации подходов в теории информационного права.

Настоящее учебное пособие является относительно кратким изложением научно-теоретического материала по всем темам учебного курса. Некоторые темы излагаются в пособии весьма фрагментарно. Это объяснимо. Во-первых, современное информационное законодательство включает в себя огромное количество важных и необходимых для познания студентами законов и иных нормативных правовых актов. Этот факт не позволяет детально рассматривать в учебнике данные и иные информационно-правовые институты. Во-вторых, авторы учебника рекомендуют для изучения соответствующие нормативные правовые акты, в которых содержатся нормы, регулирующие соответствующие управленческие отношения. Внимательное ознакомление с текстами рекомендуемых законов позволит студентам всесторонне изучить учебный материал. Студентам рекомендуется, основываясь на общих представлениях о сущности той или иной темы, самостоятельно анализировать соответствующие федеральные законы, законы субъектов РФ и иные нормативные правовые акты, рекомендуемые для изучения информационно-правовых институтов.

Необходимо также помнить, что международное право, международные договоры и соглашения, общепризнанные нормы и правовые принципы входят в правовую систему РФ. Поэтому информационное право должно развиваться и с учетом требований международных правовых институтов, на основе принципов «интернационализации» правовых систем мира.

РАЗДЕЛ 1
ОБЩИЕ ПОЛОЖЕНИЯ

Глава 1. Информационное право как отрасль права

1. Понятие информации

Создание современных сложных информационных технологий нового поколения обусловило почти безграничные возможности общества и государства в получении и использовании информации. В результате информация превратилась в важнейший ресурс государства наряду с его другими основными ресурсами — природными, экономическими, трудовыми, материальными.

В философской литературе сложилась устойчивая традиция рассмотрения информации на основе философских категорий отражения и различия (разнообразия). Информация не существует без отражения, как и отражение без информации. Свойство отражения заключается в способности любого объекта воспроизводить некоторые особенности воздействующих на него объектов. Однако для определения понятия информации одной категории отражения недостаточно. Информация имеет место только там, где среди некоторого тождества существует определенное различие. Единицей измерения информации может считаться элементарное различие, т.е. различие между двумя объектами в каком-либо одном фиксированном свойстве. Чем больше в совокупности отличных друг от друга элементов, тем больше эта совокупность содержит информации. Таким образом, информация в философии определяется как

отраженное разнообразие, а именно *разнообразие, которое отражающий объект содержит об отражаемом.*

Выделяются *четыре вида отражения:* в неживой естественной природе (элементарное отражение), в живой природе (биологическое отражение), в обществе (социальное отражение) и в искусственной природе.

Основным формам отражения соответствуют *четыре вида информации:*

— элементарная (в неживой природе);

— биологическая (в объектах живой природы);

— социальная (в обществе);

— технико-кибернетическая (в автоматизированных устройствах).

Как отмечает И.А. Юрченко, особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее. Даже тогда, когда информация отражается сознанием человека, она существует лишь в единстве с определенными нейрофизиологическими процессами, т.е. имеет свой материальный носитель[1]. Следует отметить, что в идеалистическом представлении допускается существование информации самостоятельно, без носителя, например душа человека, информационное поле Земли и т.п.

Социальная информация — это информация, *получаемая и используемая людьми.* Она существует в двух формах — материальная и идеальная. Материальная социальная информация — это «потенциальная» информация, существующая как «вещь в себе». Она присутствует в объектах, испытавших на себе воздействие человека (это, например, техника, другие предметы, созданные человеком, новые сорта растений и породы животных и т.п.). Информация, которую человек извлекает из окружающей среды и отобра-

[1] *Юрченко И.А.* Информация конфиденциального характера как предмет уголовно-правовой охраны: Автореф. дис.... канд. юрид. наук. — М., 2000. С. 15.

жает своим сознанием, превращается в идеальную социальную информацию.

Идеальная социальная информация — это *воспринятое содержание сообщения относительно того или иного факта, передаваемое индивидом или группой таковых в вербальной или любой другой знаковой либо образной форме другому индивиду или группе таковых.* Именно этот вид социальной информации является объектом правового регулирования. То есть правовое регулирование информации как предмета возможно, только если эта информация отображена человеком.

В конце 50-х гг. один из основоположников кибернетики Н. Виннер определил информацию как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде»[1]. В данном определении ученый впервые затрагивает проблему неполноты получаемой индивидом информации, с одной стороны, а с другой — необходимость защиты сведений от «случайностей внешней среды».

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводит в юридическую сферу понятия, ранее применявшиеся в кибернетике и информатике.

Кроме того, для того чтобы информацию можно было подвергнуть правовому регулированию, она должна обладать соответствующими так называемыми юридическими свойствами.

К юридическим свойствам информации[2] относятся следующие.

1. Физическая неотчуждаемость — информацию невозможно отделить от материального носителя. Например, если

---

[1] *Виннер Н.* Кибернетика и общество. — М., 1958. С. 31.

[2] Подробнее о юридических свойствах информации см.: *Копылов В.А.* Информационное право: Учебник. — М.: Юрист, 2002. С. 49-51.

человек сочинил стихотворение или написал рассказ и хочет его продать, эта информация не исчезнет у него после совершения сделки, как если бы он продал машину или шкаф; таким образом, отчуждение информации заменяется передачей прав на ее использование.

2. Обособленность — информация для включения в гражданский оборот используется в виде символов, знаков, таким образом обособляется от производителя и существует отдельно.

3. Двуединство информации и носителя — заключается в том, что информация — это вещь на материальном носителе.

4. Распространяемость (тиражируемость) — возможность распространения неограниченного количества экземпляров без изменения содержания информации.

5. Организационная форма информации — документ.

6. Экземплярность — существование информации на отдельном материальном носителе, отсюда учет количества экземпляров через учет количества носителей.

Конечно, правовое понятие информации несколько уже, чем философское. Так, ст. 2 Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» дает следующее определение: **«Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»**[1]. Новый Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»[2] (далее — Закон об информации) в ст. 2 расширил понятие «информация»: «Информация — сведения (сообщения, данные) независимо от формы их представления). В приведенном контексте термин «информация» становится универсальным, он обозначает любые сведения о ком-либо или о чем-либо, получаемые из любого источника в любой форме: письменной, устной, визуальной и т.п. В дан-

[1] СЗ РФ. 1995. № 8. Ст. 609; 2003. № 2. Ст. 167. (утратил силу)
[2] СЗ РФ. 2006. № 31. (часть I). Ст. 3448.

ном определении сведения понимаются как реальные объекты социальной жизни: лица, предметы, факты, события, явления, процессы. Эти сведения могут служить и объектом познания, и ресурсом пополнения информационной базы: с одной стороны, сведения могут быть получены в результате исследования окружающей действительности и приобщены к уже существующей объективной системе знаний о мире, а с другой — быть объектом поиска, производимого конкретным потребителем для достижения его целей.

2. Виды информации. Документированная и недокументированная информация

Существует множество критериев классификации информации. Кроме исследователей, работающих в сфере кибернетики, экономики и информатики, попытки рассмотреть структуру информации предпринимают специалисты по массовым коммуникациям и социальному управлению. Так, например, Б. Евладов выделяет четыре основных вида информации: контрольно-измерительную, учетно-статистическую, научно-техническую и общественно-политическую. Контрольно-измерительная информация — та, которая связана с постоянным техническим контролем на производстве, и та, которая добывается в естественно-научных исследованиях. Она фиксируется приборами и первичными учетными документами (таблицами, перфокартами и т.п.) и используется в целях регуляции процессов. Учетно-статистическая информация включает в себя данные, которые поступают главным образом в цифровом виде и отражают развитие экономики, культуры, здравоохранения, образования и т.д. Так, например, при решении комплексных задач государственного и хозяйственного управления в сфере природопользования находят широкое применение разного рода кадастры, реестры и регистры в области водного, лесного и рыбного хозяйства, геодезии и картографии, геологии и экологии, гидрометеорологии, землеустройства и землепользования, стройиндуст-

рии, а также данные государственного учета ресурсов животного и растительного мира. Наиболее полное отражение статистическая информация находит в специфических отчетах, используемых в сфере управления. Научно-техническая информация включает в себя разнообразные данные, характеризующие состояние тех или иных наук, технические достижения. Эта информация отражается обычно в массе специальной литературы по разным отраслям науки, промышленного и сельскохозяйственного производства и используется в основном узким кругом специалистов этих отраслей. Общественно-политическая информация — сведения, рождаемые в повседневной экономической, политической и культурной жизни общества[1].

По степени организованности (упорядоченности) информацию можно разделить на документированную и недокументированную.

В трех федеральных законах дается понятие документированной информации. В одном случае (в узком смысле слова) документированная информация — это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими ее идентифицировать, определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель (ст. 2 Закона об информации). В другом (широком смысле слова) — под документом понимается материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования (ст. 1 Федерального закона от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов», ст. 1 Федерального закона от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле»).

[1] Цит. по: *Коган В.З.* Человек в потоке информации. — Новосибирск, 1981. С. 18.

Таким образом, документированная информация — это особая организационная форма выражения информации.

Информационные ресурсы составляют определенные документы или массивы документов, имеющие реквизиты.

Недокументированная информация остается за пределами правового регулирования.

Кроме того, по категориям доступа информация делится на:

1) информацию с ограниченным доступом, которая, в свою очередь, делится на:

— информацию, существующую в виде государственной тайны;

— информацию, существующую в виде конфиденциальной информации;

2) открытую (общедоступную) информацию.

Следует подчеркнуть, что исходя из подхода, предполагающего обязательное наличие субъекта, воспринимающего информацию, закрытой информации не бывает; так, это означало бы, что существует информация не известная никому, т.е. информация без субъекта, ее воспринимающего.

К открытой информации относится: вся неправовая информация, а также информация о выборах и референдуме; официальные документы, обязательно представляемая информация.

Статья 5 Закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»[1] определяет перечень сведений, составляющих государственную тайну. Перечень сведений, составляющих государственную тайну, конкретизируется в утвержденном Указом Президента РФ Перечне сведений, отнесенных к государственной тайне[2].

К *сведениям конфиденциального характера* в соответствии с Указом Президента от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» отнесены:

---

[1] СЗ РФ. 1997. № 41. Ст. 4673; 2003. № 46 (часть II). Ст. 4449; 2004. № 27. Ст. 2711; № 35. Ст. 3607.

[2] СЗ РФ. 1998. № 5. Ст. 561; 2005. № 39. Ст. 3925

персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на: 1) информацию, свободно распространяемую; 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению; 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Информация делится по роли в системе права на правовую и неправовую.

Определение сущностной характеристики и содержание термина «правовая информация» даны как в широком, так и в узком смысле. Иногда под правовой информацией понимается только информация, которая содержится в нормах права. Более широкое понимание предполагает понимание правовой информации как совокупности сведений о праве, всех процессах и явлениях, с ним связанных. Наблюдается тенденция использовать этот термин в еще более широком значении. Им наряду с имеющимся информационным фондом обозначается также и совокупность норм, знаний и информации, определяющих поведение личности и различных социальных групп в правовой сфере. Здесь уже правовая информация рассматривается под углом социального механизма действия права, который зависит от многих факторов.

Таким образом, уровень доступности правовой информации, в частности законодательства, — один из важнейших показателей правовой культуры любого общества, способный влиять на функционирование всех элементов механизма социального действия права. Он определяется не только состоянием правовых норм, их систематизированностью и т.д., но и факторами, находящимися в сфере правовой культуры личности, функционирования каналов правового информирования граждан, в том числе Интернета.

Понятие доступности правовой информации может быть охарактеризовано и в широком смысле. В этом случае в его содержании следует различать два аспекта: предпосылки знания

личностью содержания юридических норм и результат реализации этих предпосылок, определенный уровень знания права, достигнутый в обществе.

Обеспечение доступности правовой информации, контроль за ее состоянием — это обязанность государства. К этому его обязывает необходимость формирования статуса гражданина демократического общества, предполагающего информированность по всем важнейшим вопросам общественной жизни.

Представляется возможным выделить следующие факторы доступности правовой информации[1] с использованием Интернета.

Это прежде всего качественный уровень правовой информации. К числу факторов, влияющих на качество информации, В.М. Боер относит следующие[2]:

— научность и объективность. Научность предполагает ее соответствие требованиям объективных закономерностей развития общества, обобщенности, систематичности, скоординированности ее потоков и каналов. Научность, объективность правовой информации должна быть неразрывно связана с жизнью, практикой создания гражданского общества, реализацией современных задач;

— достоверность. Данное качество воспитывает чувство ответственности. Условиями достоверности являются плюрализм мнений, критика правовой реальности устаревших законов. Достоверность — предпосылка доверия личности к государству, необходимое средство формирования правовой культуры, повышения социальной активности членов общества;

— конкретность (информация должна иметь конкретного адресата);

— полнота (сведения должны отличаться разнообразием);

---

[1] *Коган В.З., Уханов В.А.* Человек: информация, потребность, деятельность. — Томск: Изд-во Томского ун-та, 1991. С. 130.

[2] *Боер В.М.* Правовая информированность и формирование правовой культуры личности (вопросы теории): Дис. ... канд. юрид. наук. — СПб., 1993. С. 44

— достаточность — возможность из данного информационного сообщения уяснить суть, сформировать определенные навыки, неоднократно воспроизвести некоторые положения для лучшего усвоения, разъяснить термины;

— актуальность и новизна. Своевременное поступление к гражданам информации позволяет быстро и эффективно решать необходимые задачи, формировать общественное мнение. Ее отсутствие влечет невозможность в полной мере реализовать права граждан. Эффективному управлению правовыми процессами может служить только систематизированная, комплексная правовая информация, которая сочетает в себе различные сведения, исторически и логически увязанные, поступающие в определенном порядке и последовательности. Соблюдение этого требования позволит личности видеть явление во всей его сложности и многообразии в общей системе права, корригировать его функционирование и развитие соответственно каждой конкретной ситуации;

— оптимальность, точность, лаконичность.

Правовая информация создается в результате правотворческой, правоприменительной и правоохранительной деятельности. Она делится на:

а) нормативную, т.е. содержащую нормы права (например, закон);

б) ненормативную, т.е. не содержащую норму права (например, приговор суда).

Неправовая информация создается не как результат правотворческой деятельности, обращается в обществе с предписанием правовых норм.

Неправовая информация, в свою очередь, делится на:

а) массовую информацию (содержится в СМИ, например);

б) информацию, являющуюся объектом гражданских прав.

3. Предмет информационного права

Сущность и характер общественных отношений, возникающих между различными субъектами в информационной сфере, во многом определяются особенностями и юридическими свойствами информации — основного объекта, по поводу кото-

рого и возникают эти отношения. Объект информационных отношений обладает несомненными специфическими свойствами. Данная специфика предопределена многоаспектностью и многогранностью самого понятия «информация». Соответственно информационные отношения, как правило, не выступают в чистом виде. Чаще всего они «сопровождают» другие отношения в сфере управления, государственного строительства, международного сотрудничества, в области экономики, жизни граждан и т.д. Процессы этого «сопровождения» все чаще и чаще регламентируются законодательными и иными нормативными актами: устанавливаются обязательность предоставления соответствующих видов информации, порядок ее распространения, правила доступа к ней и ограничения, ответственность за определенные правонарушения, обеспечение информационной безопасности и т.д. Отношения, складывающиеся между участниками этих процессов, в реальной правовой действительности обособляются и тем самым переходят в категорию *предмета информационного права*.

Процесс расширения границ информатизации современного общества, всех его государственных и негосударственных структур приводит к расширению сферы отношений, регулируемых нормами информационного права. Содержание таких отношений определяется постепенно под воздействием внешних объективно происходящих и исторически обусловленных процессов социально-экономического, политического и иного характера.

Предмет информационного права — часть общественных отношений, которая связана с созданием, оформлением, хранением и обработкой, распространением, использованием информационных ресурсов, связывается с развитием в области формирования и управления информационными ресурсами,, с развитием и использованием новых технологических работ с информацией и технологиями ее передачи в системах и сетях коммуникаций, с установлением мер по обеспечению безопасности в информационных сферах и включает в себя юридическую ответственность в названных областях.

Предметная область информационного права включает в себя процесс информатизации — организацию социально-экономических и научно-технических оптимальных условий для удовлетворения информационных потребностей и реализации прав субъектов на основе формирования и использования информационных ресурсов.

Информационное право — совокупность правовых норм, относительно охраняемых государством, возникающих в информационной сфере производства, преобразования и потребления информации. Право является информационной системой, следовательно, информационное право изучает и информационную сущность права.

4. Особенности формирования информационного права

Благодаря техническим и технологическим процессам сегодня быстро осуществляются накопление информации, информационный обмен, информационное взаимодействие как в пределах одного государства, так и межгосударственные. Повсеместное же внедрение информационных телекоммуникационных технологий и основанных на них информационных телекоммуникационных сетей привело к формированию глобального межгосударственного информационного виртуального пространства, в котором информация вращается в непривычной для традиционного права электронной форме. Формируется мировое информационное пространство, закладываются основы перехода к открытому информационному обществу.

В информационном обществе резко возрастает роль права как главного механизма регулирования общественных отношений. Однако информационное общество развивается такими стремительными темпами, что право отстает от его потребностей, и потому многие общественные отношения, уже действующие в информационной сфере (в первую очередь в информационных сетях, например Интернете, и в условиях применения других информационных технологий), остаются неурегулированными.

Лавинообразно нарастающие потребности информационного общества в правовом регулировании возникающих в нем общественных отношений приводят к формированию новой комплексной отрасли права, называемой ныне информационным правом. Особенности структуры и содержания информационного права определяются особенностями основных составляющих это право элементов.

Обоснованным является утверждение, что в эпоху персональных компьютеров и сетевых информационных технологий информационная сущность процессов управления в социальных системах приобретает все большее значение. И это положение должно быть включено в объект исследования всех социально ориентированных наук, включая как общую теорию права, так и отдельные его отрасли. Кстати, в современном понимании законотворческие процессы в своей реализации все более приближаются к виду специальных информационных технологий. А в правоприменительной сфере некоторые отрасли права, например то же административное право или таможенная и налоговая деятельность, уже просто немыслимы без компьютерных технологий ведения соответствующих документальных массивов.

Стремительно развивающаяся тенденция перехода к информационному обществу придает особую актуальность исследованиям информационного содержания социальных процессов, попадающих в сферу интересов права, а формы представления, движения, использования соответствующей информации необходимо активно включать в совокупность объектов правовых исследований. Именно здесь заложено обоснование объективности выделения информационного права в самостоятельную комплексную отрасль.

Таким образом, информационное право включает в себя многие правовые проблемы административного права, фокусируя их в плоскости регулирования информационных отношений, которые становятся иногда для административного права специфическими и недоступными для разрешения собственными средствами.

В последние годы в связи с развитием машинных информационных технологий в сфере социального управления происходит своеобразное вытеснение многих вопросов информационного обеспечения из сферы, традиционно принадлежащей административному праву. Основой таких процессов является нарастающая дифференциация процессов информационного обеспечения принятия решений в сфере государственного управления (использования баз и банков данных, «ситуационных комнат» и т.п.). Одним из основополагающих принципов информационного обеспечения для сферы государственного управления в демократизирующемся обществе становится требование «информационной прозрачности» административной системы. Таким образом, вся процедура информационного обеспечения административной системы перемещается в область информационного права.

Кроме того, формирование информационного права тесно связано с формированием информационного общества. Выделим особенности формирования информационного общества.

1. Наличие информационной инфраструктуры (трансграничные информационно-телекоммуникационные сети и информационные ресурсы в них).

2. Массовое применение персональных компьютеров и подключение их к трансграничным информационно-телекоммуникационным сетям.

3. Подготовка членов общества к работе на компьютерах в трансграничных информационно-телекоммуникационных сетях.

4. Новые формы и виды работы в трансграничных информационно-телекоммуникационных сетях и виртуальном пространстве.

5. Возможность практически мгновенно получать из трансграничных информационно-телекоммуникационных сетей информацию.

6. Возможность мгновенно общаться.

7. Интеграция СМИ и трансграничных информационно-телекоммуникационных сетей.

8. Отсутствие географических и геополитических границ государств, участвующих в трансграничных информационно-телекоммуникационных сетях.

Для достижения цели формирования новой цивилизации необходимо ликвидировать разрыв в области информационных технологий, изменить методы взаимодействия между государствами в целях продвижения социального прогресса. Чтобы достичь этой цели, нужно построить новые правила поведения и новые правила взаимоотношений между субъектами. Практика правового регулирования информации как предмета правовых отношений позволяет сделать вывод о том, что этот вопрос не может быть урегулирован в одной из так называемых классических отраслей права.

Основные отграничения информационного права от других отраслей.

1. Значительный массив законодательства.

2. Экономическая и социальная заинтересованность государства в развитии информационных отношений.

3. Возникновение и бурное развитие правоотношений в информационной сфере, влекущие за собой постоянное расширение отношений субъектов и объектов.

4. Наличие самостоятельного предмета правового регулирования.

5. Международный характер информационного права

Информационное общество размывает государственные границы, следовательно, правовое регулирование информационных отношений обладает международной составляющей. Это проявляется в появлении большого количества межнациональных правовых норм.

Российская Федерация ратифицировала Федеральным законом от 30 марта 1995 г. № 37-ФЗ «О ратификации Устава и Конвенции Международного союза электросвязи»[1] Устав[2] и Конвенцию Международного союза электросвязи, подписан-

[1] СЗ РФ. 1995. № 14. Ст. 1211.

[2] Бюллетень международных договоров. 1997. № 3. С. 3.

ную в Женеве 22 декабря 1992 г.[1] Осуществление связи с помощью Интернета и других телекоммуникационных сете? подпадает под определение электросвязи, данное в Уставе Международного союза электросвязи. В его п. 1012 зафиксировано, что электросвязь — это «любая передача, излучение или прием знаков, сигналов письменного текста, изображений и звуков или сообщений любого рода по проводной, радио-, оптической или другим электромагнитным системам».

Устав Международного союза электросвязи предусматривает следующие положения.

1. Государство обязано обеспечить передачу сообщений от населения при помощи международной службы общественной корреспонденции с предоставлением по каждой категории корреспонденции одинаковых условий обслуживания, тарифов и гарантий без предоставления какого-либо приоритета или предпочтений (ст. 33 Устава).

2. Государство вправе прервать любую «частную электросвязь, которая могла бы представлять угрозу безопасности государству или противоречить его законам, общественному порядку или правилам приличия» (ст. 34 Устава).

3. Государство вправе прекращать службу международной электросвязи вообще или для отдельных видов электросвязи либо корреспонденции с немедленным уведомлением других членов Союза международной электросвязи (ст. 35 Устава).

4. Не принимается никакая ответственность «по отношению к пользованию службами международной электросвязи, в частности в отношении претензий по возмещению убытков» (ст. 36 Устава).

5. Принимаются меры для сохранения тайны международных сообщений, с резервированием за государством права передавать эти сообщения компетентным властям во исполнение внутреннего законодательства либо международных соглашений (ст. 37 Устава).

---

[1] Бюллетень международных договоров. 1997. № 3. С. 30.

Данные положения являются базовыми при изучении правового статуса общедоступных сетей электросвязи, в том числе международной сети «Интернет».

Другим международным актом, определяющим принципиальный подход России к политике развития и правового регулирования процессов информатизации, среди которых ведущим следует признать процесс расширения доступности и информационной наполненности сети «Интернет», является Окинавская хартия глобального информационного общества, принятая на совещании «стран восьмерки» 22 июля 2000 г.[1] Участники данного договора подтверждают приверженность принципу участия людей во всемирном информационном процессе (ликвидации международного разрыва в области информации и знаний (цифрового разрыва)): все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость последнего основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей.

Данная Хартия провозглашает также принцип содействия развитию конкуренции в телекоммуникационной сфере, защиты прав интеллектуальной собственности на информационные технологии, развития трансграничной электронной торговли в контексте жестких рамок Всемирной торговой организации (ВТО), продолжение практики освобождения электронных переводов от таможенных пошлин до тех пор, пока она не будет рассмотрена вновь на следующей министерской конференции ВТО, развитие механизма защиты частной жизни потребителя, а также электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

Рядом международных соглашений предусматривается информационный обмен путем передачи данных. Это, в част-

[1] Дипломатический вестник. 2000. № 8.

ности, заключенное в рамках Содружества Независимых Государств Соглашение об обмене экономической информацией от 26 июня 1992 г.[1], Соглашение о межгосударственном обмене научно-технической информацией от 26 июня 1992 г.[2], Соглашение об обмене правовой информацией от 21 октября 1994 г.[3], Конвенция о сотрудничестве в области культуры, образования, науки и информации в Черноморском регионе, подписанная в городе Стамбуле 6 марта 1993 г.[4], и др.

Кроме этого, сотрудничество по развитию трансграничных коммуникаций предусматривается двусторонними договорами РФ. Среди них соглашения о сотрудничестве в области информации и вычислительной техники с Правительством Французской Республики от 15 февраля 1996 г.[5], Правительством Республики Беларусь от 27 февраля 1996 г.[6] и др.

Правовое обеспечение государственной информационной политики реализуется в рамках информационного права. В настоящий момент международное сообщество делает особый акцент на развитие отдельных государств в информационной сфере, что позволит обеспечить информационную безопасность общества, личности, отдельно взятых государств, кроме того, позволит отладить внутригосударственное законодательство.

6. Комплексный характер информационного права

Суть: нормы информационного права имеют вторую прописку.

1. Нормы информационного права регулируют отношения в основных отраслях права.

---

[1] Бюллетень международных договоров. 1993. № 6. С. 39-40.

[2] Указ. соч. С. 33-35.

[3] Указ. соч. 1995. № 2. С. 34-36.

[4] Treaty Series. Volume 1861. — New York: United Nations, 1999. P. 436-441.

[5] Бюллетень международных договоров. 1996. № 6. С. 48-51.

[6] Указ. соч. № 8. С. 42-45.

2. Одновременно входят во вторую отрасль правового информирования. Информационное право входит в семейство отраслей административного права, которое выражается в следующем.

Информация уже достаточно давно рассматривается как ресурс для самых различных видов социальной деятельности, в числе которых и государственное управление. Для характеристики роли информации в государственном управлении следует обратить внимание на то, что она одновременно выступает в нескольких качествах. С одной стороны, информация необходима для осуществления качественного управления любой сферой общественной жизни, т.е. она является особым ресурсом государственного управления[1]. С другой стороны, деятельность в сфере информации, как и любой другой социальный процесс, является объектом государственного управления, и существует установленный законодательством круг субъектов, которые это управление осуществляют. Кроме того, многие ученые отмечают, что правовые акты и иные решения, принимаемые органами власти, являются информацией особого вида, т.е. процесс управления понимается как частично или полностью информационный[2], а информация оценивается как результат деятельности органов власти. И наконец, в настоящее время в ряде исследований выделяется информация как средство управляющего воздействия на социальный процесс[3].

Таким образом, информация является:

а) особым ресурсом государственного управления;

б) объектом государственного управления;

---

[1] См., например: *Бачило И.Л.* Организация советского государственного управления. — М., 1984. С. 114—133.

[2] См.: *Кудрявцев Ю.В.* Нормы права как социальная информация. — М., 1989; *Тихомиров Ю.А.* Публичное право. — М., 1995. С. 198-199.

[3] См.: *Кульба В.В., Малюгин В.Д., Шубин АЛ., Вуе М.А.* Введение в информационное управление: учебно-методическое издание. — СПб., 1999. С. 13-14.; *Лопатин В.Н.* Концепция развития законодательства в сфере обеспечения информационной безопасности РФ (проект). '• — М., 1998. С. 113-121; *Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С.* Информационное оружие как геополитический фактор и инструмент силовой политики. — к., 1997. С. 7-18.

в) результатом деятельности органов власти;

г) средством управляющего воздействия на социальный процесс.

В последующие годы с развитием информационных технологий основным принципом информационного обеспечения должна стать «информационная прозрачность», что потребует четкого государственного регулирования информационных процессов.

Взаимосвязь информационного права с конституционным правом, правом граждан на информацию обеспечивается Конституцией РФ. Свобода массовой информации гарантируется нормами Конституции. Пределы осуществления права на информацию регулируются нормами конституционного и административного права одновременно.

Взаимосвязь информационного права с гражданским правом выражается в том, что информация может выступать объектом гражданско-правовых отношений в условиях рыночной экономики, и потому часть информационных отношений регулируется нормами гражданского права. Вопросы авторского права, интеллектуальной собственности являются институтами гражданского права.

Все это позволяет более наглядно обосновывать тезис о комплексности информационного права.

7. Методы информационного права

Метод отрасли права — это характер волеизъявления одного субъекта правоотношений в отношении другого. Любая отрасль права использует следующие методы в качестве правового регулирования:

— предписания;

— запреты или дозволения.

В информационном праве используется вся совокупность способов регулирующего воздействия на информационные правоотношения, т.е. как диспозитивное регулирование (свобода выбора, равенство сторон, децентрализация, координация), так и императивное регулирование (центра-

лизованное осуществление властных полномочий, строгая субординация).

Включенность различных методов в систему информационного права не означает их произвольного столкновения или конкуренции. Дискуссии по вопросам значительности тех или иных методов для информационного права можно примирить, только выработав самостоятельную правовую систему для разрешения проблем, возникающих в отношениях информационного свойства.

8. Правовое регулирование информационных отношений за рубежом

Глобальное информационное сообщество основано на фундаментальном компромиссе: с одной стороны, его существование требует передачи огромных массивов информации, с другой стороны, если не обеспечивается соответствующий контроль, могут быть существенно нарушены частные права. Защита частных интересов должна основываться на следующих принципах:

— тот, кто собирает информацию, должен поставить в известность потребителя о том, какая информация собирается и как с ней предполагается поступить;

— тот, кто собирает информацию, должен обеспечить возможность для потребителя ограничить использование персональной информации. Вопросы, связанные с защитой частных интересов, решаются во многих странах мира на уровне законов, принципов саморегуляции и административных мер. Различие в подходах может вызвать нарушение трансграничного обмена информацией. Так, Европейское сообщество приняло директиву, которая запрещает обмен персональными данными с теми странами, где, по его мнению, не обеспечена необходимая защита персональных данных лиц, проживающих в странах ЕС. США намерены обсуждать вопросы обмена персональными данными со своими торговыми партнерами с целью выработки решений на основе рыночных механизмов для недопущения блокирования информационных потоков.

США являются пионером по практическому осуществлению информационной инфраструктуры — впервые создана основа информационного общества.

В 1993 г. Правительство США выпустило доклад с планами развития национальной информационной инфраструктуры, была создана рабочая группа по информационной инфраструктуре.

В соответствии с этим докладом в США было утверждено строительство информационной супермагистрали как технического средства, позволяющего каждому найти нужную информацию. Под информационной супермагистралью понималась совокупность всех технологий, связанных с информацией:

— телевидение;
— компьютерные сети;
— спутниковое вещание;
— технологии on-line;

В феврале 1996 г. в США издан Закон о телекоммуникациях — самый квалифицированный документ, регулирующий информационные отношения.

Администрация США рассматривает вопрос о защите персональных данных как имеющий критическое значение и полагает, что частные усилия предпринимателей и потребителей предпочтительней вмешательства власти. Тем не менее, если эти усилия не приведут к эффективному решению проблемы, правительство пересмотрит свою политику в данном вопросе.

Политика США в области безопасности

Если не будут соблюдены требования к конфиденциальности информации в Интернете, то это поставит под сомнение развитие электронной коммерции в целом. Необходимо обеспечить безопасность и надежность телекоммуникационных сетей, а также подготовку пользователей глобальной информационной инфраструктуры, которые понимают, как защищать свои системы и данные. Для обеспечения этих требований Администрация США поддерживает развитие самостоятельных, действующих на рыночных принципах криптографических инфраструктур,

которые будут обеспечивать идентификацию, целостность и конфиденциальность. Тем не менее Администрация работает совместно с конгрессом над разработкой законодательства, которое будет способствовать развитию криптографических инфраструктур. *В области телекоммуникационных инфраструктур* и *информационных технологий* Администрация США формулирует несколько принципов, которые должны служить основой национальных политик:

— поддержка частных инвестиций путем приватизации подконтрольных государству телекоммуникационных компаний;

— развитие и поддержка конкуренции с помощью обеспечения конкурентных условий на монопольных рынках телефонных сетей, обеспечение приемлемых тарифов при межсетевых подключениях, открытие рынков для иностранных инвестиций и обеспечение антитрестовских мер;

— гарантирование открытого доступа к сетям на недискриминационной основе;

— внедрение на основе независимой регуляции проконкурентного управления, которое шагает в ногу с развитием технологий.

Политика США в области информационного «содержимого» Интернета

Несмотря на то что становятся доступными технологии «фильтрации», содержание ресурсов в Интернете не должно регулироваться по тем же правилам, как на радио и телевидении. Ненужное регулирование будет наносить вред развитию и многообразию Интернета. Исходя из этого Администрация США будет поддерживать саморегуляцию в этой области, внедрение конкурентных рейтинговых систем и развитие легкоприменимых сетевых решений по блокированию информации. В проведении своей политики Администрация придерживается следующих четырех приоритетов.

Регулирование содержания. Администрация озабочена различием государственных подходов к этой проблеме и со-

бирается вести диалог со своими ключевыми партнерами в мире по поводу политики в отношении к оскорбительным высказываниям, пропаганде насилия, антиправительственной агитации, порнографии и другим формам «вредного» содержания в Интернете, с тем чтобы различия в регулировании, особенно те, которые определяются культурными традициями, не служили маскировкой торговых барьеров.

Квотированиеиностраннойинформации. Администрация будет вести диалог с другими государствами о том, как, сохраняя культурное и языковое различие, обеспечить многообразие содержания без ограничительных мер.

Регулирование рекламы. В США нет той регуляции, которая принята во многих странах (ограничения по языку, частоте показа, продолжительности и т.п.). По мнению Администрации, подход по принципу «страна происхождения» должен служить основанием для контроля над рекламой в Интернете и убрать препятствия, воздвигаемые национальными законодательствами в качестве торговых барьеров.

Борьбасмошенничеством. Соответствующиефедеральные структуры США рассматривают вопрос о необходимости введения новых правовых норм, направленных на борьбу с мошенничеством. Администрация намерена использовать возможности международного сотрудничества для защиты потребителей и пресечения обманных и мошеннических действий в области коммерции в киберпространстве. В области технических стандартов сам рынок, а не правительства, должен определять стандарты и другие механизмы. Сферы, где необходима выработка соответствующих стандартов:

— электронные платежи;

— безопасность (конфиденциальность, аутентичность, целостность данных, контроль доступа, безотказность);

— инфраструктура услуг безопасности (система сертификации открытых ключей и т.п.);

— системы обслуживания авторских прав;

— видео- и цифровые конференции;

— высокоскоростные сетевые технологии;

— обмен данными и цифровыми объектами.

В целом Администрация США считает, что успех электронной коммерции требует эффективного сотрудничества между частным и общественным секторами, где частный сектор должен лидировать. Участие правительственных структур должно быть осторожным, последовательным и скоординированным. До недавнего времени в законодательстве Соединенных Штатов в области Интернета действовали две основные правовые нормы, принятые в 1996 г. («Telecommunications Act of 1996» как дополнения к Федеральному закону «Communications Act of 1934» в виде нового параграфа 230 «Охрана личного блокирования и защиты от оскорбительных материалов») и касающиеся содержания информационных ресурсов в Интернете. Первая норма определяет, что ни провайдер, ни пользователь интерактивной компьютерной услуги не несут ответственности за содержание информации, публикуемой другим провайдером. Вторая норма снимает с провайдера всякую ответственность за действия по ограничению доступа к информации, которую он расценивает как оскорбительную, лживую, пропагандирующую насилие и т.д., а также за действия по распространению средств, предназначенных для осуществления этих действий. Несмотря на то что подобные подходы были весьма либеральными, общественная реакция оказалась неоднозначной, и эти нормы поначалу были расценены как вмешательство в «суверенитет» пользователей Интернета. Вторым наиболее значимым прецедентом в иностранном законодательстве, регулирующем область Интернета и вопросы электронной коммерции, явился германский «Мультимедийный закон» («О регулировании информационных и телекоммуникационных услуг»), принятый в 1997 г.

В 1995 г. Совет Европы издает резолюцию о стратегии вхождения Европы в информационное общество, учреждается Форум для обсуждения общих проблем становления информационного общества. Результат — каждая из стран Европы обязана иметь программу, посвященную формированию на-

циональной политики в целях построения информационного общества.

В Японии была принята Программа инициативы в отношении США, Китая и России, которая содержит следующие основные положения.

1. Создание сетей INTERNET.

2. Внедрение информационных технологий в открытых сетях.

3. Проведение терминалов кабельных сетей во все школы, а терминалы INTERNET — во все классы.

4. Реорганизация законодательной системы.

5. Развитие электронной коммерции с учетом американской стратегии глобализации информационной инфраструктуры.

6. Развитие глобальных стандартов взаимодействия.

Наиболее последовательными в стремлении регулировать Интернет оказались Китай, некоторые страны Азии и арабские страны. Так, власти Саудовской Аравии воспользовались тем, что у них в стране один единственный провайдер, и без всяких судов запретили деятельность арабских интернет-клубов, базирующихся на том же портале «Yahoo!».

В Китае для доступа в Интернет гражданину нужно получить платную лицензию и указать, какие сетевые ресурсы он намерен посещать — иностранные или отечественные. Провайдеров обязывают фильтровать содержимое иностранных сайтов. В правилах органов государственной безопасности Китая говорится: «Всем организациям и частным лицам запрещается размещать информацию, составляющую государственную тайну, на электронных досках объявлений, в чат-залах или новостных рубриках Интернета». Поскольку понятие «государственная тайна» четко не определено, данное положение является действенной угрозой наказания. Китайцам также запрещено распространять через Интернет какую-либо аудиовизуальную продукцию. При этом отношение властей в Китае к Интернету противоречиво. С одной стороны, они были бы рады «прикрыть лавочку» (и прикрывают —

только в Шанхае закрыто полторы сотни молодежных интернет-кафе), с другой — иностранный бизнес, развивающийся в стране, не может подчиниться столь жестким ограничениям в использовании возможностей Интернета. Поэтому силовые министерства КНР требуют усиления контроля, а экономические ратуют за открытость. Количество граждан КНР — пользователей Интернета почти удвоилось за первые шесть месяцев 2000 г., достигнув 16,9 млн человек.

Таким образом, в глобальном информационном пространстве сложились следующие **модели правового регулирования.**

Континентальная (европейская) модель направлена на обеспечение баланса международным контролем со стороны государства и частной инициативой.

Ее особенностями являются следующие:

— личная инициатива имеет жесткую регламентацию со стороны законодательства;

— на первое место выдвигается развитие услуг по функциональному и практическому информированию граждан.

Кроме того, следует отметить, что существует специфика в правовом регулировании глобального информационного пространства в отдельных европейских странах, например Швеции — стимулирование социальных программ, во Франции — техническое обеспечение.

Другим примером может служить Германия. В отличие от американского подхода германские законодатели возлагают на провайдеров услуг ответственность за содержание, предоставляемое третьей стороной, если они осведомлены об этом содержании и блокирование его технически возможно и обосновано. Здесь в императивной форме провайдеру предписывается обязанность по блокировке «незаконной» информации. Закон также возлагает на провайдеров услуг ответственность за содержание «собственной» информации, которую они предоставляют для использования. Закон освобождает провайдеров услуг от ответственности за содержание, предоставляемое третьей стороной, только в том случае, если они обеспечивают только доступ к информации. Закон ФРГ содержит также существенные положе-

ния, касающиеся электронной коммерции, обязывает поставщика товара или услуг предоставлять потребителю необходимые данные о себе, определяет принципы, соблюдение которых требуется при работе с персональными данными, определяет обязанности провайдера по защите данных, а также определяет понятие данных, вытекающих из договорных отношений между провайдером услуг и пользователем (договорные данные), и действия, которые провайдер должен совершить с текущими данными и данными для расчетов. Этот опыт в регулировании вопросов, связанных с электронной коммерцией, повлиял на европейскую политику в данной области.

Характерные черты англо-американской модели:

— полная либерализация рынка информационных технологий;

— контроль государства сведен до минимума, частная инициатива поддерживается максимально;

— главная цель правового регулирования — стимулирование обеспечения технического прогресса;

— очень гибкое законодательство;

— информационные технологии ориентированы на развлечения.

Азиатская модель имеет следующие особенности:

— государство участвует в обеспечении крупных вложений в развитие информационных технологий;

— создание как материальных, так и социальных структур;

— основано на иерархичности общества.

Однако в процессе правового регулирования глобального информационного пространства существуют проблемы. К ним относятся:

1) отсутствие единого нормативного регулирования;

2) отсутствие правовой основы разноуровневой интеграции информационного пространства: мировое, региональное, российское, муниципальное;

3) отсутствует ответственность за формирование единого информационного пространства;

4) необходимо создание центра формирования единого информационного пространства;

5) необходимость полноценного мониторинга единого информационного пространства;

6) необходима сертификация информационных продуктов и деятельности субъектов;

7) необходимо законодательное ограничение информационной экспансии.

Глава 2. Информационно-правовые нормы и отношения. Система и источники информационного права

1. Информационная норма: понятие, особенности, виды

Информационно-правовые нормы регулируют обособленную группу общественных отношений применительно к особенностям информационной сферы. Информационно-правовая норма задает содержание прав и обязанностей субъектов, участвующих в правоотношении.

Особенности информационно-правовых норм способствуют реализации информационных прав и свобод, а также реализуют информационные процессы при обращении информации.

Структура информационно-правовых норм не отличается от классического определения и представляет собой:

— гипотезу;

— диспозицию;

— санкцию.

Выделим виды информационно-правовых норм по способу воздействия.

1. Диспозитивные (автору принадлежит право на использование произведения, информация может быть накоплена в государственных и негосударственных ресурсах, информация — товар).

2. Императивные:

а) нормы-определения (ст. 2 Закона об информации);

б) нормы-принципы (ст. 2 Федерального закона от 2 января 2000 г. № 28-ФЗ «О государственном земельном кадастре»);

в) нормы-цели (преамбула Закона);

г) нормы-санкции (КоАП, УК РФ);

д) обязывающие нормы (Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документа»).

Виды информационно-правовых норм:

S по содержанию:

— материальные;

— процессуальные;

S по масштабу действия:

— федеральные;

— субъектов Федерации;

— местные.

2. Информационно-правовые отношения: понятие, виды, соотношение с правовой нормой, структура и защита

Правовые отношения есть урегулированные правом и находящиеся под охраной государства общественные отношения, участники которых выступают в качестве носителей взаимно корреспондирующих друг другу юридических прав и обязанностей[1]. Таким образом, можно попытаться дать определение информационных правоотношений — это общественные отношения, урегулированные правом, субъекты которых являются носителями взаимных информационных прав и обязанностей.

Т.Ш. Иззатов дает более конкретное определение, понимая под информационными правоотношениями процесс це-

[1] См.: Теория государства и права / Под ред. Н.И. Матузова, А.В. Малько. — М., 2004. С. 515.

левого перераспределения в обществе сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления[1].

Регулирование информационных отношений с помощью права осуществляется посредством установления определенных информационно-правовых норм, т.е. путем установления правил поведения субъектов информационных отношений и применения норм информационного права. Информационно-правовые нормы регулируют взаимоотношения граждан, СМИ, организаций, фирм между собой, их взаимные права и обязанности и вследствие этого придают этим регулируемым отношениям особый характер — характер информационно-правовых отношений. Субъекты данных отношений выступают в качестве носителей специфических информационных прав и обязанностей. Поэтому можно сказать, что информационные отношения между самыми разнообразными участниками — гражданами, редакциями газет, телестудиями, предприятиями, организациями, фирмами и другими, в которых последние участвуют в качестве носителей прав и обязанностей, установленных нормами информационного права, называются информационно-правовыми отношениями или информационными правоотношениями.

Информационные отношения возникают, изменяются и прекращаются в информационной сфере и регулируются информационно-правовыми нормами. Являясь разновидностью правовых отношений, они выражают все основные признаки правового отношения[2], а именно:

— первичность информационно-правовых норм;

— идеологический (мировоззренческий) характер, так как возникновение, изменение и прекращение информационных

---

[1] См.: *Иззатов Т.Ш.* Механизм реализации конституционного права граждан на информацию в РФ: Автореф. дис.... канд. юрид наук — М., 2002. С. 11.

[2] Правоотношение — это вид общественных отношений, в которых реализуются урегулированные правом взаимодействия двух и более субъектов (См.: Бачило И.Л. Информационное право: основы практической информатики: Учеб. пособие. — М., 2003. С. 178).

отношений проходит через сознание людей, прежде всего такую его сферу, как правосознание;

— волевой характер, так как информационные отношения всегда являются результатом волеизъявления его сторон или одной из сторон;

— двусторонний или многосторонний характер, т.е. это всегда связь между его участниками через их субъективные права и юридические обязанности;

— взаимосвязанный, корреспондирующий характер отношений сторон, т.е. эти отношения выражаются во взаимных правах, обязанностях и юридической ответственности;

— наличие информационной правосубъектности сторон в информационных отношениях;

— регулирующая роль, заключающаяся в том, что информационные отношения определяют конкретное поведение сторон и вносят элемент урегулированности и порядка в общественную практику, формируя или определяя общественную волю.

Что же касается особенностей информационных отношений, то, как полагает Копылов В.А.[1], они сводятся к тому, что эти отношения:

— возникают, развиваются и прекращаются в информационной сфере при обращении информации;

— опосредуют государственную политику признания, соблюдения и защиты информационных прав и свобод человека и гражданина в информационной сфере;

— отражают особенности применения публично-правовых и гражданско-правовых методов правового регулирования при осуществлении информационных прав и свобод с учетом специфических особенностей и юридических свойств информации и информационных объектов.

Правоотношения — это функция, в которой абстрактная норма приобретает свое реальное бытие.

---

[1] *Копылов В.А.* Информационное право: Учебник. 2-е изд., перераб. и доп. — М.: Юристъ, 2005. С. 98.

Виды правоотношений

1. Правоотношения, возникающие в области поиска, получения и потребления информации (например, правоотношения, регулируемые ст. 29 Конституции РФ).

2. Информация, связанная с производством и распределением исходной и производной информации (правоотношения в сфере СМИ, авторские права в гражданском праве).

3. Информация в области формирования информационных ресурсов и предоставления информационных услуг (например, правоотношения, регулируемые Законом об обязательном экземпляре документа[1], Законом о библиотечном деле[2], Законом об архивном деле в Российской Федерации[3]).

4. Правоотношения в области создания и применения информационных технологий, их сетей и средств их обеспечения (например, право на создание информационных сетей, обязанность заключения договоров на создание таких объектов для государственных нужд).

5. Информация в области обеспечения информационной безопасности (например, право на защиту личной жизни, информации от несанкционированного доступа, защита различных видов тайны).

Кроме того, по степени конкретизации и субъектному составу можно выделить следующие информационные правоотношения: абсолютные, относительные и общерегулятивные. В абсолютных точно определена лишь одна сторона (например, собственник информационных ресурсов, информационных систем, технологий и средств обеспечения, которому противостоят все те, кто с ним соприкасается или может соприкоснуться и которые обязаны уважать это его право), и в этом смысле право собственности есть право абсолютное. В относительных строго определены обе стороны (например, учредитель средства массовой информации

[1] СЗ РФ. 1995. № 1. Ст. 1; 2002. № 7. Ст. 630; 2005. № 23. Ст. 2203.
[2] СЗ РФ. 1995. № 1. Ст. 2; 2004. № 35. Ст. 3607.
[3] СЗ РФ. 2004. № 43. Ст. 4169.

и главный редактор этого же СМИ: они в соответствии с требованиями закона обязаны заключить между собой договор и утвердить устав редакции СМИ)[1]. Общерегулятивные правоотношения выражают юридические связи более высокого уровня между государством и гражданами, а также последних между собой по поводу гарантирования и осуществления основных прав и свобод личности, а равно обязанностей. Они возникают, таким образом, на основе норм Конституции, других основополагающих актов и являются базовыми, исходными для отраслевых правоотношений[2]. В нашем случае это гарантированное в ст. 29 ч. 4 Конституции РФ право: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

Рассмотрим структуру информационного правоотношения.

Субъекты:

— физические лица;
— юридические лица всех форм собственности;
— органы государственной власти;
— должностные лица;
— общественные организации;
— другие субъекты, признаваемые субъектами права.

Информационное право призвано обеспечить достаточность правового регулирования с учетом специфики субъектов, которые участвуют в правоотношении (использование блокиратора на телевидении от детей).

Объект правоотношений — это те явления (предметы) окружающего мира, на которые направлены субъективные юридические права и обязанности. Объектами правоотношений выступают явления (предметы) материального и духов-

[1] См.: Статья 18 Закона РФ от 27 декабря 1991 г. «О средствах массовой информации».

[2] См.: Теория государства и права / Под ред. Н.М. Матузова, А.В. Малько. — М., 2004. С. 513-514.

ного мира, т.е., иными словами, разнообразные материальные и нематериальные блага, способные удовлетворять потребности субъектов[1].

Объект информационного права — это все те материальные, духовные и иные социальные блага, явления и процессы, по поводу которых субъекты информационного права вступают в информационно-правовые отношения, и что является предметом их интересов, прав и обязанностей[2].

Если говорить более определенно, то объектом информационных правоотношений является сама информация в ее многочисленных и многообразных формах, таких, например, как документированная информация: документ, информационные ресурсы, средства обеспечения автоматизированных информационных систем, различные виды конфиденциальной информации.

В информационных правоотношениях основными объектами являются разнообразные информационные ресурсы: печатные издания, газеты, журналы, книги, аудио- и аудиовизуальные материалы, рекламная продукция, компьютерные программы, базы и банки данных, информационные сети и системы, средства связи и т.п. Именно они наиболее часто попадают в поле зрения информационных споров, сделок, договоров.

Поведение субъектов права, их поступки и действия в информационных отношениях также могут быть объектом права. Это может быть, если норма информационного права, регулирующая определенные отношения, закрепляет какие-либо действия. Например, Федеральный закон «О библиотечном деле» запрещает соответствующим государственным органам и должностным лицам принимать решения, ущемляющие законные интересы библиотек и их пользователей под угрозой обращения в суд (ст. 15).

К особой группе объектов информационного права относят нематериальные блага, т.е. не имеющие экономиче-

[1] См.: *Алексеев С.С.* Общая теория права. Т. 2. — М., 1982. С. 154.
[2] См.: *Рассолов М.М.* Информационное право. — М., 1999. С. 47.

ского содержания и не отделимые от личности их носителя блага и свободы, признанные действующим законодательством.[1] Проявление нематериальных благ в качестве информации возможно в тех случаях, когда необходимо защищать честь, достоинство и личную репутацию гражданина, т.е. об информации, которая искажена и не соответствует личностным качествам данного человека. Нематериальные блага характеризуются двумя признаками: отсутствием материального содержания и неразрывной связью с личностью носителя.

Таким образом, основным объектом правоотношений в информационной сфере является информация в ее многочисленных и многообразных материализованных формах, т.е. информация, находящаяся в гражданском, административном или ином общественном обороте, в зависимости от которой возникают общественные отношения, подлежащие правовому регулированию.

Предмет — само произведение, документ, т.е. информационный продукт (информационная технология). Но в некоторых случаях права и обязанности.

Юридический факт (событие или действие)

Чтобы факт (совершившееся действие, событие) превратился в факт юридический, должны быть определенные условия, и важнейшее из них связано с состоянием нормативно-правовой системы национальной, корпоративной или международной. Факты, которые не попадают в правовое поле действующего законодательства, остаются таковыми, существуют, но не превращаются в юридические факты. Например, если нет закона, устанавливающего правовой режим программ для электронно-вычислительных машин, то факт создания таких программ, их использования будет неюридическим до тех пор, пока законом не будет легитимировано существование такого предмета отношений. В Российской Федерации Закон РФ от 23 сентября 1992 г.

[1] См.: *Туманова Л.В., Снытников А.А.* Обеспечение и защита права на информацию. — М., 2001. С. 129-130.

№ 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»[1] был принят в 1992 г., но это не означает, что такие предметы ранее не производились и не потреблялись. Однако строить правоотношения в данной области было сложнее, чем при наличии специального нормативно-правового акта по этому поводу.

Следовательно, для возникновения и реализации правоотношений, в том числе в области информационной сферы, необходимо в качестве объективных условий, во-первых, наличие реальных фактов, связанных с интересами различных субъектов общества, и, во-вторых, наличие нормативно-правовой основы, соответствующих правовых норм, позволяющих ввести отношения по конкретному факту в систему юридических фактов и правовых отношений. Например, ряд ситуаций, возникающих в сетях и системах Интернета, нуждается в правовом регулировании. Отсутствие каких-либо общих международных норм в этой области осложняет дело.

Один юридический факт может породить множество правоотношений (уголовно-правовые отношения, административные, межгосударственные правоотношения) и наоборот: множество правоотношений — один юридический факт (регистрация рождения ребенка — данные о браке, родителях, медицинские документы).

Содержание правоотношения: права и обязанности субъектов. Они зависят от вида информационных правоотношений. Так, например, при производстве такой информации у субъектов — ее производителей возникают следующие права и обязанности[2]:

— право на создание произведений науки и литературы, иной подобного рода информации;

---

[1] Ведомость СНД РФ и ВС РФ. 1992. № 42. Ст. 2325; СЗ РФ. 2002. № 52 (часть I). Ст. 5133; 2004. № 45. Ст. 4377; 2006. № 6. Ст. 636

[2] Перечисленные здесь и ниже перечни прав, обязанностей и ответственности являются приблизительными и могут дополняться и развиваться в реальных условиях.

— право интеллектуальной собственности на результаты творческой деятельности и право вещной собственности на документированную информацию, отражающую эти результаты (право передачи исключительных прав на результаты интеллектуальной деятельности);

— ограничение права на создание документированной информации ограниченного доступа;

— ограничение права на создание вредной, опасной для общества информации;

— обязанность по созданию информационных ресурсов в соответствии с установленной компетенцией и предоставлению информации из них потребителям информации;

— обязанность исполнения условий авторских договоров;

— ответственность за непредоставление информации;

— ответственность за недостоверность создаваемой информации, недоброкачественную и ложную информацию и дезинформацию;

— ответственность за качество информационных ресурсов, информационных продуктов, предоставление информационных услуг;

— ответственность за создание и распространение контрафактных экземпляров.

При производстве массовой информации возникают следующие права и обязанности участников информационных отношений:

— право на создание массовой информации (журналист, редакция);

— право на защиту чести и достоинства (любой член общества);

-— право интеллектуальной собственности на распространяемые СМИ результаты творческой деятельности (автор распространяемой информации);

— обязанность по достоверному, оперативному, полному информированию населения (пользователей Интернета) (редакции и журналисты);

— обязанность по обеспечению гарантий свободы слова (государство);

— ограничение права на распространение информации ограниченного доступа (все участники производства и распространения массовой информации);

— ограничение права на распространение вредной, опасной для общества информации (все участники производства и распространения массовой информации);

— ответственность за недостоверность создаваемой информации, недоброкачественную и ложную информацию и дезинформацию, введение цензуры (все участники производства и распространения массовой информации).

В процессе производства, передачи и распространения такой информации возникают следующие права и обязанности участников таких правоотношений:

— обязанность по производству и распространению (или обеспечению распространения) нормативных правовых актов в соответствии с установленной компетенцией;

— обязанность за предоставление информации из таких документов;

— ответственность за создание официальных документов неудовлетворительного качества.

В информационных процессах по обращению информации с ограниченным доступом возникают следующие права и обязанности:

— обязанность по установлению состава информации ограниченного доступа;

— обязанность по установлению информации, которая не может относиться к категории ограниченного доступа;

— ограничение имущественных прав при отнесении созданной автором информации к государственной тайне;

— обязанность лицензирования деятельности по обработке информации ограниченного доступа;

— обязанность по установлению ограничений по доступу к информации ограниченного доступа;

— обязанность по обеспечению защиты информации и информационных ресурсов, содержащих такую информацию, от несанкционированного доступа;

— ответственность за нарушение условий ограниченного доступа, за разглашение информации ограниченного доступа.

Информационные отношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, основываются на следующих правах и обязанностях их участников:

— право на создание и применение информационных систем, их сетей, средств их обеспечения (все участники этих процессов);

— право интеллектуальной собственности на результаты творческой деятельности при создании таких объектов (физические лица, юридические лица, органы государственной власти и местного самоуправления);

— ограничение права на создание таких объектов для информации ограниченного доступа;

— обязанность создания и применения информационных систем, их сетей, средств их обеспечения в соответствии с установленной компетенцией (государственные структуры);

— обязанность по заключению и исполнению договоров на создание таких объектов для государственных нужд (физические лица, юридические лица, органы государственной власти и местного самоуправления);

— ответственность за недоброкачественность созданной продукции, нарушение сроков исполнения договора, другие нарушения.

Информационные отношения в сфере обеспечения информационной безопасности основаны на следующих правах и обязанностях их участников:

— право на защиту личности от воздействия недостоверной, ложной информации;

— право на защиту информации, информационных ресурсов, продуктов от несанкционированного доступа;

— право на защиту интеллектуальной собственности;

— право на защиту информационных систем, информационных технологий и средств их обеспечения как вещной собственности;

— право на защиту информационных прав и свобод;

— ограничение права на раскрытие личной тайны, а также иной информации ограниченного доступа без санкции ее собственника или владельца;

— обязанность по защите государства и общества от вредного воздействия информации, защите самой информации, по защите прав личности, по защите тайны;

— ответственность за нарушение информационной безопасности, в том числе прав и свобод личности, тайны и других ограничений доступа к информации, за компьютерные преступления.

Существует два способа защиты информационных правоотношений:

— защита в административном порядке;

— защита в судебном порядке.

3. Система информационного права

Система информационного права как учебной и научной дисциплины включает в себя 4 раздела.

1. Общие положения. Включает в себя такие составляющие, как понятие и виды информации, субъекты информационного права, система информационного права, взаимосвязь информационного права с другими отраслями права и т.д.

2. Государственное регулирование информационной сферы.

Правовые режимы информационных ресурсов, порядок создания и применения информационных технологий, международный информационный обмен, информационный рынок (электронная коммерция), внутриорганизационное управление с использованием информационных систем, регулирование средств массовой информации, права граждан в информационной сфере, архивное и библиотечное дело.

3. Информационная безопасность.

Обеспечение безопасности личности, государства, общества и в глобальном информационном пространстве.

4. Ответственность в информационной сфере:
— уголовная;
— административная;
— дисциплинарная;
— гражданско-правовая.

4. Виды источников информационного права

В связи с тем что главными особенностями информационного права является его комплексный и международный характер, источники информационного права можно разделить на:

— международно-правовые нормативные акты;
— Конституцию РФ;
— нормативно-правовые акты в составе информационного права;
— нормативные акты других отраслей права.

Информационное законодательство имеет свою систематизацию в государственном классификаторе.

Различают следующие классификации.

1. Законодательство, регулирующее общие положения.
2. Управление в сфере информации и информатизации.
3. Информационные ресурсы пользования.
4. Информатизация, использование информационных технологий.
5. Средства массовой информации.
6. Реклама.
7. Информационная безопасность.

Проанализировав существующую систему информационного права и действующего законодательства, можно сделать вывод о том, что подавляющая часть источников информационного права — это нормативные акты других отраслей права. Поэтому информационное законодательство логично разделить на следующие группы.

1. Об осуществлении права на поиск, получение информации (нормы конституционного права).

2. О гражданском обороте информации.

3. О формировании информационных ресурсов, их подготовке и предоставлении информационных услуг.

4. О создании и применении информационных систем, их сетей, информационных технологий и средств их обеспечения.

5. Об информационной безопасности.

6. О средствах массовой информации.

7. О библиотечном деле.

8. Об архивах.

9. О государственной тайне.

10. О коммерческой, служебной тайне (отсутствует).

11. О персональных данных.

5. Принципы информационного права

Принципы — это зафиксированные в правовых нормах основные начала, определяющие сущность и содержание данной отрасли права, придающие ей системный характер и позволяющие ей говорить о целостности механизма правового регулирования.

Под принципами информационного права будем понимать основные исходные положения, юридически закрепляющие объективные закономерности общественной жизни, проявляющиеся в информационной сфере. Принципы информационного права позволяют формировать это право как самостоятельную отрасль и в этой связи являются системообразующими.

Принципы информационного права базируются на:

— Конституции РФ;

— федеральных законах и других нормативных актах.

Принципы, базирующиеся на Конституции РФ, — общеправовые, а все остальные — специальные.

Выделяют следующие общеправовые принципы.

1. Принцип приоритетности прав.

В информационном праве возможен как приоритет прав личности (ст. 2 Конституции РФ), так и приоритет прав государства, например при столкновении интересов государства и личности в правоотношениях, когда требуется установить

пределы осуществления права на тайну государства и тайну отдельно взятой личности.

2. Принцип законности.

3. Принцип ответственности (за нарушение прав и обязанностей).

Специальные принципы делят на две категории:

— принципы, обеспечивающиеся Конституцией РФ, но имеющие свою специфику в информационном праве;

— принципы, которые формулируются на основе свойств информации.

Принципы, обеспечивающиеся Конституцией РФ, но имеющие свою специфику в информационном праве:

1) принцип свободного производства, распределения, доступа к информации;

2) принцип запрещения производства и распространения информации вредной и опасной для развития личности, общества и государства. Он реализуется через нормы безопасности государства.

Обозначим принципы, которые формулируются на основе свойств информации.

Принцип информационных отношений как отношений, образующих комплексную отрасль информационного права, означает, что информационные отношения, возникающие исходя из особенностей и юридических свойств информации и ее многофункциональности как основного объекта информационного права, обладают на этом основании спецификой, отличающей их от других общественных отношений, и составляют основу общественных отношений в информационной сфере.

Принцип информационной собственности означает, что при передаче и распространении информации как основного объекта информационного права объективно существуют особые категории субъектов информационного права (создатели, обладатели и потребители информации) и их поведение реализуется на основании информационных правомочий — права знать, обладать и применять информацию.

Принцип неотчуждаемости информации от ее создателя, обладателя и потребителя (невозможность лишить субъекта полученных знаний) означает, что механизм отчуждения информации должен заменяться механизмом добровольного отказа от определенных информационных правомочий через установление по договору прав, обязанностей и ответственности по использованию этой информации после ее передачи указанными субъектами.

Принцип информационной вещи, основанный на двуединстве материального носителя и информации, отображенной в нем, означает, что при обращении информационных вещей объективно существуют особые категории собственников информационных вещей (собственники — создатели информационных вещей, собственники — обладатели информационных вещей и собственники — потребители информационных вещей), которые реализуют традиционные правомочия собственников, однако при обязательном соблюдении ими информационных правомочий.

Статья 3 Закона об информации устанавливает следующие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

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

2) установление ограничений доступа к информации только федеральными законами;

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

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

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

6) достоверность информации и своевременность ее предоставления;

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

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Принципы, устанавливаемые законодательством для информационных правоотношений, не являются тождественными принципам информационного права, однако именно они определяют характер информационно-правового регулирования.

Глава 3. Понятие и виды субъектов информационного права

1. Понятие субъектов информационного права (общая характеристика)

Правовой статус субъектов информационного права включает в себя:

— информационную правоспособность;

— информационную дееспособность.

Правовой статус субъектов определяется информационной правосубъектностью, а также правами и обязанностями субъектов, ответственностью, гарантиями осуществления своих прав.

При осуществлении своих информационных прав субъекты информационных правоотношений обязаны действовать разумно и добросовестно (ст. 157, 220, 234 ГК РФ), соблюдая основы нравственности (ст. 169 ГК РФ) и другие принятые в обществе нормы (ст. 241 ГК РФ).

В законах и иных нормативных актах закреплены в настоящее время официальные определения субъектов инфор-

мационных правоотношений. Например, в ст. 2 Закона об информации используются понятия:

— **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;

— **оператор информационной системы** — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

В Законе об обязательном экземпляре документа применяются понятия «производитель документов» и «получатель документов» (ст. 1). В Основах законодательства РФ о культуре от 9 октября 1992 г. приводится определение «Творческий работник — физическое лицо, которое создает или интерпретирует культурные ценности, считает собственную творческую деятельность неотъемлемой частью своей жизни, признано или требует признания в качестве творческого работника, независимо от того, связано оно или нет трудовыми соглашениями и является или нет членом какой-либо ассоциации творческих работников»[1]. В Законе РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»[2] (далее — Закон о СМИ) закреплены понятия «главный редактор», «журналист», «издатель», «распространитель», «редакция». В авторском праве используются понятия «автор», «изготовитель аудиовизуального произведения и фонограммы», «исполнитель». В федеральных законах «О связи» (далее — Закон о связи) от 7 июля 2003 г. № 126-ФЗ[3] и «О библиотечном деле» применяются понятия «пользователи сети» и «пользователь библиотеки» соответственно. В статье 3 Федерально-

[1] См.: Статья 3 Основ законодательства РФ о культуре от 9 октября 1992 г. // Ведомости СНД и ВС РФ. 1992. № 46. Ст. 2615.

[2] Ведомости СНД РФ и ВС РФ. 1992. № 7. Ст. 300; СЗ РФ. 2005. № 30 (часть I). Ст. 3104.

[3] СЗ РФ. 2003. № 28. Ст. 2895; 2005. № 19. Ст. 1752; 2006. № 6. Ст. 636; № 10. Ст. 1069.

го закона от 13 марта 2006 г. № 38-ФЗ «О рекламе»[1] закреплены понятия «рекламодатель», «рекламопроизводитель» и «потребитель рекламы».

По отношению к информации все субъекты можно разделить на три группы.

1. Производители.
2. Обладатели, собственники информации.
3. Потребители.

По общеправовому критерию:

— Российская Федерация;
— субъекты РФ;
— муниципальные образования;
— граждане и другие физические лица;
— общественные объединения;
— коммерческие организации.

Субъектами информационного права могут выступать лица, обладающие только информационной правоспособностью. Но субъектами информационных правоотношений могут выступать только те, которые обладают информационной дееспособностью:

— органы государственной власти и их должностные лица;
— местные органы власти и их должностные лица;
— физические лица;
— юридические лица.

2. Российская Федерация, субъекты РФ и муниципальные образования как субъекты информационного права

Российская Федерация, субъекты РФ, муниципальные образования обладают только информационной правоспособностью, т.е. они являются субъектами права, но не могут являться субъектами информационных правоотношений, так как реализуют их права и обязанности, т.е. обладают информационной дееспособностью, — органы государственной, местной власти и (или) их должностные лица.

[1] СЗ РФ. 2006. № 12. Ст. 1232.

Их правовой статус устанавливается Конституцией РФ и федеральными законами РФ. Являясь гарантом защиты прав и свобод, органы государственной власти обязаны обеспечивать и защищать все без исключения информационные права физических и юридических лиц. Так, Конституция РФ вменяет в обязанность органам государственной власти:

• *S* обеспечивать свободу слова;

• *S* обеспечивать достоверное информирование граждан о состоянии экологии;

S обязательно публиковать нормативные акты, затрагивающие права, свободы и обязанности человека и гражданина;

• *S* обеспечивать свободу массовой информации и не допускать цензуры;

S пресекать действия, направленные на сокрытие данных о фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей;

• *S* обеспечивать бесплатный доступ к знаниям при обучении в государственных и муниципальных образовательных учреждениях и на предприятиях;

• *S* не допускать использование не по назначению конфиденциальной информации, полученной в ходе служебной деятельности.

Органы государственной власти субъектов Федерации обязаны:

• *S* обеспечивать соблюдение принципа идеологического многообразия в общественном сознании жителей региона, т.е. плюрализма идеологий в России и ее регионах[1];

• *S* обеспечивать соблюдение принципа отделения религии от государства;

•/ не допускать пропаганды и агитации, возбуждающих социальную, религиозную, расовую или национальную ненависть и вражду, а также пресекать пропаганду социаль-

[1] См.: Конституция РФ. Научно-практический комментарий / Под ред. Б.Н. Топорнина. — М., 2003. С. 159.

ного, расового, национального или религиозного превосходства (эта обязанность исходит из ч. 2 ст. 29 Конституции РФ);

S в ходе предвыборной кампании обеспечивать кандидатам равные условия в информационной сфере;

S обеспечивать полноту, достоверность, своевременность, открытость статистической информации по всем направлениям жизнедеятельности региона.

Важнейшей информационной обязанностью субъектов РФ является создание региональной государственной информационной системы, интегрированной с Федеральной информационной системой и аналогичными системами других регионов.

Информационной обязанностью субъектов РФ является создание и обеспечение целостности, сохранности, функционирования и развития различных информационных фондов (библиотечного, музейного, архивного, кино-, фото-, художественного и т.п.).

Правила соотнесения информационного поля и полномочий органов власти: применительно к органам власти, к должностным лицам важно установить структуру информационных ресурсов, способы получения информации и использование информации в процессе служебной деятельности.

Задачи деятельности органов власти в информационной сфере:

— информационное обеспечение деятельности органов (работа по структуризации информации и выбор наиболее правильных легитимных средств обработки информации);

— предоставление каждым органом власти информации другим пользователям.

Штат Иллинойс, США. Конституция, ст. Б, раздел I: губернатор, секретарь, контролер, казначей должны обеспечивать хранение официальных документов и постоянно проживать в месте пребывания правительства штатов с целью сохранения документов.

Документ «Постоянные правила Сената США» в редакции 1979 г. предусматривает строгий режим конфиденциальности по вопросам, обсуждаемым сенатом по предложению исполнительной власти.

«Правила административной процедуры» информации:

— бесплатная;

— копируется ограниченно;

— режим допуска.

Выделяют основные направления деятельности органов власти.

1. Отбор информации, необходимый для обеспечения деятельности.

2. Систематизация информации.

3. Подготовка и ведение банков информационных данных.

4. Ответственность за адекватность информационных ресурсов задачам органов власти, а также ответственность за полноту и своевременность сведений и ответственность за использование информации по назначению.

5. Организация информационной системы.

6. Обеспечение безопасности.

3. Граждане и другие физические лица как субъекты информационного права

Субъект права — это лицо, участник общественных отношений, которое характеризуется такими главными признаками, как способность быть носителем субъективных юридических прав и обязанностей, а также способностью участвовать в правоотношениях в силу действующего законодательства[1]. В качестве субъектов информационных правоотношений могут выступать либо отдельные индивиды, либо определенные коллективы людей. Отдельные индивиды — это могут быть не только граждане РФ, но и иностранные граждане и лица без гражданства. Конституция РФ в главе 2 «Права и свободы человека и гражданина» признает и гарантирует права согласс-

[1] См.: *Алексеев С.С.* Общая теория права. Т. 2. — М., 1982. С. 138.

но общепринятым принципам и нормам международного права. Статья 62 Конституции устанавливает, что иностранные граждане и лица без гражданства пользуются в РФ правами и несут обязанности наравне с гражданами России, кроме случаев, установленных федеральными законами или международным договором РФ. Для осуществления своих информационных прав и реализации обязанностей конкретные лица должны обладать правоспособностью и дееспособностью. Правоспособностью здесь будет называться способность лица (журналиста, автора программы для ЭВМ и др.) иметь информационные права и обязанности. Дееспособность будет характеризовать способность лица претворять в жизнь, на практике своими действиями имеющиеся у него информационные права и обязанности.

Очевидно, что правоспособность в информационной сфере имеют все граждане независимо от их пола, возраста, расовой принадлежности, национальности, вероисповедания и происхождения. Однако в информационной сфере правоспособность может быть дополнительно ограничена. Например, Закон о СМИ устанавливает, что не может выступать учредителем средства массовой информации гражданин, не достигший восемнадцатилетнего возраста, либо отбывающий наказание в местах лишения свободы по приговору суда, либо душевнобольной, признанный судом недееспособным[1].

Дееспособность в информационной сфере возникает не у каждого лица, а лишь у тех лиц, которые в силу своей подготовки, способностей, должности и т.п. получают по информационному законодательству возможность лично использовать свои права и принимать на себя обязательства. Например, граждане в возрасте от 14 до 18 лет могут лишь с согласия своих родителей или законных представителей совершать сделки с программными продуктами, с компьютерной техникой, т.е. обладают ограниченной дееспособностью.

[1] См.: Часть 2 ст. 7 Закона РФ «О средствах массовой информации» // Ведомости СНД и ВС РФ. 1992. № 7. Ст. 300.

Однако правоспособность может наступать до рождения (право наследования). Права нерожденных в информационном праве:

1) право на доступ к завещанию;

2) право на защиту здоровья матери от вредной информации.

До 6 лет физическое лицо может иметь следующие права:

1) выходить в Internet с разрешения родителей;

2) пользоваться телефонными услугами с соглашения родителей.

Следует иметь в виду, что на информационно-правовой статус гражданина оказывают влияние специальные административные статусы.

Среди гарантий информационных прав граждан можно выделить следующие:

— создание условий для предотвращения методов психопрограммирования (например, 25-й кадр) в средствах телекоммуникации;

— школьные программы — единообразный информационный ресурс школьникам;

— государственные образовательные стандарты;

— государственные гарантии удовлетворения интересов потребителей средств массовой информации.

4. Правовой статус общественных объединений и коммерческих организаций как субъектов информационного права

Наряду с отдельными индивидами в качестве субъектов информационных правоотношений могут выступать и организации (юридические лица). Это коллективные субъекты информационных правоотношений. За юридическим лицом как субъектом информационного права всегда стоит определенным образом организованный коллектив людей, который, однако, не всегда может или должен быть юридическим лицом. Статья 30 Конституции РФ утверждает право граждан на объединение для защиты своих интересов. Это может быть, например, национальная община, которая также становится субъектом информационных отношений.

Л.В. Туманова и А.А. Снытников выделяют особую группу субъектов — физические и юридические лица, профессионально занимающиеся сбором и обработкой информации (частные детективы, действующие как предприниматели без образования юридического лица, брокеры, патентные бюро, пенсионные фонды и т.д.)[1].

Правовой статус организации реализуется через права и обязанности, установленные для всех видов организации, — общий статус, а также через права и обязанности, установленные для отдельных видов юридических лиц, — специальный статус.

Общий информационный статус юридических лиц связан с информационным обеспечением юридических лиц; информационное обеспечение включает в себя создание и приобретение информационных ресурсов и информационных технологий, учет своих информационных ресурсов и распространение своими информационными ресурсами. Для устранения проблем, возникающих в сфере информационного обеспечения организаций, требуется унификация этих процессов. Общий статус организаций реализуется в том числе и через субъективные права юридических лиц (объекты информационных ресурсов могут входить в состав уставного капитала).

Специальный статус организаций, наделенных определенными полномочиями по сбору, обработке и хранению информации, обязательно закрепляется законом (библиотеки, архивы и др.).

Например, обязательное лицензирование деятельности данных юридических лиц. Так, лицензированию подлежат:

— работы с информацией персонального характера;

— проектирование права средств защиты информации и обработки персональных данных, а также деятельность, в результате которой вывозятся за пределы РФ государственные информационные ресурсы либо ввозятся.

В связи с развитием интернет-технологий специальные статусы субъектов, участвующих в международном информационном обмене, требуют серьезных уточнений.

---

[1] См.: *Туманова Л.В., Снытников А.А.* Обеспечение и защита права на информацию. — М., 2001. С. 129-130. С. 110.

РАЗДЕЛ 2
ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ

Глава 4. Система органов государственной власти, регулирующих информационную сферу

1. Государственное управление в информационной сфере

За последнее время резко увеличился поток информации, как внешней, так и внутриотраслевой. В связи с постоянной потребностью улучшения эффективности управления растет необходимость более качественной обработки информации. Все это вместе взятое и заставляет искать новые пути и методы организации приема, обработки и передачи информационных потоков.

Глобализация мирового пространства привела к трансформации пространства как такового: наряду с географическим пространством формируется, в частности, электронное. Традиционное противостояние между государствами осуществляется сегодня как в физическом пространстве, так и в новом, виртуальном, или киберпространстве. Информационная деятельность государств диктуется их внутренними интересами: интересами финансово-промышленных групп, их потребностью в сырье, в рынках сбыта продукции, которые невозможно удовлетворить в пределах одного государства.

Итак, говоря о государственном управлении в информационной сфере, следует сказать, что это специфический вид социального управления посредством реализации своих

властных полномочий всеми органами государственной власти (в широком смысле) либо органами исполнительной власти (в узком смысле) по регулированию отношений, возникающих по поводу информации и в связи с ее оборотом в социальных системах.

Государственные СМИ обязаны публиковать сообщения и материалы федеральных органов государственной власти и органов государственной власти субъектов Федерации в порядке, установленном Федеральным законом от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»[1].

Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене»[2] имел своей целью создание условий для эффективного участия России в международном информационном обмене в рамках мирового информационного пространства, защиты интересов РФ, ее субъектов и муниципальных образований, интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

Функции государственного управления в области информации и информатизации реализуются в процессе управленческой деятельности Правительства РФ, федеральных органов исполнительной власти РФ, органов государственной власти субъектов РФ, органов местного самоуправления.

Главными целями российского государства в сфере информатизации являются информационное обеспечение деятельности органов государства, информационное обеспечение внешних по отношению к государственным органам субъектов, в том числе физических лиц; сохранение и структурирование информационного пространства[3].

---

[1] См: СЗ РФ. 1995. № 3. Ст. 170.

[2] См: СЗ РФ. 1996. № 28. Ст. 33-47; 2003. № 27 (часть I). Ст. 2700; 2004. № 27. Ст. 2711 (утратил силу).

[3] См: Указ Президента РФ «Об основах государственной политики в области информатизации» от 20 января 1994 г. № 170.

Политика по информационному обеспечению должна проводиться по многим взаимоувязанным направлениям, прежде всего Правительство РФ обязано разрабатывать программы в области информационного обеспечения граждан, государства, общества.

Финансирование и экономическое регулирование деятельности в этой области следует осуществлять из федерального и местных бюджетов по статье расходов «Информационное обеспечение», в процессе деятельности должны использоваться современные электронные системы и средства для коллективного анализа и обсуждения принимаемых решений.

В случаях, когда для реализации полномочий федерального органа исполнительной власти, в частности для исполнения поручений, необходимо получение информации, заключений, экспертиз (далее — информация) от других федеральных органов исполнительной власти, заинтересованный федеральный орган исполнительной власти обращается с запросом в соответствующий федеральный орган исполнительной власти. Срок получения необходимой информации указывается в запросе.

Срок получения информации, необходимой для исполнения поручений, содержащихся в актах Президента РФ и Правительства, протоколах заседаний и совещаний, проводимых в Правительстве, а также поручений Президента РФ, Председателя Правительства и заместителя Председателя Правительства, определяется исходя из сроков исполнения указанных поручений, при этом в запросе указываются номер и дата поручения, для исполнения которого запрашивается информация.

В случаях, когда запрашиваемая информация не может быть предоставлена в срок, указанный в запросе, федеральный орган исполнительной власти, получивший запрос, в 5-дневный срок с даты получения запроса согласовывает с федеральным органом исполнительной власти, направившим запрос, срок предоставления информации.

Изменение сроков предоставления информации, необходимой для исполнения поручений, содержащихся в актах Президента РФ и Правительства, протоколах заседаний и совещаний, проводимых в Правительстве, а также поручений Президента РФ, Председателя Правительства и Заместителя Председателя Правительства, не допускается.

Для обеспечения требуемой оперативности и достоверности приема, передачи и представления информации органам государственного управления должны применяться электронная цифровая подпись, электронное визирование документов.

Именно разработка этих направлений способна дать значительный эффект в сфере информационного обеспечения органов государственного управления и действительно улучшить положение дел в данной сфере.

Во все времена совершенствованию государственного управления придавалось первостепенное значение. Достижения научно-технического прогресса во многих отраслях, в том числе в информатике и связи, обеспечили возможность практической реализации идей формирования в целом информационного общества. Эта проблема, будучи общегосударственной, комплексной, фокусирует в себе широкий спектр межотраслевых, отраслевых, региональных и международных составляющих.

Большое внимание уделяется информационному обеспечению деятельности парламентов зарубежных стран, внедрению новых информационных технологий. Здесь выделяются на это значительные финансовые ресурсы. Во всех парламентах образованы соответствующие самостоятельные структурные подразделения, укомплектованные высококвалифицированными специалистами, занимающиеся разработкой, внедрением и сопровождением парламентских систем и сетей.

В РФ повышение информационной открытости деятельности федеральных органов государственной власти, доступности соответствующей информации для граждан и органи-

заций, а также создание механизмов общественного контроля их деятельности будут обеспечиваться путем создания:

1) общегосударственных информационных ресурсов, а также информационных ресурсов, содержащих информацию о деятельности федеральных органов государственной власти, с предоставлением доступа к ним граждан и организаций, в том числе через сеть «Интернет»;

2) единой системы навигации в сети «Интернет» по общегосударственным информационным ресурсам, а также информационным ресурсам федеральных органов государственной власти;

3) инфраструктуры пунктов общественного доступа к информации о деятельности федеральных органов государственной власти и государственным информационным ресурсам;

4) систем учета и обработки запросов граждан о предоставлении информации и контроля их исполнения;

5) системы публикации и распространения сведений о деятельности федеральных органов государственной власти;

6) системы подтверждения передачи информации в электронном виде, ее подлинности, а также любых действий по ее изменению в процессе межведомственного взаимодействия, а также взаимодействия федеральных органов государственной власти с населением и организациями;

7) механизмов обучения граждан в области их прав и возможностей использования информационных технологий при взаимодействии с федеральными органами государственной власти.

2. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации

Конституция РФ закрепляет право свободного доступа к информации, поэтому государственное управление в информационной сфере осуществляется всеми ветвями власти. Общее управление осуществляют:

— Федеральное Собрание РФ;

— Президент РФ;

— Правительство РФ;

— суды;

— Совет Безопасности.

Полномочия этих органов следующие.

1. Осуществление государственной политики через принятие нормативных актов.

2. Подготовка и реализация государственных программ в информационной сфере.

3. Реализация прав физических и юридических лиц.

4. Государственный контроль и надзор в сфере информатизации (при Совете Безопасности формируется межведомственная комиссия по информационной безопасности).

Наиболее информационно-емкие структуры государственной власти на федеральном уровне[1] — это:

1) министерства:

— Министерство культуры и массовых коммуникаций;

— Министерство образования и науки;

— Министерство промышленности и энергетики;

— Министерство информационных технологий и связи;

— Министерство юстиции;

— Министерство внутренних дел и др.;

2) агентства:

— Государственное агентство по патентам и товарным знакам;

— Федеральное архивное агентство;

— Федеральное агентство по науке и инновациям;

— Федеральное агентство кадастра объектов недвижимости;

— Федеральное агентство геодезии и картографии;

— Федеральное агентство по образованию;

— Федеральное агентство по культуре и кинематографии;

— Федеральное агентство по печати и массовым коммуникациям;

[1] Указ Президента РФ от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» // СЗ РФ. 2004. № 11. Ст. 945; № 21. Ст. 2023; 2005. № 41. Ст. 4119; 2006. № 14. Ст. 1509.

— Федеральное агентство по техническому регулированию и метрологии;

3) службы:

— Федеральная служба безопасности;

— Федеральная служба государственной статистики;

— Федеральная регистрационная служба;

— Государственная фельдъегерская служба РФ (федеральная служба);

— Федеральная служба по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия;

— Федеральная служба по финансовому мониторингу;

— Федеральная служба по интеллектуальной собственности, патентам и товарным знакам;

— Федеральная служба по надзору в сфере образования и науки.

К полномочиям этой группы органов относят следующие.

1. Осуществление регулирования в информационной сфере, направленного на удовлетворение потребностей физических, юридических лиц и органов власти.

2. Координация деятельности федеральных исполнительных органов и органов исполнительной власти субъектов РФ.

3. Осуществление государственного учета (ведение государственных сводок): реестры, кадастры, списки, перечни.

4. Лицензирование, сертификация и экспертиза информационных услуг.

5. Обеспечение подготовки кадров.

6. Проведение научно-исследовательских работ.

7. Осуществление методических и консультационных работ по обеспечению развития информационных систем.

8. Осуществление запросов у юридических, физических лиц и органов власти по информационно-аналитическим материалам.

9. Формирование временных творческих коллективов и экспертных советов.

10. Привлечение к ответственности лиц, нарушивших нормы права в информационной сфере.

3. Система и компетенция органов, обеспечивающих **охрану государственной тайны**

Система органов, обеспечивающих охрану государственной тайны, включает в себя:

— Федеральное Собрание РФ;

— Президента РФ;

— Правительство РФ;

— ОГВ РФ, субъектов РФ (ФСБ, Министерство обороны, Службу внешней разведки, судебную власть).

Полномочия Федерального Собрания РФ:

— Федеральное Собрание определяет законодательство в области государственной тайны;

— определяет средства и статьи федерального бюджета, направленные на реализацию программ по защите государственной тайны;

— определяет полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.

Полномочия Президента РФ:

— утверждает программу по охране государственной тайны;

— утверждает структуру межведомственной комиссии по защите;

— утверждает перечень должностных лиц, которые имеют право относить информацию к государственной тайне, а также перечень сведений, относящихся к государственной тайне;

— заключает международные договоры о совместном использовании и защите сведений, составляющих государственную тайну;

— определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ.

Полномочия Правительства РФ:

— организует исполнение законов по охране государственной тайны;

— предлагает структуру межведомственной комиссии по защите государственной тайны;

— предлагает перечень должностных лиц, имеющих право относить сведения к государственной тайне;

— устанавливает порядок разработки перечня сведений, составляющих государственную тайну;

— организует разработку и выполнение государственных программ, направленных на защиту государственной тайны;

— определяет льготы гражданам, допущенным к работе с государственной тайной (3 уровня секретности);

— устанавливает порядок определения ущерба в случае разглашения государственной тайны, а также ущерб собственнику информации в результате засекречивания.

— определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства РФ.

Полномочия органов государственной власти РФ, субъектов РФ:

— обеспечивают защиту государственной тайны, переданной им другими органами государственной власти, а также на подведомственных им предприятиях и учреждениях;

— обеспечивают проведение проверочных мероприятий по допуску лиц к государственной тайне;

— реализуют меры по ограничению прав граждан, имеющих доступ к государственной тайне и по предоставлению им льгот;

— вносят предложения по улучшению защиты государственной тайны.

Полномочия судебной власти:

— при расследовании дел, связанных с нарушением законодательства о государственной тайне;

— обеспечивает судебную защиту физических, юридических лиц в связи с их деятельностью по защите государственной тайны;

— определяет полномочия должностных лиц по охране государственной тайны в органах судебной власти.

4. Компетенция органов государственной власти по обеспечению правовых режимов конфиденциальной информации

Органы государственной власти обязаны обеспечить охрану коммерческой тайны, полученной ими в соответствии с законом, от разглашения и неправомерного использования с выполнением ими своих служебных обязанностей. Информация, составляющая коммерческую тайну, охраняется в указанных органах как служебная тайна.

Государственные органы обязаны возместить убытки, причиненные владельцам конфиденциальной информации вследствие своих неправомерных действий. Устанавливается ответственность и для владельцев конфиденциальной информации при нарушении правил ее предоставления в государственные органы. Государственные органы власти могут стать пользователем профессиональной тайны в установленных законом случаях. Информация охраняется как служебная тайна.

Органы государственной власти обладают следующими полномочиями по работе с персональными данными, составляющими тайну частной жизни.

1. Лицензирование деятельности, связанной с работой с персональными данными.

2. Регистрация массивов и держателей персональных данных.

3. Сертификация информационных систем и информационных технологий, предназначенных для обработки персональных данных.

4. Заключение межгосударственных соглашений трансграничной передачи персональных данных.

5. Взаимодействие органов местного самоуправления и органов государственной власти в условиях информатизации общества

Взаимодействие органов местного самоуправления и органов государственной власти осуществляется по многим направлениям: во-первых, это правовое регулирование государством проблем

местного самоуправления; во-вторых, это наделение органов местного самоуправления отдельными государственными полномочиями и контроль за их выполнением; в-третьих, это взаимодействие в финансовой сфере и некоторые другие вопросы.

В то же время основными направлениями деятельности органов местного самоуправления и органов государственной власти в области информатизации являются следующие:

— установление принципов отбора информации, необходимой для обеспечения деятельности органа власти с учетом его места в системе власти;

— обеспечение моделирования блоков информации по функциям органа в целях результативной подготовки решений органа в пределах его компетенции;

— систематизация всего комплекса информации, ведение делопроизводства, сдача дел в архив, предоставление информации в специализированные фонды;

— формирование информации, которая предназначена для внешних организаций и граждан, опубликование и доведение до сведения заинтересованных лиц;

— организация информационной системы в рамках ведения органа власти, обеспечение постоянных инноваций коммуникативных информационных процессов в своей системе;

— обеспечение безопасности и использования информации, соблюдение правил передачи другим органам государственной власти и органам местного самоуправления;

— подготовка и ведение банков информации официальной и массовой;

— организация ведения учета информационных ресурсов органа власти, установление ответственности за его адекватность задачам и функциям органа, полноту, своевременность представления, хранение и использование исключительно по назначению[1].

[1] *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право: Учебник / Под ред. Б.Н. Топорнина. — СПб.: Юридический центр Пресс, 2001. С. 212-213.

Отсюда следует, что взаимодействие органов местного самоуправления и органов государственной власти в условиях информатизации общества будет содержать весьма специфические проблемы.

В настоящее время, например, за органами местного самоуправления в области почтовой связи закрепляются следующие полномочия:

— оказывают содействие организациям почтовой связи в размещении на территории муниципального образования объектов почтовой связи, рассматривают предложения данных организаций о выделении нежилых помещений или строительстве зданий для размещения отделений почтовой связи и других объектов почтовой связи;

— способствуют оснащению объектов почтовой связи средствами механизации, автоматизации и информатизации, необходимыми для эффективного функционирования и расширения сферы услуг, оказываемых гражданам и организациям;

— устанавливают режим работы объектов почтовой связи, находящихся в муниципальной собственности, по обслуживанию пользователей услуг почтовой связи;

— способствуют созданию и поддержанию устойчивой работы местных почтовых маршрутов, оказывают содействие операторам почтовой связи в доставке почтовых отправлений в труднодоступные населенные пункты в установленные контрольные сроки;

— оказывают содействие организациям почтовой связи в обеспечении сохранности доставляемых по почтовым маршрутам почтовых отправлений и денежных средств;

— при планировании комплексного и социального развития муниципального образования рассматривают вопросы развития, финансирования и технического обеспечения объектов почтовой связи;

— рассматривают предложения организаций почтовой связи о предоставлении им льготы по уплате налогов, зачисляемых в соответствующие местные бюджеты, и арендной

платы за пользование имуществом, находящимся в муниципальной собственности, а также устанавливают льготы по указанным налогам и арендной плате;

— оказывают содействие организациям почтовой связи в размещении почтовых ящиков на территории муниципального образования, контролируют обеспечение организациями, эксплуатирующими жилые дома, собственниками жилых домов сохранности и поддержания в исправном состоянии абонентских почтовых шкафов и почтовых абонентских ящиков.

Органы местного самоуправления вправе вносить в органы государственной власти субъектов РФ предложения о развитии сети почтовой связи на территории муниципального образования*.

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»[2] уже не предусматривает полномочий органов местного самоуправления в этой сфере, так как в условиях усиления вертикали власти был принят Федеральный закон от 6 октября 2003 г. № 131-ФЗ «Об общих принципах местного самоуправления в Российской Федерации»[3], который в значительной мере конкретизировал вопросы местного значения и не включил в этот перечень вопросы в области связи, т.е. эта сфера ушла полностью в область государственного регулирования и теперь может передаваться органам местного самоуправления только при условии использования механизма наделения органов местного самоуправления государственными полномочиями.

Что кается возможностей участия муниципальных образований в международном информационном обмене, то они участвуют в международном информационном обмене в качестве субъектов права, представляющих интересы населе-

[1] Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи»// СЗ РФ. 1999. № 29. Ст. 3697.

[2] СЗ РФ. 2003. № 28. Ст. 2895.

[3] Российская газета. 2003. № 202.

ния муниципальных образований по вопросам, отнесенным к предметам ведения местного самоуправления.

Правом выступать от имени муниципальных образований по вопросам международного информационного обмена обладают органы местного самоуправления в рамках их полномочий, установленных нормативными правовыми актами, определяющими статус этих органов. Муниципальные информационные службы и средства массовой информации муниципальных образований вправе самостоятельно участвовать в международном информационном обмене[1]. Пожалуй, этот вопрос один из немногих, которые имеют нормативное закрепление.

Информационное обеспечение деятельности органа власти включает в себя установление порядка работы с документами, установление режима информации, структуризацию информации в пределах функционального влияния органов государственного управления и органов местного самоуправления. Эти вопросы, к сожалению, недостаточно полно урегулированы.

Существует также проблема фильтрации всего массива входящей информации, так как, с одной стороны, этот ресурс обеспечивает связь органа власти с внешней средой, с другой стороны, объем и содержание этой информации могут застопорить работу органов государственного управления и органов местного самоуправления. Поэтому необходима тщательная разработка положений и инструкций для работы структурных подразделений органов, обеспечивающих обработку и подготовку к представлению руководству входящих документов.

Следующая проблема в этой сфере — это систематизация поступающей и исходящей информации с учетом категорий информации ограниченного доступа. Необходимо выделять

[1] См.: Федеральный закон от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // СЗ РФ. 2003. № 40. Ст. 3822; 2004. № 25. Ст. 2484; № 33. Ст. 3368; 2005. № 1 (часть I). Ст. 9. Ст. 12. Ст. 17. Ст. 25. Ст. 37; № 17. Ст. 1480; № 27. Ст. 2708; № 30 (часть I). Ст. 3104. Ст. 3108; № 42. Ст. 4216; 2006. № 1. Ст. 9. Ст. 10. Ст. 17; № 6. Ст. 636; № 8. Ст. 852; № 23. Ст. 2380; № 30. Ст. 3296; № 31 (часть I). Ст. 3427. Ст. 3452.

блоки информации по категориям: открытая информация, отнесенная к государственной тайне, отнесенная к персональным данным, отнесенная к коммерческой тайне субъектов, с которыми орган власти взаимодействует, отнесенная к тайне частной жизни, профессиональной и т.д. Пока эта информация находится в пределах функциональной деятельности органа, он обязан обеспечивать надлежащий режим доступа к такого рода информации. Поэтому целесообразно создать в структуре органа власти специальные банки данных по каждой категории информации и урегулировать работу с такими банками данных специальными инструкциями[1].

Кроме получения информации, необходимой для осуществления функций органов государственного управления и органов местного самоуправления в целях обеспечения постоянного взаимодействия со своими подразделениями, с другими органами власти, предприятиями, учреждениями и гражданами особое значение имеет и деятельность по предоставлению органами государственного управления и органами местного самоуправления информации другим пользователям. К такого рода деятельности относится не только предоставление органами государственного управления и органами местного самоуправления информации различным организациям, гражданам и средствам массовой информации, но и предоставление информации органами государственного управления и органами местного самоуправления друг другу. Что, в свою очередь, является одним из необходимых условий осуществления взаимодействия органов власти на всех трех уровнях: федеральном, региональном и местном. Необходимо урегулирование правил использования информации в соответствии с ее правовым режимом, с одной стороны, и в соответствии с правилами открытости, гласности свободного доступа к информации — с другой.

---

[1] См.: *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право: Учебник / Под ред. Б.Н. Топорнина. — СПб.: Юридический центр Пресс, 2001. С. 209.

Действующее законодательство РФ пока не имеет специального закона о служебной информации, законов об информационном обеспечении деятельности органов государственного управления и органов местного самоуправления, законов о тайне частной жизни, не урегулирован вопрос о тайне персональных данных и т.д. Все это отрицательно сказывается на информационной дисциплине и культуре в государственном и местном управлении. Частично эти вопросы решаются в положениях о подразделениях, в регламентах отдельных органов, но при этом весь объем нормативного регулирования этих вопросов не обеспечивается.

6. Электронное государство

Электронное государство — это реализация интернет-решений и базовой инфраструктуры для предоставления физическим и юридическим лицам информационных ресурсов и информационных услуг государственными органами с целью обеспечить прозрачность работы государственного сектора и обеспечить интерактивное участие среди первых лиц в принятии решений.

Виды государств на разных этапах развития человеческого общества:

— контрольное государство — доиндустриальное общество;
— правовое государство — индустриальное общество;
— социальное государство — постиндустриальное общество;
— электронное государство — информационное общество.

Цель электронного государства — обеспечить интерактивное участие физических и юридических лиц и прозрачную работу госсектора.

Реализация идей электронного государства осуществляется через создание государственных web-сайтов, которые: а) реализуют право граждан на информацию, и за информацию, размещенную на этом сайте, субъект несет полную ответственность; б) выполняют коммуникативную функцию.

Возможности государственных web-сайтов

1) подача заявлений, регистрация, подача таможенных деклараций;

2) ликвидация бумажного документного оборота и перестройка государственных архивов;

3) создание единого центра для контроля деятельности по сбору личной информации и их автоматизированной обработке.

Сегодня в российской системе государственного управления используется программа «Электронная Россия»[1], в рамках которой разработаны такие проекты, как «Электронное правительство», «Телемедицина», «Дистанционное образование». Постепенно складывается современная информационная система государственного управления, которая использует преимущественно информационные технологии для публичного властвования.

Василенко И.А.[2] выделяет следующие основные характеристики государственного управления[3] в XXI в.:

— разработка государственной политики с использованием инфокоммуникативных технологий, политической аналитики и прогностики;

— разработка, осуществление и оценка государственных программ с использованием современных методов социально-политической и социально-экономической диагностики, идентификации и распознавания образов, агрегирования информации и ее компьютерной обработки (с помощью методов математического моделирования социальных процессов при разработке управленческих решений на локальном, региональном и национальном уровнях);

— прогнозирование и учет в практической деятельности позитивных и негативных тенденций в развитии обществен-

---

[1] См.: Приложение 3.

[2] *Василенко И.А.* Государственное и муниципальное управление: Учебник. — М.: Гардарики, 2005. С. 79-80.

[3] Государственное управление — это целенаправленное организующе-регулирующее воздействие государства (через систему его органов и должностных лиц) на общественные процессы, отношения и деятельность людей (См.: *Глазунова Н.И.* Система государственного управления: Учебник для вузов. — М.: ЮНИТИ-ДАНА, 2003. С. 13).

ных явлений, разработка мероприятий по локализации и устранению недостатков, определение потребностей в изменениях и нововведениях и осуществление практических действий по их реализации;

— анализ, обобщение и интерпретирование социальных, политических и экономических показателей, характеризующих состояние района, региона, страны;

— организация и проведение эмпирических исследований по изучению социально-политических и социально-экономических процессов в области (регионе, стране) для поиска оптимальных управленческих решений, принятие таких решений;

— применение рациональных приемов поиска, обработки, хранения и использования необходимой социальной, политической, экономической и научной информации.

Электронное правительство — это концепция осуществления государственного управления, присущая информационному обществу. Данная концепция основывается на возможностях информационно-телекоммуникационных технологий и ценностях открытого гражданского общества.

Во многих странах «электронное правительство» только создается, а в некоторых странах оно давно и успешно функционирует.

Закон США «Об электронном государстве» 2002 г. состоит из пяти разделов (титулов).

1. Электронная государственная служба административного и бюджетного управления.

2. Федеральное управление электронной государственной службы.

3. Информационная безопасность.

4. Утверждение ассигнований и сроков.

5. Защита конфиденциальной информации и достоверности статистики.

Цели создания электронного государства:

1) обеспечение межведомственного сотрудничества;

2) развитие распространения электронного государственного управления;

3) расширение участия граждан в государственном управлении;

4) повышение уровня информированности лиц, принимающих властные решения;

5) сокращение издержек и затрат на государственные структуры;

6) доступ к надежной государственной информации.

Система органов власти, реализующих полномочия в области создания и функционирования электронного государства:

1) агентства по информации;

2) чиновник по информации;

3) совет высших должностных лиц по информации (межведомственный характер);

4) управление по вопросам электронного государства;

5) администратор управления (назначается президентом);

6) административное и бюджетное управление;

7) директор административного и бюджетного управления;

8) межведомственная комиссия по государственной информации.

Однако сегодня «электронное правительство», за редким исключением, пока еще не стало реальностью[1]. Появляется все больше примеров «правительства он-лайн» (government on-line), которое по своей сути не тождественно «электронному правительству». «Правительство он-лайн» представляет собой статичные сайты правительственных структур, которые редко содержат что-либо, помимо общей информации о работе данной правительственной структуры и контактных телефонов. Самые продвинутые из них предлагают гражданам небольшое количество электронных операций, например оплату налогов.

[1] Объясняется это, на наш взгляд, не недостатком средств, а скорее отсутствием организационной воли.

Естественно, среди специалистов существуют различные точки зрения на содержание понятия «электронное правительство». Рассмотрим лишь некоторые из толкований этого термина. Так, электронное правительство определяется следующим образом:

— организация государственного управления на основе электронных средств обработки, передачи и распространения информации, предоставления услуг государственных органов всех ветвей власти всем категориям граждан (пенсионерам, рабочим, бизнесменам, государственным служащим и т.п.) электронными средствами, информирования теми же средствами граждан о работе государственных органов;

— информационные технологии в государственном управлении;

— автоматизированные государственные службы, основными функциями которых являются: обеспечение свободного доступа граждан ко всей необходимой государственной информации, сбор налогов, регистрация транспортных средств и патентов, выдача необходимой информации, заключение соглашений и оформление поставок необходимых государственному аппарату материалов и оснащения. Это может привести к снижению затрат и экономии средств налогоплательщиков на содержание и финансирование деятельности государственного аппарата, увеличению открытости и прозрачности деятельности органов управления;

• — использование в органах государственного управления новых технологий, в том числе и интернет-технологий.

По мнению некоторых специалистов[1], данные определения представляют электронное правительство скорее как способ модернизации уже существующих структур и услуг, а не как самостоятельную идею комплексной трансформации самих принципов организации управления государством. С этой точки зрения такой подход неверен, поскольку в пер-

[1] *Голобуцкий А., Шевчук О.* Электронное правительство // http://golob.narod.ru/egovperru.html.

вую очередь он экономически неоправдан. Электронное правительство как обеспечение государственных структур современными информационными технологиями, реализующими традиционные услуги, означает дополнительные бюджетные затраты, направленные на простое дублирование в электронном виде офф-лайновой (off-line) деятельности. Но существует и другой подход. Во многих странах, в первую очередь в США и Великобритании, электронное правительство рассматривается, скорее, как концепция, направленная на повышение эффективности деятельности государства в целом.

Рассмотрим основные положения концепции электронного правительства на примере зарубежного опыта.

В общественной жизни любой страны существует три основных субъекта — государство, граждане и коммерческие организации. Поэтому в идеале электронное правительство должно состоять из трех основных модулей: G2G (government for government) — правительство правительству; G2B (government to business) — правительство бизнесу; G2C (government to citizens) — правительство гражданам.

Электронное правительство содержит он-лайновые сервисы для граждан и бизнеса на едином портале, электронный документооборот в правительственных и парламентских структурах, общую для разных правительственных структур базу данных для предотвращения дублирования информации и повторных затрат, часто — закрытую специализированную информационную сеть для внутриправительственных трансакций (например, Govnet), разветвленную информационно-телекоммуникационную инфраструктуру, системы криптографии и прочие способы защиты информации, в том числе и персональных данных, цифровую подпись, электронный ключ, смарт-карты, другие средства санкционирования доступа к информации и операций с ней.

Таким образом, «электронное правительство» дает возможность правительственным органам использовать новые технологии, чтобы предоставить людям более удобный доступ к правительственной информации и услугам, повысить

качество этих услуг и в большей мере обеспечить возможность участия в работе демократических институтов.

Говоря об улучшении системы государственного управления, в числе основных достижений «электронного правительства» называют следующие.

1. *Возможность «экономного государственного управления»*. Экономия от замены бумажных информационных потоков электронными огромна. Только правительство США тратит около миллиарда долларов в год на издание в печатном виде ряда документов, публикуемых также и в Сети. Основной тираж — 30 миллионов экземпляров федерального регистра, 1 миллион экземпляров стенографических отчетов слушаний и 65 миллионов экземпляров президентского бюджета — предназначается для официальных лиц, имеющих доступ к Интернету[1]. Таким образом, большая часть этой печатной продукции отправляется прямиком в столичные мусорные ящики.

Другой пример. Электронная публикация номеров телефонов, почтовых и физических адресов служащих государственных учреждений позволила штату Флорида сэкономить 295 тыс. долл.[2] в год на тиражировании и распространении бумажных справочников, а также решить проблему обновления этой информации, 30% которой через год (от издания до издания) оказывается устаревшей. Помножьте на 50 штатов да прибавьте справочник по аппарату федерального правительства — и вот вам еще один источник огромной экономии.

Свод федеральных правил по найму и увольнению работников в США весит в печатном виде 490 кг, а описание требований к печенью, входящему в рацион военнослужащих, занимает 15 страниц[3]. Публикация всех правительственных

---

[1] Гейтс Б. Бизнес со скоростью мысли. Изд. 2-е, испр. — М.: ЭКСМО-Пресс, 2001. С. 365.

[2] http://www. News.ru.

[3] *Гейтс Б.* Бизнес со скоростью мысли. Изд. 2-е, испр. — М.: ЭКСМО-Пресс, 2001. С. 366.

документов в Сети поможет одновременно и сократить издержки, и сделать информацию наиболее доступной. Кроме того, электронная форма гораздо лучше подходит для сложных спецификаций. Печатная документация по государственному конкурсу на создание нового грузового самолета весит 3,5 тонны, а в электронной форме она легко могла бы поместиться на пару компакт-дисков[1].

Переведя свои ключевые структуры в Интернет, правительство могло бы само, без участия кого-либо из внешних союзников, дать гражданам мощнейший стимул для принятия веб-стиля жизни. Если государство — обычно самое крупное «предприятие» в любой стране — встанет во главе внедрения новых технологий, это автоматически поднимет технический уровень всего национального хозяйства и даст импульс развитию информационного рынка. Административным предписанием или различными льготами оно способно побудить к необходимым шагам все компании, имеющие с ним хоть какие-нибудь отношения.

2. *Экономия времени.* Например, раньше администрация штата Южная Австралия еженедельно издавала свой 50-страничный официальный список вакансий тиражом в 5 тыс. экземпляров[2]. При этом объявления о появившемся свободном месте доходили до адресатов с задержкой на время тиражирования буклета и его распространения по нескольким сотням разбросанных по всему штату офисов, так что дата окончания приема заявлений от претендентов началась с учетом сроков их пересылки обычной почтой.

Теперь же весь процесс осуществляется в системе автоматизации электронного документооборота на базе ПО Microsoft Exchange. Сначала информация об открывающихся вакансиях поступает в отделы кадров государственных учреждений и в ряд агентств по найму, занимающих привилегированное положение. Если окажется, что на освободивше-

[1] *Гейтс Б.* Указ. соч. С. 366.
[2] http://www. News. ru.

еся место хотел бы перевестись кто-либо из государственных служащих, нанимающий менеджер автоматически получит уведомление по электронной почте и отменит широкую публикацию объявления, так что никто не потратит времени зря на предложение своих услуг. А если таких желающих не найдется, объявление пойдет в прессу и нанимающий менеджер так же по электронной почте будет получать уведомления о его публикации с указанием названий и номеров газет. Таким образом правительство штата рассчитывает не только сэкономить за счет внедрения новой системы 50-80% своих ежегодных расходов на вербовку новых работников, но и значительно уменьшить время заполнения вакансий при безусловном соблюдении принципа равенства возможностей, в том числе и для сотрудников удаленных офисов государственных учреждений.

3. *Возможность открытия государственными организациями своих систем управления знаниями и учета коммерческих операций для доступа общественности.* Немецкое Федеральное министерство финансов ведет разработку электронной системы управления архивами публичных актов. Проект предусматривает автоматическую маршрутизацию, хранение и публикацию документов на закрытых или общедоступных веб-узлах — в зависимости от грифа.

Еще одним примером может служить система проведения конкурсов администрацией штата Массачусетс. Условия участия, все документы, которые могут для этого потребоваться, а впоследствии и информация о победителях публикуются в сети. Результатом внедрения этой системы стало не только сокращение расходов на проведение конкурсов, но и появление у различных общественных организаций реальной возможности приобретать нужные им товары по более низким ценам. Как и в большинстве штатов, в Массачусетсе муниципалитеты, сельские администрации и школьные округа могут покупать у производителей их продукцию на тех же условиях, что и правительство. В бумажном мире, однако, отыскать следы «государственных» цен на большинство нуж-

ных товаров бывает практически невозможно. Теперь же любое городское учреждение или школа могут узнать лучшую в штате цену на веб-узле новой системы.

4. *Возможность для граждан непосредственно воздействовать на принятие управленческих решений.* Так, например, в случае, когда правительственная структура собирается внести изменения в процедуру предоставления определенной услуги, она сможет разместить информацию о предлагаемых изменениях своей политики на своем сайте в сети «Интернет» и предложить заинтересованным лицам высказать свое мнение по поводу этой услуги и предлагаемой новой политики. Полученные отклики могут затем быть использованы для усовершенствования этой политики.

5. *Повышение качества услуг, предоставляемых правительственными организациями гражданам.* Реализация правительственных услуг через Интернет позволит гражданам воспользоваться ими, не выходя из дома. Это повысит гибкость, скорость и доступность правительственных услуг, а также, возможно, снизит их себестоимость.

6. *Возможность получать комплексные услуги, так как различные правительственные организации смогут более эффективно взаимодействовать друг с другом.* Например, в результате аварии человеку требуется связаться с несколькими различными государственными организациями и в каждой изложить свою ситуацию и нужды. Если бы у всех этих организаций была возможность обмениваться информацией и интегрировать свои услуги, человеку пришлось бы проделывать все требуемые процедуры всего один раз.

7. *Повысить уровень информированности населения, которое сможет получить свежую всеобъемлющую информацию о государственных законах, правилах, политике и услугах.* Если сделать эту информацию обо всех существующих правилах и нормативах доступной в Интернете, люди получат больше возможностей заниматься любой деятельностью, как личной, так и профессиональной, безопасно и в рамках законов.

Естественно, реализация такой масштабной концепции связана с преодолением многих трудностей. Для того чтобы стимулировать участие граждан в управлении государством, при разработке способов использования информационных и коммуникационных технологий необходимо учесть следующие моменты.

8. *Возможность разделения населения на тех, кто обладает навыками и инструментами для использования новых технологий, и тех, у кого их нет.* Если граждане не вооружены и не владеют техникой, то они вряд ли смогут воздействовать каким-либо образом на электронное правительство. Электронное правительство должно объединять людей, а не разъединять их. Поэтому «электронное правительство» следует организовать таким образом, чтобы, с одной стороны, были сохранены привычные способы доступа к правительственным услугам для тех, кто в них нуждается, а с другой — были созданы места общественного доступа в Интернет и работали программы образования, задача которых — помочь гражданам освоить новые технологии.

Что же касается процесса создания правительственной сетевой инфраструктуры в РФ, он соответствует этапам, которые проходят все правительства[1].

Первый этап, который характеризуется созданием начальных «ведомственных интерфейсов», практически завершен. У подавляющего числа федеральных органов исполнительной власти созданы и устойчиво функционируют интернет-сайты[2].

По поручению Президента РФ в Правительстве РФ был подготовлен и утвержден Перечень регулярной обязатель-

---

[1] См, например: http://www.cnews.ru/Newkom/index.shtml. 2003/01/20.

[2] Информационные технологии в среде взаимодействия государства и гражданского общества (Концепция. Мировой опыт. Перспективы в России). Материалы научно-практической конференции в Российской академии государственной службы при Президенте РФ. Москва, 6 июня 2002 г.

ной информации для размещения федеральными органами исполнительной власти в российском сегменте сети «Интернет». Перечень требует в обязательном порядке размещать следующую информацию:

— официальное наименование федерального органа исполнительной власти и официальные реквизиты (адрес, телефоны справочной службы, адрес электронной почты);

— положение о федеральном органе исполнительной власти;

— организационная структура федерального органа исполнительной власти (руководство, структура центрального аппарата, территориальные органы, подведомственные учреждения и предприятия);

— нормативные акты, регламентирующие деятельность федерального органа исполнительной власти;

— нормативные правовые акты, затрагивающие права и обязанности граждан и организаций, принятые федеральными органами исполнительной власти в соответствии со своей компетенцией;

— информация о положении дел в отрасли (сфере ведения);

— информация о федеральных целевых программах, в реализации которых участвует федеральный орган исполнительной власти, в том числе информация об исполнении положений программ;

— ежедневная информация пресс-службы (управлений по связям с общественностью) о деятельности федерального органа исполнительной власти;

— реквизиты общественных приемных федерального органа исполнительной власти (адрес, телефоны, порядок работы с гражданами и организациями).

Указанная выше информация должна предоставляться в полном объеме, за исключением информации, отнесенной в соответствии с законодательством к информации с ограниченным доступом.

В развитие указанного Перечня Департамент правительственной информации разработал в июле 2001 г. «Рекоменда-

ции по созданию и сопровождению интернет-сайта федерального органа исполнительной власти», которые учитывают опыт по созданию «электронной» инфраструктуры ведущими правительствами мира, детализируют многие задачи и вопросы, связанные с разработкой и сопровождением государственных интернет-сайтов.

Следующим этапом является развертывание в сети «Интернет» инфраструктуры, предоставляющей пользователям возможные сервисы сугубо информационного характера, работающие с пользователем во внешнем информационном контуре.

Сегодня в рамках работ по созданию интернет-портала Правительства РФ формируется более совершенная инфраструктура системы информирования общественности о деятельности органов государственной власти. Речь идет о создании горизонтально и вертикально интегрированных правительственных новостных ресурсах, поддерживаемых информационными подразделениями различных федеральных ведомств и местных органов власти.

В рамках правительственного сетевого информационного контура создаются механизмы, поддерживающие он-лайновые ведомственные сообщества, прежде всего информационные подразделения министерств и ведомств (пресс-службы или управления по связям с общественностью), которые в большей степени, чем другие, готовы осваивать новые технологии сети «Интернет». По мере отработки этих сетевых механизмов и сервисов опыт и решения можно будет переносить и в другие сферы правительственного контура управления.

Создается инфраструктура сетевых механизмов диалога (взаимодействия) правительства (ведомств) и граждан (сообществ) в виде специализированных он-лайновых форумов по тем или иным общественно значимым проблемам. Форумы могут решать задачи по поддержке постоянно действующих экспертных сообществ. Портал содержит специализированный интерактивный модуль, позволяющий оперативно поддержать любую диалоговую задачу.

Создаются он-лайновые сервисы для журналистов и редакций средств массовой информации. Речь идет о создании системы виртуальной аккредитации, обеспечивающей онлайновый доступ журналистов на мероприятия, проводимые в Доме Правительства, министерствах и. ведомствах (что особенно важно региональным СМИ).

На портале будет современный Каталог сетевых ресурсов органов государственной власти, обеспечивающих полноценный поисковый и иные сервисы. Это не только полезно и удобно для пользователей, но и позволяет вести мониторинг ситуаций в сфере государственных сетевых ресурсов.

Для пользователей создана справочно-информационная база данных правительственных документов, интегрирующая тексты более 17 тыс. правительственных документов с интерфейсами, обеспечивая удобный поиск.

Перспективным может стать развитие сетевой правительственной инфраструктуры, позволяющей решать задачи информационного обеспечения деятельности правительства, министерств и ведомств в нестандартных (кризисных, проблемных) ситуациях. Новые технологии позволяют оперативно создавать «виртуальные площадки "под задачу"», достаточно легко их администрировать. Но самое главное — не создавать дополнительных структур off-line.

Разрабатывается инфраструктура поддержки сетевых проектов для различных государственных структур, а также он-лайновая система обучения и профессиональной подготовки государственных служащих.

Проект «электронного правительства» с 2002 г. определен как приоритетный в Федеральной целевой программе «Электронная Россия (2002—2010 годы)».

В частности, Программа включает задачи обеспечения информационной прозрачности деятельности органов государственной власти и открытости государственных информационных ресурсов для гражданского общества, создания предпосылок для эффективного взаимодействия между органами государственной власти и гражданами на основе широкого

использования информационно-коммуникационных технологий. Предусматривается реализация комплекса мер по повышению открытости государственных информационных ресурсов не только на федеральном, но и на региональном и местном уровнях (посредством внедрения информационно-коммуникационных технологий).

В целях ускорения формирования инфраструктуры интерактивного взаимодействия граждан и органов государственной власти будет разработана единая Концепция государственной политики в области развития российского сегмента инфраструктуры платежных карт и использования электронных персональных инструментов в автоматизированных системах взаимодействия органов государственной власти.

Безусловно, реализация данной программы сыграет важную роль для развития РФ как демократического, «информационного» государства.

Глава 5. Правовые режимы информационных ресурсов

1. Понятие правового режима информационных ресурсов

Содержание правового режима информационных ресурсов не предусмотрено в действующем Законе об информации, однако данное правовое явление занимает особое место в правовых отношениях. Смысл понятия «правовой режим» заключается в возможности совершения или несовершения с объектом права определенных действий, влекущих известный юридический результат. В зависимости от характера действий и юридических последствий их совершения или несовершения, составляющих содержание правовых режимов, различают следующие виды гражданско-правовых режимов:

— правовой режим собственности;
— режим исключительных прав;
— режим обязательственного права.

В содержание правового режима информационных ресурсов включаются:

1) порядок документирования информации;

2) положения о доступе к информационным ресурсам в зависимости от их категорий;

3) принятие мер по охране информации (способы охраны и порядок их применения). Следует отметить, что охрана — более широкое понятие, чем понятие «защита информации», и включает в себя также меры, направленные на предупреждение нарушения.

В свою очередь, следует отметить, что порядок защиты одинаков для всех объектов правоотношений, в том числе для информации. Различают юрисдикционный и неюрисдикционный порядок защиты. **Юрисдикционный порядок защиты** — это деятельность государственного органа, направленная на восстановление права и пресечение действий, нарушающих право. Юрисдикционный порядок делится, в свою очередь, на судебный и административный. Неюрисдикционный порядок имеет место при самозащите и при применении мер оперативного воздействия.

Следует отметить, что элементы правового режима информационных ресурсов закрепляются также в законодательстве субъектов РФ. Так, И.Л. Бачило говорит о том, что в законодательстве субъектов РФ насчитывается до 7—8 элементов правового режима информационных ресурсов, к ним, в частности, законодатель относит: порядок создания информационного продукта, стандарт его документального оформления, порядок финансирования, определение субъекта права собственности или исключительного права, установление категории доступа, правила учета и регистрации, условия обеспечения безопасности, порядок правоохранительной процедуры.

2. Понятие и виды охраноспособной информации

Информация с ограниченным доступом определяется двумя признаками.

1. Доступ ограничен в соответствии с законом.

2. Цель ограничения — защита основ конституционного строя, нравственности, здоровья, прав и законных интересов

других лиц, обеспечение обороны страны и безопасности государства.

Признаки охраноспособности информации:

1) охране подлежит только документированная информация;

2) информация должна соответствовать ограничениям, установленным законом;

3) защита информации устанавливается законом.

Виды информации с ограниченным доступом:

1) государственная тайна;

2) конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:

— коммерческая тайна;

— тайна частной жизни,

— служебная тайна;

— профессиональная тайна.

Следует отметить, что термин «защита информации» закреплен в ст. 16 Закона об информации, анализ законодательства РФ позволяет говорить о том, что данное понятие является широко употребляемым. Толковый словарь «Бизнес и право» правовой системы «Гарант» под данным понятием подразумевает «все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей. Она включает криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера».

Между тем в ряде международных соглашений можно найти термин «защита информации». Под ним подразумевается:

— деятельность, направленная на предотвращение утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на конфиденциальную информацию[1];

[1] Соглашение между Правительством РФ и Правительством Республики Белоруссия о сотрудничестве в области защиты информации (Москва, 9 июля 1997 г.)

— комплекс административных, организационных и технических мероприятий по ограничению доступа к информации и ее носителям в целях обеспечения ее сохранности и недоступности третьим сторонам, предусмотренный законодательством РФ[1].

Таким образом, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

---

[1] Соглашение между Правительством РФ и Правительством Словацкой Республики о защите информации ограниченного доступа (Братислава, 29 апреля 1997 г.)

6) постоянный контроль за обеспечением уровня защищенности информации.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

3. Режимы защиты информации

Цели защиты информации:

1) предотвращение хищения, утечки, искажения, утраты и подделки информации;

2) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;

3) реализация права на государственную тайну и конфиденциальную информацию.

На основании ст. 16 Закона об информации защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации осуществляется от:

— утечки (неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками);

— несанкционированного воздействия (воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации);

— непреднамеренного воздействия (воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических

и программных средств информационных систем, природных явлений или иных не целенаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации);

— разглашения (несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации);

— несанкционированного доступа (получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации);

— разведки (получения защищаемой информации технической, агентурной разведкой).

Режим защиты информации устанавливается в отношении трех групп сведений.

1. Сведения, относящиеся к государственной тайне: режим устанавливается уполномоченным государственным органом на основании Закона РФ о государственной тайне[1].

2. Конфиденциальная информация. Режим защиты информации устанавливается собственником информационных ресурсов или уполномоченным им лицом на основании Закона об информации.

3. Персональные данные. Режим защиты информации устанавливается специальным Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных»[2] (вступает в действие по истечении ста восьмидесяти дней со дня его опубликования).

Контроль за соблюдением требований к защите информации, а также обеспечение органами мер защиты информационной системы, образующие информацию с ограниченным доступом в негосударственных структурах, возложены на го-

[1] СЗ РФ. 1997. № 41. Ст. 4673; 2004. № 35. Ст. 3607.

[2] СЗ РФ. 2006. № 31 (часть 1). Ст. 3451.

сударственные органы. Собственник информации также имеет право осуществить аналогичный контроль. Законом устанавливаются только перечни сведений, которые не могут быть отнесены к конкретному виду информации с ограниченным доступом. Исключение — перечень сведений, составляющих государственную тайну.

4. Государственная тайна как предмет, изъятый из гражданского оборота

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ[1].

Рассмотрим принципы засекречивания информации.

1. Принцип законности: конкретная информация должна соответствовать перечню сведений, составляющих государственную тайну.

2. Принцип обоснованности: целесообразность отнесения указанных сведений к государственной тайне устанавливается путем экспертной оценки вероятного ущерба интересам государства и общества и на основании баланса жизненно важных интересов личности, общества и государства.

3. Принцип своевременности:

— засекречивание с момента получения сведений;

— засекречивание заблаговременно.

4. Принцип обязательной защиты: сведения защищаются компетентными на то органами.

Перечень сведений, составляющих государственную тайну:

1) сведения в военной области:

— о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизацион-

[1] Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне// СЗ РФ. 1997. № 41. Ст. 4673; 2004. № 35. Ст. 3607.

ному развертыванию Вооруженных Сил РФ, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, создании и использовании мобилизационных ресурсов;

— о планах строительства Вооруженных Сил РФ, других войск РФ, направлениях развития вооружения и военной техники, содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

— о разработке, технологии, производстве, объемах производства, хранении, утилизации ядерных боеприпасов, их составных частей, делящихся 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;

— о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

— о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

— о дислокации, действительных наименованиях, организационной структуре, вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

— о содержании планов подготовки РФ и ее отдельных регионов к возможным военным действиям, мобилизационных мощностях промышленности по изготовлению и ремонту во-

оружения и военной техники, объемах производства, поставок, запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

— об использовании инфрастуктуры РФ в целях обеспечения обороноспособности и безопасности государства;

:— о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, степени обеспечения безопасности населения, о функционировании транспорта и связи в РФ в целях обеспечения безопасности государства;

— об объемах, планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, наличии и наращивании мощностей по их выпуску, связях предприятий по кооперации, о разработчиках или изготовителях указанных вооружения, военной техники и другой оборонной продукции;

— о достижениях науки и техники, научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

— о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней РФ, Центральном банке РФ, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых РФ (по списку, определяемому Правительством РФ);

3) сведения в области внешней политики и экономики:

— о внешнеполитической, внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства;

— о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распрост-

ранение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

— о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

— о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

— об организации, силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

— о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной, связи, о шифрах, разработке, изготовлении шифров и обеспечении ими, методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

— о методах и средствах защиты секретной информации;

— об организации и фактическом состоянии защиты государственной тайны;

— о защите Государственной границы РФ, исключительной экономической зоны и континентального шельфа РФ;

— о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в РФ;

— о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

Не подлежит засекречиванию следующие сведения.

1. Сведения о чрезвычайных происшествиях, катастрофах, угрожающих безопасности и здоровью граждан.

2. Сведения о состоянии экологии, здравоохранения, демографии, образования, культуры, сельского хозяйства и преступности.

3. Сведения о привилегиях, компенсациях, льготах, предоставляемых всем субъектам.

4. Сведения о фактах нарушения прав и свобод человека и гражданина.

5. Сведения о ресурсах золотого запаса и государственных валютных резервов.

6. Сведения о состоянии здоровья высших должностных лиц.

7. Сведения о фактах нарушения здравоохранения органами государственной власти и должностными лицами.

Степени секретности

1. Особая важность — сведения, разглашение которых может нанести ущерб интересам РФ (лицам, допущенным к сведениям, имеющим гриф «Особая важность», устанавливается компенсация в размере 30% надбавки к заработной плате).

2. Совершенно секретно — сведения, разглашение которых может нанести ущерб, может быть причинен министерствам и ведомствам (лицам, допущенным к сведениям, имеющим гриф «Совершенно секретно», устанавливается компенсация в размере 25% к заработной плате).

3. Секретно — ущерб, причиненный предприятиям, учреждениям, организациям (лицам, допущенным к сведениям, имеющим гриф «Секретно», устанавливается компенсация в размере 10% к заработной плате). Следует отметить, что до 1991 г. такого рода сведения относились к служебной тайне.

Основания рассекречивания

1. Взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими государственную тайну.

2. Изменение объективных обстоятельств.

3. Истечение установленного срока засекречивания (общий срок — 30 лет, но возможно установление большего сро-

ка межведомственной комиссией по защите государственной тайны).

Допуск к сведениям, составляющим государственную тайну, представляет собой процедуру оформления права на доступ к сведениям, составляющим государственную тайну элементов.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

1) принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

2) согласие на частичные, временные ограничения их прав в соответствии со ст. 24 Закона о государственной тайне; ограничения могут касаться:

— права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

— права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

— права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

3) письменное согласие на проведение в отношении них полномочными органами проверочных мероприятий;

4) определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных Законом о государственной тайне;

5) ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;

6) принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну;

7) социальные гарантии:

— процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

— преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством РФ. Целью проведения проверочных мероприятий является выявление оснований, предусмотренных ст. 22 Закона о государственной тайне.

Доступ к сведениям, составляющим государственную тайну, представляет собой непосредственное санкционированное ознакомление.

Защита прав государства на государственную тайну осуществляется в административном, судебном порядке в закрытом заседании.

5. Служебная и профессиональная тайна

В Советском Союзе существовала определенная система защиты информации с ограниченным доступом, в которой выделялось три вида такой информации: государственная тайна (информация с грифами «особой важности», «совершенно секретно»), служебная тайна (информация с грифом «секретно») и информация «для служебного пользования». С принятием в 1993 г. Закона РФ о государственной тайне гриф «секретно» был отнесен к сведениям, составляющим государственную тайну, а новый институт служебной тайны так и не получил достаточной правовой регламентации. То есть образовалась некая нормативная ниша, причем в первую очередь дефинитивного характера: формулировка «служебная тайна» встречается во многих нормативных актах, но соответ-

ствующего этим нормам законодательного определения служебной тайны не существует. Однако, если в- этом вопросе нет четкой правовой регламентации, невозможна реализация права на информацию и теряет значимость само ограничение доступа к ней.

Признаки отнесения сведений к служебной тайне:

1) сведения, содержащие служебную информацию о деятельности государственных органов или подведомственных им предприятий, организаций, запрет на распространение которых установлен законом или диктуется служебной необходимостью;

2) сведения, являющиеся конфиденциальной информацией для других лиц, но ставшие известными представителям государственных органов в силу исполнения ими служебных обязанностей.

Служебная тайна — защищаемая законом конфиденциальная информация, ставшая известной в государственных органах или органах местного самоуправления на законных основаниях, в силу исполнения ими служебных обязанностей, а также служебная информация о деятельности самого органа.

Критерии охраноспособности информации, составляющей служебную тайну:

1) информация, составляющая собственную служебную информацию о деятельности самого органа власти;

2) охраноспособная конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну, тайну частной жизни, — «чужая тайна»;

3) сведения, не являющиеся государственной тайной и не подпадающие под перечень сведений, доступ к которым не может быть ограничен;

4) получена информация в силу исполнения служебных обязанностей.

Объекты служебной тайны

1. Военная тайна.

2. Тайна следствия.

• 3. Судебная тайна.

4. Налоговая тайна.

5. Охраноспособная конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну, тайну частной жизни.

Определение служебной тайны дано в Указе Президента РФ об утверждении Перечня сведений конфиденциального характера, согласно которому служебная тайна представляет собой служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами[1].

Законодательного акта, который бы более подробно регулировал правовой режим служебной тайны, не было никогда, нет и сейчас.

В силу этого понятие служебной тайны по-разному трактуется в научной литературе. Большинство ученых склонно придерживаться мнения, что к служебной тайне относятся те сведения о физических и юридических лицах, которые становятся известными различным должностным лицам по роду их служебной деятельности, однако в силу своего особого характера не могут свободно распространяться. В силу этого к служебной тайне относят тайну следствия, врачебную тайну, налоговую тайну, адвокатскую тайну и др.[2]

Некоторые, однако, склонны считать, что к служебной тайне должны относиться лишь сведения о «скрытой» служебной деятельности государственных и муниципальных органов (например, сведения, связанные с организацией и проведением оперативной деятельности налоговых органов в целях выполнения задач, возложенных на них законом). При таком подходе налоговая, адвокатская и прочие тайны должны счи-

[1] См.: Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 1997. № Ю. Ст. 1127.

[2] См.: *Костров Д.* Чтобы лучше защитить, надо точно разграничить // http://www.bytemag.ru (по состоянию на 18 марта 2006 г.).

таться не служебными, а так называемыми «профессиональными»[1].

Представляется, однако, что все вышеуказанные виды конфиденциальной информации являются служебными тайнами, так как имеется общий признак: они становятся известными соответствующим должностным лицам в связи с их служебной деятельностью. При этом можно выделить два вида служебной тайны: 1) тайна деятельности соответствующего органа; 2) профессиональная тайна. Последняя зачастую может тесно пересекаться с личной, коммерческой, банковской и иными тайнами. Так, например, сведения о планах развития коммерческой организации, составляющие коммерческую тайну, ставшие известными на законных основаниях должностным лицам органов государственной власти, будут охраняться одновременно институтами коммерческой и служебной тайны. Информация об усыновлении или удочерении, относящаяся к личной тайне, будучи получена адвокатом в рамках его профессиональной деятельности, становится также адвокатской (служебной) тайной и т.д.

Правовой режим отдельных видов информации, составляющей служебную тайну, регулируется соответствующим законодательством.

Тайна предварительного расследования установлена ст. 161 УПК РФ. В соответствии с ч. 1 этой статьи данные предварительного расследования не подлежат разглашению.

Тайна совещания судей предусмотрена ст. 298 УПК РФ. Она устанавливает, что приговор постановляется судом в совещательной комнате. Во время постановления приговора в этой комнате могут находиться лишь судьи, входящие в состав суда по данному уголовному делу. Судьи не вправе разглашать суждения, имевшие место при обсуждении и постановлении приговора.

---

[1] См.: *Туманова Л.В., Снытников А.А.* Обеспечение и защита права на информацию. — М., 2001. С. 234.

Аналогичным образом ст. 341 УПК РФ регулирует тайну совещания присяжных заседателей. Гарантией соблюдения тайны совещания судей и тайны совещания присяжных заседателей является ст. 381 УПК РФ, которая указывает, что нарушение тайны совещания коллегии присяжных заседателей при вынесении вердикта или тайны совещания судей при постановлении приговора является безусловным основанием отмены или изменения судебного решения.

В соответствии со ст. 102 Налогового кодекса РФ налоговую тайну составляют любые полученные налоговым органом, органами налоговой полиции, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: 1) разглашенных налогоплательщиком самостоятельно или с его согласия; 2) об идентификационном номере налогоплательщика; 3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; 4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам).

Таможенный кодекс РФ от 28 мая 2003 г. № 61-ФЗ, хотя напрямую и не использует термины «служебная тайна» или «таможенная тайна», также устанавливает, что любая информация, полученная таможенными органами в соответствии с актами таможенного законодательства, иными правовыми актами РФ, правовыми актами федерального органа исполнительной власти, уполномоченного в области таможенного дела, может использоваться исключительно в таможенных целях (п. 1 ст. 10).

Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

Необходимость проставления пометки «Для служебного пользования» на документах и изданиях, содержащих служебную информацию ограниченного распространения, опре-

деляется исполнителем и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации.

Документы с пометкой «Для служебного пользования»:

— печатаются в машинописном бюро. На обороте последнего листа каждого экземпляра документа машинистка должна указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах;

— учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка «ДСП»;

— передаются работникам подразделений под расписку;

— пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;

— размножаются (тиражируются) только с письменного разрешения соответствующего руководителя. Учет размноженных документов осуществляется поэкземплярно;

— хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

При необходимости направления документов с пометкой «Для служебного пользования» по нескольким адресам составляется указатель рассылки, в котором поадресно про-

ставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка «Для служебного пользования».

Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения соответствующего руководителя.

При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-сдачи этих документов, который утверждается соответствующим руководителем.

Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования» проводится не реже одного раза в год комиссиями, назначаемыми приказом руководителя. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

В библиотеках и архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой «Для служебного пользования», проверка наличия может проводиться не реже одного раза в пять лет.

Результаты проверки оформляются актом.

О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для

расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные документы, дела и издания с пометкой «Для служебного пользования» составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

При снятии пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

Профессиональная тайна определяется тремя признаками.

1. Профессиональная принадлежность.

2. Конфиденциальная информация добровольно доверяется лицу, исполняющему соответствующие профессиональные обязанности, по выбору владельца этой информации.

3. У лица, к которому поступает такая информация, возникает обязанность обеспечить ее сохранность.

Профессиональная тайна — защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой. Распространение этой информации может нанести ущерб доверителю, но при этом информация не является государственной коммерческой тайной.

Критерии охраноспособности

1. Информация стала известной в силу профессиональных обязанностей.

2. Держатель не состоит на государственной, муниципальной службе.

• 3. Запрет на распространение установлен законом.

4. Не относится к государственной, коммерческой тайне.

Объекты информации, составляющей профессиональную тайну.

1. Врачебная тайна.
2. Тайна связи.
3. Нотариальная тайна.
4. Адвокатская тайна.
5. Тайна усыновления.
6. Тайна страхования.
7. Тайна исповеди.

Субъекты профессиональной тайны:

1) доверитель;

2) держатель;

3) пользователь (государственные органы, которым становится известна государственная тайна в связи с использованием служебных обязанностей).

Так, например, *адвокатская тайна* в настоящее время установлена Федеральным законом от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»[1]. Адвокатской тайной являются любые сведения связанные с оказанием адвокатом юридической помощи своему доверителю. Гарантией адвокатской тайны является запрет допроса адвоката в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. Полученные в ходе оперативно-розыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей.

Наконец, нотариальная тайна регулируется ст. 16 Основ законодательства о нотариате от 11 февраля 1993 г.

[1] СЗ РФ. 2002. № 23. Ст. 2102; 2004. № 52 (часть I). Ст. 5267.

№ 4462-1[1]: нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности. Суд может освободить нотариуса от обязанности сохранения тайны, если против нотариуса возбуждено уголовное дело в связи с совершением нотариального действия.

Медицинская (врачебная) тайна. К сведениям, составляющим медицинскую тайну, закон относит информацию о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении (ст. 61 Основ законодательства РФ об охране здоровья граждан от 22 июля 1993 г. № 5487-1[2]), сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья (ст. 9 Закона РФ от 2 июля 1992 г. № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»[3]). Передача этих сведений третьим лицам допускается лишь с согласия гражданина или его законного представителя. На медицинский персонал и лиц, которым в установленном порядке переданы эти сведения, возлагается обязанность обеспечивать конфиденциальность этих сведений и предотвращать нарушение врачебной тайны со стороны третьих лиц. За незаконный сбор и разглашение сведений, составляющих медицинскую тайну, журналист будет нести ответственность по ст. 137 УК РФ (если имелась корыстная или иная личная заинтересованность) как за нарушение неприкосновенности частной жизни. С нарушителя в пользу пострадавшего может быть взыскана также денежная компенсация морального вреда.

---

[1] Ведомости СНД РФ и ВС РФ. 1993. № 10. Ст. 357; СЗ РФ. 2004. №45. Ст. 4377; 2005. № 27. Ст. 2717; 2006. № 27. Ст. 2881.

[2] Ведомости СНД РФ и ВС РФ. 1993. № 33. Ст. 1318; СЗ РФ. 2004. № 49. Ст. 4850; 2006. № 1. Ст. 10; № 6. Ст. 640.

[3] Ведомости СНД РФ и ВС РФ. 1992. № 33. Ст. 1913; СЗ РФ. 2004. № 35. Ст. 3607.

Журналистская тайна. В соответствии со ст. 41 Закона о СМИ редакция СМИ не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне, обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени. Единственное исключение из этого правила — случай поступления требования о предоставлении сведений об источнике информации от суда в связи с находящимся в его производстве делом (причем даже тогда редакция вправе взять всю полноту ответственности на себя, дабы сохранить инкогнито автора или иного источника информации). Поскольку редакция — коллективный субъект, она не может давать свидетельские показания, а может только письменно ответить на судебный запрос. Соответственно и юридической ответственности за лжесвидетельство или отказ от дачи свидетельских показаний редакция не несет. Журналист также обязан сохранять конфиденциальность информации и ее источника (п. 4 ст. 49 Закона о СМИ). Никто, в том числе и суд, не вправе заставить его раскрыть содержание и источник доверительной информации. Угрозы о применении к журналисту мер уголовной ответственности за отказ от дачи свидетельских показаний в данном случае являются необоснованными, поскольку по смыслу ст. 51 Конституции РФ и п. 4 ст. 49 Закона о СМИ журналист освобожден от обязанности давать свидетельские показания о содержании и источнике доверительной информации. За распространение сведений, предоставленных под условием неразглашения, за раскрытие псевдонима или инкогнито источника информации возможны в зависимости от содержания разглашенной информации и последствий разглашения различные виды ответственности: как уголовная (ст. 137 УК РФ (см. выше)), так и гражданско-правовая (денежная компенсация морального вреда, возмещение причиненных в результате разглашения убытков).

Тайна записи актов гражданского состояния. Акты гражданского состояния — действия граждан или события, влияю-

щие на возникновение, изменение или прекращение прав и обязанностей, а также характеризующие правовое состояние граждан (брак, гражданство, семейную и национальную принадлежность). Государственной регистрации подлежат: рождение, заключение брака, расторжение брака, усыновление (удочерение), установление отцовства, перемена имени и смерть (ст. 3 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»[1]). Сведения, ставшие известными работнику органа ЗАГС в связи с государственной регистрацией акта гражданского состояния, являются персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат (ст. 12 упомянутого Закона). Таким образом, в книге ЗАГС фиксируются сведения, относящиеся к частной жизни, и, следовательно, журналист, незаконно собирающий или распространяющий такую информацию, сознавая противоправность своих действий, несет за это юридическую (уголовную (ст. 137 «Нарушение неприкосновенности частной жизни», ст. 155 «Разглашение тайны усыновления» УК РФ) или гражданскую) ответственность наравне с предоставившим такую информацию. То же самое можно сказать и об ответственности **за** разглашение без согласия субъектов информации нотариальной тайны и тайны совершения сделок: вид ответственности зависит от характера распространенной информации, мотивов и последствий ее распространения.

6. Тайна частной жизни

Тайна частной жизни — составной элемент права на неприкосновенность частной жизни, но тайна частной жизни включает в себя личную, семейную тайну и охрану персональных данных.

Правовая охрана права на неприкосновенность частной жизни осуществляется установлением конституционных гарантий. Информация, затрагивающая неприкосновенность частной

[1] СЗ РФ. 1997. № 47. Ст. 5340; 2003. № 17. Ст. 1553; 2006. № 1. Ст. 10.

жизни и ставшая известной на законных основаниях другим лицам, должна охраняться в режиме профессиональной или служебной тайны.

Институт защиты персональных данных. Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Эти сведения не могут быть использованы без письменного согласия субъекта персональных данных.

Критерий охраноспособности: распространение этих сведений может нанести вред чести, достоинству, деловой репутации, доброму имени или другим нематериальным благам и имущественным интересам.

К объектам персональных данных относятся следующие.

1. Биографические и опознавательные данные.
2. Личные характеристики.
3. Семейное положение.
4. Имущественное, финансовое положение.
5. Состояние здоровья.

Так как каждый гражданин в процессе своей жизни вступает во взаимоотношения с различными предприятиями, организациями, учреждениями, а также другими гражданами и при этом у последних происходит накопление данных о конкретном индивиде, начиная с самых простых (фамилия, имя, отчество, дата и место рождения и т.п.) и заканчивая очень специфическими (сведения о заболеваниях, судимостях, размерах доходов, имуществе и пр.). Все это исходя из предложенного определения и следует считать примерами персональных данных.

Впервые нормы, касающиеся персональных данных, были введены Конституцией РФ 1993 г., провозгласившей право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (см. ч. 1

ст. 23) и право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (см. ч. 2 ст. 23), а также недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (см. ч. 1 ст. 24).

Пункт 9 ст. 9 Федерального закона об информации устанавливает, что персональные данные относятся к категории конфиденциальной информации:

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

По поводу персональных данных возникают правоотношения между субъектами персональных данных (лица, к которым относятся данные, их наследники) и операторами (государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных).

Правовой статус субъекта персональных данных

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны со-

держаться персональные данные, относящиеся к другим субъектам персональных данных. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных 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 Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, когда наличествует согласие в письменной форме субъекта персональных данных или в иных случаях, предусмотренных федеральными законами.

Правовой статус оператора

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на .основании исключи-

тельно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов. Оператор обязан рассмотреть возражение в течение семи рабочих дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

Оператор при обработке персональных данных 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. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением таких технологий ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

Оператор обязан сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

В случае отказа оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя, либо с даты получения запроса субъекта персональных данных или его законного представителя.

Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением нижеследующих случаев:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

Персональные данные по общему правилу относятся к конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях:

— обезличивания персональных данных;

— по желанию субъекта персональных данных;

— в отношении общедоступных персональных данных. (Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.)

В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных

данных либо по решению суда или иных уполномоченных государственных органов.

Субъект персональных данных самостоятельно принимает решение о предоставлении кому-либо своих персональных данных. Обработка персональных данных может проводится только с согласия субъекта персональных данных.

Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением следующих случаев:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Как отмечает Павел Анни[1], в решении на базе «тонких» клиентов все пользовательские данные и запускаемые приложения хранятся и управляются централизованно. Системный администратор определяет, какие приложения будут доступны пользователям (с точностью до пользователя), контролирует хранимые данные (на вирусы, конфиденциальность, мусор), управляет распределением ресурсов.

[1] *Анни П.* О «тонком» клиенте замолвите слово // РГ. 2003. № 65.

В то же самое время работодатель не имеет права незаконно собирать или распространять сведения о частной жизни работника, составляющие его личную или семейную тайну, без его согласия; нарушать тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. Нарушение указанных запретов влечет уголовную ответственность (ст. 137, 138 УК РФ).

Выходом из сложившейся ситуации может стать разработка работодателем политики компании в отношении использования электронной почты и доступа в Интернет на рабочем месте служащего. Эффективной с точки зрения работодателя будет политика уведомления работника о том, что все частные, не относящиеся к работе действия последний совершает на свой риск и не может рассчитывать в данном случае на неприкосновенность личной жизни. Работодатель должен разъяснить служащим, в каких случаях можно использовать телефонную связь и электронную почту в личных целях и какое использование может повлечь применение дисциплинарного взыскания.

Работодатель может в договоре с работником установить, что последний согласен на контроль и блокировку сообщения и на разглашение сведений о возможных получателях информации. Однако в данном случае возникает другая проблема. Дело в том, что другая сторона, участвующая в информационном обмене, также пользуется правом неприкосновенности частной жизни, переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Это означает, что согласие последней на контроль и блокировку сообщения также необходимо. Таким образом, наблюдение в режиме реального времени за сообщениями работников, общающихся с лицами, не давшими согласия на такое наблюдение, может повлечь применение соответствующих мер ответственности. В данном случае целесообразно сначала получить необходимое согласие и только потом исследовать сообщение, сохранившееся на сервере компании.

Кроме того, работодатель может предоставить служащим возможность пользоваться персональными средствами связи.

В Великобритании проблема противоречия между потребностями работодателя и правом служащего на конфиденциальность информации появилась при рассмотрении и принятии Закона о регулировании следственных действий (The Regulation of Investigatory Powers Act (RIPA))[1], который предусматривает контроль и блокировку как сообщений, отправляемых по электронной почте, так и телефонных переговоров и, что наиболее спорно, раскрытие ключей шифрования. Причем служащие и работодатели одинаково подпадают под сферу действия данного Закона.

Вместе с тем в октябре 2000 г. в Великобритании вступили в силу Акт о правах человека 1998 г. и так называемые нормы «Законной Деловой Практики» (The Lawful Business Practice regulations), которым работодатели также должны подчиняться. В Акте о правах человека указано, что каждый имеет право на защиту частной и семейной жизни, жилища, корреспонденции.

Профессиональные союзы заявили, что RIPA предоставляет слишком значительные полномочия работодателям по контролю персональной информации. Представители работодателей утверждали, что получение согласия отправителя и получателя информации (как основание для законного контроля) проблематично. В итоге правительством были выработаны определенные ограничения[2].

Теперь контроль и блокировка сообщений допускается, если работодатель обоснованно убежден, что будет получено согласие отправителя и получателя сообщения на его контроль. Если согласие не получено, то контроль и блокировка могут быть осуществлены для:

---

[1] RIPA (2000) был одобрен 28 июля 2000 г. и поэтапно вступил в силу в течение осени 2000 — весны 2001.

[2] Shaw Pittman. Regulation of Investigatory Powers Act. ALERT. December 2000. Number 5: http://library.lp.findlaw.com/articles/00104/003812.pdf

1) установления существования фактов (например, сделки) или согласия с применяемыми методами и процедурами;

2) предотвращения или обнаружения признаков преступления или несанкционированного использования системы;

3) обеспечения эффективной работы самой системы.

Даже если такой контроль осуществлялся в рамках «законной деловой практики», он будет допущен только:

1) для целей бизнеса;

2) если работодатель предпринял все «разумные меры», чтобы предупредить отправителя и получателя информации о том, что сообщение может быть перехвачено (например, путем телефонного сообщения или с помощью электронной почты).

Возникновение в России новых общественных отношений в связи с функционированием Интернета, их трансформация в основных сферах общественной жизни существенно влияют на становление информационных правоотношений, которые требуют особого регулирования. В данном случае представляется целесообразным использование положительного опыта зарубежных стран.

7. Коммерческая и банковская тайна

Коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду[1].

Информация составляет **коммерческую** тайну, если это научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность

[1] См.: Статья 3 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283; 2006. № 6. Ст. 636.

в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны[1].

Таким образом, можно выделить три признака относимости информации к коммерческой тайне:

— информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;

— отсутствует свободный доступ к информации;

— обладатель информации принимает меры к охране ее конфиденциальности.

Первый признак означает, что к коммерческой тайне не могут быть отнесены сведения, которые заведомо не могут обладать коммерческой ценностью. Например, не может быть коммерческой тайной информация о планировке офиса фирмы и т.п.

Информация теряет свой статус коммерческой тайны в случае, если она становится общедоступной, т.е. отсутствует второй признак коммерческой тайны. Речь идет о случаях, когда сам владелец информации опубликовал ее в СМИ и тем самым сделал ее известной широкому кругу лиц.

Информация не будет признана коммерческой тайной также в тех случаях, когда ее владелец, хотя и не разгласил информацию сам, но не принял мер по ее охране от доступа других лиц, т.е. доступ к ней был открыт для каждого[2].

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения

---

[1] См.: Статья 3 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283; 2006. № 6. Ст. 636.

[2] См.: *Строганова И.В.* Правовой режим конфиденциальной информации (гражданско-правовой аспект): Автореф. дис. ... канд. юрид. наук. — Екатеринбург, 2004. С. 7.

записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, составе работников, системе оплаты труда, об условиях труда, в том числе об охране труда, показателях производственного травматизма и профессиональной заболеваемости, наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, размерах и составе их имущества, их расходах, численности и об оплате труда их работников, использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами (ст. 5 Федерального закона о коммерческой тайне).

Субъекты коммерческой тайны:

1) обладатели коммерческой тайны — сама организация и сотрудники, работающие в ней;

2) правопреемники — лица, которым информация, составляющая коммерческую тайну, стала известна в силу служебного положения, в силу исполнения профессиональных обязанностей, в силу договора, на ином законном основании.

Режим коммерческой тайны:

1) конфиденциальное отношение по контракту — с момента трудоустройства между сотрудником и юридическим лицом оформляется в трудовом договоре (контракте) или в приложении к нему;

2) конфиденциальное отношение по служебным функциям — такие отношения возникают между сотрудниками одной фирмы, определяется должностными инструкциями;

3) конфиденциальное отношение по условиям договора — между заказчиком и исполнителем, оформляется в гражданском договоре.

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

Субъекты банковской тайны:

1) владельцы банковской тайны — клиенты;

2) пользователи банковской тайны — банки.

Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате РФ, налоговым органам, таможенным органам РФ в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора — органам предварительного следствия по делам, находящимся в их производстве.

В соответствии с законодательством РФ справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений.

Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, организации, осуществляющей функции по обязательному страхованию вкладов, при наступлении страховых случаев, предусмотренных федеральным законом о страховании вкладов физических лиц в банках РФ, а при наличии согласия прокурора — органам предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан — иностранным консульским учреждениям.

Информация по операциям юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, и физических лиц предоставляется кредитными организациями в уполномоченный орган, осуществляющий меры по противодействию легали-

зации (отмыванию) доходов, полученных преступным путем, в случаях, порядке и объеме, которые предусмотрены Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[1].

Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные ими в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

Уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, не вправе раскрывать третьим лицам информацию, полученную от кредитных организаций в соответствии с Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», за исключением случаев, предусмотренных указанным Федеральным законом.

За разглашение банковской тайны Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, кредитные, аудиторские и иные организации, уполномоченный орган, осуществляющий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

[1] СЗ РФ. 2001. № 33 (часть I). Ст. 3418; 2005. № 47. Ст. 4828.

Организация, осуществляющая функции по обязательному страхованию вкладов, не вправе раскрывать третьим лицам информацию, полученную в соответствии с федеральным законом о страховании вкладов физических лиц в банках РФ.

Информация по операциям юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, и физических лиц с их согласия представляется кредитными организациями в целях формирования кредитных историй в бюро кредитных историй в порядке и на условиях, которые предусмотрены заключенным с бюро кредитных историй договором в соответствии с Федеральным законом от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»[1].

Глава 6. Правовое регулирование, создание и применение информационных технологий

1. Понятие и виды информационных технологий

Технология — это комплекс научных и инженерных знаний, реализованных в приемах труда, наборах материальных, технических, энергетических, трудовых факторов производства, способах их соединения для создания продукта или услуги, отвечающих определенным требованиям. Поэтому технология неразрывно связана с машинизацией производственного или непроизводственного, прежде всего управленческого процесса. Управленческие технологии основываются на применении компьютеров и телекоммуникационной техники.

Согласно определению, принятому ЮНЕСКО, информационная технология — это комплекс взаимосвязанных, научных, технологических, инженерных дисциплин, изучающих

[1] СЗ РФ. 2005. № 1 (часть I). Ст. 44; № 30 (часть II). Ст. 3121.

методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы. Сами информационные технологии требуют сложной подготовки, больших первоначальных затрат и наукоемкой техники. Их введение должно начинаться с создания математического обеспечения, формирования информационных потоков в системах подготовки специалистов.

Информационные технологии — это комплекс объектов, действий и правил, связанных с подготовкой, переработкой и доставкой информации при персональной, массовой и производственной коммуникации, а также все технологии и отрасли, интегрально обеспечивающие перечисленные процессы.

Правовое регулирование информационных технологий должно охватывать следующие аспекты.

1. Вид продукции.
2. Автор продукции.
3. Функциональная сфера применения продукта.
4. Его назначение.
5. Опытное, случайное или массовое изготовление.
6. Включение в сферу обмена.
7. Использование.

Выделяют два блока правового регулирования:

1) правовое регулирование создания информационных технологий (авторское право);

2) правовое регулирование применения информационных технологий в социальной, культурной, экономической жизни.

Виды информационных технологий

1. Высокие интеллектуальные информационные технологии — генерация технических решений, реализующих ситуационное моделирование, позволяющих выявить связь элементов, их динамику и обозначить объективные закономерности среды.

2. Вспомогательные информационные технологии — ориентированы на обеспечение выполнения определенных функций (бухгалтерский учет и статистика, ведение системы кадров, документооборота, ведение финансовых операций, системы для стратегического управления и т.д.).

3. Коммуникационные информационные технологии — призваны обеспечивать развитие телекоммуникации и ее систем.

2. Порядок создания информационных технологий

Порядок создания информационных технологий регламентируется главой 38 ГК «Выполнение научно-исследовательских, опытно-конструкторских и технологических работ», в соответствии с которой выделяют два субъекта создания информационных технологий: исполнителя и заказчика. Их правовой статус включает в себя следующие обязанности.

Исполнитель обязан:

— выполнить работу;

— передать заказчику ее результаты;

— согласовать с заказчиком необходимость использования охраняемых результатов интеллектуальной деятельности, принадлежащих третьим лицам, а также должен незамедлительно информировать заказчика о невозможности получить ожидаемые результаты.

Обязанности заказчика:

— передать исполнителю необходимую для выполнения работы информацию;

— принять, оплатить работу.

Порядок создания информационных технологий частично регулируется Законом от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

Обеспечение защиты интеллектуальной собственности в сфере использования информационных технологий осуществляется следующим образом.

В сфере государственного управления используются программно-технические средства, имеющие соответствующие

лицензии. Ответственность за выполнение данного требования несут федеральные органы государственной власти в соответствии с законодательством РФ.

Обеспечение использования лицензионных программно-технических средств в деятельности федеральных органов государственной власти должно осуществляться на основе:

• *S* ускоренной разработки отечественных программно-технических средств и их применения в государственных информационных системах и ресурсах;

S свободного распространения типовых решений, разработанных в рамках создания государственных информационных систем и ресурсов за счет средств федерального бюджета;

• *S* обеспечения открытости и возможности анализа кода закупаемого готового программного обеспечения зарубежного производства;

• *S* увеличения финансирования по статьям бюджета, обеспечивающим возможность лицензионного сопровождения программно-технических средств для нужд федеральных органов государственной власти;

• *S* централизации проведения закупок в сфере лицензионного программного обеспечения в интересах федеральных органов государственной власти;

• *S* инвентаризации используемого в федеральных органах государственной власти программного обеспечения, результатов НИОКР, разработанных за счет средств федерального бюджета в научно-исследовательских организациях;

S закупки лицензионных программно-технических средств, соответствующих открытым стандартам взаимодействия.

В целях повышения эффективности работы в этой сфере в ежегодном докладе об использовании современных информационных технологий в деятельности федеральных органов государственной власти предусматривается представление материалов об объемах применения лицензионных программно-технических средств, а также о выявленных фактах нарушения прав интеллектуальной собственности.

Материалы по указанной проблеме ежегодно представляются на рассмотрение Правительственной комиссии по противодействию нарушениям в сфере интеллектуальной собственности. Целесообразным является создание в составе указанной Комиссии межведомственной рабочей группы, ответственной за разработку и реализацию мероприятий, направленных на недопущение использования в системе федеральных органов государственной власти программно-технических средств, не имеющих соответствующих лицензий.

В России отсутствуют необходимые условия для наращивания потенциала информационных технологий и их использования в интересах общества.

Необходимо создать следующие условия:

1) финансирование;

2) занятость населения в данной сфере;

3) обеспечить компьютерами;

4) усилить инфраструктуру производства, создать государственное (централизованное) управление в области создания информационных технологий;

5) создать единые стандарты информационных технологий.

Государственная политика в сфере использования информационных технологий направлена на решение следующих основных задач:

— реализация стратегических приоритетов в использовании информационных технологий в государственном управлении, формирование единого механизма межведомственной координации реализации государственных программ и проектов создания государственных информационных систем и ресурсов в соответствии с целями социально-экономического развития;

— формирование общей информационно-технологической инфраструктуры для обеспечения деятельности федеральных органов государственной власти;

— распространение практики предоставления гражданам и организациям доступа к открытой информации о деятельности федеральных органов государственной власти, соответ-

ствующим государственным информационным ресурсам, в том числе через сеть «Интернет»;

— организация интерактивного информационного обслуживания граждан и организаций с использованием современных информационных технологий;

— обеспечение информационной безопасности деятельности федеральных органов государственной власти и элементов информационно-технологической инфраструктуры;

— развитие единой защищенной телекоммуникационной инфраструктуры для государственных нужд, системы удостоверяющих центров в области электронной цифровой подписи и электронной среды взаимодействия, обеспечивающей эффективный межведомственный информационный обмен;

— разработка стандартов в сфере использования информационных технологий в деятельности федеральных органов государственной власти, создания государственных информационных систем, их интеграции и совместного использования в рамках создания общего информационного пространства федеральных органов государственной власти;

— централизованное создание общих государственных информационных ресурсов (регистров, кадастров, реестров, классификаторов), содержащих полную, непротиворечивую, достоверную, актуальную информацию, необходимую для выполнения основных функций государственного управления, обеспечения доступности соответствующих данных на межведомственном уровне, а также для граждан и организаций в соответствии с требованиями, установленными законодательством РФ;

— построение единой системы управления процессом использования информационных технологий в деятельности федеральных органов государственной власти, обеспечивающей эффективную межведомственную координацию реализуемых государственных программ и проектов, их согласованное и взаимоувязанное выполнение в соответствии с основными приоритетами социально-экономического развития;

— распространение на уровне федеральных органов государственной власти практики долгосрочного планирования

государственных программ и проектов использования информационных технологий, повышение эффективности управления их выполнением;

— увеличение объемов, объединение и централизация закупок однотипной продукции в сфере информационных технологий в интересах федеральных органов государственной власти для получения эффекта экономии на масштабе;

— создание единой системы мониторинга и контроля эффективности использования информационных технологий в деятельности федеральных органов государственной власти;

— реализация комплексных программ подготовки и повышения квалификации государственных служащих в части использования информационных технологий, развитие необходимой образовательной инфраструктуры и методического обеспечения;

— совершенствование законодательной и иной нормативной правовой базы в целях повышения эффективности использования информационных технологий в деятельности федеральных органов государственной власти с учетом международной практики;

— защита интеллектуальной собственности, недопущение использования в деятельности федеральных органов государственной власти программного обеспечения, не имеющего соответствующей лицензионной поддержки.

3. Применение информационных технологий государственными органами, юридическими лицами и физическими лицами

Применение информационных технологий выражается во включении программного продукта в рынок информационных технологий и использовании информационных технологий.

Включение в рынок может осуществляться следующими способами.

1. Выпуск в свет — опубликование осуществляется, как правило, на бумажном носителе, число копий информационных технологий должно соответствовать числу потребителей.

2. Воспроизведение — один раз воспроизводится на электронном носителе и передается определенному потребителю.

3. Распространение — число копий информационных технологий неограниченно и передается неопределенному числу потребителей, например продажа, прокат, наем, заем и т. д.

Стремительное развитие информационных технологий, возрастающие в геометрической прогрессии мировые информационные ресурсы-создают необходимость для разработки технологии использования мировых информационных ресурсов, способствующих минимизации рисков в различных областях человеческой деятельности. Инструментом или фильтром для получения необходимой информации из мировых информационных ресурсов может являться «Методика получения релевантной информации», включающая следующие методы:

— метод получения релевантной информации с помощью Интернета;

— метод получения релевантной информации с помощью магнитных носителей;

— метод получения релевантной информации с использованием технологии лингвистических роботов;

— метод обработки информационных потоков на предмет правомерности использования (соблюдение авторских прав);

— метод определения статуса легитимности документов, полученных из электронных источников. Количественный и качественный состав предложенной методики меняется с развитием информационно-лингвистических технологий.

Только на федеральном уровне (Дума, Президент, Правительство, федеральные ведомства) ежегодно выпускается до 35 000 документов нормативного характера. По данным, обнародованным на Совещании руководителей юридических служб федеральных органов государственной власти и их аппаратов, в России сейчас действует около полутора миллионов нормативных актов, включая акты субъектов Федерации. Порядок обязательного опубликования нормативных актов (ст. 15 Кон-

ституции РФ и другие документы) по различным причинам нарушается, реально публикуется не более 40% действующих документов, причем зачастую с большим опозданием. Остальное поступает по рассылке только государственным органам, причем не все и не всем. На ведомственном уровне существует тенденция ограничения доступа к собственной информации для прочих государственных органов и ее полного закрытия для негосударственных структур. Электронные справочно-правовые системы (Эталон, Контур, Кодекс, Гарант, Консультант Плюс, всего их в России порядка 30), каждая в отдельности, не решают проблемы полного, оперативного, достоверного получения информации. Существующие методики оценки справочно-правовых систем указывают на орфографические и смысловые ошибки в текстах нормативно-правовых актов, от 3 до 18 ошибок на 100 страниц текста.

В рамках создания единого мирового хозяйства в настоящий момент закладывается фундамент международной информационной магистральной системы, в которой, как в зеркале, должны найти отражение все основные виды человеческой деятельности при условии реализации принципа взаимного доверия на мировом, государственном, региональном, местном уровнях. Инструментом или фильтром для адекватного представления видов человеческой деятельности в мировой информационной магистральной системе может стать технология использования мировых информационных ресурсов, количественный и качественный состав которой меняется с развитием информационно-лингвистических технологий. Для получения максимального положительного эффекта реализацию принципа взаимного доверия и задачи по определению зон риска необходимо совместить с технологией использования мировых информационных ресурсов.

Доктрина информационной безопасности (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895)[1] включила информаци-

[1] Текст доктрины опубликован в «Российской газете» от 28 сентября 2000 г. № 187.

онные технологии как третью составляющую (информационные ресурсы) национальных интересов в России в информационной сфере.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

— развивать и совершенствовать инфраструктуру единого информационного пространства РФ;

— развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

— развивать производство в РФ конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

— обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Существуют ограничения в применении информационных технологий.

1. Разработка и распространение программ, нарушающих нормативное функционирование информационной и телекоммуникационной систем.

2. Внедрение в апробированные программы изделий и компонентов, реализующих функции, не предусмотренные документацией на эти программы.

3. Компрометация ключей и средств криптографической защиты информации.

4. Воздействие на параллельно-ключевые системы защиты автоматизирующих систем обработки и передачи информации.

5. Внедрение электронных устройств для перехвата информации в технических устройствах обработки, хранения и передачи информации.

4. Нарушение порядка применения информационных технологий: информационная война, информационное оружие

Информационная война — это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий и использованию наших собственных военных информационных функций. Это определение является основой для следующих утверждений. Информационная война — это любая атака против информационной функции независимо от применяемых средств. Бомбардировка АТС — операция информационной войны. То же самое можно сказать и про вывод из строя программного обеспечения компьютера АТС. Информационная война — это любое действие по защите наших собственных информационных функций независимо от применяемых средств. Укрепление и оборона здания АТС против бомбардировок — тоже часть информационной войны. То же самое можно сказать и про антивирусную программу, которая защищает программное обеспечение АТС. Информационная война — только средство, а не конечная цель аналогично тому, как бомбардировка — средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия. Военные всегда пытались воздействовать на информацию, требующуюся врагу для неэффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как

эти стратегии воздействовали на информацию, получаемую врагом, косвенно, путем восприятия, они атаковали информацию врага косвенно. То есть для того, чтобы хитрость была неэффективной, враг должен был сделать три вещи: наблюдать обманные действия, посчитать обман правдой, действовать после обмана в соответствии с целями обманывающего.

Тем не менее современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляциям с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящих к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить (но не до нуля) эту уязвимость.

Составные части информационной войны:

1) психологические операции — использование информации для воздействия на аргументацию солдат врага;

2) электронная война — не позволяет врагу получить точную информацию;

3) дезинформация — предоставляет врагу ложную информацию о наших силах и намерениях;

4) физическое разрушение — может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем;

5) меры безопасности — стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях;

6) прямые информационные атаки — прямое искажение информации без видимого изменения сущности, в которой она находится.

Существуют три цели информационной войны:

— контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши воен-

ные информационные функции от вражеских действий (контр-информация);

— использовать контроль за информацией для ведения информационных атак на врага;

— повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

Информационная война — действия, направленные на достижение информационного превосходства, поддержку национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственника информации.

Определим особенности информационной войны.

1. Объект воздействия — все виды информации и информационной системы.

2. Объект воздействия может выступать как оружие и как объект защиты.

3. Расширяются территория и пространство ведения войны.

4. Информационная война ведется как при объявлении войны, так и в кризисных ситуациях.

5. Информационная война ведется как военными, так и гражданскими структурами.

Концепция информационной войны:

1) подавление элементов инфраструктуры государственного, военного управления;

2) радиоэлектронная борьба (электронно-магнитное воздействие);

3) радиоэлектронная разведка;

4) хакерная война;

5) формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации (тенденциозной информации для воздействия на оценку намерения и ориентацию населения и лиц, принимающих решение). Оно может осуществляться путем

применения следующих мер информационного воздействия:

— реструктуризация — перевод события из одной зоны восприятия в другую;

— умолчание;

— тиражирование;

— утечка;

— периферийный ввод информации в обиход;

— неадекватное форматирование;

6) получение интересующей информации путем перехвата и обработки открытой информации.

Способы защиты информации в Интернете

Организационные (административные) меры, направленные на разработку и создание информационной системы, на построение адекватной требованиям текущего момента времени политики безопасности: на данную группу мер приходится до 50-60% от всех ресурсов, расходуемых на защиту информации. В качестве примера такого рода мер можно привести разработку и принятие правил информационной безопасности на конкретном предприятии.

Физические меры защиты направлены на управление доступом физических лиц, автомобилей, грузов в охраняемую зону, а также на противодействие средствам агентурной и технической разведки. На данные меры тратится примерно 15-20% от всех ресурсов, расходуемых на защиту информации. Наиболее типичным образцом является организация контрольно-пропускного режима на предприятии.

Технические (иногда говорят «технологические, или аппаратно-программные») меры защиты направлены на обеспечение безопасности непосредственно на каждом компьютерном рабочем месте, в локальной сети, на серверах, устройствах, входящих в состав телекоммуникаций. На долю этой группы мер выпадает до 20-25% от всех ресурсов, расходуемых на защиту информации. К такого рода мерам можно отнести использование различных антивирусов, файерволов и т.д.

Законодательные меры, связанные с разработкой и исполнением законодательных и нормативных актов, направленных на пресечение несанкционированных действий с защищаемой информацией и на защиту прав граждан, общества, государства в информационной сфере. На данные меры тратится примерно 5% от всех ресурсов, расходуемых на защиту информации.

Зарубежный опыт показывает, что наиболее эффективной защитой от компьютерных правонарушений является введение в штатное расписание организаций должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб, как частных, так и централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации, по оценкам зарубежных специалистов, снижает вероятность совершения компьютерных преступлений вдвое.

Кроме того, в обязательном порядке должны быть реализованы следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к служебной и коммерческой тайне, должны быть определены категории доступа;

2) определена административная ответственность за сохранность и санкционированность доступа к информационным ресурсам;

3) налажен периодический системный контроль за качеством защиты информации;

4) проведена классификация информации в соответствии с ее важностью, дифференциация на основе этого мер защиты;

5) организована физическая защита служебной и коммерческой тайны.

Помимо организационно-управленческих мер, существенную роль в борьбе с компьютерными преступлениями могут играть меры технического характера (аппаратные, программные и комплексные).

Аппаратные методы предназначены для защиты компьютерной техники от нежелательных физических воздействий

и закрытия возможных каналов утечки конфиденциальной информации. К ним относятся источники бесперебойного питания, устройства экранирования аппаратуры, шифрозамки и устройства идентификации личности.

Программные методы защиты предназначаются для непосредственной защиты информации. Для защиты информации при ее передаче обычно используют различные методы шифрования данных. Как показывает практика, современные методы шифрования позволяют достаточно надежно скрыть смысл сообщения. Например, в США в соответствии с директивой Министерства финансов начиная с 1984 г. все общественные и частные организации были обязаны внедрить процедуру шифрования коммерческой информации по системе *DES (Data Encryption Standard)*. Как правило, российские пользователи справедливо не доверяют зарубежным системам, взлом которых стал любимым развлечением хакеров и всяких «джеймсов бондов». Однако и российские государственные системы тоже могут быть ненадежными: когда над Охотским морем советскими истребителями был сбит корейский пассажирский самолет, правительство США уже через неделю представило в ООН дешифровку переговоров наших военных летчиков со станциями слежения. Но с тех пор прошло много лет. Разработаны, сертифицированы и активно используются десятки отечественных систем шифрования. Некоторые из них имеют криптографическую защиту, т.е. теоретически не могут быть взломаны за разумное время (менее десяти лет) даже сотрудниками ФАПСИ и уж тем более любопытствующими хакерами.

Информационное оружие — это средство уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничение, воспроизведение доступа к ним заказных пользователей, дезорганизация работы технических устройств, вывода из строя телекоммуникационных сетей и средств высокотехнологического обеспечения жизни общества и государства.

Отличие информационного оружия от обычных средств:

1) скрытность (возможность применения без видимой подготовки);

2) масштабность (применение без учета географических и геополитических границ);

3) универсальность (применяется как военными, так и гражданскими организациями).

Виды информационного оружия:

1) обычное оружие, направляемое по целеуказаниям средств радиотехнической разведки с частичным самонаведением на конечном участке, на уничтожение информационных центров, объектов;

2) высокоинтеллектуальное — самонаводящиеся боеприпасы;

3) радиочастотные маскирующие помехи;

4) большие уровни электромагнитных или ионизирующих излучений;

5) воздействие импульсом высокого напряжения через электрическую сеть;

6) воздействие систем связи на ЭВМ;

7) средства генерации естественной речи конкретного человека (изменение голоса).

Поражающие свойства информационного оружия направлены в первую очередь на человека. Особенно опасно, если воздействие осуществляется на мозг человека (трансформируется матрица памяти — искусственная амнезия на определенный период). Подобные изменения могут осуществляться программными закладками: речь в речи (акростих); изображение в изображении.

Можно выделить пять основных способов поражения и разрушения сознания.

1. Поражение нейромозгового субстрата, снижающее уровень функционирования сознания, может происходить на основе действия химических веществ, длительного отравления воздуха, пищи, направленных радиационных воздействий.

2. Понижение уровня организации информационно-коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует и «живет» сознание.

3. Оккультное воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения.

4. Специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания (условно может быть обозначено как психотропное оружие).

5. Разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и к деперсонализации.

Информационное воздействие осуществляется по следующим правилам: необходима невербальная поддержка (частые повторы, системный подход).

Защита от подобных вторжений в психическую деятельность человека:

1) эстетичные фильтры;

2) необходимы защитные фильтры от дезорганизации общественного информационного сознания путем замены ценностных ориентации (информационные войны, интерпретация свободы через что-то).

Пропаганда информационного оружия активно ведется в США, и эти пропагандистские мероприятия связаны со стратегическими инициативами создания Национальной и Глобальной информационных инфраструктур, так как основу практически всех направлений международной и внутренней политики США составляет идея лидерства этой страны в мире. Технологические достижения США совместно с сильной и динамичной экономикой позволяют демонстрировать могущество страны. Информационное оружие, базирующееся на самых передовых информационных и телекоммуникационных технологиях, способствует решению этой задачи. Уязвимость национальных информа-

ционных ресурсов стран, обеспечивающих своим пользователям работу в мировых сетях, — вещь обоюдоострая. Информационные ресурсы взаимно уязвимы. В докладе Объединенной комиссии по безопасности, созданной по распоряжению министра обороны и директора ЦРУ в США в июне 1993 г. и завершившей свою работу в феврале 1994 г., говорится: «Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с "электронными скоростями" при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны».

Считается, что *для предотвращения или нейтрализации последствий применения информационного оружия* необходимо принять следующие меры:

— защита материально-технических объектов, составляющих физическую основу информационных ресурсов;

— обеспечение нормального и бесперебойного функционирования баз и банков данных;

— защита информации от несанкционированного доступа, искажения или уничтожения;

— сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях, — это естественная защитная реакция на появление нового оружия. Экономическую и научно-техническую политику подключения государства к мировым открытым сетям следует рассматривать, прежде решив вопрос национальной информаци-

онной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна предусматривать защиту сетевого оборудования на территории страны от проникновения в него скрытых элементов информационного оружия. Это особенно важно сегодня, когда осуществляются массовые закупки зарубежных информационных технологий. Очевидно, что без подключения к мировому информационному пространству страну ожидает экономическое отставание. Оперативный доступ к информационным и вычислительным ресурсам, поддерживаемым сетью «Интернет», дает возможность преодоления международной экономической и культурной изоляции, преодоления внутренней дезинтеграции, развития социальной инфраструктуры. Однако следует учитывать, что участие России в международных системах телекоммуникаций и информационного обмена невозможно без комплексного решения проблем информационной безопасности. Особенно остро проблемы защиты собственных информационных ресурсов в открытых сетях встают перед странами, которые технологически отстают в области информационных и телекоммуникационных технологий от США или Западной Европы. Сегодняшнее состояние российской экономики, неразвитость информационной инфраструктуры, неподготовленность российских пользователей к эффективной работе в сетях открытого информационного обмена не позволяют реализовать полноценное участие страны в таких сетях и пользоваться всеми возможностями новых технологий. Поэтому необходимо активное участие России в проектах развития мировых информационных сетей, в работе международных организаций, общественных комитетов и комиссий этого направления. Кроме того, должен соблюдаться принцип постепенности вхождения России в международные сети в соответствии с действительными потребностями, экономическими и технологическими возможностями.

Запретить разработку и использование информационного оружия невозможно. Ограничить усилия многих стран по формированию единого глобального информационного пространства также нереально. Однако Россия может выступить инициатором заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозу применения информационного оружия.

Обозначим практические мероприятия программного характера по защите от информационного оружия.

1. Организация мониторинга и прогнозирования потребностей экономических и других структур в различных видах информационного обмена через международные сети. Возможно создание специализированной структуры для контроля трансграничного обмена, в том числе посредством Интернета; координация мер государственных и негосударственных ведомств по предотвращению угроз информационной безопасности в открытых сетях; организация международного сотрудничества.

2. Разработка государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных и корпоративных сетей к мировым открытым сетям при соблюдении требований безопасности информационных ресурсов.

3. Организация системы комплексной подготовки и повышения квалификации массовых пользователей и специалистов по информационной безопасности для работы в мировых информационных сетях.

4. Разработка национального законодательства в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей открытых мировых сетей. Установление перечня информации, не подлежащей передаче по открытым сетям, и обеспечение контроля за соблюдением установленного статуса информации. Активное участие в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей.

Глава 7. Правовое регулирование информационных систем

1. Понятие и виды информационных систем

Информационная система — технологическая система, представляющая совместимость технических, программных и иных средств, объединяющих структурно и функционально несколько видов информационных процессов и предоставляющая информационные услуги.

В соответствии со ст. 2 Закона об информации «**информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

Признаки информационной системы

1. Выполнение одной, нескольких функций в отношении информации.

2. Единство системы (наличие: общая файловая база, единые стандарты и протоколы, единое управление).

3. Возможность композиции и декомпозиции объектов системы при выполнении заданных функций (выдержки из законов в «Гаранте», закладки — все в одном файле).

Основные требования к информационной системе:

1) эффективность;

2) качество функционирования:

— точность;

— защищенность;

— согласованность со стандартами;

3) надежность — те пороги, когда система отказывает:

— по качеству информации;

— по времени доступа;

— по производительности;

4) безопасность.

Виды информационных систем

По степени открытости:

1) открытые;

2) закрытые.

По форме собственности:

1) государственные;

2) муниципальные;

3) иные.

По техническим характеристикам информационные системы делятся на малые, средние и крупные.

Малые информационные системы имеют непродолжительный жизненный цикл, невысокую цену, для их функционирования достаточно одного персонального компьютера, у них практически отсутствуют средства обеспечения безопасности, нет средств аналитической обработки данных.

Средние информационные системы имеют длительный жизненный цикл, средства аналитической обработки данных, средства обеспечения безопасности, для их функционирования необходим штат сотрудников и взаимодействие с фирмой-разработчиком.

Крупные информационные системы имеют длительный жизненный цикл, предназначены для решения масштабных и сложных задач, для их функционирования требуется разнообразное программное обеспечение, для них характерна территориальная распределяемость, миграция в другие информационные системы.

2. Порядок разработки и официальная регистрация программ для ЭВМ и баз данных

Программа для ЭВМ и баз данных регулируется специальным законом и нормами авторского права. Программа для ЭВМ — произведение; для базы данных — сборники. Авторское право на программы для ЭВМ и баз данных не связано с правом собственности на их материальный носитель Законами РФ «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351- I[1] (далее — Закон об авторском праве) и Законом о правовой охране программ для электронных вычислительных машин и баз данных. Программа ЭВМ формально приравнена к произведению лите-

[1] Ведомости СНД РФ И ВС РФ. 1993. № 32. Ст. 1242; СЗ РФ. 2004. № 30. Ст. 3090.

ратуры, авторское право на них возникает автоматически, в момент создания, но де-факто данные законы закрепляют совершенно разный статус литературного произведения и программы ЭВМ. Причем режим использования программ ЭВМ более ограничен. Так, в ст. 18 Закона РФ об авторском праве п. 2 не допускает без согласия автора и без выплаты авторского вознаграждения воспроизведение правомерно обнародованного произведения в виде программ для ЭВМ и баз данных. В соответствии со ст. 4 данного Закона «репрографическое воспроизведение не включает в себя хранение или воспроизведение копий в электронной (включая цифровую) форме», а п. 2 ст. 18 данного Закона однозначно запрещает репродуцирование в личных целях книг полностью. Однако в сложившихся обычаях делового оборота сети «Интернет» считается нормальной практикой копирование веб-страниц с информацией для личного употребления с размещенных для свободного обозрения веб-сайтов. Такие действия, являющиеся нарушениями действующего законодательства РФ, имеют массовый характер, нарушители не несут никакой ответственности, и, более того, ни у одного правообладателя авторских прав, как правило, не возникает предмета спора по нарушению авторских прав, пока его произведение используется в личных целях.

Таким образом, положения законов РФ об авторском праве и о правовой охране программ для электронных вычислительных машин и баз данных ограничивают права пользователя сети «Интернет» в возможностях копирования и использования произведений в личных целях. Эти положения также ограничивают конституционное право человека свободно искать, получать, передавать, производить и распространять информацию.

В соответствии со ст. 4 Закона РФ «О правовой охране программ для электронных вычислительных машин и баз данных» правообладатель для оповещения о своих правах может использовать знак охраны авторского права (копирайт). Такой знак должен состоять из трех элементов:

1) буквы С в окружности или в круглых скобках;
2) наименования (имени) правообладателя;
3) года первого выпуска охраняемого объекта.

Таким образом, размещение копирайта на сервере (сайте) способно оптимизировать процедуру правовой охраны объектов, составляющих сайт. Информация, оповещающая об исключительных правах правообладателя, должна быть доступна пользователям.

Положения Закона РФ «О правовой охране программ для электронных вычислительных машин и баз данных» распространяются на любые программы или базы данных, которые могут быть выражены на любом языке и в любой форме (п. 3 ст. 3) независимо от назначения и достоинства этих программ или баз данных (п. 1 ст. 3). Исходя из этого совокупность данных, находящихся в информационном ресурсе, доступном в Интернете, можно признать базой данных. Если в состав информационной системы входят также компоненты по компьютерной обработке данных, то эти компоненты являются программами для ЭВМ.

Тем не менее нормативная правовая база, имеющая своим назначением регулирование отношений в данной сфере, характеризуется значительными пробелами, что негативно сказывается на формировании правовой культуры, создает предпосылки для неправомерного поведения отдельных пользователей.

Информационные системы как в целом, так и составляющие их многочисленные компоненты в отдельности, являющиеся результатом творческой деятельности, охраняются как объекты авторского права. Автором согласно ст. 4 Закона об авторском праве является физическое лицо, творческим трудом которого создано произведение. Субъективное авторское право состоит из личных неимущественных и исключительных имущественных прав. Закон об авторском праве предусматривает следующие личные неимущественные права автора в отношении созданного им объекта авторского права:

— право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);

— право обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;

— право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Под «правом на отзыв» понимается часть права на обнародование — право автора отказаться от ранее принятого решения об обнародовании произведения. Автор может воспользоваться правом на отзыв в любое время в течение всей своей жизни независимо от того, выпущено ли произведение в свет или еще нет. Непременным условием реализации данного правомочия является возмещение пользователю произведения причиненных таким решением убытков, включая упущенную выгоду. Если произведение уже было обнародовано, то автор обязан публично оповестить о его отзыве. При этом закон предоставляет автору возможность изъять из обращения ранее изготовленные экземпляры произведения, но также за свой счет. Несмотря на обязанность автора в случае такого изъятия возместить убытки, данное положение конфликтует с нормами института права собственности. В отношении произведений, созданных в порядке выполнения служебных обязанностей или служебного задания работодателя (служебные произведения), право на отзыв не применяется.

Отличительная черта личных неимущественных прав состоит в том, что принадлежат они автору независимо от имущественных авторских прав и сохраняются за ним даже в случае уступки последних в полном объеме. Другими словами, неимущественные права непередаваемы, неотчуждаемы, не переходят по наследству и прекращаются в момент смерти их обладателя. Поэтому любые соглашения о передаче неимущественных прав ничтожны. После смерти автора защита этих прав осуществляется его наследниками.

Исключительные имущественные авторские права на использование произведения означают право их обладателя

осуществлять самому, разрешать и запрещать другим лицам определенные действия, в том числе:

— воспроизводить произведение (право на воспроизведение);

— распространять экземпляры произведения любым способом: путем продажи, сдачи в прокат, мены, дарения и т.д. (право на распространение);

— импортировать экземпляры произведения в целях распространения, включая экземпляры, изготовленные с разрешения обладателя исключительных авторских прав (право на импорт);

— сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения по кабелю, проводам или с помощью иных аналогичных средств (право на сообщение для всеобщего сведения по кабелю);

— переводить произведение (право на перевод);

— переделывать, аранжировать или другим образом перерабатывать произведение (право на переработку).

Имущественные права переходят по наследству и могут передаваться по авторскому договору на исключительной или неисключительной основе. Авторский договор о передаче исключительных прав разрешает использование произведения определенным способом и в установленных договором пределах только лицу, которому эти права передаются, и дает такому лицу возможность запрещать подобное использование произведения другим лицам (п. 2 ст. 30 Закона об авторском праве). Передача неисключительных прав может осуществляться путем выдачи разрешений (лицензий) неограниченному кругу пользователей.

Вместе с тем даже исключительные права зачастую находятся в распоряжении нескольких лиц. Авторский договор, в частности, должен предусматривать конкретные способы использования произведения, срок и территорию, в пределах которых использование осуществляется (ст. 31 Закона об авторском праве).

Следовательно, комплекс исключительных имущественных прав может быть поделен между разными субъектами по

способам, срокам и территории использования одного и того же произведения.

Статьями 17-26 Закона об авторском праве установлены ограничения перечисленных имущественных прав, которые применяются при условии, что такое использование не наносит неоправданного ущерба нормальному использованию произведения и не ущемляет необоснованным образом законные интересы автора. Пункт 3 ст. 16 устанавливает принцип исчерпания права на распространение: если экземпляры правомерно опубликованного произведения введены в гражданский оборот посредством их продажи, то допускается их дальнейшее распространение без согласия автора и без выплаты авторского вознаграждения.

Вместе с тем согласно основополагающим нормам гражданского законодательства защиту нарушенных или оспоренных гражданских прав осуществляет в соответствии с подведомственностью дел, установленной процессуальным законодательством, суд, арбитражный суд или третейский суд (п. 1 ст. 11 ГК РФ). Согласно п. 3 ст. 49 Закона об авторском праве за защитой своего права обладатели исключительных авторских прав вправе обратиться в установленном порядке в суд, арбитражный суд, третейский суд, орган дознания, органы предварительного следствия в соответствии с их компетенцией.

Собственник информационных систем, технологий и средств их обеспечения в случае нарушения авторских прав- их разработчика третьими лицами не сможет обратиться в суд за защитой данных прав или защищать их самостоятельно, если не имеет на это полномочий от автора или не является законным представителем автора либо не обладает этими правами лично на основе закона или договора.

Исходя из положений гражданского законодательства, в том числе Закона об авторском праве, нельзя говорить и о прямой обязанности защищать авторские права ни непосредственного их носителя (автора, наследников автора, иных правообладателей), ни тем более субъекта, обладающего правом собственности на материальные носители произведений.

Осуществление защиты прав автора не является обязанностью, в том числе и его работодателя, в рамках отношений с которым в порядке выполнения служебных обязанностей или служебного задания было создано произведение (ст. 14 Закона об авторском праве). Работодатель в пределах имеющегося у него объема исключительных прав вправе (но не обязан) запрещать несанкционированное использование произведения другим лицам или требовать применения к нарушителю иных установленных законодательством мер ответственности.

Во избежание конфликта интересов обладателя исключительных прав и автора Закон об авторском праве предусматривает право автора запрещать использование произведения другим лицам в том случае, если лицо, которому переданы исключительные права на его использование, не осуществляет защиту данных прав (ч. 2 п. 2 ст. 30 Закона об авторском праве).

Правообладатель может зарегистрировать программу для ЭВМ и баз данных путем подачи заявки в российское агентство по правовой охране программ для ЭВМ, баз данных, топологии и топологий интегральных микросхем.

Лицо, владеющее на законных основаниях экземпляром программы, вправе декомпилировать программу для ЭВМ (внести изменения в уже закрытую программу) для организации взаимодействия разработанной данным лицом программы для ЭВМ с другими программами, если иначе получить эту информацию невозможно.

Следует отметить, что в соответствии с п. 3. ст. 13 Закона об информации права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

Кроме того, п. 7 ст. 14 упомянутого Закона устанавливает, что не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

Глава 8. Особенности правового регулирования Интернета

1. Общая характеристика Интернета как особой информационно-телекоммуникационной сети

Исследование правовой сущности Интернета, правовой культуры личности и их взаимодействия является необходимой предпосылкой для анализа особенностей формирования правовой культуры личности в условиях становления информационного общества.

Интернет как глобальное информационное пространство «не признает» государственных границ и является не только эффективнейшим средством доступа к информационным ресурсам, накопленным человечеством, но и становится средством распространения массовой информации. Функционирование сети является мощным фактором развития и использования передовых технологий. С другой стороны, с использованием сети «Интернет» связаны: возможность бесконтрольного распространения вредной информации, проникновения в системы управления, нарушения прав человека, что, несомненно, требует особого внимания к вопросам информационной защиты. Бурное развитие Интернета в цивилизованном мире опережает процесс создания и совершенствования нормативных правовых актов, необходимых для регулирования возникающих проблем. По мере развития Интернета за последние годы правовые проблемы сети становятся все более актуальными на фоне заметной трансформации в мире подходов к их урегулированию: от упора на саморегуляцию — к жесткой правовой регламентации. В нашей стране уже в конце 1996 г. как отклик на большое внимание широкой общественности, органов государственной власти и управления, деловых людей к правовым проблемам сети «Интернет» в России состоялись парламентские слушания, проведенные комитетами Государственной Думы по безопасности и по информационной по-

литике и связи. Основные проблемы, требующие законодательного урегулирования в России в связи с развитием сети «Интернет», практически не отличаются от таковых в других развитых странах мира: 1) обеспечение свободного подключения к Интернету и обмена информацией в сети; 2) правовая охрана авторских прав и иных объектов интеллектуальной собственности; 3) защита персональных данных, в частности тех данных, которые собираются в процессе деятельности операторов сети (в том числе адреса, телефоны и другие персональные данные подписчиков или покупателей в системе «электронной коммерции»); 4) подключение государственных органов к Интернету и обеспечение граждан информацией о деятельности этих органов; 5) предотвращение распространения оскорбительной и непристойной информации, призывов к разжиганию национальной, расовой, религиозной розни и т.п.; 6) электронный документооборот, электронная подпись, подтверждение подлинности информации в информационных продуктах, средствах просмотра и передачи информации; 7) электронная коммерция; 8) информационная безопасность: компьютерные вирусы, несанкционированный доступ к информации, взлом серверов и сетей, разрушение и подмена информации; 9) применение средств криптозащиты; 10) юрисдикция: законодательство какого государства необходимо применять для урегулирования действий, совершаемых в сети. Анализ действующего российского законодательства показывает, что вопросы правового регулирования, связанные с функционированием и развитием системы «Интернет» в России, образуют обширную нормативную базу, включающую только на федеральном уровне более 50 федеральных законов, не говоря уже о многочисленных нормативных правовых актах Президента и Правительства РФ. Спектр этих законодательных актов исключительно широк, и их толкование с позиций специфики правоотношений, возникающих при использовании современных информационных технологий, затруднительно, тем более что при разработке этих законов в них не предусматривались соответствующие возможности.

Понятно, что для судов данная область правоотношений совершенно новая.

Интернет, будучи сетью для передачи информации, является средой обитания информационного общества, органично сплавляясь с общими тенденциями информатизации различных сторон общественной жизни[1]. Большинство из определений информации имеют нечто общее. В частности, они предполагают существование по крайней мере четырех компонентов:

1) процесса познания чего-либо, о чем передается информация;

2) передающего информацию;

3) воспринимающего информацию;

4) самой информации.

Исходя из изложенного выше информация, передаваемая через Интернет, представляет собой сведения об окружающем мире, его объектах, процессах и явлениях, представленные в форме, позволяющей провести расшифровку закодированных данных (данные находятся в двоичном виде и не нуждаются в преобразовании, как, например, при сканировании изображения либо при оцифровке звука[2]).

Таким образом, Интернет как информационно-телекоммуникационная сеть — это средство передачи сведений об окружающем мире, его объектах, процессах и явлениях, объективированных в форме, позволяющей провести их машинную обработку (расшифровку).

Интернет с технической точки зрения представляет собой крупнейшую телекоммуникационную сеть, образованную путем объединения более десяти тысяч пятисот телекоммуникационных сетей различных типов. Такое объединение ста-

---

[1] *Клименко С, Уразметов В.* Интернет: среда обитания информационного общества. — Протвино, 1995. С. 17-22.

[2] *Петровский СВ.* Правовое регулирование оказания интернет-услуг: Дис: ... канд. юрид. наук. — М., 2002. С. 24.

ло возможным за счет использования межсетевого протокола TCP/ IP, играющего роль своеобразного переводчика стандартов при передаче данных между разнотипными телекоммуникационными сетями.

В соответствии с п. 3 и 4 ст. 2 Закона об информации информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

Получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только

в порядке и на условиях, которые установлены федеральными законами.

В процессе правового регулирования Интернета возникают новые предметы отношений:

— сайт — совокупность веб-страниц с повторяющимся дизайном, объединенных тематически, связанных ссылками навигационно и физически находящихся на веб-сервере локальной сети или Интернета по одному адресу (доменному имени);

— веб-страница — электронный документ, выполненный на основе языка гипертекстовой разметки HTML (HyperText Markup Language) и входящий как единица представления информации в состав набора страниц с взаимными гиперссылками — веб-сайт в локальной сети или Интернете;

— домен — каждому компьютеру, подключенному к сети «Интернет», выделяется уникальный идентификационный номер, называемый IP-адресом. IP означает Internet Protocol, т.е. протокол, посредством которого происходит взаимодействие компьютеров в сети «Интернет». IP-адрес представляет собой последовательность из четырех чисел, разделенных точками, и выглядит следующим образом: 82.116.44.1. Представленный в таком виде IP-адрес сложен для запоминания человеком. В связи с этим для удобства запоминания и восприятия была создана доменная система имен (Domain name System — DNS). С помощью данной системы стало возможным сопоставить каждому IP-адресу уникальное символьное имя, называемое доменным именем;

— электронная почта — разновидность электросвязи, осуществляемая посредством интернет-технологий.

2. Деятельность, осуществляемая посредством Интернета

Деятельность сети «Интернет» может быть обозначена в следующих позициях:

1) информация справочного характера;
2) реклама;
3) предоставление полнотекстовых источников;
4) консалтинг;

5) электрические средства массовой информации;
6) размещение и распространение произведений;
7) распространение аудиовизуальной продукции;
8) размещение официальной информации;
9) совершение бесконтактных сделок;
10) телефаксы;
11) почтовые услуги;
12) телеконференция (прямой эфир).

Субъекты правоотношений в Интернете

1. Создатели программных технологий (частей информационной инфраструктуры).

2. Производители и распространители информации в Интернете, в том числе оказывающие услуги по подключению (провайдеры).

3. Потребители.

Кроме того, субъектами указанных отношений выступают собственник (владелец) интернет-сайта, администратор доменного имени интернет-сайта, оператор связи, пользователь.

Закон об информации в ст. 2 определяет отдельные понятия следующим образом: «**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.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных».

В соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи» оператор связи — это юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии. Операторов связи называют по-разному: ISP, ASP, владельцы служб информационных объявлений (от досок объявлений до интернет-аукционов), в европейском законодательстве в ходу

термин «intermediary service providers», в американской практике — on-line service provider, provider of access, provider of the informational content.

Следует иметь в виду, что государство берет на себя создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей. А также особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Объекты отношений в Интернете

I. Информационные ресурсы, продукты (информация), информационные услуги.

II. Информационные права и свободы (легитимности, общества, государства), права на доменное имя.

III. Информационная целостность.

IV. Информационный суверенитет.

V. Информационная безопасность.

Основные направления правового регулирования отнбшений в Интернете:

1) защита от вредной, незаконной информации;

2) соблюдение авторских и смежных прав в условиях распространения информации в электронном виде;

3) вопросы электронного документооборота;

4) вопросы киберэкономики;

5) информационная безопасность;

6) правонарушения в Интернете.

3. Государственное регулирование Интернета в России и за рубежом

Государственная политика может быть направлена на ограничение доступа к определенной информации для взрослых. Этот подход используется в австралийском фе-

деральном законе (хотя он до сих пор не вступил в силу), в Китае, Саудовской Аравии, Сингапуре, Объединенных Арабских Эмиратах, Вьетнаме. Некоторые страны требуют от интернет-провайдеров блокировать подобную информацию, в то время как другие страны допускают ограниченный доступ в Интернет, контролируемый государственными органами.

Наконец, государство может запрещать открытый доступ к Интернету. Отдельные страны требуют от пользователя зарегистрироваться или получить лицензию для того, чтобы получить доступ с ограничениями, перечисленными выше (см. п. 3). Например, на Кубе пользование Интернетом ограничено и контролируется правительством. Требуется официальное разрешение и необходимое оборудование, включая наиболее современное, которое ограничено и может быть куплено только в специальных управляемых государством магазинах, снова только со специальным разрешением. Декрет 209 («Доступ к Мировой компьютерной сети с Кубы»), принятый в июне 1996 г., гласит: сеть не может использоваться «в нарушение моральных принципов Кубинского общества и законов» и сообщения электронной почты не должны «подвергнуть опасности национальную безопасность»[1].

В США госрегулирование Интернета началось с ограничений. В феврале 1996 г. конгресс принял Communications Decency Act («Акт о соблюдении приличий в средствах массовой коммуникации»). Целью его было оградить детей от доступа к порнографии. В связи с Communications Decency Act нельзя не вспомнить историю порноиздателя Ларри Флинта (американское правосудие так и не смогло справиться с Флинтом, который умело воспользовался Первой поправкой, гарантирующей свободу слова). И вспомнили: уже летом 1997 г. «Акт...» был отменен по решению Верховного Суда,

[1] The Internet under Surveillance. Reporters without Borders 2003. Editions La Decouverte & Syros, 2003. P. 46.

так что родителям теперь приходится обходиться в столь важном вопросе без помощи государства. Этот случай продемонстрировал, что государственное регулирование Интернета в правовом государстве может оказаться невозможным. Федеральный бостонский судья Марк Вульф так охарактеризовал ситуацию: «Нам действительно надо выработать совершенно новые подходы и концепцию. И в этом обсуждении должны участвовать и президент, и конгресс, и Верховный Суд. Но я думаю, на это уйдет немало времени».

Куда жестче государственный напор оказался во Франции, что вполне в духе исторических традиций этой страны. Весной 2000 г. Национальная ассамблея проголосовала за законопроект об обязательной регистрации владельцев всех веб-сайтов и об уголовной ответственности провайдеров за предоставление хостинга (услуга по размещению информации в Интернете) неидентифицированным пользователям. Мало того, сенат (верхняя палата французского парламента) принял законопроект, предписывающий провайдерам сообщать сведения о владельцах сайтов заинтересованным третьим лицам. Впоследствии закон все же был смягчен: провайдер или хостинговая компания обязаны требовать от пользователя указания данных о себе, но не обязаны проверять их достоверность.

Необходимость регулирования доступа к материалам, размещенным в Интернете, признается во многих странах мира. Однако то, что является легальным в одной стране, может не быть таковым в другой стране. Например, во Франции запрещается размещение на веб-страницах нацистской тематики, в то время как австралийские законы этого не запрещают. Существуют и другие примеры неэффективности национальных законов, касающихся цензуры в Интернете. В данном случае представляется целесообразным приятие соответствующего акта на международном уровне.

Необходимо отметить, что чрезмерное регулирование содержания информационных ресурсов, размещенных в Ин-

тернете, может негативно сказаться на развитии правовой культуры, на формировании правовой активности личности. Вместе с тем отсутствие минимально необходимых ограничений на доступ к определенной информации также может привести к подобному результату. В связи с чем представляется целесообразным законодательное регулирование данного вопроса на основе сочетания интересов как личности, так и общества и государства.

В последние годы все больше внимания уделяется разработке законодательных актов, регулирующих правоотношения, возникающие в связи с функционированием сети «Интернет». Очевидно, это связано с тем, что Интернет из глобальной «оффшорной» информационной зоны все более превращается в повседневную реальность, из киберпространства в обычное экономическое пространство, из мира «продвинутого» интернет-сообщества, пусть даже весьма обширного, в область интересов всего общества. Второй причиной более строгого отношения к правовым вопросам стала проблема безопасности данных, в первую очередь персональных данных, защиты от информационных атак на почтовые ящики и надежности экономических отношений в Интернете. То, что казалось сдерживающим фактором развития, стало необходимым условием развития, а права и гарантии, репродуцированные в глобальный информационный мир, потребовали такой же законодательной защиты, как и в обычном мире. На уровне законодательных инициатив только в Соединенных Штатах было подготовлено и предварительно рассмотрено в комитетах конгресса более пятидесяти (!) законопроектов. Сферы, затрагиваемые этими законодательными инициативами, можно условно разделить на следующие:

— регулирование потоков информации, поступающих в личные (частные) электронные почтовые ящики, в том числе коммерческой информации. Это предполагает: защиту электронного ящика от потока информации, если владелец ящика отказывается от принятия этих сообщений; ответственность за передачу искаженной информации; обязанности поставщика информации по

отношению к владельцу почтового ящика; требования к составу реквизитов отправителя;

— защита персональных данных: раскрытие целей сбора персональных данных; обязанности оператора сайта, собирающего и использующего персональные данные, по отношению к частным лицам; ограничение на распространение персональных данных без соответствующего согласия частного лица; требования по защите персональных данных от несанкционированного распространения;

— предупреждение мошенничества в Интернете и запрет несанкционированного использования Интернета для азартных игр и т.п., в том числе: распространение на Интернет норм уголовного законодательства, относящихся к мошенническим действиям; действия органов исполнительной власти по предупреждению и профилактике мошенничества в Интернете;

— обеспечение свободы конкуренции в Интернете. Установление норм применения требований антимонопольного законодательства к субъектам, действующим в Интернете;

— программы оснащения образовательных учреждений и библиотек новыми информационными технологиями и защиты учащихся от нежелательной информации, содержащейся в Интернете. Это предполагает предписание школам и библиотекам внедрить компьютерные технологии, позволяющие блокировать нежелательную информацию из Интернета под угрозой лишения их государственных субсидий.

Возникновение в России новых общественных отношений в связи с функционированием Интернета, их трансформация в основных сферах общественной жизни существенно влияют на становление информационных правоотношений, которые требуют особого регулирования. В данном случае представляется целесообразным использование положительного опыта зарубежных стран.

С помощью Интернета формируется мировое информационное пространство, которое и составляет основу информационного общества.

Глава 9. Правовое регулирование информационных ресурсов

1. Понятие и виды информационных ресурсов

Информационные ресурсы — отдельные документы и отдельные массивы документов, а также документы и массивы документов в информационных системах.

Информационный ресурс — это информация, созданная и(или) обнаруженная, зарегистрированная, оцененная, с определенными (заданными) законами деградации и обновления. Это тоже документ, но с четко определенными качественными и количественными характеристиками.

Важнейшей проблемой практического использования ИР является проблема их классификации. При рассмотрении ИР как объекта гражданских прав Федеральный закон «Об информации, информатизации и защите информации» определяет, что признаком классификации ИР является признак собственности. Далее следует еще один признак классификации: федеральный ИР, совместного пользования и т.д. Однако следует отметить, что при применении Закона нарушается один из основных принципов классификации — принцип единства классификационных признаков. Представляется целесообразным создание общероссийского классификатора информационных ресурсов, утверждаемого Госстандартом России.

Информационные ресурсы делятся на следующие группы.

I. По специфике возникновения:

1) естественные, производственные, социально-экономические информационные ресурсы;

2) созданные в результате интеллектуальной деятельности.

II. По сферам использования:

1) научно-технические;

2) социально-экономические;

3) правовые;

4) культурные;

5) образовательные;

6) развлекательные и т.д.

III. По принадлежности определенным субъектам:

1) физическим лицам;
2) юридическим лицам;
3) государственным органам власти и управления;
4) должностным лицам;
5) органам местного самоуправления;
6) общественным объединениям;
7) государству в целом.

Правовой режим информационных ресурсов устанавливается следующими критериями.

I. Информационные ресурсы — всегда в виде документированной информации.

Документ — это выделенная информация по определяющей цели, зафиксированная в любой знаковой форме с установленными реквизитами, позволяющими ее идентифицировать, и представленная на любом носителе.

II. Требование по установлению права собственности и исключительных прав на объекты информационных ресурсов. Информационные ресурсы, являясь элементом различных прав, могут быть товаром (объектом рыночных отношений), обладать признаками вещи и одновременно интеллектуальными свойствами. Но вопросы правового регулирования информационных ресурсов гражданским правом не охватывается. Административное право, регулируя информационные ресурсы, включает в себя следующие моменты:

1) обязательный экземпляр документа;
2) обязанность органов государства на сбор информации по целевому признаку;
3) обязанность организаций, ответственных за сбор информации, предоставить ее;
4) обязательность лицензирования деятельности по специальному хранению информации.

III. Обязательное установление степени открытости информации применительно к каждому объекту информационных ресурсов.

IV. Защита информационных ресурсов — обеспечение информационной безопасности.

Общегосударственные информационные ресурсы, включая регистры, кадастры, реестры, классификаторы, создаются в целях предоставления оперативного доступа к целостной, актуальной, достоверной и непротиворечивой информации об основных объектах, формах, способах и результатах государственного управления и ее совместного использования на межведомственном уровне органами государственной власти.

Создание общегосударственных информационных ресурсов позволяет устранить дублирование, упорядочить и регламентировать процедуры сбора, хранения и актуализации соответствующей информации, а также осуществлять контроль доступа к ним и их использования.

Необходимо централизованно сформировать общегосударственные информационные ресурсы и обеспечить в установленном порядке доступ федеральных органов государственной власти, органов местного самоуправления, граждан и организаций к этим ресурсам.

При этом должны быть созданы предпосылки для:

— обслуживания и технической поддержки межведомственных государственных информационных систем и ресурсов;

— контроля использования межведомственных общегосударственных ресурсов в целях предотвращения возможных несанкционированных действий со стороны государственных служащих и иных лиц;

— размещения, резервирования и технологической поддержки в случае экономической целесообразности информационных систем и ресурсов федеральных органов государственной власти по согласованию с ними.

Права, обязанности и ответственность владельца информационных ресурсов

Владелец информационных ресурсов, если иное не предусмотрено федеральными законами, вправе: 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; 2) использовать информацию, в том числе распространять ее, по своему усмотрению; 3) передавать информацию другим лицам по договору или на ином

установленном законом основании; 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами; 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Владелец информационных ресурсов при осуществлении своих прав обязан: 1) соблюдать права и законные интересы иных лиц; 2) принимать меры по защите информации; 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

В ТК РФ предусмотрены общие требования при обработке персональных данных работника (ст. 86 ТК РФ):

— обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

— работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

— работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законом.

Конкретный порядок обработки персональных данных работника определяется документами организации.

Согласно п. 1 ст. 17 Закона об информации владелец информационных ресурсов несет юридическую ответственность за нарушение указанного Закона, например правил работы с информацией. Правила работы с информацией включают

в себя положения о порядке сбора, хранения, использования и распространения информации; положения о защите информации; о требованиях, предъявляемых к деятельности, связанной с осуществлением перечисленных действий с информацией. Эти положения устанавливаются нормативными правовыми актами РФ.

За нарушение правил работы с информацией законодательством предусмотрена уголовная, административная, гражданская и дисциплинарная ответственность. Так, уголовная ответственность предусмотрена за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Административная ответственность установлена за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП РФ), нарушение правил защиты информации (ст. 13.12 КоАП РФ), за незаконную деятельность в области защиты информации (ст. 13.13 КоАП РФ); за разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ).

Гражданская ответственность наступает, если в силу нарушения правил работы с информацией нарушаются имущественные или личные неимущественные права лица, к которому эта информация имеет отношение. Формы гражданской ответственности предусмотрены в ст. 12 ГК РФ.

Дисциплинарная ответственность применяется к лицу, в трудовые обязанности которого входило соблюдение или обеспечение соблюдения правил работы с информацией. Виды дисциплинарных взысканий предусмотрены в ст. 192 ТК РФ.

2. Порядок формирования информационных ресурсов и предоставления информационных услуг

Государственная практика в сфере формирования информационных ресурсов направлена на создание эффективной и качественной информации, обеспечение решения стратегических военных задач. Правовая основа формирования инфор-

мационных ресурсов — институт обязательного экземпляра документа.

Обязательный экземпляр документа — ресурсная база национальной информационной инфраструктуры. Не подлежат обязательному предоставлению документы личного характера (письма), документы секретного характера, документы, содержащиеся в единичном исполнении, архивные документы и управленческая информация.

Обязательному представлению подлежат:

1) издания С;

2) издания для слепых;

3) официальные документы, подлежащие опубликованию;

4) аудиовизуальная продукция;

5) электронные издания;

6) неопубликованные издания (диссертации, научные исследования).

Информационные услуги:

— бесплатное опубликование библиографической информации;

— хранение производственных документов;

— включение библиографической информации в отечественные и международные автоматизированные банки данных;

— бесплатное предоставление по запросам хранимой информации;

— использование телерадиопроизводителями документов, созданных физическими, юридическими лицами, в собственном эфире и т.д.

3. Государственные информационные ресурсы

В настоящее время в России органы государственной власти создают свои сайты, в структуру которых входят в числе прочих специальные разделы, предназначенные для обратной связи и оперативного обмена информацией с посетителями. Например, сайт Министерства юстиции России —

www.minjust.ru — содержит в своей структуре «Вопрос министру», являющийся формой открытого письма министру юстиции, отсылаемого по e-mail. Ответ министра юстиции направляется по адресу заявителя, а в случае его отсутствия размещается на сайте Министерства[1].

Информационные обязанности государства перед гражданами возрастают. Информация, собранная на средства налогоплательщиков, должна быть им доступна. Так, в целях обеспечения реализации прав граждан и организаций на доступ к информации о деятельности Правительства РФ и федеральных органов исполнительной власти 12 февраля 2003 г. Правительство РФ приняло постановление № 98 «Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти»[2]. Согласно п. 2 данного постановления федеральным органам исполнительной власти необходимо:

1) обеспечить доступ граждан и организаций к информации о деятельности федеральных органов исполнительной власти, за исключением сведений, отнесенных к информации ограниченного доступа, путем создания информационных ресурсов в соответствии с перечнем, утвержденным данным постановлением;

2) своевременно и регулярно размещать указанные информационные ресурсы в информационных системах общего пользования, в том числе в сети «Интернет»;

3) систематически информировать граждан и организации о деятельности федеральных органов исполнительной власти иными способами, предусмотренными законодательством РФ.

Органам исполнительной власти субъектов РФ и органам местного самоуправления рекомендуется принять меры по обеспечению доступа граждан и организаций к информации о своей деятельности с учетом положений указанного постановления.

---

[1] *Морозов А.* Сайт Министерства юстиции России — www.minjust.ru // Российская юстиция. 2002. № 9. С. 72.

[2] СЗ РФ. 2003. № 3. Ст. 658.

Необходимо отметить создание российского сегмента сети «Интернет» для органов государственной власти РФ — Russian Government Internet Network (далее по тексту — сеть RGIN) — на базе домена GOV.RU сети «Интернет», который является совокупностью территориально распределенных сетей и серверов доступа, принадлежащих организациям, имеющим статус органа государственной власти РФ. Иерархически структурированная сеть RGIN предоставляет пользователям доступ к информационному пространству сообщества сетей Интернета и размещает на своих серверах только официальные материалы, относящиеся к деятельности органов государственной власти РФ. В настоящее время на сервере органов государственной власти РФ «Официальная Россия» содержатся лишь общие сведения как о федеральных, так и о региональных органах государственной власти. Более подробную информацию можно получить, используя ссылки на официальные сайты указанных органов государственной власти. Таким образом, объем размещенной информации и система навигации требуют значительных доработок.

В настоящее время значительная часть государственных информационных ресурсов не предусматривает какой бы то ни было интерактивности. Причиной этого является отсутствие административных ресурсов даже для того, чтобы поддерживать форум (например, портал Минтруда России (www.mintrud.ru), который задуман как главный информационный ресурс страны, посвященный социально-трудовой сфере). Вместе с тем существуют официальные сайты, например Верховного Суда РФ (http://www.supcourt.ru/), Высшего Арбитражного Суда РФ (http://www.arbitr.ru/), Министерства юстиции РФ (http://www.minjust.ru) и другие, поддерживающие интерактивные конференции, содержащие ссылки на различные органы государственной власти, специализированные серверы по законодательству. Особо ценно наличие в структуре данных сайтов в числе прочих специальных разделов, предназначенных для обратной связи и оперативного обмена информацией с посетителями.

Следует отметить, что уровень взаимодействия судебной власти и СМИ, в том числе Интернета, пока не соответствует потребностям общества: «...складываются настороженные, а иногда и конфликтные отношения». С одной стороны, это объясняется позицией судов, склонных к информационной закрытости, а с другой — наличием поверхностных материалов, вытесняющих серьезные материалы, ориентированные на анализ вопросов правосудия, развитие гражданского оборота. Непрозрачность работы судов для СМИ и граждан, которые не всегда могут оперативно и беспрепятственно ознакомиться с решениями и приговорами, вынесенными и публично провозглашенными в судебном заседании, нарушает важные конституционные принципы публичности и гласности правосудия.

Вступление России в Совет Европы накладывает на страну обязательства, связанные с достижением международных стандартов по обмену правовой информацией (включая судебную) в электронном виде по сети «Интернет». В целях реализации принципа гласности судопроизводства в европейских странах все судебные процессы транслируются в Интернете в режиме реального времени («в прямом эфире»). Любой желающий может следить за ходом разбирательства через персональный компьютер. Причем европейцы активно пользуются такой возможностью, особенно если это касается дел, получивших общественный резонанс. Очевидно, что о скорой реализации этой программы в России говорить пока не приходится. Но ориентироваться нужно на уровень, достигнутый в этом направлении в наиболее развитых странах.

4. Государственное регулирование библиотечного дела

Согласно Федеральному закону о библиотечном деле[1] библиотекой называется информационное, культурное, образовательное учреждение, располагающее организованным фондом тиражированных документов и представляющее их во временное пользование физическим и юридическим лицам.

[1] СЗ РФ. 1995. № 1. Ст. 2; 2004. № 35. Ст. 3607.

Библиотеки могут быть учреждены органами государственной власти всех уровней, органами местного самоуправления, юридическими и физическими лицами. В соответствии с порядком учреждения и формами собственности выделяются следующие виды библиотек:

1) государственные библиотеки, учрежденные органами государственной власти (в том числе федеральные библиотеки, библиотеки субъектов РФ, библиотеки министерств и иных федеральных органов исполнительной власти);

2) муниципальные библиотеки;

3) библиотеки Российской академии наук, других академий и научно-исследовательских институтов, образовательных учреждений;

4) библиотеки предприятий, учреждений, организаций;

5) библиотеки общественных объединений;

6) частные библиотеки;

7) библиотеки, учрежденные иностранными юридическими и физическими лицами, а также международными организациями.

Государственные и муниципальные библиотеки, централизованные библиотечные системы получают статус юридического лица с момента их регистрации.

В основе государственной политики в области библиотечного дела лежит принцип создания условий для всеобщей доступности информации и культурных ценностей, собираемых и представляемых в пользование библиотеки.

Государство поддерживает развитие библиотечного дела путем финансирования, проведения соответствующей налоговой, кредитной, ценовой политики, разрабатывает федеральные программы развития библиотечного дела, координирует межрегиональные связи по библиотечному обслуживанию в целях информатизации общества. Государство не вмешивается в профессиональную деятельность библиотек, за исключением случаев, предусмотренных законодательством РФ.

Федеральным органом исполнительной власти, осуществляющим государственное регулирование в области

библиотечного дела и контроль за хранением и использованием отнесенных к культурному наследию народов РФ библиотечных фондов, является Федеральная служба по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Организация кооперированных библиотечных систем и информационно-библиотечных сетей, сводного каталога библиотек РФ, современных систем безопасности государственных музеев и библиотек возложена на Федеральное агентство по культуре и кинематографии.

Субъектами отношений в сфере библиотечного дела являются:

— библиотека;
— автор произведений;
— пользователь.

Особенностями библиотечного дела являются:

— публичный характер;
— массовое обслуживание пользователей.

Стремительное развитие электронной издательской деятельности и рост количества электронных публикаций приводит к весьма серьезным проблемам. Перечислим наиболее важные.

1. При подготовке электронной информации, прежде всего полнотекстовой, очень часто игнорируются или учитываются не в полной мере опыт, правила и нормы, существующие в сфере производства и распространения печатной информации, что приводит не только к нарушению сложившихся традиций, но и усложняет коммуникативные процессы, в которых участвует и будет участвовать как электронная, так и печатная информация. Это относится к шрифтовому оформлению, к организации и структурированию информации, к атрибутированию произведений и т.п.

2. Современные информационные технологии предоставляют эффективные средства надежного сохранения электронной информации. Однако на практике процесс накопления и сохранения электронной информации носит случайный ха-

рактер. Например, создаваемые в рамках традиционной издательской деятельности электронные оригинал-макеты часто просто уничтожаются. Известны случаи, когда выполнялись дорогостоящие операции преобразования в электронную форму книг, электронные оригинал-макеты которых были уничтожены. Другой пример дают некоторые телеконференции: их материалы выставляются для доступа в Интернете, а по истечении некоторого времени уничтожаются. Число таких примеров можно значительно увеличить. Решение проблемы сохранения электронной информации нуждается в организационных, методических и технологических проработках.

3. Особую проблему представляет инвентаризация электронной информации, включающая в себя определение самостоятельных единиц электронной информации, их адекватное и унифицированное описание. Сюда же входят вопросы учета и каталогизации.

4. Сохраняемая электронная информация должна эффективно использоваться. Здесь сразу же встают вопросы совместимости программного обеспечения и форматов, вопросы реализации разнообразных функциональных возможностей, предусматриваемых создателями электронных документов. На решение указанных и ряда других проблем направлена деятельность по созданию электронных библиотек. Область деятельности, связанная с электронными библиотеками, является достаточно новой и поэтому еще не имеет устойчивой терминологии. Безусловно, не следует отождествлять эту область деятельности с автоматизацией традиционных библиотечных процессов, хотя провести между ними точную границу вряд ли возможно.

В рамках установленных действующим законодательством норм и правил для библиотек и информационных органов России центральными являются проблемы, связанные с «ножницами» между правами пользователей на свободный и широкий доступ к информации и правами собственников информационных продуктов, включая и авторское право. В про-

цессе выполнения массовых и требующих оперативного удовлетворения запросов пользователей, связанных с необходимостью снятия копий с запрашиваемых документов, библиотечные и информационные работники постоянно попадают в положение, которое вынуждает их либо нарушать имущественные права собственников интеллектуальной продукции, либо право граждан и организаций на получение требуемой информации.

В Законе об авторском праве определено: «Допускается без согласия автора и без выплаты авторского вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования репродуцирование в единичном экземпляре без извлечения прибыли:

а) правомерно опубликованного произведения библиотеками и архивами для восстановления, замены утраченных или испорченных экземпляров, предоставления экземпляров произведения другим библиотекам, утратившим по каким-либо причинам произведения из своих фондов;

б) отдельных статей и малообъемных произведений, правомерно опубликованных в сборниках, газетах и других периодических изданиях, коротких отрывков из правомерно опубликованных письменных произведений (с иллюстрациями или без иллюстраций) библиотеками и архивами по запросам физических лиц в учебных и исследовательских целях;

в) отдельных статей и малообъемных произведений, правомерно опубликованных в сборниках, газетах и других периодических изданиях, коротких отрывков из правомерно опубликованных письменных произведений (с иллюстрациями или без иллюстраций) образовательными учреждениями для аудиторных занятий».

Таким образом, данный Закон запрещает изготовление копий многих видов документов, запрашиваемых пользователями, хотя и разрешает брать из них «короткие отрывки».

Экономическая ситуация, в которой существуют российские библиотеки, вынуждает сокращать приобретение оте-

явственной и зарубежной литературы как по номенклатуре, так и по количеству (до одного экземпляра). Кроме того, многие популярные и необходимые издания (например, в области бизнеса, банковского дела и т.д.) выпускаются небольшими частными издательствами Москвы и Санкт-Петербурга весьма ограниченным тиражом, и до периферийных библиотек они просто не доходят. В сложившихся условиях многие библиотеки России вынуждены давать отказ либо удовлетворять запросы копированием целых изданий с нарушением закона, например копированием изданий «по частям».

Указанная практика поддерживается не только экономическими условиями. Как правило, организация — заказчик копии готова оплатить ее стоимость, а организация-изготовитель — выплатить все необходимые отчисления собственнику и(или) автору информационной продукции. Следуя действующему порядку, библиотеки или информационные органы, получившие подобные заказы, должны в каждом случае получить разрешение от держателя прав собственности на запрашиваемое издание. Помимо требуемых значительных затрат времени на переписку часто бывает неясно, кто владеет правом собственности: автор, издательство или кто-либо еще. Понятно, что даже при очень небольшом потоке запросов на копирование таких произведений служба МБА и доставки документов удовлетворить их не в состоянии.

Необходим механизм, обеспечивающий оперативное взаимодействие библиотек (информационных органов) и держателей прав собственности на информационную продукцию и, возможно, создание организации или нескольких организаций, выполняющих функции посредников между ними.

Не менее актуальной является также проблема, связанная с защитой авторских прав российских авторов при копировании их произведений зарубежными библиотеками. Наши зарубежные партнеры просто не знают, куда обращаться в указанных случаях. Российское авторское общество (РАО) многие из этих функций не выполняет. Эту проблему можно было бы попробовать решить, например для США, возложив

ее на Международный библиотечно-информационный центр (МБИАЦ), в котором ГПНТБ России действует от имени российского библиотечного сообщества. Функция организации-посредника между зарубежными службами копирования и российскими собственниками или авторами интеллектуальной продукции может стать одной из основных для этого Центра. Кстати, деятельность службы копирайт Библиотеки Конгресса США является одним из показательных примеров решения подобных вопросов.

Однако сказанным проблемы с охраной авторских прав и прав собственников информационной продукции, а также прав на распространение и пользование информацией не ограничиваются. Представление любых видов данных в цифровой форме, с одной стороны, существенно повышает легкость и скорость копирования, а также трансформирования и распространения исходного материала; с другой стороны, создает новые виды информационных продуктов (в частности, разнородных видов баз данных, полнотекстовых документов и программных продуктов), а также связанных с ними новых условий неопределенности отношений субъектов информационной деятельности.

Эти проблемы характерны не только для российского, но и международного законодательства. В частности, в соответствии с законами США запись защищенного авторским правом произведения в память ЭВМ является репродукцией этого произведения, поскольку она может «восприниматься, репродуцироваться или передаваться с помощью машины или других средств». Таким образом, когда произведение записывается в память ЭВМ более чем на очень короткий период, создается его копия. Когда печатное произведение сканируется и трансформируется в цифровой вид, также создается его копия.

Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» гласит: «База данных (БД) — это объективная форма представления и организации совокупности данных (например, статей, расчетов),

систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ». Являясь объектом защиты интеллектуальной собственности, БД приравнивается к сборникам. При этом авторское право на БД признается при условии еще соблюдения авторского права на каждое из включенных в нее произведений. В соответствии с п. 4 ст. 5 этого Закона «авторское право на базу данных не препятствует другим лицам осуществлять самостоятельный подбор и организацию произведений и материалов, входящих в эту базу данных». Из сказанного следует, что закон защищает авторским правом структуру «сборника», т.е. базы данных, а не ее состав.

В современной практике библиотек и информационных органов России можно считать достаточно распространенным явлением параллельное ведение многими организациями электронных каталогов, имеющих одинаковую структуру составляющих их библиографических баз данных, которая определяется выбранным форматом. Другой признак структуры — порядок следования записей на физическом носителе — в современной программной среде значения не имеет, поскольку легко изменяется, например операцией «сортировки». Таким образом, признаков, позволяющих идентифицировать конкретную базу данных с ее владельцем или автором, нет. К счастью, библиотеки России, являющиеся владельцами электронных каталогов, еще не приступили к их регистрации и недостатков данного Закона не ощутили. Сказанное можно распространить на информационные и справочно-информационные (в том числе на так называемые «полнотекстовые») базы данных. В результате порождаются дополнительные проблемы, в том числе связанные с уже упомянутыми выше в области репродуцирования литературных и других произведений или их частей при включении их в структуру создаваемых баз данных.

В связи со всем вышеизложенным в мировой практике появилась точка зрения на защиту авторских прав, в соответствии с которой эта защита должна быть ослаблена, так как обществен-

ность «желает иметь свободный доступ к информации», а закон должен отражать это желание. Указанное мнение опирается также на прогресс в области информационных технологий. В частности, поскольку компьютерные сети делают возможным нелегальное копирование и распространение информации, то считается, что закон должен легитимизировать эту ситуацию. В противном случае он будет обречен на постоянные нарушения.

Очевидно, цитируемый подход не может быть принят хотя бы потому, что он может оказать негативное влияние на процессы создания новых интеллектуальных продуктов, поскольку не поощряет авторов на творческую деятельность. По-видимому, наиболее приемлемым является принятие в информационном законодательстве России так называемого принципа «свободного использования». В соответствии с этим принципом пользователь не должен просить разрешения у владельца прав или оплачивать лицензию за использование произведений (в том числе цитирование, включение в новое произведение частей или фрагментов другого произведения и т.д.) при выполнении ряда условий, связанных с:

— целями и характером использования, характером защищенного авторским правом произведения;

— размером и существенностью заимствованного фрагмента по отношению ко всему произведению;

— характером воздействия использования на рынок или ценность защищенного произведения.

Национальные библиотеки находятся в федеральной собственности и призваны формировать полное собрание отечественных документов.

5. Государственное регулирование архивного дела

Государству, обществу и гражданам необходимо упорядоченное сохранение, комплектование, учет и использование документов Архивного фонда РФ, который действует на основании ФЗ об архивном деле в Российской Федерации[1]. Ар-

[1] СЗ РФ. 2004. № 43. Ст. 4169.

хивный фонд РФ — исторически сложившаяся и постоянно пополняющаяся совокупность архивных документов, отражающих материальную и духовную жизнь общества, имеющих историческое, научное, социальное, экономическое, политическое и культурное значение, являющихся неотъемлемой частью историко-культурного наследия народов РФ, относящихся к информационным ресурсам и подлежащих постоянному хранению.

Архивным делом называется деятельность государственных органов, органов местного самоуправления, организаций и граждан в сфере организации, хранения, комплектования, учета и использования документов Архивного фонда РФ и других архивных документов, представляющих собой материальный носитель с зафиксированной на нем информацией, имеющий реквизиты, позволяющие его идентифицировать, и подлежащий хранению в силу значимости, указанной на носителе, для граждан, общества, государства.

Архив — учреждение или структурное подразделение организации, осуществляющие хранение, комплектование, учет и использование архивных документов. Существуют государственные (создаваемые Правительством РФ или субъектом РФ) и муниципальные архивы (структурные подразделения органа местного самоуправления муниципального района, городского округа либо муниципальное учреждение, создаваемое этим органом).

Федеральным органом исполнительной власти, осуществляющим государственное регулирование в области архивного дела и контроль за сохранностью, комплектованием и использованием документов Архивного фонда РФ, является Федеральное архивное агентство,[1] которое осуществляет свою деятельность во взаимодействии с федеральными

[1] См.: Положение о Федеральном архивном агентстве, утв. постановлением Правительства РФ от 17 июня 2004 г. № 290 // СЗ РФ. 2004. № 25. Ст. 2572.

и субъектов Федерации органами государственной власти, а также Российской академией наук, Российским обществом историков-архивистов и другими общественными объединениями.

Росархив осуществляет следующие функции и полномочия в установленной сфере деятельности: организует информационное обеспечение граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе документов Архивного фонда РФ и других архивных документов, в том числе путем создания и ведения информационных поисковых систем по архивным документам; работу по подготовке документальных публикаций, а также документальных экспозиций и справочников о составе и содержании документов Архивного фонда РФ; экспертизу архивных документов, заявленных к вывозу за пределы РФ и экспертизу документов Архивного фонда РФ, временно вывезенных за пределы РФ, после их возвращения; работу федеральных архивных учреждений по рассекречиванию в установленном порядке носителей сведений, составляющих государственную тайну; координацию деятельности научно-методических советов архивных учреждений федеральных округов; осуществляет в порядке и пределах, определенных федеральным законодательством, полномочия собственника в отношении федерального имущества, необходимого для обеспечения исполнения функций федеральных органов государственной власти в установленной сфере деятельности, в том числе имущества, переданного федеральным государственным унитарным предприятиям, федеральным государственным учреждениям и казенным предприятиям, подведомственным Агентству; ведет государственный учет документов Архивного фонда РФ и Государственный реестр уникальных документов Архивного фонда РФ; осуществляет функции главного распорядителя и получателя средств федерального бюджета, предусмотренных на содержание Агентства и реализацию возложенных на него функций и функции государственного заказчика федеральных целевых, научно-

технических и инновационных программ и проектов в сфере деятельности Агентства; экспертизу проектов национальных стандартов в области архивного дела и документационного обеспечения управления; обеспечение соблюдения правил хранения, комплектования, учета и использования архивных документов; осуществляет иные функции и полномочия по управлению государственным имуществом и оказанию государственных услуг в установленной сфере деятельности, если они предусмотрены федеральным законодательством.

Архивные фонды — масса информационных ресурсов. Правовое регулирование архивного дела направлено на обеспечение открытости информации и динамичности процесса получения информации.

Открытость информации в архивных фондах обеспечивается:

1) существованием различных режимов доступа к информации;

2) переходом информации из одной категории доступа в другую.

Ответственность за сохранность информации в библиотеках и архивах плохо урегулирована. Отсутствует ответственность за неправильное хранение подлинных документов, за несанкционированное копирование документов, распространение.

Глава 10. Электронный документ

1. Понятие и структура электронного документа

Во многих сферах деятельности широкое распространение получило использование электронных документов, причем последние применяются не только наряду с традиционными бумажными документами, но и вместо них. Как отмечает А. Серго, использование систем электронного документооборота позволяет добиться огромного экономического эффекта, а применительно к России такое снижение издержек с учетом

территориальной протяженности может быть колоссальным[1]. В связи с этим одним из важнейших направлений развития российского законодательства и правоприменительной практики в настоящее время является правовое регулирование отношений в области электронного документооборота и придание юридической силы электронным документам.

До настоящего времени ни законодатель, ни современная доктрина не выработали общего однозначного определения электронного документа. Легальное определение данного термина появилось лишь в 2002 г. в Федеральном'законе от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»[2]: «Электронный документ — документ, в котором информация представлена в электронно-цифровой форме». Законодатель в этом определении обратил внимание лишь на форму предоставления информации данного класса документов, отличающую его от других документов. В юридической литературе многократно отмечалось, что это определение достаточно широкое и оно далеко не полностью раскрывает рассматриваемое понятие, что дает почву для его неоднозначного толкования при решении задач правового регулирования вопросов использования электронных документов.

Более удачным представляется понятие электронного документа, предложенное СИ. Семилетовым: «Электронный документ — документ, созданный при помощи электронных аппаратно-технических (ЭВМ) и программных средств, фиксируемый в цифровом коде в форме идентифицируемого именного файла(ов) или записи в файле(ах) базы данных, доступный для последующей обработки в информационных системах, использования, воспроизведения (отображения) и визуального восприятия, а также для передачи и получения по телекоммуникационным каналам связи»[3].

---

[1] *Серго А.* Электронный документ // Российская юстиция. 2003. № 5. С. 69.

[2] СЗ РФ. 2002. № 2. Ст. 127.

[3] *Семилетов СИ.* Электронный документ как продукт технологического процесса документирования информации и объект правового регулирования // Государство и право. 2003. № 1. С. 101.

Как справедливо отмечает СИ. Семилетов, электронные цифровые документы в качестве объекта права следует рассматривать как обособленные или выделенные объекты и в тех же формах, в которых эти документы реально существуют как объекты деятельности и оборота в конкретных правоотношениях. При этом файл как форма электронного документа должен выступать в качестве главного объекта правового регулирования.

Три элемента электронного документа:

1) само содержание информации;

2) форма предоставления содержания;

3) носитель информации.

Хэш-функция — контрольная характеристика файла, позволяющая определить факт внесения в документ несанкционированных изменений.

В России нет закона об электронном документе и не решена проблема долгосрочного хранения электронного документа.

2. Правовой статус электронной цифровой подписи

Электронно-цифровая подпись — реквизит электронного документа, полученный в результате преобразования информации с использованием закрытого ключа электронно-цифровой подписи и позволяющий установить подлинность и целостность содержащейся в электронном документе информации, а также обладателя электронно-цифровой подписи. Электронно-цифровая подпись в электронном документе становится равнозначной собственноручной подписи при следующих условиях (одновременно).

1. Сертификат ключа электронно-цифровой подписи не утратил силу.

2. Подтверждена подлинность электронно-цифровой подписи в электронном документе.

3. Электронно-цифровая подпись используется в отношениях, имеющих юридическое значение.

Субъекты электронно-цифровой подписи:

— пользователи информационной системы;

— обладатели электронно-цифровой подписи;

— удостоверяющие центры;
— уполномоченные ФОИВ.

Электронная цифровая подпись — это современный надежный юридический инструмент, позволяющий практически мгновенно, вне зависимости от времени суток и расстояний, заключить юридически полноценную сделку, а также в случае необходимости однозначно и без сомнений решить самые разнообразные споры, в том числе и в судебном порядке.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

ЭЦП была известна и использовалась еще задолго до принятия закона. Ее внутренний стандарт утвердил Центральный банк РФ в 1993 г., с ее помощью Пенсионный фонд РФ принимал отчетность от организаций через Интернет. И только 13 декабря 2001 г. в третьем чтении Госдумой РФ был принят Федеральный закон «Об электронной цифровой подписи», который регулирует правовые условия использования электронной цифровой подписи (далее — ЭЦП) в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Помимо основных понятий и целей, Закон содержит нормы применения ЭЦП.

Итак, **ЭЦП** — это программно-криптографическое (т.е. зашифрованное соответствующим образом) средство, которое позволяет подтвердить, что подпись, стоящая на том или ином электронном документе, поставлена именно его автором, а не каким-либо другим лицом.

Для автора документа генерируется закрытый ключ — последовательность цифр определенной длины. Любой электронный документ с технической точки зрения также представляет собой последовательность цифр. ЭЦП представляет собой некое число, полученное в результате преобразования электронного документа как цифровой последовательности с помощью закрытого ключа автора. На базе закрытого ключа создается открытый ключ, доступный любому. Любой может проверить ЭЦП под документом при помощи соответствующих преобразований с использованием электронного образца документа, открытого ключа отправителя и собственно значения ЭЦП. Открытый и закрытый ключи однозначно связаны между собой, однако вычислить закрытый ключ по открытому практически невозможно; как минимум, это требует очень продолжительного периода времени.

Закрытый ключ, разумеется, содержится в тайне и известен только владельцу, что бы никто, кроме владельца, не смог сформировать ЭЦП под документом. В то же время буквально любое заинтересованное лицо может проверить с помощью опубликованного открытого ключа, что документ подписал именно владелец, что документ не искажен (иначе меняется производная величина). Таким образом, подделать электронный документ, подписанный ЭЦП, существенно сложнее, чем документ на бумажном носителе. Защищенным оказывается и сам текст документа, причем не требуется помощи экспертов для выявления факта искажения документа. Проверка осуществляется строго математическим путем, причем автоматически, не нужно самому проделывать какие-либо вычисления. В результате запуска программы открытого ключа пользователь получает результаты проверки в наглядном виде как сообщение о том, что документ подписан таким-то

лицом, возможно, некоторые другие дополнительные данные. Или получает отрицательный результат.

Не менее важно, чтобы информация о принадлежности открытого ключа определенному пользователю была документально оформлена, причем такое оформление должно быть выполнено соответствующим ответственным органом. Соответствующий документ получил название сертификата открытого ключа ЭЦП (сертификат ключа подписи). Требования к сертификату ключа подписи изложены в ст. 6 Закона об ЭЦП. Сертификат подтверждает принадлежность открытого ключа ЭЦП владельцу сертификата ключа подписи, т.е. лицу, на имя которого выдан сертификат ключа подписи и которое владеет закрытым ключом ЭЦП, соответствующим открытому ключу, указанному в сертификате. Такой документ выдает удостоверяющий центр, статус и основные функции которого определены ст. 8 и 9 Закона. Наличие сертификата важно при разрешении споров о принадлежности той или иной информации конкретному пользователю. Для исключения внесения изменений в сертификаты ключей со стороны пользователей этот сертификат в виде электронных данных подписывается ЭЦП удостоверяющего центра, а сам сертификат выдается его владельцу в бумажной форме. В случае судебного разбирательства удостоверяющий центр может подтвердить подлинность ЭЦП. Стороны, участвующие в электронной коммерции, при создании ЭЦП могут обойтись и без участия удостоверяющих центров, однако доказательная сила такой подписи резко падает.

Сертификаты ключей могут распространяться среди участников информационной системы как в бумажном, так и в электронном виде. Бумажный сертификат должен быть оформлен на бланке удостоверяющего центра и заверен подписью уполномоченного лица с печатью центра. Электронный сертификат должен быть заверен ЭЦП удостоверяющего центра. Удостоверяющий центр изготавливает сертификаты ключей подписей; создает ключи ЭЦП с гарантией сохранения в тайне закрытого ключа; приостанав-

ливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их; ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему клиентов; проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра; осуществляет подтверждение подлинности электронной цифровой подписи в электронном документе.

Действие данного Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством РФ случаях. Однако в некоторых странах сфера применения подобных законов гораздо шире и определяется методом исключения.

Например, в США согласно Закону об электронных подписях в мировой и национальной торговле (Electronic Signatures in Global and national Commerce Act), известному как закон об электронной подписи (E-Sign Act), вступившему в силу 1 октября 2000 г., любой контракт, соглашение, документ, закладная или другая форма документа, имеющего отношение к недвижимости, или любой другой деловой документ может быть подписан с помощью электронной подписи. Более того, документы, имеющие отношение к вещным правам, недвижимости, могут быть нотариально засвидетельствованы через электронные средства информации, если уполномоченный государственный нотариус работает в режиме on-line, т.е. имеет возможность видеть, что человек «подписал» документ и подтверждает подлинность подписи. В связи с чем документ, отправленный, подписанный и нотариально засвидетельствованный с помощью электронных средств связи, может быть использован в суде и при отсутствии на нем традиционной подписи[1].

[1] *Randell D.* Wallace and Don F. Dagenais. The Changing World of Electronic Signatures//http://library.lp.findlaw.com/articles/

Однако указанный Закон предусматривает ряд исключений, в частности последний не признает электронные подписи на завещаниях, дополнениях к завещанию, завещаниях с установлением доверительной собственности, бумагах, связанных с разводом и усыновлением; документах, сопровождающих опасные материалы. Судебные приказы также должны фактически подписываться судьей. С помощью электронной подписи не может быть осуществлен переход заложенной недвижимости в собственность залогодержателя, аннулирован страховой полис медицинского страхования страховыми компаниями. Необходимо отметить, что данный список имеет тенденцию к сокращению. В связи с чем представляется целесообразным создание правовых основ для использования электронной цифровой подписи в России не только в гражданском электронном документообороте, но и во взаимоотношениях с государственными и муниципальными органами власти.

Расхождение между названными актами еще и в том, что российский Закон не распространяется на другие формы аналогов собственноручной подписи.

Собственноручная подпись не отделима от человека, а наиболее важный с юридической точки зрения компонент — электронно-цифровая подпись (далее — ЭЦП) — секретный закрытый ключ — пока вполне отделим. Отсутствие норм, уникально увязывающих электронную цифровую подпись с физическим лицом, породит множество проблем правоприменительной практики. Так, если третьему лицу станет известен закрытый ключ, то отличить подлог подписи до аннулирования ключей будет невозможно. В силу этого возникает необходимость в установлении правомерности владения секретным ключом лица, подписавшего документ. Практически это не всегда достижимо, поэтому должна быть закреплена презумпция, согласно которой бремя юридических последствий за использование третьими лицами закрытого ключа лежит на его владельце. Иными словами, кто бы ни подписал электронный документ, он будет счи-

таться подлинным лицом, обладающим закрытым ключом, если владелец не известил участников системы о необходимости его аннулировать в связи с выходом из-под контроля.

Важным вопросом представляется обеспечение защиты и сохранности секретного ключа. Такие ключи никогда не должны храниться в явном виде на носителях, с которых они могут быть скопированы и, соответственно, скомпрометированы. В числе способов обеспечения сохранности секретных ключей можно назвать следующие:

1) хранение на носителях, которые трудно копируются, например специальные чип-карты, доступ к которым имеет лишь владелец ключа, знающий PIN-код;

2) использование методов, позволяющих с очень высокой степенью достоверности обеспечить привязку электронно-цифровой подписи к подписанту (примером может служить технология цифровой обработки папиллярного узора отпечатка пальца, радужной оболочки глаза, автографа и других биометрических параметров);

3) шифрование секретных ключей на других ключах, которые могут быть тоже зашифрованы.

Недостаточно проработаны вопросы ответственности третьих лиц, участников электронного оборота документов и органов, ответственных за проведение сертификации средств ЭЦП. Не установлено, кто несет ответственность в случае, если убытки будут по причине несанкционированного взлома сертифицированных средств цифровой подписи или наличия в них разного рода незаконно установленных программных или аппаратных закладок. Не определен также порядок хранения и доступа к закрытым ключам ЭЦП в удостоверяющих центрах. Следует отметить, что эти проблемы можно решить договором с удостоверяющим центром, однако типовую форму такого договора только еще предстоит разработать.

Неурегулированным вопросом является проверка уникальности открытых ключей. Такая проверка проводится в ре-

естре сертификатов ключей подписей и архиве удостоверяющего центра, причем удостоверяющий центр проводит проверку по данным своего реестра и архива. Вследствие этого без внимания остаются реестры и архивы других удостоверяющих центров, где могут храниться идентичные ключи. Выход из сложившейся ситуации видится в том, чтобы создать единый реестр ключей ЭЦП, возложив ведение этого реестра на государство, и сделать его доступным для граждан через сеть «Интернет». Это позволило бы существенно сократить издержки, связанные с функционированием множества удостоверяющих центров. Принятие на себя государством расходов, связанных с созданием и ведением реестра ключей ЭЦП, сократило бы затраты граждан на оплату услуг удостоверяющих центров, а следовательно, удешевило бы технологии цифровых подписей.

Электронный документ с ЭЦП как форма является универсальным для документов, в которых фиксируется динамика отношений, особенно в гражданско-правовой сфере, что и закреплено законодательно. Но динамики не меньше и в системе государственного и муниципального управления. Потребность органов государственной власти в ускорении доведения информации до исполнителей управленческих отношений, более широкие финансовые возможности системы государственного управления и меньший риск негативных последствий в случае возникновения сбоев и ошибок обусловливают развитие системы электронного документооборота. Однако эта сфера остается вне законодательного регулирования.

Что касается опыта зарубежных стран, то необходимо отметить следующее. Государства с разной правовой культурой традиционно расходятся в оценке подписи. Страны общего права (США, Великобритания) не предъявляют особых требований к подписи, стоящей в конце документа, который может быть подписан либо одной стороной, либо двумя сторонами. При этом сама подпись может быть сделана любым способом. В романо-германских правовых системах

(в странах континентальной Европы), где правовая доктрина традиционно играла существенную роль, сложилась иная концепция подписи. Она воспринимается как факт окончательного выражения воли сторон, придания документу характера юридически значимого — в этом заключается основная функция подписи. Кроме того, в США и Европе структура сертификационных центров на практике сложилась самостоятельно, без какого-либо участия государства, при этом она существует на средства коммерческих компаний.

Государства и предприниматели заинтересованы в стандартизации регулирования электронной подписи, что было бы удобно и целесообразно при осуществлении международной торговли через Интернет. Однако практика пошла по пути разработки национальных моделей. Законы приняты в Германии, Австрии, Великобритании, Японии, ряде латиноамериканских стран. Национальное законодательство чрезвычайно разнообразно. Германия и Япония уделяют большое внимание техническим стандартам, Сингапур и Малайзия — юридическому значению электронной подписи, государственному контролю за деятельностью удостоверяющих (сертифицирующих) органов.

Таким образом, действующее законодательство характеризуется наличием определенных пробелов, что, в свою очередь, негативно сказывается на развитии соответствующих общественных отношений.

Глава 11. Права граждан в информационной сфере

1. Право на доступ к информации

Реализация основных прав и свобод граждан в информационной сфере занимает важное место среди национальных интересов России. Право на поиск, получение и передачу информации (право на доступ к информации или право знать

является определяющим институтом информационного права. Юридический фундамент этого института составляют информационно-правовые нормы Конституции РФ. Основа права на доступ к информации содержится в ст. 29 ч. 4 Конституции РФ: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

В современной юридической литературе существуют различные мнения на природу права гражданина на информацию. Например, Ю.А. Дмитриев и А.А. Златопольский считают право гражданина на информацию составной частью свободы слова и печати[1]. Существует точка зрения, в соответствии с которой свобода информации — условное обозначение группы прав и свобод: свободы слова, мнений, свободы печати и иных средств массовой информации, права на получение информации, свободы распространения информации[2]. Имеется и противоположное суждение, когда право на доступ к информации рассматривается как отдельное, самостоятельное право в группе других информационных прав и свобод[3]. И действительно, анализируя ст. 29 Конституции РФ, можно сделать вывод, что право гражданина на информацию — все же самостоятельное право, так как в этой статье оно за-

---

[1] См.: *Дмитриев Ю.А., Златопольский А.А.* Гражданин и власть. — М., 1994. С. 37.

[2] См., например: Конституционное (государственное) право зарубежных стран. Т. 1 / Под ред. Б.А. Страшуна. — М., 1993. С. 102; *Туманова Л.В., Снытников А.А.* Обеспечение и защита права на информацию. — М., 2001. С. 10.

[3] См., например: *Копылов В.А.* Информационное право. — М., 2002. С. 130; *Иззатов Т.Ш.* Механизм реализации конституционного права граждан на информацию в РФ: Автореф. дис. ...канд.юрид.наук. — М., 2002.С. 11; *Корченкова Н.Ю.* Становление теоретико-правовой концепции права на информацию: Автореф. дис. ... канд. юрид. наук. — Н. Новгород, 2000. С. 8; *Шевердяев С. Н.* Проблемы конституционно-правового регулирования информационных отношений в Российской Федерации: Автореф. дис. ... канд. юрид. наук. — М., 2002. С. 7; *Малько А.В.* Право гражданина на информацию // Общественные науки и современность. 1995. № 5. С. 58.

креплено в части, отдельной от той, где речь идет о гарантии свободы мысли и слова. Кроме того, имеются отдельные нормативные акты, посвященные данному вопросу, например Федеральный закон «Об информации, информатизации и защите информации». Да и сам факт активного формирования такой отрасли российского права, как информационное, доказывает это. Хотя, несомненно, право человека и гражданина на информацию очень тесно связано со свободой слова и печати. Но право на информацию не охватывается полностью свободой слова и печати. Оно выполняет свою роль в удовлетворении определенных интересов субъекта.

Таким образом, **право на информацию** — нормативный определенный порядок реализации полномочий различных субъектов в области производства (создания, получения, доступа, сбора, хранения, использования и распространения) информации в целях, не противоречащих свободам, правам и интересам личности, общества и государства. Правда, здесь необходимо сделать уточнение о том, что по общему правилу цели доступа к информации не должны противоречить правам и интересам других лиц, общества, государства. Но об ограничениях права на информацию речь пойдет во втором параграфе.

Существует еще ряд прав, относимых к информационным:

— право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, прописанное в ст. 23 ч. 1 Конституции России: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени»;

— право на тайну переписки, телефонных переговоров, почтовых и телеграфных и иных сообщений — ч. 2 ст. 23 Конституции РФ: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений...» Тем самым ограничивается право на доступ к персональным данным любых лиц, кроме самих этих лиц;

— свобода мысли и слова — ч. 1 ст. 29 Конституции РФ: «Каждому гарантируется свобода мысли и слова»;

— право на свободу выражения своих мнений и убеждений — ч. 3 ст. 29 Конституции: «Никто не может быть принужден к выражению своих мнений и убеждений»;

— право граждан обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления — ст. 33 Конституции РФ: ««Граждане РФ имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления». Тем самым данная норма Конституции обязывает государственные органы и органы местного самоуправления создавать информационные ресурсы в сфере их деятельности и предоставлять из них информацию обратившимся субъектам по их запросам;

— право каждого на достоверную информацию о состоянии окружающей среды — ст. 42 Конституции: «Каждый имеет право на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением»;

— свобода преподавания — ч. 1 ст. 44 Конституции РФ;

— право на доступ к культурным ценностям и участие в культурной жизни — ч. 2 ст. 44 Конституции России. Тем самым эта статья возлагает на учреждения культуры, другие структуры, обладающие культурными ценностями, обязанности обеспечивать доступ каждого к этим ценностям, т.е. поиск и получение информации об этих ценностях. При этом на каждого, допущенного к соответствующим культурным ценностям и учреждением культуры, возлагается обязанность сохранять эти ценности — ст. 44: «Каждый обязан заботиться о сохранении исторического и культурного наследия, беречь памятники истории и культуры»;

— право на получение квалифицированной юридической помощи — ст. 48 Конституции.

Гарантии получения каждым сообщений, извещающих о положении дел, о получении свободной массовой информа-

ции, закрепляются ч. 5 ст. 29 Конституции РФ: «Гарантируется свобода массовой информации. Цензура запрещается».

Перечисленные выше права и свободы личности при своей реализации могут быть ограничены как правами и свободой других лиц, так и по другим основаниям и в случаях, прямо указанных в федеральных законах. Цель ограничений — сузить свободу и сдержать реализацию антиобщественных интересов личности[1].

Принципы ограничения прав граждан содержатся в Конституции РФ в ст. 17: «Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц». Анализируя ч. 3 ст. 17 и ч. 3 ст. 55 Конституции, можно сделать вывод, что к основаниям ограничения основных информационных прав и свобод граждан законодатель относит:

— защиту основ конституционного строя;

— нравственности;

— здоровья;

— прав и законных интересов других лиц;

— обеспечение обороны страны и безопасности государства.

В ст. 56 Конституции указывается на возможность ограничения прав и свобод в условиях чрезвычайного положенш в соответствии с федеральным конституционным законом.

Часть 2 ст. 29 Конституции РФ устанавливает правовые барьеры против злоупотребления свободой слова, выражения мнения. Не допускается пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

Гарантии и одновременно пределы осуществления информационных прав и свобод человека и гражданина закреплены

[1] См.: *Хижняк В.С.* Право человека на информацию: механизм реализации / Под ред. В.Т. Кабышева. — Саратов, 1998. С. 40.

в ст. 24 Конституции РФ, которая устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Данное конституционное положение является одной из гарантий закрепленного в ст. 23 Конституции права на неприкосновенность частной жизни. Оно призвано защитить частную жизнь, личную и семейную тайну от проникновения в нее со стороны как государственных органов, органов местного самоуправления, так и негосударственных структур, отдельных граждан.

В.Н. Лопатин в качестве оснований ограничения информационных прав граждан на основе анализа конституционных положений выделяет следующее:

— защита основ конституционного строя;

— защита нравственности, здоровья, прав, законных интересов других лиц;

— обеспечение обороны страны и безопасности государства;

— обеспечение общественного спокойствия в целях предотвращения беспорядков и борьбы с преступностью;

— предотвращение разглашения конфиденциальной информации;

— обеспечение авторитета и беспристрастности правосудия;

— условия чрезвычайного положения.[1]

Случаи прямого ограничения информационных прав, по его мнению, имеют место в следующих ситуациях:

— использование прав в целях насильственного изменения конституционного строя;

— пропаганда социальной ненависти, социального, расового, национального, религиозного, языкового превосходства, насилия и войны;

— нарушение права на неприкосновенность частной жизни (на личную, семейную тайну, неприкосновенность жили-

[1] См.: *Лопатин В.Н.* Право на информацию // Информационное право / Под ред. Б.Н. Топорнина. — СПб., 2001. С. 432.

ща, права на уважение и защиту чести, достоинства и репутации, тайны переписки, телефонных переговоров, телеграфных и иных сообщений). К сфере частной жизни автор относит и право на отказ от свидетельствования против себя самого, своего супруга и близких родственников;

— нарушение права на государственную, служебную, профессиональную, коммерческую и банковскую тайну[1].

Кроме того, пользователи — граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения — обладают равными правами на доступ к государственным информационным ресурсам. Так гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы. В свою очередь, организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности, (п. 2 и 3 ст. 8 Федерального закона об информации).

Но существует и понятие информации с ограниченным доступом, т.е. такой информации, которая не предназначена для широкого распространения и в связи с этим подлежит правовой охране от несанкционированного доступа.

Таким образом, основаниями для ограничения информационных прав могут служить:

1) защита основ конституционного строя;
2) защита нравственности;
3) защита здоровья;
4) защита прав и законных интересов других лиц;

[1] См.: *Лопатин В.Н.* Право на информацию // Информационное право / Под ред. Б.Н. Топорнина. — СПб., 2001. С. 432.

5) обеспечение обороны страны и безопасности государства.

Необходимо создать единый перечень оснований для ограничений и перечень случаев прямого ограничения прав на информацию.

Виды доступа информации

1. Обязательное доведение информации до всеобщего сведения.

2. Свободный доступ сообщения информации для всеобщего сведения.

3. Предоставление информации по запросу (может быть платным).

В целях охраны прав на доступ к информации необходимо законодательное установление оснований для разрешения коллизий при реализации прав на информацию и права на «тайну». Необходимо определение в законе механизма доступа к открытой информации и создание единой системы ответственности за правонарушения в информационной сфере.

Защита права на доступ к информации может осуществляться в неюрисдикционной форме (самозащита своих прав и законных интересов) и юрисдикционной форме (в специальном, административном порядке или по общему правилу в судебном порядке).

В административном порядке — защита может осуществляться только в случаях, прямо указанных в законах, — через подачу жалобы лицом, чьи права нарушены, на должностное лицо (орган) в вышестоящую инстанцию, специальный орган — ранее в Судебную палату по информационным спорам при Президенте РФ[1].

В судебном порядке — лицо может выбрать любой способ защиты нарушенного права через подачу иска (жалобы) для рассмотрения в гражданском, административном или уголовном судопроизводстве.

---

[1] См.: Соответствующий Указ Президента РФ от 31 декабря 1993 г. «О дополнительных гарантиях прав граждан на информацию» // САПП РФ. 1994. № 2. Ст. 74.

2. Право интеллектуальной собственности

Авторское право и смежные права

Право интеллектуальной собственности понимается в двух смыслах:

— право собственности на «право» и охраняется факт создания (Германия, Россия);

— охраняется факт фиксации произведения (США, Англия, Франция). Происходит отделение объекта от формы.

В России ст. 6 Закона об авторском праве оставляет свободное пространство для применения института собственности на интеллектуальный объект, оставляя неурегулированным продукт, не подпадающий под авторское право, что, в свою очередь, влечет и правовую незащищенность формы объекта.

Реализация права интеллектуальной собственности происходит в конкретных формах, которые изменяют субъектные права автора, хотя реализуются они с согласия автора, например:

— право на воспроизведение влечет за собой изменение формы информации;

— запись с использованием технических устройств влечет смену носителя;

— трансляция произведения влечет перевод его в форму СМИ;

— перевод влечет изменение языка;

— аранжировка или переделка влечет изменение формы и содержания.

Законодательство об авторском праве и смежных правах начинает действовать с момента факта и создания произведения.

Субъекты авторского права:

— автор;

— пользователь.

Объекты:

— произведения науки;

— произведения литературы;

— произведения искусства.

Является результатом творческой деятельности независимо от назначения достоинства произведения. Они могут быть в следующих формах:

1) письменной;

2) устной (без носителя);

3) звуко- и видеозаписи;

4) изображения и др.

Кроме произведений:

— сборники;

— производные произведения (переводы, аранжировки).

Служебный заказ

Авторское право принадлежит автору, а исключение права на использование — у обладателя, у работодателя. Личное неимущественное право — неотчуждаемое:

— право авторства;

— право на имя;

— право на обнародование;

— право на защиту репутации автора.

Эти права охраняются и после смерти неограниченный срок.

Имущественные исключительные права:

— право на воспроизведение;

— право на распространение;

— право на импорт;

— право на публичное исполнение, показ;

— право на передачу в эфире;

— право на сообщение для всеобщего сведения по кабелю;

— право на перевод;

— право на переработку.

Российское авторское право отмежевалось относительно носителя информации, защищает только функции произведения, а содержание остается незащищенным.

Одним из основных принципов информационного права является двуединство информации и носителя. Следовательно, с позиции информационного права недопустимо разделе-

ние правового регулирования охраны формы и содержания произведения.

Возможности пользователя сети «Интернет» по мгновенному копированию и передаче информации на любые расстояния независимо от границ и территориальной юрисдикции государств позволяют устанавливать совершенно новые отношения посредством неведомых прежде инструментов, отличающихся от привычных аналогов. Естественно, следом за размещением авторских произведений в Интернете встали проблемы охраны и защиты авторского права, возникла необходимость разработки новых правовых механизмов регулирования.

Система российского законодательства в сфере авторского права довольно проста. В нее входят Бернская конвенция о защите литературных и художественных произведений от 9 сентября 1886 г., Всемирная конвенция об авторском праве от 6 сентября 1952 г., Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм от 29 октября 1971 г., несколько законодательных актов и ряд подзаконных актов. Центральное место в системе занимает Закон РФ от 9 июля 1993 г. № 5351-1 «Об авторском праве и смежных правах», а также Закон РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

Согласно п. 3 ст. 13 Закона РФ «Об авторском праве и смежных правах» последний распространяет авторское право на произведения науки, литературы и искусства, существующие в объективной форме, независимо от способа их выражения, что позволяет применять нормы данного Закона к отношениям, связанным с созданием и использованием произведений, объективированным в виде последовательности сигналов, передаваемых по каналам сети «Интернет». Из сферы охраны авторским правом исключаются «идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты» (ст. 6 Закона), «официальные документы (законы, судебные

решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы... сообщения о событиях и фактах, имеющие информационный характер» (ст. 8 Закона).

Очевидно, что способы защиты авторского права в Интернете ничем не отличаются от традиционных способов защиты. Сущность нарушений авторского права в Интернете такая же, как и вне сферы сети. Отличие в том, что простота копирования и нематериальная сущность объектов авторского права в Интернете не позволяет так же просто решить проблему обеспечения доказательств нарушений авторского права. Некоторые действия по защите авторских прав при нарушениях, связанных с использованием Интернета, намного сложнее.

Анализируя Закон об авторском праве, можно заметить, что основные положения данного Закона сформулированы законодателем исходя из представления, что авторские произведения, как правило, распространяются издателем путем опубликования тем или иным способом определенным тиражом и на твердом материальном носителе, в частности на бумажной основе. Издатель как посредник в отношениях между автором и читателем-пользователем играет существенную роль.

Но в Интернете информация и авторские произведения существуют исключительно в форме электронных документов (файлов), причем материальный носитель и физическое место, где конкретно записан машинный код такого документа, в таких системах несущественен, а пользователь всегда будет иметь дело с виртуальным образом таких электронных документов, отображаемых на экране дисплея. Использование Интернета изменило общественные отношения между автором, издателем и пользователем, а законодательство по авторскому праву осталось прежним.

Использование авторских произведений в личных целях пользователя вызывает много вопросов. Копирование пользо-

вателем авторских документов на своем периферийном оборудовании (т.е. запись в электронной форме в память ЭВМ, на винчестер, дискету; распечатка на принтере) является актом воспроизведения. Некоторые из этих действий пользователя не урегулированы действующим законодательством РФ, а некоторые противоречат требованиям Законов об авторском праве и о правовой охране программ для электронных вычислительных машин и баз данных.

Патентные права

Патентные права включают в себя три категории.

1. Право на изобретение.
2. Право на полезную модель.
3. Право на промышленные образцы.

Изобретение — право на устройство, способ, вещество, штамп, а также применение ранее известных изобретений.

Полезная модель — конструкторское выполнение средств производства, предметов потребления и их составных частей.

Промышленный образец — художественное конструктивное решение изделия, определяющее его внешний вид.

Патентные права подтверждаются патентом на изобретение, свидетельством на полезную модель, патентом на промышленный образец.

Авторами изобретения считаются все, кто участвовал в создании изобретения, кроме тех, кто оказывал организационную, техническую или материальную помощь.

Информационный объект — патент.

Законодательство о «ноу-хау»

Ноу-хау — это охраняемые в режиме коммерческой тайны результаты интеллектуальной деятельности, которые могут быть переданы другому лицу и использованы на законном основании только по усмотрению лица, обладающего тайной информацией на законном основании, и не обеспечены патентной защитой:

- право использовать;
- право передавать;
- право получать денежное вознаграждение.

Глава 12. Правовое регулирование средств массовой информации

1. Понятие и виды средств массовой информации

Средства массовой информации — юридическая фикция с точки зрения Гражданского кодекса РФ.

Массовая информация — разновидность информации. Средства массовой информации — форма периодического распространения информации. Смешение СМИ с организацией, осуществляющей выпуск СМИ, т.е. смешение объекта с субъектом — достаточно типичная ошибка. Например, в постановлении Пленума Верховного Суда РФ от 18 августа 1992 г. № 11 «О некоторых вопросах, возникших при рассмотрении судами дел о защите чести и достоинства граждан и организаций» (утратило силу) СМИ ошибочно отождествлялись с юридическим лицом, когда говорилось о предъявлении иска «к средству массовой информации» и о «возложении на средство массовой информации обязанности». Очевидно, что СМИ рассматривались здесь не как объект права, а как его субъект, что не соответствало Закону о СМИ.

К какому же виду объектов права следует отнести СМИ? В соответствии со ст. 128 ГК РФ вполне логично рассматривать массовую информацию как разновидность информации. Но СМИ — это не сама информация, а форма ее периодического распространения.

Вот почему СМИ следует рассматривать как объект права, сходный с другими объектами интеллектуальной собственности и сконструированный как юридическая фикция. В случае СМИ мы имеем дело именно с юридической фикцией, поскольку в реальности существует каждый отдельный экземпляр каждого отдельного номера газеты, но не существует газеты как некоего обобщенного объекта, объемлющего как все вышедшие ранее, так и все будущие номера этого периодического издания. Более того, все прошлые и будущие выпуски одной и той же газеты объединяются не чем иным, как названием данного СМИ. Постоянство названия особо подчер-

кивается в содержащихся в ст. 2 Закона о СМИ определениях понятий «периодическое печатное издание» и «радио- и телепрограмма». Отсюда вытекает связь СМИ как объекта права с таким самостоятельным объектом права, как средства индивидуализации юридического лица, его продукции, выполняемых услуг или работ.

Однако средство массовой информации не тождественно средству индивидуализации, т.е. своему названию, поскольку СМИ включает в себя весь тот объем исключительных прав, которые связаны с его содержанием, облеченным в определенную форму и являющимся результатом интеллектуальной деятельности редакции.

Вот почему наиболее адекватным правовой природе СМИ представляется определение средства массовой информации как результата интеллектуальной деятельности, имеющего название в качестве средства индивидуализации и форму периодического печатного издания, радио-, теле- видеопрограммы, кинохроникальной программы или иную форму периодического распространения массовой информации.

Отсюда следует, что содержащуюся в ст. 1 Закона о СМИ норму о владении, пользовании и распоряжении средствами массовой информации следует понимать как владение, пользование и распоряжение исключительными правами на СМИ. Одновременно могут существовать и вещные права, например на имущество редакции.

Специфичность средства массовой информации как объекта права проявляется, помимо прочего, в том, что исключительные права на него могут не быть связаны с правом собственности на организацию, осуществляющую выпуск СМИ, как на имущественный комплекс. Это особенно характерно для государственных печатных СМИ, среди которых достаточно распространена такая правовая схема, при которой, например, законодательное собрание является учредителем издания, а редакция, организованная в форме коммерческой организации, принадлежит как имущественный комплекс совершенно другому субъекту. Причем если редак-

ция организована в форме предприятия, то в состав ее имущественного комплекса, помимо прочего, входят и ее продукция, и права на обозначения, индивидуализирующие редакцию и ее продукцию.

Название СМИ, товарный знак, фирменное наименование

Право на название является едва ли не более значимым, чем право на имущество редакции. С названием связаны имидж издания, его рейтинг, круг постоянных авторов, читателей, рекламодателей и партнеров, а также права на денежные средства, собранные в ходе подписки, и соответствующие обязательства перед подписчиками.

Как известно, ст. 20 Закона о СМИ обязывает решать вопрос о передаче и сохранении права на название в уставе редакции. Казалось бы, широта выбора здесь безгранична. Однако не нужно забывать, что исключительные права на средства индивидуализации продукции входят в имущественный комплекс организации, осуществляющей выпуск СМИ, как нематериальные активы. И никто не вправе произвольно отобрать эти права. Правда, наименования СМИ не тождественны таким более традиционным видам средств индивидуализации, как товарные знаки и фирменные наименования. Причем невозможно требовать, чтобы наименование СМИ было защищено товарным знаком или совпадало с фирменным наименованием организации, осуществляющей его выпуск.

Отличие наименования СМИ от словесного товарного знака состоит, во-первых, в том, что продукция СМИ совсем не обязательно является товаром. Средства индивидуализации здесь нужны прежде всего для того, чтобы различать не товары, а источники информации и мнений, направления общественной мысли и практики.

Правовая категория наименования СМИ имеет некоторые черты сходства и различия с правовой категорией фирменного наименования. Хотя в ГК РФ такой объект исключительных прав, как фирменное наименование, упоминается неоднократно, однако ввиду отсутствия специального феде-

рального закона отдельные вопросы по сей день регулируются Положением о фирме, утвержденным постановлением ЦИК СССР и СНК СССР от 22 июня 1927 г.

Гражданский кодекс однозначно связывает фирменное наименование только с коммерческими юридическими лицами и гражданами, зарегистрированными в качестве индивидуальных предпринимателей. Однако, как отмечалось выше, свобода массовой информации относится не к экономическим, а к гражданским свободам. Вот почему гражданину, вознамерившемуся учредить СМИ или взять на себя функции редакции СМИ, совсем не обязательно учреждать коммерческую организацию или регистрироваться в качестве индивидуального предпринимателя, если его деятельность, конечно, не имеет целью извлечение прибыли.

В правовой науке выделяют институт «право массовой информации». Субъект права массовой информации — учредитель, редакция, издатель, распространитель и собственник имущества редакции.

В настоящее время выделяют несколько видов средств массовой информации: традиционные, к ним относятся телерадиовещание, периодические печатные издания; традиционные средства массовой информации, интегрированные в сетевые, т.е. периодические печатные издания в электронном виде, телерадиоканалы, имеющие свой сайт в Интернете, и т.д.; собственно сетевые СМИ, т.е. рожденные в сети Интернет.

2. Правовой статус средств массовой информации

Правовой статус — категория комплексная, интеграционная, отражающая взаимоотношения личности и общества, гражданина и государства, индивида и коллектива, другие социальные связи[1].

Категория административно-правового статуса СМИ призвана отразить юридическое опосредование их факти-

[1] Теория государства и права: Курс лекций / Под ред. Н.И. Матузова и А.В. Малько. — М., 1997.

ческого положения. Его структура может быть представлена как совокупность следующих основных элементов: правовое состояние, правосубъектность, законные права и обязанности, гарантии их реализации. При этом мы имеем в виду, что юридический статус не сводится к содержанию соответствующих правовых норм и представляет собой не только формально-нормативную предпосылку включения субъекта права в конкретные правоотношения, но и «своеобразную эманацию этих отношений, прав и обязанностей их участников»[1].

Элементы правового статуса "СМИ включают в себя:

1) обязательную государственную регистрацию;

2) лицензирование (TV и радиовещания);

3) порядок выпуска средств массовой информации;

4) обязательное наличие устава редакции и устава юридического лица;

5) обеспечение государством редакционной самостоятельности;

6) экономическую государственную поддержку;

7) регулирование рекламы в средствах массовой информации.

Рассмотрим каждый элемент правового статуса СМИ подробнее.

1. Обязательная государственная регистрация имеет не разрешительный, а уведомительный характер; происходит в региональном отделении Министерства культуры и массовых коммуникаций.

Редакция средства массовой информации осуществляет свою деятельность после его регистрации. Из этого положения имеется ряд исключений. Не требуется регистрация:

— средств массовой информации, учреждаемых органами государственной власти и органами местного самоуправ-

[1] *Явич Л.С.* Сущность права. Социально-философское понимание генезиса, развития и функционирования юридической формы общественных отношений. — Л., 1985. С. 63.

ления исключительно для издания официальных сообщений и материалов, нормативных и иных актов;

— периодических печатных изданий тиражом менее одной тысячи экземпляров;

— радио- и телепрограмм, распространяемых по кабельным сетям, ограниченным помещением и территорией одного государственного учреждения, учебного заведения или промышленного предприятия либо имеющим не более десяти абонентов;

— аудио- и видеопрограмм, распространяемых в записи тиражом не более десяти экземпляров.

Редакция имеет право подать заявку в государственный орган, организацию, учреждение, орган общественного объединения на аккредитацию при них своих журналистов.

Как правило, все периодические печатные издания тиражом более одной тысячи экземпляров регистрируются в Национальном агентстве ISSN в Российской книжной палате с присвоением соответствующего международного стандартного номера (ISSN). На периодические печатные издания полностью распространяется положение о предоставлении обязательных экземпляров изданий (ФЗ «Об обязательном экземпляре документов»).

Правила учреждения и регистрации СМИ, необходимые для оформления юридического факта рождения нового СМИ и признания за ним правового состояния средства массовой информации, несколько отличаются от правил, касающихся создания юридических лиц и закрепленных в Гражданском кодексе РФ. Это связано с тем, что, во-первых, согласно ч. 3 ст. 2 под средством массовой информации понимается «форма периодического распространения массовой информации», которая, естественно, не может быть юридическим лицом. Во-вторых, как это предусмотрено ч. 2 ст. 19, редакция может быть юридическим лицом, но может им и не быть, если, например, она является внутренним подразделением какого-либо предприятия, организации или учреждения либо вообще в этом качестве выступает частное физическое лицо.

Если же редакция организуется в форме юридического лица, то она подлежит регистрации по общим правилам ГК РФ, но только после регистрации СМИ. Это вытекает из требований ч. 1 ст. 8 Закона о СМИ, где устанавливается, что редакция СМИ «осуществляет свою деятельность после его регистрации».

Что касается процесса учреждения СМИ, то здесь необходимо отметить следующее.

Во-первых, учредителем СМИ может быть любой совершеннолетний, т.е. достигший 18-летнего возраста гражданин РФ, за исключением отбывающих наказание в местах лишения свободы по приговору суда и душевнобольных, признанных судом недееспособными. На лиц без гражданства (апатридов), постоянно проживающих на территории РФ, распространяется национальный режим, и, таким образом, они приравниваются к российским гражданам. Иностранцы, напротив, этого права лишены, однако ничто не мешает им законным путем учредить российское юридическое лицо или приобрести предприятие, которое выступит в качестве учредителя СМИ.

Во-вторых, правом на учреждение СМИ обладают объединения граждан: общественные, религиозные, трудовые и журналистские коллективы и т.д. При этом им вовсе не обязательно являться юридическими лицами. Так, согласно ч. 4 ст. 3 и ч. 1 ст. 21 Федерального закона от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях» создаваемые гражданами общественные объединения могут «функционировать без государственной регистрации и приобретения прав юридического лица». Статья 27 данного Закона, признавая за общественными объединениями право учреждать СМИ, никак не увязывает это правомочие с фактом наличия их государственной регистрации.

В-третьих, учреждать СМИ вправе предприятия, учреждения, организации (корпорации, банки, клубы, библиотеки, университеты, научные центры и т.д.). Единственное существующее здесь ограничение — деятельность таких

предприятий, учреждений и организаций не должна быть запрещена в соответствии с законом. Иными словами, например, общественная организация, в отношении которой имеется вступившее в законную силу решение о ликвидации, утрачивает право быть учредителем СМИ. Причем в этом случае ее права и обязанности в полном объеме переходят к редакции, если иное не предусмотрено уставом редакции (ч. 4 ст. 18).

Наконец, в-четвертых, учредителями СМИ могут быть государственные органы. Разумеется, это относится как к органам государственной власти, так и к органам местного самоуправления.

Учредителей может быть несколько. В этом случае каждый из них считается соучредителем, и только совместно они могут выступать в качестве учредителя. Согласно ч. 1 ст. 22 Закона о СМИ соучредители заключают договор, в котором определяются их взаимные права, обязанности, ответственность, порядок, условия и юридические последствия изменения состава соучредителей, процедура разрешения споров между ними. Хотя закон текстуально не обязывает соучредителей заключить договор, но, предопределяя его содержание, делает его необходимым. Если же учреждается не только СМИ, но и редакция, обладающая правами юридического лица, то учредительный договор становится обязательным в силу требований ст. 52 ГК РФ.

Следует обратить внимание также на ст. 17 Закона о СМИ, где устанавливается, что права и обязанности учредителя возникают с момента регистрации средства массовой информации. Соответственно, появление нового соучредителя допускается лишь при условии перерегистрации СМИ (ч. 1 ст. 11). Следовательно, юридически некорректной будет, например, формула, использованная в решении Смоленской областной Думы «О журнале "Край Смоленский"» от 26 апреля 1994 г.: «Считать областную Думу соучредителем журнала». На самом же деле Дума может стать соучредителем лишь с согласия других соучредителей и редакции и только после пе-

перегистрации СМИ, а не с момента принятия Думой данного решения.

Заявление о регистрации подается в письменной форме. В нем указываются, в частности, сведения об учредителе, обусловленные требованием Закона. Например, если учредитель — физическое лицо, необходимо сообщить о наличии у него гражданства РФ, достижении 18-летнего возраста и отсутствии ограничений дееспособности, что легко подтвердить с помощью паспорта. Кроме того, обязательно должно быть указано, что учредитель постоянно проживает в РФ: в противном случае СМИ будет считаться зарубежным. Однако показывать паспорт вовсе не обязательно, поскольку регистрирующим органам запрещено предъявлять при регистрации какие-либо дополнительные требования, не предусмотренные законом о СМИ.

В заявлении должны быть указаны также: название регистрируемого СМИ; язык, на котором оно будет выходить; адрес редакции; форма периодического распространения массовой информации; примерная тематика и специализация СМИ. Если СМИ намерено специализироваться на сообщениях и материалах для детей и подростков, инвалидов, а также образовательного и культурно-просветительского назначения, то согласно ч. 1 ст. 14 с него причитается пониженный регистрационный сбор. Если же СМИ будет специализироваться на сообщениях и материалах рекламного и эротического характера, то его ожидает не только повышенный регистрационный сбор, но и согласно ст. 37 особые условия распространения своей продукции.

Закон о СМИ обязывает учредителя сообщить в заявлении об источниках финансирования, предполагаемых периодичности выпуска и максимальном объеме средства массовой информации. Содержащийся в ч. 1 ст. 13 Закона о СМИ перечень оснований для отказа в регистрации является исчерпывающим и не допускает расширительного толкования. Отказ в регистрации возможен, во-первых, если заявление подано от имени субъекта, не обладающего правом на учреж-

дение СМИ, например иностранцем или лицом без гражданства, не проживающего постоянно в РФ. Во-вторых, если указанные в заявлении сведения не соответствуют действительности. Для закона не имеет значения, на какой вопрос заявитель дал неверный ответ, по какой причине, умышленно или случайно. В то же время следует еще раз подчеркнуть, что на большинство вопросов заявитель может и должен отвечать в предположительном ключе. Однако если в заявлении указано, например, что газета будет выходить на латыни тиражом 1 млн экземпляров, иметь рекламный характер и распространяться в районах Крайнего Севера, то налицо веские основания для сомнений, а значит, для тщательной проверки.

В-третьих, отказ возможен, если название, примерная тематика или специализация СМИ представляют собой злоупотребление свободой массовой информации в смысле ч. 1 ст. 4. Однако не известно ни одного случая, чтобы в заявлении о регистрации указывались такие цели, как совершение уголовно наказуемых деяний, призыв к захвату власти, разжигание национальной, классовой, социальной, религиозной нетерпимости и розни или пропаганда войны.

Наконец, в-четвертых, отказ возможен, если регистрирующим органом ранее зарегистрировано СМИ с тем же названием и той же формой распространения массовой информации. Цель данного запрета состоит в том, чтобы не создавать путаницу на рынке массовой информации. Однако запрет на повторяемость названий является не абсолютным, а относительным. Так, если в Мурманской области зарегистрирована газета «Имярек», то это не мешает использовать данное название при учреждении в той же области журнала или телепрограммы (при этом, однако, следует помнить о правилах, защищающих товарные знаки как интеллектуальную собственность). Можно учредить и одноименную газету, но только в другом регионе. Но если «Имярек» зарегистрирован федеральным регистрирующим органом, то путь к созданию одноименной газеты где бы то ни было закрыт.

Обращают на себя внимание тенденции, сложившиеся в регистрации аудиовизуальных СМИ. Примечательно, что телепрограммы регистрируются чаще, чем радиопрограммы, хотя их производство значительно дороже. Видимо, не последнюю роль здесь играют такие особенности телевидения, как относительно более высокий потенциал воздействия на аудиторию и повышенная привлекательность для рекламодателя. Кроме того, нужно учитывать и достаточно широко распространенную практику создания производящих, но не имеющих собственного вещания телекомпаний (например, «Вид», «Авторское телевидение» и т.д.). В сфере радио такая организационная схема пока не получила развития, хотя для нее есть очевидная ниша на информационном рынке.

Особо нужно отметить резкое увеличение числа сетевых СМИ, т.е. тех средств массовой информации, которые распространяют свою продукцию в сети «Интернет». Известно, что пока не найдено надежных юридических критериев, позволяющих однозначно квалифицировать определенные информационные ресурсы в Интернете именно как сетевые СМИ, не касаясь так называемых «домашних страниц», «досок объявлений» и т.п. В этой ситуации регистрация сетевых СМИ может быть только добровольной, основанной на привлекательности статуса средства массовой информации.

В целом российский рынок СМИ имеет тенденцию к достаточно резкому расширению. Причем темпы роста численности региональных и местных средств массовой информации значительно превышают аналогичные показатели на федеральном уровне. Такое явление представляется вполне естественным, если учесть размеры страны, а следовательно, дороговизну доставки продукции СМИ не только в отдаленные, но и в относительно близкие регионы. Одним из вариантов решения проблемы в сфере печатных СМИ является использование достаточно дорогостоящей системы децентрализованного печатания, созданной еще в советское время для обеспечения своевременной доставки центральных газет ЦК КПСС в день выхода. Другой вариант — передача газетных полос в типографии по Интернету.

Однако для аудиовизуальных СМИ пока довольно затруднительно и нерентабельно вещание, особенно телевизионное, в Интернете. Вот почему развитие этого вида средств массовой информации идет прежде всего по пути создания на местах телекомпаний и радиостанций, объединенных с электронными СМИ, выходящими в столице, с помощью сетевых соглашений.

2. Лицензирование.

Для аудиовизуальных СМИ регистрация является необходимым, но, как правило, вовсе не достаточным условием для начала деятельности по производству и выпуску средства массовой информации. Поскольку эта категория СМИ использует для передачи информации естественным образом ограниченный ресурс (эфирные частоты), постольку российское государство по примеру многих других цивилизованных стран ввело систему лицензирования в этой сфере.

Данная модель действует и поныне благодаря постановлению Правительства РФ «О лицензировании телевизионного вещания, радиовещания и деятельности по связи в области телевизионного и радиовещания в Российской Федерации» от 7 декабря 1994 г. № 1359. Правда, партнером Госкомтелекома является теперь Федеральная служба по телевидению и радиовещанию (ФСТР). Следует подчеркнуть, что при создании системы лицензирования в нее был вкраплен важный демократический элемент, призванный обеспечить разумное, справедливое и гласное распределение частот, — Комиссия по вещанию. Этот межведомственный орган включал не только представителей заинтересованных министерств и ВГТРК, но и авторитетных независимых журналистов, социологов, юристов. Поскольку лицензии могли выдаваться только на основании заключений Комиссии, постольку она сразу нажила себе много недоброжелателей.

Особого комментария заслуживает ч. 4 ст. 15 Закона «О связи». Она гласит: «Выдача лицензий на деятельность в области связи для целей телерадиовещания, а также присвоение частот, занесенных в перечень частот, исполь-

зуемых и планируемых к использованию для целей телерадиовещания, осуществляются на основе лицензии на вещание без проведения конкурса Министерством связи РФ в соответствии с законодательством РФ по заявлению физических и юридических лиц, владеющих, пользующихся и распоряжающихся средствами связи, используемыми для целей телерадиовещания, либо имеющих намерение вступить в права владения, пользования и распоряжения средствами связи, используемыми для целей телерадиовещания».

Избранная законодателем формула, с одной стороны, закрепляет существующую практику парных лицензий на одну и ту же частоту. Причем приоритет закрепляется за лицензией на вещание. Именно она составляет основу для выдачи лицензии на деятельность в области связи для целей телерадиовещания. Не вполне ясен, правда, в этом контексте смысл формулы «без проведения конкурса». Видимо, законодатель желал подчеркнуть, что Минсвязи обязано выдать требуемую лицензию на безальтернативной основе именно тому заявителю, который указан в лицензии на вещание.

Сопоставив эти правила с содержащимися в ст. 31 Закона о СМИ, приходим к заключению, что лицензия на вещание касается лишь ее держателя, поскольку именно ему предоставляется право, используя технические средства эфирного, проводного или кабельного телерадиовещания, в том числе находящиеся в его собственности, осуществлять распространение продукции аудиовизуальных средств массовой информации, зарегистрированных в соответствии с Законом. Отсюда следует, что лицензия на деятельность в области связи полагается тому, кто имеет лицензию на вещание.

С другой стороны, заявителями признаются лишь физические и юридические лица, в чьей собственности (ст. 209 ГК РФ), хозяйственном ведении (ст. 294 ГК РФ) или оперативном управлении (ст. 296 ГК РФ) находятся или предположитель-

но будут находиться средства связи, используемые для телерадиовещания. Иными словами, лицензию на деятельность в области связи может получить лишь тот, кому принадлежит или будет принадлежать передатчик и кто выступает в качестве оператора связи. Упоминание о лицах, «имеющих намерение вступить в права владения, пользования и распоряжения средствами связи», может рассматриваться в данном контексте как предусмотрительно оставленная лазейка для тех телерадиокомпаний, которые не имеют собственных передатчиков, но готовы их приобрести.

Таким образом, сохраняя систему парных лицензий, Федеральный закон о связи объективно способствует их концентрации в руках операторов связи. Это особенно больно ударяет по интересам независимых вещателей, не располагающих крупными финансовыми ресурсами. Что же касается общероссийских и региональных государственных телерадиокомпаний (ГТРК), то в большинстве случаев, поглотив ранее самостоятельные радиотелевизионные центры (РТЦ) со всеми студийными комплексами и прочей материально-технической базой, они до недавних пор не могли проделать аналогичную операцию с радиотелевизионными передающими центрами (РТПЦ), входящими в систему Минсвязи.

Аннулирование лицензии производится при систематическом нарушении законодательства о порядке лицензирования.

3. Порядок выпуска средств массовой информации (внутренние и внешние отношения).

Правоотношения, которые складываются в сфере массовой информации, можно поделить на внутренние и внешние. Первые затрагивают вопросы внутренней организации СМИ и включают отношения между основными действующими лицами: учредителем, редакцией, издателем, распространителем и собственником. Другая группа включает правоотношения, возникающие в связи с деятельностью СМИ, между вышеперечисленными субъектами и третьими лицами. Это

могут быть и органы государственной власти, и местного самоуправления.

Внутренние правоотношения касаются внутриредакционного менеджмента, формирования органов управления, границ профессиональной самостоятельности журналистов, вопросов собственности. Эти отношения особенно сложны потому, что здесь переплетаются право собственности на имущество и исключительные права на результаты интеллектуальной деятельности (интеллектуальную собственность) — авторское право на периодическое издание в целом и право на наименование, товарный знак и т.д.

Закон СССР «О печати и других средствах массовой информации» установил, что редакция СМИ является юридическим лицом, действующим на основании своего устава. В Законе о СМИ редакция определяется как организация, учреждение, предприятие либо гражданин, объединение граждан, осуществляющие производство и выпуск средства массовой информации.

Путаница, порожденная союзным Законом, создавала многочисленные проблемы уже потому, что сам по себе факт регистрации средства массовой информации не мог породить статус юридического лица у редакции. Редакция становилась юридическим лицом только в том случае, если она обладала предусмотренными законом признаками, перечень которых на момент действия союзного Закона о печати определялся прежде всего статьями Гражданского кодекса.

Учреждение СМИ и учреждение редакции — по сути, различные правовые явления. Появление в Гражданском кодексе нормы, устанавливающей, что юридическое лицо считается созданным с момента его государственной регистрации, резко изменило ситуацию. Закон о СМИ говорит о статусе юридического лица применительно к редакции, а не к самому средству массовой информации, которое является всего лишь формой периодического распространения массовой информации.

Имущественные отношения между учредителем, редакцией, издателем и собственником определяются в договоре.

Этим же документом определяются и производственные, финансовые отношения между ними. Здесь устанавливается порядок выделения и использования средств на содержание редакции, распределения прибыли, образования фондов и возмещения убытков, обеспечения надлежащих производственных и социально-бытовых условий труда сотрудников редакции.

Основным условием, которое является определяющим при составлении договора, является организационно-правовая форма существования редакции. Выбор той или иной организационно-правовой формы юридического лица важен потому, что каждая из форм имеет свои плюсы и минусы. Так, если редакция создается в форме акционерного общества, возникает необходимость тем или иным образом согласовывать правовые нормы, устанавливающие, что высшим органом управления в этом случае является общее собрание его акционеров (что требуется в соответствии с Гражданским кодексом), а с другой —- что редакцией руководит главный редактор (Закон о СМИ). Единственная возможность избежать противоречий — это разделить функции принятия финансово-хозяйственных решений и определения редакционной политики. Общее собрание акционеров, совет директоров и генеральный директор будут осуществлять все функции, которые за ними закреплены в соответствии с законодательством об акционерных обществах. В то же время главный редактор будет осуществлять все функции, которые предусматривает Закон о СМИ. Есть много примеров, когда соучредителями СМИ являются государственные и муниципальные органы разного уровня либо субъекты различных форм собственности. Например, газета, учрежденная областным управлением печати и районной администрацией. Редакция такой газеты может быть организована либо в форме государственного (областного), либо муниципального учреждения (унитарного предприятия). Но смешанного государственно-муниципального учреждения или предприятия быть не может, так как субъекты права собственности разные. В подобном случае со-

учредителям достаточно заключить между собой договор, в котором определить взаимные права, обязанности, ответственность, порядок, условия и юридические последствия изменения состава учредителей, процедуру разрешения споров между ними. При этом один из них должен принять на себя функции учредителя редакции как учреждения или предприятия. Этот орган закрепляет за редакцией то имущество, которым ему будет поручено распоряжаться, например оборудование. Другую часть необходимого имущества — служебные помещения — редакция получает по договору аренды от второго соучредителя газеты.

Другой стороной во внутренних правоотношениях является издатель. Этим статусом наделяется издательство, иное учреждение или коммерческая организация, осуществляющие материально-техническое обеспечение производства продукции средства массовой информации. К ним приравниваются юридические лица и граждане, для которых эта деятельность не является основной либо не служит главным источником дохода. Под издательством понимаются предприятия, структурные подразделения предприятий, организаций, учреждений, осуществляющие издательскую деятельность, т.е. подготовку, выпуск печатных изданий любого вида.

4. Обязательное наличие устава редакции и устава юридического лица. Устав редакции — фактический договор между редакцией и учредителем.

Поскольку программное заявление по сути является договором между владельцем СМИ и журналистами, заключаемым в том числе в пользу третьего лица — аудитории, постольку он вполне укладывается в принцип свободы договора. Ссылка на программное заявление в трудовых контрактах с главным редактором и нанимаемыми им журналистами (главный редактор должен быть связующим звеном между владельцем СМИ и творческим коллективом) превращает его в юридически обязательный документ.

В действующем Законе о СМИ институт программного заявления, к сожалению, не предусмотрен, хотя здесь закреп-

лен принцип профессиональной самостоятельности редакций и журналистов. Этот принцип на практике подвергается постоянной эрозии из-за того, что сложившиеся в этой сфере теневые экономические отношения не способствуют установлению цивилизованных отношений между редакциями и владельцами. Широко распространенная практика «двойной зарплаты» — через кассу в рублях и через конверты с долларами — не позволяет поставить эти отношения на правовую почву. Причем обе стороны вполне довольны такой практикой: сотрудники получают сравнительно приличную оплату за свой труд, а владельцы экономят на невыплаченных налогах. Может быть, именно этим объясняется та очевидная недосказанность, которая стала в последние годы характерной чертой внутримедийных конфликтов. Поэтому достижение прозрачности СМИ является, помимо прочего, необходимым условием редакционной самостоятельности.

По сути редакционный устав является договором между этими субъектами. Как справедливо заметила Судебная палата по информационным спорам при Президенте РФ, в пользу договорного характера редакционного устава свидетельствуют три момента. Во-первых, ч. 3 ст. 20 Закона о СМИ допускает замену устава договором, если редакция только создана или состоит менее чем из десяти человек. Во-вторых, устав по необходимости должен в равной степени соответствовать интересам и редакции, и учредителя, поскольку принимается на общем собрании коллектива журналистов — штатных сотрудников редакции (простым большинством голосов при наличии не менее двух третей его состава) и утверждается учредителем. В-третьих, именно в уставе должны быть определены взаимные права и обязанности учредителя и редакции[1].

[1] См.: Экспертное заключение Судебной палаты по информационным спорам при Президенте РФ от 31 марта 2000 г. № 23 «О некоторых вопросах перерегистрации средств массовой информации в связи со сменой учредителя и необходимости внесения соответствующих изменений в устав СМИ» // Законодательство и практика средств массовой информации. 2000. № 4.

Однако устав не является собственно договором, поскольку журналистский коллектив может не быть юридическим лицом, хотя не следует забывать, что журналистский коллектив может самоорганизоваться, например в автономную некоммерческую организацию, ЗАО или производственный кооператив, с которым учредитель СМИ может вступить уже в чисто договорные отношения. Естественно, нет никаких правовых оснований для того, чтобы представлять устав созданного самими журналистами ЗАО на утверждение учредителя СМИ, однако договор между ними должен соответствовать требованиям Закона о СМИ, предъявляемым к редакционным уставам.

Кроме того, журналистский коллектив как сторона в отношениях с учредителем по поводу устава редакции может выступать в качестве группы граждан либо общественного объединения без образования юридического лица.

5. Обеспечение государством редакционной самостоятельности.

Как показывает анализ практики, существующие в Законе о СМИ возможности защитить редакционную самостоятельность, как правило, используются лишь в малой степени или не используются вообще. Как отмечалось выше, во многих редакциях до сих пор отсутствуют редакционные уставы. Строго говоря, от отсутствия этого важнейшего юридического документа должны в первую очередь страдать интересы учредителя СМИ, так как он не вправе ни назначить главного редактора, ни уволить его, ни приостановить, ни прекратить выпуск СМИ.

Более того, ч. 3 ст. 18 Закона о СМИ устанавливает: «Учредитель не вправе вмешиваться в деятельность средства массовой информации за исключением случаев, предусмотренных настоящим Законом, уставом редакции, договором между учредителем и редакцией (главным редактором)». Следовательно, в отсутствие устава учредитель не вправе вмешиваться в их деятельность. Однако практически этот запрет никого не останавливает, и в случае возникновения судебного

или публичного спора учредитель старается доказать, что в деятельность СМИ он не вмешивался, а лишь решал отнесенные к его компетенции предпринимательским правом вопросы деятельности редакции как коммерческой (некоммерческой) организации.

Возможен, например, такой сценарий, когда владелец контрольного пакета акций и генеральный директор издательства пытаются доказать, например, что уволили не главного редактора газеты, а просто сотрудника издательства, должность которого лишь называлась «главный редактор газеты». На самом же деле по такой логике учредителя речь вообще не может идти об увольнении главного редактора, поскольку ввиду отсутствия устава редакции главный редактор просто не мог быть назначен. Все это доказывает, что редакционный устав лучше иметь, чем не иметь.

Стремясь облегчить задачу журналистских коллективов и учредителей СМИ, Госкомитет России по печати, СПИС и Союз журналистов России разработали модельные уставы для редакций государственных и муниципальных средств массовой информации. Эти уставы предусматривают, в частности, что основной целью деятельности редакции является производство и выпуск газеты в соответствии с примерной тематикой, заявленной учредителем (соучредителями) газеты при ее регистрации как средства массовой информации. Тем самым учредителю дается возможность определить именно стратегическую линию СМИ.

В то же время в модельных уставах закрепляется право редакции по своему усмотрению публиковать материалы по любым вопросам, относящимся к заявленной при регистрации примерной тематике газеты. В своих публикациях по текущим экономическим, политическим, социальным и религиозным вопросам редакция должна соблюдать надлежащую беспристрастность и уважение к правде, в равной мере представлять противоположные точки зрения, избегая тенденциозности. Мнения и сообщения о фактах должны быть четко разграничены. Учредитель же обязан обеспечивать профес-

сиональную и творческую самостоятельность редакции, защищать профессиональные интересы журналистов редакции как лиц, выполняющих общественный долг.

В модельных уставах предлагаются оптимальные механизмы приостановления и прекращения деятельности СМИ. Так, учредителю дается право приостановить с согласия коллектива журналистов выпуск газеты на срок до трех месяцев в случае длительного отсутствия средств на ее производство и выпуск при условии сохранения за работниками редакции существенных условий оплаты труда и наличия на данной территории других региональных (местных) периодических печатных изданий (за исключением рекламных и эротических). Он может также прекратить деятельность газеты, но тоже только с согласия коллектива журналистов и исключительно в случае, если тираж газеты на протяжении длительного времени снижается до уровня менее одного процента населения, при условии наличия других региональных периодических печатных изданий, устойчиво имеющих более высокий тираж. Разумеется, для принятия решения о прекращении выпуска газеты могут быть и другие основания, но важно, чтобы они не противоречили закону и были прямо указаны в редакционном уставе.

Определенную роль в обеспечении редакционной самостоятельности может сыграть редакционный совет. В модельных уставах он определен как коллегиальный консультативный орган управления. Он формируется совместно учредителем и редакцией на паритетных началах из числа наиболее авторитетных людей, проживающих на территории распространения газеты. В случае спора между учредителем и редакцией по вопросам, затрагивающим общественные интересы, редакционный совет выносит свое суждение, которое является обязательным для рассмотрения сторонами спора[1].

[1] Профессиональная самостоятельность редакции. Как ее обеспечить? // Сборник материалов расширенного заседания секретариата Союза журналистов России. — М., 1999.

Разумеется, с помощью модельных уставов можно решить лишь малую часть проблем. Необходимо законодательно укрепить гарантии независимости редакционной политики от владельцев и иных лиц, контролирующих деятельность СМИ. При этом целесообразно использовать опыт стран с устойчивыми демократическими традициями и правовыми системами.

В Испании, например, существуют два способа защиты редакционной независимости: основанный на саморегуляции и установленный законодательством. Первый способ реализуется через заключение соглашений между корпорациями журналистов и владельцев СМИ, а также через собственные механизмы саморегуляции внутри журналистских профсоюзов, связанные прежде всего с применением правил профессиональной этики (Comision de la Federation de Asociaciones de Prensa en Espana и Consejo de Prensa del Colegio de Periodistas de Catalunya). Второй способ, опирающийся на конституционные нормы, позволяет испанским журналистам прекращать профессиональные отношения и требовать компенсации, если предприятие СМИ, с которым они сотрудничают, радикальным образом меняет свою редакционную политику. Однако у этого конституционного положения ограниченная сфера применения. Вплоть до 1997 г. законодательная власть не занималась развитием этого положения, и до сих пор этот закон не оказывает большого влияния на политику средств массовой информации.

Во Франции, напротив, аналогичный механизм защиты независимости журналиста существует давно и действует вполне эффективно. Так, согласно ст. 7617 Трудового кодекса журналист вправе претендовать на получение компенсации в размере до 15 месячных зарплат в случае, если он расторгает контракт с предприятием по изданию периодики по следующим причинам: а) закрытие газеты или журнала; б) прекращение выпуска издания вне зависимости от его причины; в) значительные изменения в характере или направлении издания, если эти изменения создают для журналиста ситуа-

цию, наносящую ущерб его чести, репутации либо моральным интересам. Причем последняя причина дает право журналисту не соблюдать установленный Кодексом срок предварительного уведомления работодателя о расторжении контракта.

Как показывает зарубежный опыт, становление корпоративной солидарности журналистов может сыграть огромную роль в укоренении представлений о принципиальном отличии бизнеса в сфере массовой информации от журналистики как свободной профессии и разновидности публичной службы.

6. Экономическая государственная поддержка (налоговые льготы, государственные дотации при определенных условиях).

Выстроенная в 90-х гг. XX в. система государственной поддержки СМИ исходила из того, что те средства массовой информации, которые по объективным причинам не могли компенсировать свои расходы через размещение рекламы, продажу тиража и т.д., имели право на определенные льготы. Однако законодатель не сумел создать действенную систему дифференциации льгот, ограничившись формулой «всем, кроме...».

Согласно Федеральному закону от 5 августа 2000 г. «О введении в действие части 2 Налогового кодекса»[1] с 1 января 2002 г. налоговые льготы, установленные в подп. 21 п. 3 ст. 149 Налогового кодекса РФ, были отменены.

До 31 декабря 1998 г. федеральное законодательство освобождало от таможенной пошлины и сборов, связанных с импортом и экспортом, все периодические печатные издания, ввозимые на таможенную территорию РФ и вывозимые с нее редакциями СМИ и издательствами. От пошлины освобождались также ввозимые редакциями, издательствами, полиграфическими предприятиями и телерадиокомпаниями бумага и технологические материалы, аудио- и видеоинформация,

[1] СЗ РФ. 2000. № 32. Ст. 3340.

инженерное оборудование, используемое для производства продукции СМИ.

Законом от 22 августа 2004 г. № 122-ФЗ[1] «О внесении изменений в законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с принятием федеральных законов "О внесении изменений и дополнений в Федеральный закон "Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации" и "Об общих принципах организации местного самоуправления в Российской Федерации"» указанные льготы были отменены. Ныне действуют лишь те льготы, которые вытекают из присоединения России с апреля 1995 г. к Соглашению о ввозе материалов образовательного, научного и культурного характера от 17 июня 1950 г. (Флорентийское соглашение)[2].

Кроме того, редакциям, издательствам и телерадиокомпаниям (ТРК) дано право пользоваться услугами почтовой, телеграфной и телефонной связи по тарифам, предусмотренным для бюджетных организаций. Причем согласно положениям главы IV Закона о связи государственное регулирование тарифов возможно независимо от форм собственности на сети и средства связи.

Еще одно средство финансовой поддержки СМИ успешно действовало на территории России — система государственных дотаций, впервые введенная постановлением Верховного Совета РФ от 17 июля 1992 г. «Об экономической поддержке и правовом обеспечении деятельности средств массовой информации». Дотации устанавливались Мининформпечатью РФ под контролем депутатской комиссии пропорционально результатам подписки и тиражу периодических печатных изданий. От получателей дотаций никто не требовал политической лояльности, в результате чего реципиентами становились

[1] СЗ РФ. 2004. № 35. Ст. 3607.

[2] Бюллетень международных договоров. 1999. № 3.

не только оппозиционные издания, но даже те, которые именовали власть не иначе как оккупационной[1]. Подобная система развращала редакции прежде всего в экономическом плане, приучая их жить «с протянутой рукой».

Конечно, трудно в одночасье отказаться от системы дотаций, позволяющей держать дотируемые издания в зависимом положении, и опираться исключительно на рыночные механизмы. Фактически именно на спасение местных периодических изданий был нацелен Федеральный закон от 24 ноября 1995 г. № 177-ФЗ «Об экономической поддержке районных (городских) газет»[2], утративший силу после введения в действие Закона от 22 августа 2004 г. № 122-ФЗ.

Закон имел целью «обеспечение конституционного права граждан на получение своевременной и объективной информации, информационного обеспечения реформы местного самоуправления и активного участия граждан в местном самоуправлении».

В настоящее время система государственной поддержки СМИ практически разрушена.

Поэтому особенно важно законодательно закрепить основные принципы государственной поддержки средств массовой информации как системы экономических, правовых, организационных, организационно-технических и иных мер, устанавливаемых и осуществляемых государством в целях обеспечения политического, идеологического и культурного многообразия, свободы мысли и слова, независимости средств массовой информации, а также права граждан свободно искать, получать, передавать, производить и распространять информацию.

К принципам государственной поддержки СМИ следовало бы отнести:

а) справедливость и равенство при распределении средств и предоставлении льгот;

[1] Например, газета «Сельская жизнь» во втором квартале 1993 г. получила 152 млн руб., «Рабочая трибуна» — 41 млн руб., «Советская Россия» — 69 млн руб. («Известия», 26 августа 1993 г.).

[2] СЗ РФ. 1995. № 48. Ст. 4559; 2000. № 2. Ст. 136.

б) открытость осуществления государственной поддержки;

в) учет специализации средств массовой информации;

г) необходимость обеспечения политического и идеологического многообразия;

д) недопустимость использования мер поддержки для вмешательства органов государственной власти, органов местного самоуправления, учрежденных ими организаций, должностных лиц в профессиональную деятельность редакций.

Кроме того, важно предусмотреть, что льготы, дотации и привилегии не могут предоставляться:

а) в индивидуальном порядке;

б) организациям, осуществляющим выпуск средств массовой информации рекламного или эротического характера;

в) организациям, осуществляющим выпуск средств массовой информации, с иностранным участием в уставном капитале;

г) организациям, осуществляющим выпуск содержащих рекламу периодических печатных изданий, распространяемых бесплатно или по монопольно низким ценам;

д) организациям, осуществляющим выпуск средств массовой информации, — в порядке компенсации за оказание информационных услуг органам государственной власти или органам местного самоуправления;

е) организациям, осуществляющим материально-техническое обеспечение производства и распространения продукции средств массовой информации, предлагающим свои товары и услуги по монопольно высоким ценам;

ж) позднее чем за шесть месяцев до объявления выборов в органы государственной власти или органы местного самоуправления и ранее чем через шесть месяцев после объявления итогов выборов.

7. Регулирование рекламы в средствах массовой информации.

Федеральный закон о рекламе[1] регулирует отношения, возникающие в процессе производства, размещения и распространения рекламы на рынках товаров, работ, услуг РФ.

Пункт 1 ст. 18 Закона устанавливает, что при платном справочном телефонном, компьютерном и ином обслуживании реклама может предоставляться только с согласия абонента. Стоимость такой рекламы не должна включаться в стоимость запрашиваемых абонентом справок. Таким образом, несанкционируемое пользователем интернет-услуг предоставление рекламы является неправомерным.

Данное положение имеет существенное значение, тем более что рекламный бизнес в Интернете имеет больше перспективы. Так, общий доход от рекламы в Интернете в США в 2001 г. составил 5,5 млрд долл. по сравнению с 20 млн в 2000 г.[2] Реклама в режиме on-line по прогнозам специалистов в 2010 г. достигнет 20 млн долл[3].

Под объектом регулирования, говорит Закон о рекламе, понимается распространяемая в любой форме, с помощью любых средств рекламная информация (а именно — информация о физическом или юридическом лице, товарах, идеях и начинаниях), которая предназначена для неопределенного круга лиц и призвана формировать или поддерживать интерес к этим физическому, юридическому лицу, товарам, идеям и начинаниям и способствовать их реализации.

Таким образом, от других видов массовой информации рекламу отличают цели ее создания и распространения: пробудить или поддержать интерес к конкретным товарам и услугам и способствовать их реализации. Совокупность указанных признаков является необходимой для признания распространяемой информации рекламной.

---

[1] СЗ РФ. 2006. № 12. Ст. 1232.

[2] Industry Analysis: Online Advertising Down, But not Out, Broadband networking news. Feb. 12, 2002.

[3] A Sobering Look at Internet Advertising, Cable World. Dec. 3, 2001.

Одной из целей Закона является недопущение недобросовестной конкуренции с использованием рекламных трюков. Другой целью стоит защита потребителей от ненадлежащей рекламы, под которой понимаются четыре ее разновидности — недобросовестная реклама, недостоверная реклама, неэтичная реклама, заведомо ложная реклама, а также иная реклама, в которой допущены нарушения требования законодательства к ее содержанию, времени, месту и способу распространения. Для определения каждого из этих видов существует соответствующая статья в законе. Все перечисленные виды рекламы недопустимы, т.е. незаконны. Недобросовестная реклама дискредитирует тех, кто не пользуется рекламируемым товаром, она содержит некорректные сравнения с товаром конкурентов, вводит потребителей в заблуждение путем имитации формы популярной рекламы конкурентов, скрывает часть существенной для потребителей информации.

Простым примером некорректного сравнения могла бы быть такая фраза в рекламе: пепси-кола — напиток для дураков, кока-кола — напиток для умников. Если же сравнение следующее: в кока-коле меньше сахара, чем в пепси-коле, — пейте кока-колу, то это корректное сравнение. Если это правдивое утверждение, конечно. Недобросовестной рекламой считался бы слоган: только глупый человек не станет пить кока-колу.

На практике корректность сравнения доказать чрезвычайно трудно, поэтому можно сказать, что сравнительная реклама по нашему законодательству фактически не разрешается.

Наконец, под недобросовестной рекламой понимается реклама, которая использует элементы имитации другой рекламы другого товара. То есть если некий рекламодатель в ходе кампании «раскрутил» свой рекламный символ, свой музыкальный мотив, свои образы, а конкурент начинает использовать знакомые таким образом потребителю эти элементы, то это считается недобросовестной рекламой.

В свою очередь, недостоверная реклама дает потребителю не соответствующие действительности сведения. Это мо-.

гут быть сведения об условиях гарантии, об условиях бесплатной или платной доставки товара, об условиях обмена, о любых характеристиках товара — химическом составе стирального порошка, количестве сигарет в пачке, сроках распродажи, часах работы магазина, гарантийных обязательствах изготовителя, о дипломах и призах, которые якобы этот товар получил, о результатах исследований, которые никто не проводил, о лестных рекомендациях известных лиц, которые никто не давал, и т.п.

Согласно ст. 5 Закона о рекламе «в рекламе не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений, в том числе в отношении пола, расы, национальности, профессии, социальной категории, возраста, языка человека и гражданина, официальных государственных символов (флагов, гербов, гимнов), религиозных символов, объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, а также объектов культурного наследия, включенных в Список всемирного наследия», т.е. не допускается нарушение норм морали путем оскорбления лиц по признакам расы, национальности, профессии, пола, веры и т.п. Она не может порочить культурные ценности и государственные символы.

Закон запрещает скрытую рекламу, однако юристы пока не пришли к согласию в отношении того, что следует под ней понимать. В определении скрытой рекламы говорится об использовании рекламы, оказывающей не осознаваемое потребителем воздействие на его восприятие (п. 9 ст. 5 ФЗ «О рекламе»). Большинство специалистов считают, что речь идет о скрытых технических эффектах в рекламных сообщениях (например, так называемый 25-й кадр), в то время как на уровне массового сознания под этим понимается реклама под видом новостей. Другие юристы, однако, считают, что примером скрытой рекламы могут служить репортажи с приемов, если при этом «концентрируется» внимание телезрителей «на этикетках напитков, которые там пьют, на названиях табачных

изделий, которые там курят, и т.п.». Другой приводимый ими пример касается рекламы с использованием слов «Белый орел» (марка водки) и показа логотипа «Магна», товарного знака производителя сигарет, хотя сами водка и табачные изделия в рекламе не упоминались[1].

Наконец, авторы комментария к Закону о рекламе 1995 г. считают, что понятие скрытой рекламы просто уже понятия нераспознаваемой рекламы, т.е. такой, которую нельзя распознать без специальных знаний или без применения технических средств в момент ее представления. Следовательно, реклама под видом информационного, редакционного или авторского материала, но с пометкой «на правах рекламы» (или подобной ей), не должна считаться нераспознаваемой и не будет скрытой[2].

Как и в большинстве стран мира, российское законодательство устанавливает определенные ограничения на рекламу в радио- и телепрограммах. Эти ограничения связаны с продолжительностью и частотой рекламных блоков. Существуют ограничения на прерывание рекламой религиозных передач, богослужений, событий общенационального характера, государственных мероприятий, инаугурации президента, первой сессии парламента и т.д. То есть существует некий набор передач, где рекламная вставка была бы либо неуместной, либо носила оскорбительный для аудитории характер. Об этом говорится в ст. 14 Закона о рекламе.

Некоторые запреты, направленные на предупреждение нарушений прав и законных интересов граждан и организаций, установлены в рекламе финансовых, страховых, инвестиционных услуг и ценных бумаг (ст. 28 Закона о рекламе). Реклама оружия разрешается только в специализированных изданиях, а по радио и телевидению — только после 22 ч (ст. 26 Закона о рекламе).

---

[1] *Жилинский С.Э.* Правовая основа предпринимательской деятельности (предпринимательское право): Курс лекций. — М.: НОРМА-ИНФРА-М, 1998. С. 536-537.

[2] Практический комментарий Закона РФ «О рекламе» // Российская бизнес-газета. 2001. 27 февраля.

Конвенция о правах ребенка, ратифицированная РФ, устанавливает, что ребенок ввиду его физической и умственной незрелости нуждается в специальной охране и заботе, включая надлежащую правовую защиту. С этой целью в законодательстве РФ содержится комплекс норм.

Поэтому естественно, что Закон о рекламе особо защищает интересы несовершеннолетних (лиц, не достигших возраста 18 лет) при производстве и распространении рекламы. Нельзя злоупотреблять отсутствием у детей критического восприятия сообщений средств массовой информации, отсутствием у подростков жизненного опыта.

Не допускаются также: дискредитация авторитета родителей и воспитателей (нельзя, например, в рекламе говорить: твои родители ничего не понимают, они покупают тебе плохие конфеты, лучшие конфеты такие-то); поощрение «вещизма», а именно внушение убедить родителей приобрести рекламируемые товары (т.е. нельзя использовать фразы типа «мама, купи!» или «папа, купи!»); создание искаженного впечатления о цене товара, его доступности (на практике был случай запрета рекламы компьютеров — «В моей школе у многих ребят есть компьютер», так как фактически он недоступен семейному бюджету многих родителей); привлечение внимания несовершеннолетних к тому, что обладание рекламируемыми товарами даст им преимущество перед другими детьми (рекламировать, что, скажем, съев мороженое N., ты будешь здоровее своих одноклассников, или, купив рюкзак фирмы С, ты станешь первым учеником в школе) и т.п. (ст. 6 Закона о рекламе). При этом возможный повествовательный характер сообщений, отсутствие в них признаков прямого внушения, по мнению Высшего Арбитражного Суда, значения не имеют.[1]

[1] Президиум Высшего Арбитражного Суда РФ. Информационное письмо от 25 декабря 1998 г. № 37 «Обзор практики рассмотрения споров, связанных с применением законодательства о рекламе» // ЗиП. 2000. № 3 . С. 17.

Нельзя размещать информацию в рекламе таким образом, чтобы несовершеннолетние могли оказаться в опасной для жизни и здоровья ситуации. Например, нельзя показывать, скажем, школьников в рекламе рюкзака таким образом, чтобы в ней «герой» шел по краю крыши и расхваливал достоинства товара. Нельзя внушать несовершеннолетнему, что когда у него есть новые кеды, то в них и по краю крыши не страшно пройти и т.п.

3. Правовой статус журналиста

Правовой статус журналиста — совокупность специальных прав и обязанностей. Закон о СМИ выделяет следующие категории:

— журналисты;

— приравненные к ним лица (работающие в штате редакции, но не собирающие информацию, внештатные работники).

Правовой статус журналиста включает в себя следующие элементы.

1. Трудовые отношения, иные договорные отношения лица с зарегистрированным СМИ.

2. Функции журналиста. Журналист имеет право:

1) искать, запрашивать, получать и распространять информацию;

2) посещать государственные органы и организации, предприятия и учреждения, органы общественных объединений либо их пресс-службы;

3) быть принятым должностными лицами в связи с запросом информации;

4) получать доступ к документам и материалам, за исключением их фрагментов, содержащих сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну;

5) копировать, публиковать, оглашать или иным способом воспроизводить документы и материалы при условии соблюдения требований ч. 1 ст. 42 настоящего Закона;

6) производить записи, в том числе с использованием средств аудио- и видеотехники, кино- и фотосъемки, за исключением случаев, предусмотренных законом;

7) посещать специально охраняемые места стихийных бедствий, аварий и катастроф, массовых беспорядков и массовых скоплений граждан, а также местности, в которых объявлено чрезвычайное положение; присутствовать на митингах и демонстрациях;

8) проверять достоверность сообщаемой ему информации;

9) излагать свои личные суждения и оценки в сообщениях и материалах, предназначенных для распространения за его подписью;

10) отказаться от подготовки за своей подписью сообщения или материала, противоречащего его убеждениям;

11) снять свою подпись под сообщением или материалом, содержание которого, по его мнению, было искажено в процессе редакционной подготовки, либо запретить или иным образом оговорить условия и характер использования данного сообщения или материала в соответствии с ч. 1 ст. 42 настоящего Закона;

12) распространять подготовленные им сообщения и материалы за своей подписью, под псевдонимом или без подписи.

Журналист обязан:

1) соблюдать устав редакции, с которой он состоит в трудовых отношениях;

2) проверять достоверность сообщаемой им информации;

3) удовлетворять просьбы лиц, предоставивших информацию, об указании на ее источник, а также об авторизации цитируемого высказывания, если оно оглашается впервые;

4) сохранять конфиденциальность информации и (или) ее источника;

5) получать согласие (за исключением случаев, когда это необходимо для защиты общественных интересов) на рас-

пространение в средстве массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей;

6) при получении информации от граждан и должностных лиц ставить их в известность о проведении аудио- и видеозаписи, кино- и фотосъемки;

7) ставить в известность главного редактора о возможных исках и предъявлении иных предусмотренных законом требований в связи с распространением подготовленного им сообщения или материала;

8) отказаться от,данного ему главным редактором или редакцией задания, если оно либо его выполнение связано с нарушением закона;

9) предъявлять при осуществлении профессиональной деятельности по первому требованию редакционное удостоверение или иной документ, удостоверяющий личность и полномочия журналиста;

10) соблюдать запрет на проведение им предвыборной агитации, агитации по вопросам референдума при осуществлении профессиональной деятельности.

Журналист несет также иные обязанности, установленные законодательством РФ о средствах массовой информации.

При осуществлении профессиональной деятельности журналист обязан уважать права, законные интересы, честь и достоинство граждан и организаций.

3. Аккредитация.

Аккредитация журналистов регулируется ст. 48 Закона о СМИ[1] и принимаемыми в соответствии с Законом правилами аккредитации конкретной аккредитующей организации. Статья 48 Закона дает общую характеристику содержанию прав и обязанностей журналистов и аккредитующих организаций, оставляя за рамками Закона детальную процедуру по-

[1] Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 7. Ст. 300.

лучения и основания лишения аккредитации, некоторые другие важные моменты. Конкретизация этого института в правилах аккредитации в подавляющем большинстве случаев происходит путем введения в правила многочисленных условий и оговорок реализации прав журналистов по сравнению с Законом о СМИ, что ведет к сужению прав журналистов. Трудность обжалования таких правил зачастую вызвана тем, что правила противоречат не конкретной, императивной норме Закона о СМИ или Конституции РФ, а смыслу аккредитации, содержанию прав журналистов, выраженных не в букве, а в духе закона.

Так, например, постановлением правительства Саратовской области были утверждены «Правила аккредитации представителей средств массовой информации при правительстве области», утвержденные постановлением правительства Саратовской области от 13 марта 2002 г. № 22-П[1].

28 марта 2002 г. прокурор Саратовской области обратился в суд с заявлением о признании некоторых пунктов Правил недействительными. Прокурор усмотрел нарушение законодательства в следующих положениях Правил:

в абзаце 3 п. 5, где предусмотрено указание в заявке на аккредитацию псевдонима журналиста;

в п. 13, который устанавливает в случае замены постоянно аккредитованного журналиста временным представлять справку редакции о болезни журналиста;

в п. 21, закрепившем положение, что аккредитация может быть аннулирована в случаях прекращения или приостановления деятельности соответствующего средства массовой информации или в случае неосвещения деятельности органов исполнительной власти в течение трех месяцев;

в п. 28, который установил, что журналист может быть лишен аккредитации в случаях, предусмотренных законодательством РФ и Саратовской области.

[1] «Саратов — столица Поволжья». 2002. 22 марта.

Первой инстанцией при рассмотрении данного спора являлся Саратовский областной суд.

Саратовский суд согласился с прокуратурой, что требование указывать в заявке на аккредитацию псевдоним журналиста не соответствует федеральным законам и нарушает права журналиста. В данном случае прокуратура и Саратовский суд пришли к этому выводу на основании анализа ст. 47 Закона РФ о СМИ, ст. 15 Закона РФ «Об авторском праве и смежных правах», в которых предусмотрено право журналиста, автора использовать свое произведение под псевдонимом.

Верховный Суд, толкуя те же самые нормы, пришел к иному выводу. Он отметил, что указание псевдонима не умаляет прав журналиста, «в противном случае предусмотренное указанной выше нормой (ст. 47 Закона о СМИ) право распространения журналистом информации анонимно (без подписи) означало бы незаконность указания в заявке и имени журналиста, что вовсе исключало бы возможность его аккредитации». Другими словами, Верховный Суд посчитал, что если журналист имеет право распространять свои материалы под собственным именем или под псевдонимом, то незаконность требования указывать псевдоним означает и незаконность указывать в заявке имя журналиста, что в итоге делает невозможным его аккредитацию.

4. Защита источника информации.

Журналист обязан сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

Журналист не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное право-

нарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.

Журналист не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, признанного потерпевшим, без согласия самого несовершеннолетнего и (или) его законного представителя.

Глава 13. Информационный рынок

1. Понятие и структура информационного рынка

Информационный рынок можно разделить в зависимости от направленности информационных услуг.

1. Для населения — интерактивное телевидение, видео, музыка по требованию, электронные покупки, банковские операции, управление домашними бытовыми приборами, охрана дома и др.

2. Для бизнеса — электронный обмен данными, телеконференции, корпоративное обучение, мультимедийные базы данных, презентации, настольные издательские системы, телеработы и т.д.

3. Для государства — разработка программ для обеспечения безопасности и суверенитета, данные в области статистики и образования, мультимедиа (объединение СМИ и интернет-технологий).

В зависимости от отраслей информационной индустрии:

1) массовое вещание;

2) коммуникации;

3) компьютинг.

В зависимости от области применения принципов электронной торговли:

1) корпоративные сети;

2) финансовые услуги;

3) транспортные агентства;

4) музыка, книги, автомобили, мелкая розничная торговля;

5) реклама, маркетинг.

2. Тенденции развития информационного рынка

1. Интеграция информационного рынка — вертикальная и горизонтальная.

Конвергенция — соединение разнородных технологий в единые комитеты, т.е. появление у обычных предметов новых свойств в связи с изменяющейся средой обитания (горизонтальная), пример — «умный» дом.

Вертикальная — Microsoft — разрастание крупных компаний.

2. Развитие новых типов связи.

3. Либерализация информационное рынка.

Все это вызывает развитие информационной империи.

Проблемы:

1) запрос о таможенных и налоговых сборах. Система этих сборов должна быть простой и совместимой с уже существующей;

2) электронная система оплаты;

3) необходимость создания единого торгового кода, т.е. правил юридически значимого документооборота;

4) защита интеллектуальной собственности. Правительство США для эффективной защиты интеллектуальной собственности предлагает:

— приравнять к литературным произведениям;

— должна охраняться информация об авторе;

— противодействие взлому с целью копирования;

5) тайна личной жизни. Правительство США считает, что тайна личной жизни должна охраняться исходя из двух принципов:

— уведомления;

— согласия;

6) проблема обеспечения безопасности:

— от взлома;

— вредной информации;

— вирусов.

Информационый рынок — это комплексная структура, включающая в себя правовой статус субъектов, вступающих в отношения при оказании информационных услуг и их использовании в различных отраслях информационной индустрии.

4. Правовое регулирование информационного рынка.

Основы развития глобальной электронной торговли (приняты правительством США в 1996 г.) включают в себя следующее.

1. Частный сектор должен лидировать.

2. Государства должны избегать излишних ограничений электронной торговли.

3. Государственное вмешательство необходимо только при поддержке и содействии.

4. Юридическая база должна быть предельно простой.

5. Государство должно признать уникальные свойства Интернета по саморегуляции.

6. Электронной торговле должны способствовать международные правила.

ВТО приняла в 1997 г. соглашение о дерегуляции телекоммуникационных рынков стран, входящих в организацию, главной целью которого явилась минимизация государственного и правового регулирования.

Комиссия ООН приняла модельный закон «О порядке коммерческого использования международных контрактов в электронной торговле» (о векселях, договор о закладе имущества и т.д.).

Организация экономического сотрудничества и развития в рамках Совета Европы (ОЭСР) создала комиссию по глобальной информационной инфраструктуре. Состав комиссии — управляющие наиболее крупных информационных компаний.

Электронную торговлю можно определить как заключение путем обмена следующих сделок, предусмотренных Гражданским кодексом РФ, но не ограничиваясь ими: купля-продажа, поставка, заем и т.д., а также приобретение и осуществление с использованием электронных средств и иных прав и обязанностей, возникающих в процессе предпринимательской деятельности.

Раздел 3
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Глава 14. Общая характеристика информационной безопасности

1. Понятие информационной безопасности

Национальная безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы — совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Угроза безопасности — совокупность условий и факторов, создающих опасность жизненным интересам личности, общества и государства.

Обеспечение безопасности — единая государственная политика, система мер экономического, политического, правотворческого (иного) характера, адекватного угрозам жизненно важных интересов личности, общества и государства.

Охрана безопасности — непосредственное воздействие на объект охраны.

Защита безопасности — совокупность обеспечения и охраны мер безопасности.

Информационная безопасность — состояние защищенности национальных интересов страны (национальные интересы страны — жизненно важные интересы, основанные на сбалансированной основе) в информационной сфере от внутренних и внешних угроз.

Основные направления защиты информационной сферы.

1. Защита интересов личности, общества и государства от воздействия вредной, недоброкачественной информации. Такую защиту обеспечивают институты: СМИ, документированной и др. информации.

2. Защита информации, информационных ресурсов и информационной системы от неправомерного воздействия в различных ситуациях. Такую защиту обеспечивают:

— институт государственной тайны;

— персональных данных.

3. Защита информационных прав и свобод (институт интеллектуальной собственности).

Главной задачей информационной безопасности является обеспечение баланса интересов общества, государства и человека. Этот баланс должен быть адекватен целям по безопасности страны в целом. Обеспечение информационной безопасности должно быть ориентировано на специфику информационной среды, определяемой социальной структурой.

В центре внимания обеспечения информационной безопасности должна находиться информационная среда органов государственной власти.

В контексте процесса глобализации необходимо обеспечить постоянный анализ изменений политики, законодательства других стран.

Последняя задача — это учет выполнения факторов в процессе расширения правового внимания РФ в мирном информационном пространстве, включая сотрудничество в рамках СНГ, и практики использования Интернета.

2. Национальные интересы РФ в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также систе-

мы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов РФ в информационной сфере включает в себя информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

3. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние. *К внешним источникам относятся:*

— деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;

— стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

— обострение международной конкуренции за обладание информационными технологиями и ресурсами;

— деятельность международных террористических организаций;

— увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

— деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

— разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

— критическое состояние отечественных отраслей промышленности;

— неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получе-

ния криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

— недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;

— недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

— неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

— недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;

— недостаточная экономическая мощь государства;

— снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

— недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

— отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Государственная политика в сфере информационной безопасности

Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:

— соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;

— открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;

— правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

— приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Государство в процессе реализации своих функций по обеспечению информационной безопасности РФ:

— проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению;

— организует работу законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвра-

щение, отражение и нейтрализацию угроз информационной безопасности РФ;

— поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

— осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

—- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

— способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

— формулирует и реализует государственную информационную политику России;

— организует разработку федеральной программы обеспечения информационной безопасности РФ, объединяющей усилия государственных и негосударственных организаций в данной области;

— способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

Это предполагает:

— оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

— создание организационно-правовых механизмов обеспечения информационной безопасности;

— определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;

— создание системы сбора и анализа данных об источниках угроз информационной безопасности РФ, а также о последствиях их осуществления;

— разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

— разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в Уголовный, Гражданский, Административный и Трудовой кодексы, в законодательство РФ о государственной службе;

— совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ.

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

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ при решении возникающих

в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

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

Разработка механизмов правового обеспечения информационной безопасности РФ включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов РФ и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

5. Обеспечение информационной безопасности

Предметная область обеспечения информационной безопасности — это круг правоотношений, который определяет правовое положение различных субъектов и объектов в сфере информационных коммуникационных технологий — комплекса (совокупность элементов инфраструктуры, на основе которой формируется технологическая база информационных систем стран, участвующих в глобальном

информационном пространстве). К объектам правового регулирования обеспечения информационной безопасности относятся:

— правовой режим различных элементов информационных коммуникационных технологий;

— определение правового статуса субъектов с учетом их специальной информационной среды;

— правовое обеспечение специальных субъектов, осуществляющих деятельность в сфере обеспечения информационной безопасности.

Основные направления обеспечения информационной безопасности:

1) установление различных видов ограничений;

2) повышение значимости таких видов обеспечения информационной безопасности, как сертификация, лицензирование, в том числе и экспертиза деятельности;

3) установление процедур создания, получения и использования инфраструктуры с ограниченным доступом;

4) унификация подходов и стандартов к электронным документам;

5) заключение, установление режимов служебной информации.

Правовое регулирование обеспечения информационной безопасности должно осуществляться на различных уровнях, начиная с самого нижнего:

1) участие граждан в обеспечении информационной безопасности;

2) обеспечение информационной дисциплины в корпорациях;

3) организация подразделений информационной безопасности в органах государственной власти на всех уровнях;

4) установление процессуального законодательства на федеральном уровне;

5) установление стандартов, удостоверяющих техническую безопасность информационных систем;

6) создание системы органов власти в этой области;

7) выработка соглашений и условий международного сотрудничества и обеспечение интересов РФ с учетом позиций национальной безопасности.

Вредная информация — информация, не являющаяся конфиденциальной, но обусловливающая необходимость охраны и защиты прав и законных интересов личности, общества и государства в силу возникновения вреда, который нанесет этим субъектом ее распространение.

Вредную информацию можно разделить на группы:

1) информация направлена на разжигание ненависти, вражды и насилия;

2) ложная информация (в том числе недоброкачественная, недобросовестная, ложная реклама);

3) информация, содержащая посягательство на честь, доброе имя и деловую репутацию;

4) непристойная информация;

5) информация, оказывающая деструктивное воздействие на здоровье людей (в том числе технические устройства, действующие на психику людей).

Глава 15. Информационная безопасность личности

1. Общая характеристика информационной безопасности личности

Информационная безопасность личности — состояние и условия жизнедеятельности личности, при которых реализуются ее информационные права и свободы.

Жизненно важные интересы личности в информационной сфере следующие.

1. Соблюдение и реализация конституционных прав на поиск, получение прав и распространение информации.

2. Реализация прав гражданина на неприкосновенность частной жизни.

3. Использование информации в интересах не закрепленной законом деятельности, направленной на физическое, духовное, интеллектуальное развитие.

4. Защита прав на объекты интеллектуальной собственности.

5. Обеспечение прав гражданина на защиту своего здоровья от неосознаваемой вредной информации.

Угрозы интересам личности в информационной сфере.

1. Применение нормативно-правовых актов, противоречащих конституционным правам граждан.

2. Противодействие в том числе со стороны криминальных структур, реализация гражданами прав на неприкосновенность частной жизни.

3. Неправомерное ограничение доступа к отправляемой информации.

4. Нарушение прав граждан в области массовой информации.

5. Противоправное применение специальных средств, воздействующих на сознание.

6. Манипулирование информацией (дезинформация; сокрытие информации; искажение информации).

2. Информационно-психологическая безопасность

В отношении человека государство должно обеспечивать информационно-психологическую безопасность.

Информационно-психологическая безопасность — состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере.

Основными принципами обеспечения информационно-психологической безопасности являются:

— адекватность мер безопасности существующим угрозам;

— государственная монополия на разработку и производство специальных средств информационно-психологического воздействия;

— сочетание централизованного управления силами и средствами обеспечения информационно-психологической безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов РФ и органам местного самоуправления;

— гласность и гражданский контроль за обеспечением информационно-психологической безопасности;

— обязательность участия общественных организаций в деятельности по обеспечению информационно-психологической безопасности.

К основным угрозам информационно-психологической безопасности относится возможность наступления негативных последствий для субъектов, подвергающихся информационно-психологическому воздействию, которые могут выражаться в следующих формах:

— причинение вреда здоровью человека;

— блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости;

— утрата способности к политической, культурной, нравственной самоидентификации человека;

— манипуляция общественным сознанием;

— разрушение единого информационного и духовного пространства РФ, традиционных устоев общества и общественной нравственности, а также нарушение иных жизненно важных интересов личности, общества и государства.

Источниками угроз информационно-психологической безопасности являются:

1) физические лица, обладающие природными способностями воздействия на психику людей;

2) разработка программных и технических средств;

3) религиозные и иные группы;

4) антропогенные зоны;

5) геопатогенные зоны.

Эти источники могут повлечь:

1) причинение вреда здоровью;

2) блокирование на неосознаваемом уровне волеизъявления человека;

3) манипулирование общественным сознанием;

4) разрушение единого информационного пространства.

Государственная система обеспечения информационно-психологической безопасности осуществляет следующие функции:

— выявление и учет субъектов, осуществляющих негативные информационно-психологические воздействия, и контроль за их деятельностью;

— ведение мониторинга негативных информационно-психологических воздействий;

— пресечение негативных информационно-психологических воздействий;

— подготовку кадров для обеспечения информационно-психологической безопасности с привлечением негосударственных образовательных и научных организаций;

— разработку и совершенствование методов и средств выявления и нейтрализации негативных информационно-психологических воздействий, реабилитации лиц, пострадавших от такого воздействия;

— организацию реабилитации лиц, пострадавших от негативных информационно-психологических воздействий;

— организацию системы лицензирования, сертификации, экспертизы и контроля в сфере информационно-психологической безопасности;

— организацию разработки и принятия стандартов в сфере информационно-психологической безопасности;

— разработку специальных средств и методов информационно-психологических воздействий;

— информирование общественности о деятельности лиц и организаций, нарушающих законодательство в области информационно-психологической безопасности;

— содействие разработке и принятию норм международного права в области обеспечения информационно-психологической безопасности.

3. Информационно-идеологическая безопасность

В Доктрине информационной безопасности РФ перечислены угрозы идеологической безопасности, но отдельного ее определения нет, Таким образом, налицо факт поглощения институтом информационной безопасности института идеологической безопасности, что вносит определенную сумятицу ввиду объективной необходимости применения разных подходов.

Выделение идеологической безопасности в отдельный, институт необходимо провести по следующим основаниям. Федеральный закон РФ «Об информации, информатизации и защите информации» определяет информацию как сведения о лицах, предметах, фактах, событиях, явлениях и процессах, а информационные процессы как процессы сбора, об- і работки, накопления, хранения, поиска и распространения информации. Как видно, информация определяется как статическое явление, как предмет, по поводу которого возникают общественные отношения. Следуя этому определению, может показаться, что информация не отличается ничем принципиальным от, скажем, материальных ценностей. Действительно, информация может быть ценностью, становиться объектом купли-продажи, даже кражи (несанкционированного доступа), поэтому она и поддерживающая ее инфраструктура должны быть защищены — именно так в упрощенном порядке можно определить сферу информационной безопасности. Идеологическая безопасность имеет с информационной общность по предмету правового и организационного регулирования (информация), однако если информационное право призвано регулировать общественны^ отношения по поводу создания, распространения, хранения) переработки и потребления информации, определяя последнюю как явление статическое, то институт идеологической

безопасности, регулируя те же отношения, рассматривает информацию как явление динамическое, т.е. принципиально важной характеристикой здесь уже является степень и характер ее влияния на сознание людей, а не ее степень защищенности, авторство и т.д. Отсюда уже совершенно различные методы. Они у института идеологической безопасности особые: социальная реклама, организационное и финансовое сопровождение творческих проектов, публичное государственное признание и провозглашение, некоторые методы ведения информационной войны и т.д.

Таким образом, следует разделить информационную безопасность на информационно-идеологическую и информационно-техническую. При этом под информационно-технической безопасностью следует понимать «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры»[1], а под информационно-идеологической (далее — идеологической) безопасностью — защищенность общества и личности от преднамеренного или непреднамеренного информационного воздействия, имеющего результатом нарушение прав и свобод человека и гражданина в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащего нравственным и этическим нормам, оказывающих деструктивное воздействие на общество, личность, имеющих негласный (внечувственный, неосознанный) характер, внедряющих в общественное сознание антисоциальные установки.

Здесь совершенно справедливо может возникнуть вопрос, а почему, собственно, информационная безопасность отождествляется с категорией идеологии, ведь первая предполагает состояние защищенности, а вторая — внедрение в общест-

[1] *Галатенко В.А.* Информационная безопасность // Открытые системы. 1996. № 1 (15). С. 38-43.

венное сознание определенных ценностных установок, ориен таций, определенную социальную программу. Дело в том, чт даже если общество и личность будут защищены от вредонос ного информационного воздействия, необходимо задать, кром того, определенные нравственные ориентиры, систему ценно стей, сформировать национальную идею, иначе защита теряе смысл. При этом комплекс защиты неизбежно имеет в свое: структуре императивные (запретительные) нормы, а комплек внедрения идеологии, следуя смыслу ст. 13 Конституции Р<£ должен состоять из одних только диспозитивных норм.

Попытки смоделировать на теоретическом уровне инсти тут информационно-психологической безопасности уже пред принимались[1].

При этом под информационно-психологической безопас ностью обычно понимают состояние защищенности человека общества и государства от «вредной» информации, а данна: информация характеризуется как не являющаяся конфиден циальной, но обусловливающая необходимость охраны и за щиты прав и законных интересов личности, общества и госу дарства в силу возможного вреда, который нанесет этш субъектам ее распространение (применение)[2].

Во-первых, идеологическая безопасность — это состоя ние защищенности личности, общества и государства от внеш них и внутренних информационных явлений, процессов и дейст вий, оказывающих негативное (деструктивное, искажающее дезинформационное) воздействие на интеллектуально-позна вательную или чувственную сферу сознания личности, об щества, государственных служащих.

Во-вторых, идеологическая безопасность предполагав[1] наличие определенной идеологии, системы иерархизирован

---

[1] Проект Концепции информационно-психологической безопас ности. Институт психологии РАН. М.,1995.

[2] *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное пра во: учебник / Под ред. Б.Н. Топорнина. СПб.: Юридический центр пресс 2001. С. 574.

ных ценностей, ориентации и установок, консолидирующих идей, а равно наличие определенной, четкой, прозрачной и взаимосвязанной совокупной программы в экономической, политической (внутренней и внешней), социальной, культурной, образовательной, иных сферах деятельности государства и общества с максимально четким определением общих и отраслевых приоритетов без их смешения.

Принципы обеспечения идеологической безопасности делятся на общие, особые и специальные. Общие принципы перечислены в Законе РФ о безопасности. Это:

— законность;

— соблюдение баланса жизненно важных интересов личности, общества и государства;

— взаимная ответственность личности, общества и государства по обеспечению безопасности;

— интеграция с международными системами безопасности.

Особые принципы характерны для всего института идеологической безопасности, к их числу необходимо относить:

— принцип идеологического плюрализма, необязательности государственной идеологии (конституционный принцип — ст. 13);

— сочетание принципа федерализма и жесткой централизации;

— принцип уважения и равенства религиозных и иных предпочтений различных социальных групп;

— гласность;

— привлечение к сотрудничеству общественности, общественных организаций;

— приоритет стратегических (долгосрочных) целей перед иными;

— принцип рациональных целей, приоритет цели экономического и духовного развития общества;

— безусловный приоритет диспозитивного регулирования над императивным;

— сочетание идеологического стимулирования экономики и экономического стимулирования идеологии;

— принцип безусловного уважения многоукладное™ и са> мобытности российской культуры и разумного заимствованш зарубежного опыта.

Специальные принципы в соответствии с концепцией дуа> лизма в определении идеологической безопасности следуем делить на две группы. К первой группе относятся принципь превентивной (защитной) функции:

— принцип закрепления императивных норм только в федеральном законе;

— принцип применения императивных норм только судом.

Ко второй группе следует относить принципы собственно идеологического влияния государства, построения его инфраструктуры и структуры властно-распорядительных отношений:

— принцип подконтрольности и подотчетности Президенту РФ;

— принцип интерструктурности (имеется в виду выполнение функций обеспечения идеологической безопасностр всеми государственными министерствами и ведомствами);

— принцип оперативной модернизации идеологии;

— принцип комплексного интернаучного анализа;

— принцип разностороннего информационного обеспечения

— принцип полного отсутствия императивных норм;

— принцип безусловного преобладания методов убеждения и стимулирования над методами внушения;

— принцип неприменения негласного (внечувственного неосознанного) влияния;

— принцип соблюдения конституционных принципов свободы мысли, слова, вероисповедания, свободы СМИ и т.д.

Способы обеспечения идеологической безопасность можно классифицировать в зависимости от того, подлежит ли применению императивный либо диспозитивный метод Если говорить о диспозитивных методах, то к их числу относятся две группы — организационные и информационно-пропагандистские. К числу организационных можно отнести

организационное сопровождение творческих проектов, адресное финансирование, организацию взаимодействия государственных органов, предоставление аналитических обобщений, организацию различного рода акций, направление предпринимателей за рубеж для повышения квалификации и обучения менеджменту и т.д. Информационно-пропагандистские приемы в общем относятся к методике проведения информационной войны и так называемым технологиям «пиар». Целесообразным представляется разработка комплексных программ влияния, которые можно, в свою очередь, подразделить на нейтрализующие негативное влияние определенного источника; связанные с экономическим стимулированием общества; военные программы; образовательные; культурно-просветительские; научные; демографические; специальные тактические; иные. По сфере действия можно выделить международные, федеральные, окружные, региональные, локальные программы. По направленности и продолжительности — стратегические (долгосрочные), оперативные (среднесрочные) и тактические (краткосрочные). Данная классификация предполагает наличие базовой всеобъемлющей и взаимосвязанной программы.

Угрозы национальной идеологической безопасности можно классифицировать по различным основаниям на внутренние и внешние, намеренные (организованные) и непреднамеренные (стихийные), явные и латентные (скрытые) и т.д. Представляется целесообразным расположить их по степени общественной опасности в порядке убывания:

— враждебная деятельность специальных органов иностранных государств;

— деструктивная организованная целенаправленная деятельность внутригосударственных организаций;

— аналогичная деятельность международных негосударственных организаций (транснациональных корпораций и т.п.);

— острые социальные противоречия, вызванные политическим, экономическим либо иным кризисом;

— отсутствие минимального контроля за информационными потоками в целях обеспечения нравственного здоровья населения;

— монополизирование СМИ;

— применение некорректных методов идеологического влияния;

— массовое дезинформирование в целях искажения общественного мнения;

— применение внутри страны приемов, характерных для межгосударственного информационного противоборства либо психологической войны с существенным нарушением прав и свобод человека и гражданина;

— создание и функционирование на территории РФ религиозных сект деструктивного толка и иных подобных организаций, практикующих внечувственное воздействие на психику человека, побуждающее его к совершению антисоциальных поступков;

— отсутствие у большинства населения ценностных ориентации, идеалов, побудительных стимулов к активной деятельности (идеологии);

— иные угрозы.

Глава 16. Информационная безопасность общества

1. Общая характеристика информационной безопасности общества

Информационная безопасность общества — защита экономических, социальных, международных и духовных ценностей с использованием информационных средств от внешних и внутренних угроз.

Жизненно важные интересы общества в информационной сфере.

1. Обеспечение интересов общества.
2. Построение прав государства.

3. Построение информационного общества.

4. Сохранение нравственных ценностей общества.

5. Предотвращение манипулирования массовым сознанием.

6. Приоритетное развитие современных информационных технологий.

Информационная безопасность общества обеспечивается его защитой от вредных информационных воздействий в ходе информационной войны против страны, которая преследует в отношении общества следующие основные цели:

— тактическую — навязать свою политическую волю через идеологическую, психологическую обработку народа, армии, военно-политического руководства страны в интересах создания требуемого общественного мнения;

— стратегическую — изменить образ жизни, разобщить народ, уничтожить морально-политический потенциал общества и разрушить государство изнутри путем идеологической революции, разрушения национального самосознания, размывания чувства патриотизма, культуры, традиций, исторической памяти, подрыва духовно-нравственных устоев.

Вредное информационное воздействие на общество реализуется в основном через СМИ, в том числе электронные коммуникации, путем создания и внедрения штампов, доступных для понимания человека, игры на чувствах страха, надежды, раздражения и др., вызывающих состояние агрессии или безысходности, стремление уйти из реального мира, заменить его традиционно искусственным (алкоголизм, наркомания, приход в деструктивные секты) или виртуальным (телевизионный, компьютерный), усиление социально-политических, экономических и духовных коллизий, нарастание, закрепление и развитие психологической и психической напряженности, рост агрессивности, преступности, снижение самоконтроля среди молодежи, резкую активизацию иррациональной сферы общественного сознания, дестабилизацию социальной преемственности поколений, утрату культурного наследия, проявление бездуховности и безнравственности, повышение преступности в обществе и другие последствия.

2. Угрозы информационной безопасности общества

К угрозам информационной безопасности общества относятся:

1) неисполнение требований закона;

2) дезорганизация и разрушение накопления и сохранения информации;

3) усиление зависимости общественной жизни от зарубежных инфраструктур;

4) активизация различного рода религиозных сект.

Деятельность сект содержит в себе контроль сознания своих членов, который включает:

1) контроль поведения;

2) контроль мышления;

3) контроль информации;

4) контроль эмоций;

5) снижение духовной нравственности, творческого потенциала населения России;

6) увеличение оттока специалистов за рубеж;

7) нарушение прав в сфере оборота информации (утечка, перехват, хищение, навязывание ложной информации);

8) нарушение правил в области функционирования информационной системы;

9) нарушение правил в области использования средств обеспечения информационной безопасности:

— воздействие на парольные ключи системы;

— использование несертифицированных информационных технологий.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности РФ:

— нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

— недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

— распространение дезинформации о политике РФ, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

— деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности РФ в сфере внутренней политики являются:

— создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

— активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

Глава 17. Информационная безопасность государства

1. Общая характеристика информационной безопасности государства

Информационная безопасность государства — защита конституционного строя, суверенитета, территориальной целостности с точки зрения информационных средств.

Жизненно важные интересы государства.

1. Создание целей для реализации интересов личности и общества в информационной сфере.

2. Формирование институтов общественного контроля органов государственной власти.

3. Безусловное обеспечение законности и правопорядка.

4. Создание условий для развития собственной информационной инфраструктуры.

5. Формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны.

6. Защита государственной информационной системы и информационных ресурсов (защита государственной тайны).

7. Защита единого информационного пространства страны.

8. Разделение равноправного и взаимного международного сотрудничества.

2. Угрозы безопасности государства в информационной сфере

1. Размывание единого правового пространства страны из-за принятия субъектами РФ не соответствовавших Конституции РФ правовых актов.

2. Разрушение единого информационного пространства России.

3. Вытеснение российских информационных агентств и средств массовой информации с внутреннего информационного рынка.

4. Монополизация информационного рынка.

5. Блокирование деятельности государственных средств массовой информации по информированию российской, зарубежной аудитории.

6. Ослабление роли русского языка как государственного языка РФ.

7. Целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем.

8. Низкая эффективность информационного обеспечения государственной политики (дефицит кадров, отставание информационных систем от международных стандартов).

В последнее время злоупотребление свободой массовой информации является одним из главных внутренних источников угроз информационной безопасности России. С одной стороны, в демократическом государстве журналисты должны информировать общественность по всем злободневным вопросам жизнедеятельности государства. С другой сторо-

ны - • - в то время, когда государство устраняется, журналист или те лица, которые финансируют, а значит, заказывают, сами определяют, что и как печатается в прессе, показывается по телевидению, звучит по радио. При этом «выдается» значительный объем информации, которая является объектом спецслужб. Для примера можно привести интервью руководителя аналитического отдела посольства Швеции в России, которое было показано в телепередаче «Рейтинг прессы с Александром Герасимовым». Шведский дипломат говорил о том, что его отдел ежедневно обрабатывает всю центральную и большой объем региональной прессы и в результате анализа полученной информации делается от 3 до 5 тематических докладов по вопросам, интересующим шведское государство. По мнению экспертов, около 40% разведывательной информации получается в процессе аналитической обработки открытых материалов, включая печатные и электронные СМИ.

На сегодняшний день смена угроз «холодной войны» угрозами «информационной войны» существенно повышает значение информационной безопасности в системе национальной безопасности государства, обусловливает расширение ее содержания. Потеря государственного контроля над российскими коммуникациями может привести к утрате национальной независимости.

Информационная безопасность определяется и тем, насколько каждый из субъектов в соответствии со своей позицией и интересами имеет возможность через средства массовой информации и телекоммуникаций свободно искать, получать и распространять достоверную информацию. Общество не может чувствовать себя в безопасности, если оно получает препарированную, управляемую информацию. Неотъемлемым атрибутом развитого демократического общества должно являться соблюдение законных прав личности, общества и государства по защите информации ограниченного доступа. Правовое государство не есть просто государство, соблюдающее законы. Это общество и государство, признающие право как

исторически развивающуюся в общественном сознании, расширяющуюся меру свободы и справедливости, выраженную именно в законах, подзаконных актах и практике реализации прав, свобод и законных интересов граждан.

К наиболее важным объектам обеспечения информационной безопасности РФ в сфере внешней политики относятся:

— информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;

— информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику РФ, на территориях субъектов РФ;

— информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику РФ;

— блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики РФ, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности РФ в сфере внешней политики наибольшую опасность представляют:

— информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ;

— распространение за рубежом дезинформации о внешней политике РФ;

— нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

— попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной

власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях.

Из внутренних угроз информационной безопасности РФ в сфере внешней политики наибольшую опасность представляют:

— нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику РФ, и на подведомственных им предприятиях, в учреждениях и организациях;

— информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности РФ;

— недостаточная информированность населения о внешнеполитической деятельности РФ.

Основными мероприятиями по обеспечению информационной безопасности РФ в сфере внешней политики являются:

— разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса РФ;

— разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;

— создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике РФ;

— совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

— совершенствование информационного обеспечения субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

Обеспечение информационной безопасности РФ в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала РФ, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности РФ в сфере духовной жизни относятся:

— достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;

— свобода массовой информации;

—- неприкосновенность частной жизни, личная и семейная тайна;

— русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств — участников Содружества Независимых Государств;

—- языки, нравственные ценности и культурное наследие народов и народностей РФ;

— объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности РФ:

— деформация системы массового информирования как за счет монополизации средств массовой информации, так и за

счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

— ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

— возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

— использование зарубежными специальными службами средств массовой информации, действующих на территории РФ, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

— неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности РФ в сфере духовной жизни являются:

— развитие в России основ гражданского общества;

— создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

— выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;

— совершенствование законодательства РФ, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

— государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей РФ;

— формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав й свобод в сфере духовной жизни;

— разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

— разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей РФ, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

— введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

— противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Глава 18. Информационная безопасность в глобальной информационном пространстве

1. Понятие глобального информационного пространства

Материальным подтверждением формирования информационного глобального пространства служит Internet, но он не единственный фактор формирования информационной циви-

лизации. Вопрос о глобализации экономического, культурного развития ставится в науке с начала XX в. В 30-е гг. XX в. глобализация активно обсуждалась под именем конвергенции. В итоге были сформированы транснациональные корпорации, финансовая коммерция в мировом масштабе, политика открытого общества, глобальная идеология. Главный идеолог политики открытого мира Жорж Сорос считает, что информационные технологии — движущий фактор в развитии финансово-экономических монополий. Обеспечение безопасности информации на мировом уровне — залог в развитии экономики и культурного наследия всех стран и народов.

Под влиянием глобализации правовые механизмы воздействия на общество размываются. Это обусловлено иными территориальными пространственными условиями, самостоятельностью отдельно взятого человека от социальной среды, развитием идей «открытого общества».

Глобальное информационное пространство — совокупность информационных ресурсов и информационной инфраструктуры, позволяющей на основе единых принципов и по общим правилам обеспечивать безопасное информационное взаимодействие государств, организаций и граждан при их равнодоступности к открытым информационным ресурсам, а также максимально полное удовлетворение их информационных потребностей при сохранении баланса национальных и международных интересов.

2. Структура глобального информационного пространства

Объекты глобального информационного пространства:

1) информационные ресурсы;
2) информационная инфраструктура:
а) информационные телекоммуникационные структуры;
б) информационные технологии;
в) системы СМИ;
г) организационная структура (органы власти).

Глобальное информационное пространство России включает

— информационное пространство органов государственной власти;

— информационные телекоммуникации системы государства (МЧС, в силовых структурах);

— государственные информационные ресурсы — правовая информация, информация о деятельности органов власти, информация о чрезвычайных ситуациях, информация представляющая собой культурную ценность и наследие, открытая информация о предприятиях, государственный информационный регистр;

— информационно-управленческая система органов государственной власти — есть только у тех органов государственной власти, которые обладают развитой территориальной инфраструктурой (система МВД).

Глобальное информационное пространство может создаваться и негосударственными частными органами или гражданами.

3. Обеспечение безопасности в глобальном информационном пространстве

Факторы, влияющие на правовое регулирование глобального информационного пространства:

1) особенности макроэкономической политики государства

2) идеология формирования информационного общества

3) специфика действующего законодательства;

4) особенности менталитета, национально-культурные особенности.

Основные направления развития информационной безопасности глобального информационного пространства.

1. Определение порядка доступа к информации при гуманном использовании информации.

2. Определение доступа к информации в случае использования информации во вред человеку.

Практика показала, что почти бесполезно устанавливать порядок работы по получению и использованию ин-

формации через Internet; ответственность за использование непроверенной и часто недостоверной информации никто не несет, как и за нарушение авторских и смежных прав. Наиболее эффективным может стать установление ответственности при вводе информации в Internet (установление порядка распространения служебной информации, информация авторского происхождения, официальная и справочная информация).

Основными объектами обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах являются:

— информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

— средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

— технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

— помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах являются:

— деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, проти-

возаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

— вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

— нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

— использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

— привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах являются:

—- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

— исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

— предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

— предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение,

искажение информации или сбои в работе средств информатизации;

— обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

— обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

— выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

— лицензирование деятельности организаций в области защиты информации;

— аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

— сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

— введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

— создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

Раздел 4
ОТВЕТСТВЕННОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

Глава 19. Ответственность в информационной сфере

1. Дисциплинарная и административная ответственность в информационной сфере

Юридическая ответственность реализуется с учетом специфических методов информационного права при возникновении конфликтных противоправных ситуаций.

Дисциплинарная ответственность наступает за противоправные действия, совершаемые субъектами информационного права в связи с исполнением своих прав и обязанностей (п. 6 ст. 9 Закона РФ от 23 сентября 1992 г. № 3526-1 «О правовой охране топологий интегральных микросхем»[1], ст. 46 Конституции Р Ф — ответственность служащих за непредоставление информации или предоставление недоброкачественной информации).

Административная ответственность устанавливается за нарушение определенных правил поведения. В Кодексе об административных правонарушениях предусматривается административная ответственность за:

— нарушение права гражданина на ознакомление со списком избирателей, участников референдума (ст. 5.1);

— нарушение порядка участия средств массовой информации в информационном обеспечении выборов, референдумов (ст. 5.5);

[1] Ведомости СНД РФ и ВС РФ. 1992 г. № 42. Ст. 2328; СЗ РФ. 2002. № 28. Ст. 2786; 2004. № 45. Ст. 4377; 2006. № 6. Ст. 636.

— изготовление, распространение или размещение агитационных материалов с нарушением требований законодательства о выборах (ст. 5.12);

— умышленное уничтожение или повреждение печатных материалов, относящихся к выборам, референдуму (ст. 5.14);

— непредоставление или неопубликование отчета, сведений о поступлении и расходовании средств, выделенных на подготовку и проведение выборов, референдума (ст. 5.17);

— непредоставление сведений об итогах голосования или о результатах выборов (ст. 5.25);

— нарушение порядка или сроков предоставления сведений о несовершеннолетних, нуждающихся в передаче на воспитание в семью либо в учреждение для детей-сирот или детей, оставшихся без попечения родителей (ст. 5.36);

— отказ в предоставлении гражданину информации (ст. 5.39);

— незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53);

— сокрытие или искажение экологической информации (ст. 8.5);

— невыполнение правил ведения судовых документов (ст. 8.16);

— сокрытие сведений о внезапном падеже или об одновременном массовом заболевании животных (ст. 10.7);

— самовольная установка или эксплуатация узла проводного вещания (ст. 13.1);

— воспрепятствование распространению продукции средств массовой информации (ст. 13.16);

— нарушение правил распространения обязательных сообщений (ст. 13.17);

— воспрепятствование уверенному приему радио- и телепрограмм (ст. 13.18);

— нарушение порядка предоставления статистической информации (ст. 13.19);

— непредоставление информации для составления списков присяжных заседателей (ст. 17.6) и др.

Таким образом, КоАП РФ вводит новые составы административного правонарушения, практически аналогичные содержанию ст. 4 Закона РФ о СМИ. Речь идет, в частности, о таких

правонарушениях, как пропаганда наркотических средств, психотропных веществ или их прекурсоров (ст. 6.13). В качестве административного наказания предусмотрено наложение административного штрафа на граждан в размере от двадцати до двадцати пяти МРОТ с конфискацией рекламной продукции и оборудования, использованного для ее изготовления, или без таковой; на должностных лиц — от сорока до пятидесяти МРОТ с конфискацией рекламной продукции и оборудования, использованного для ее изготовления, или без таковой; на юридических лиц — от четырехсот до пятисот МРОТ с конфискацией рекламной продукции и оборудования, использованного для ее изготовления, или без таковой. В КоАП РФ особо оговорено, что не является административным правонарушением распространение в специализированных изданиях, рассчитанных на медицинских и фармацевтических работников, сведений о разрешенных к применению в медицинских целях наркотических средствах, психотропных веществах и их прекурсорах.

Два новых состава административного правонарушения, непосредственно касающихся деятельности журналистов, установлены КоАП РФ. Речь идет об ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11), а также за разглашение информации с ограниченным доступом лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14). Первый состав может образовать, например, несоблюдение редакцией СМИ условий разглашения информации о несовершеннолетнем, совершившем преступление или административное правонарушение, либо явившемся потерпевшем (ч. 3 и 4 ст. 41 Закона РФ о СМИ). Совершение данного правонарушения влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти МРОТ; на должностных лиц — от пяти до десяти МРОТ; на юридических лиц — от пятидесяти до ста МРОТ. Второй состав прямым образом соотносится с обязанностью редакции сохранять конфиденциальность источника

информации, а также сведений, предоставленных гражданином с условием сохранения их в тайне (ч. 1 и 2 ст. 41 Закона РФ о СМИ)[1]. Данные действия караются наложением административного штрафа на граждан в размере от пяти до десяти МРОТ; на должностных лиц — от сорока до пятидесяти МРОТ.

Ответственность за нарушение законодательства о рекламе, в частности за отказ от контррекламы и ненадлежащую рекламу (ст. 14.3), КоАП РФ устанавливает для юридических лиц на уровне от четырехсот до пятисот МРОТ. Кроме ответственности за данный состав, КоАП РФ вводит еще один состав, также имеющий отношение к Закону о рекламе. Согласно КоАП РФ использование государственных символов (флага, герба, гимна) в нарушение установленных правил влечет наложение административного штрафа на граждан в размере от трех до пяти МРОТ; на должностных лиц — от пяти до десяти МРОТ (ст. 17.10).

Изменения в избирательном законодательстве затрагивают и круг субъектов такого правонарушения, как «непредставление возможности обнародовать опровержение или иное разъяснение в защиту чести, достоинства или деловой репутации». Дело в том, что данная обязанность возлагается не только на государственные и муниципальные СМИ, но и на частные СМИ. Поэтому при проведении выборов любого уровня к ответственности за ее невыполнение привлекаются все СМИ независимо от того, к какой форме собственности они относятся. Административный штраф налагается на должностных лиц в размере от двадцати до тридцати МРОТ; на юридических лиц — от ста до двухсот МРОТ.

Рассмотрим теперь **административную ответственность за нарушение права на получение информации.**

Согласно ст. 38 Закона РФ о СМИ граждане имеют право на оперативное получение через средства массовой информации достоверных сведений о деятельности государственных органов и организаций, общественных объединений, их должностных лиц.

[1] Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» // ВВС РФ. 1992. № 7. Ст. 300.

В КоАП РСФСР отсутствовала ответственность за отказ в предоставлении редакции СМИ информации, в связи с чем единственно возможными видами ответственности за эти действия являлись дисциплинарная, гражданская и уголовная ответственность.

В соответствии с КоАП РФ нарушение права на поиск и получение информации является основанием для возбуждения дела об административном правонарушении. Процедура подачи запроса информации и получения ответа редакцией СМИ подкреплена административной санкцией за отказ либо несвоевременное представление информации, как установлено ст. 5.39 КоАП РФ. Размер штрафа установлен в размере от пяти до десяти МРОТ, т.е. является достаточно низким.

Объективная сторона данного правонарушения, установленная КоАП РФ, практически аналогична объективной стороне преступления («отказ гражданину в предоставлении информации» — ст. 140 УК). Отличие между ними составляет наличие/отсутствие такого элемента, как причинение вреда правам и законным интересам гражданина (при преступлении он всегда присутствует). Поэтому отграничение административного правонарушения от преступления с аналогичным составом происходит именно по объективной стороне, а именно — причинению вреда.

Иное правонарушение — демонстрирование фашистской атрибутики или символики — карается административным штрафом в размере от пяти до десяти МРОТ с конфискацией фашистской атрибутики или символики или административным арестом на срок до пятнадцати суток с конфискацией фашистской атрибутики или символики (ст. 20.3). Примечательно, что, как установлено КоАП РФ, привлечение к ответственности возможно только в случае, если целью демонстрации была пропаганда такой атрибутики или символики. При данной оговорке положительное решение вопроса о привлечении к ответственности может быть принято, если доказано наличие цели демонстрации фашистских символов. Однако только по итогам правоприменительной практики — в отсутствие соответствующей

конкретизации в законодательстве — можно будет судить о том, в каких случаях демонстрация будет признаваться целенаправленной. Опять же, подобная ситуация может негативно отразиться на взаимоотношениях редакций СМИ с правоприменительными органами.

За действия, образующие три состава административных правонарушений, КоАП РФ предусмотрена ранее отсутствовавшая ответственность. К таким действиям относятся: воспрепятствование осуществляемому на законном основании распространению продукции средства массовой информации либо установление незаконных ограничений на розничную продажу тиража периодического печатного издания (13.16); нарушение правил распространения обязательных сообщений (13.17); воспрепятствование уверенному приему радио- и телепрограмм (13.18). Необходимость установления ответственности за действия, которые описаны в составах этих правонарушений, вытекает из ст. 60 Закона РФ о СМИ. Последний был принят, как известно, в конце 1991 г. Таким образом, потребовалось более 15 лет, для того чтобы эта норма перестала быть бланкетной и появились основания для привлечения к административной ответственности за данные действия.

Ответственность за следующий состав административного правонарушения — нарушение правил распространения обязательных сообщений — заключается в наложении административного штрафа на граждан — от одного до трех МРОТ; на должностных лиц — от трех до пяти МРОТ; на юридических лиц — от тридцати до пятидесяти МРОТ. Воспрепятствование уверенному приему радио- и телепрограмм путем создания искусственных помех карается наложением административного штрафа на граждан в размере от пяти до десяти МРОТ; на должностных лиц — от десяти до двадцати МРОТ; на юридических лиц — от ста до двухсот минимальных размеров оплаты труда.

Не подверглись существенным изменениям такие составы административных правонарушений, как нарушение порядка изготовления или распространения продукции сред-

ства массовой информации (13.21) и нарушение порядка объявления выходных данных (13.22). В отношении первого можно отметить, что отныне нарушением порядка распространения признается распространение продукции СМИ не только незарегистрированного, но также и СМИ, не прошедшего перерегистрацию. Наложение взыскания возможно и на основании факта изготовления или распространения продукции СМИ после решения о прекращении или приостановлении выпуска СМИ в установленном порядке. За данное правонарушение административный штраф может налагаться на граждан в размере от десяти до пятнадцати МРОТ с конфискацией предмета административного правонарушения; на должностных лиц — от двадцати до тридцати МРОТ с конфискацией предмета административного правонарушения; на юридических лиц — от двухсот до трехсот МРОТ с конфискацией предмета административного правонарушения. Что же касается ответственности за нарушение порядка объявления выходных данных, то здесь корректировка была проведена в отношении размера штрафов. Данное правонарушение влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти МРОТ с конфискацией продукции средства массовой информации или без таковой; на должностных лиц — от пяти до десяти МРОТ с конфискацией продукции средства массовой информации или без таковой; на юридических лиц — от пятидесяти до ста МРОТ с конфискацией продукции средства массовой информации или без таковой.

Отсюда следует, что при административном судопроизводстве могут быть наложены следующие виды административных взысканий:

— предупреждение — мера административного наказания, выраженная в официальном порицании физического или юридического лица, выносимого в письменной форме;

— административный штраф — денежное взыскание;

—- возмездное изъятие орудия совершения или предмета административного правонарушения — принудительное изъя-

тие и последующая реализация с передачей бывшему собственнику вырученной суммы, за вычетом расходов на реализацию;

— конфискация орудия совершения или предмета административного правонарушения;

— лишение специального права;

— административный арест;

— административное выдворение за пределы РФ иностранного гражданина или лица без гражданства;

— дисквалификация — лишение права занимать руководящие должности в исполнительных органах управления юридических лиц;

— административное приостановление деятельности.

Закон о правовой охране программ для электронных вычислительных машин и баз данных устанавливает (ст. 17) следующее.

1. Физическое или юридическое лицо, которое не выполняет требований настоящего Закона в отношении исключительных прав правообладателей, в том числе ввозит в РФ экземпляры программы для ЭВМ или базы данных, изготовленные без разрешения их правообладателей, является нарушителем авторского права.

2. Контрафактными признаются экземпляры программы для ЭВМ или базы данных, изготовление или использование которых влечет за собой нарушение авторского права.

3. Контрафактными являются также экземпляры охраняемой в РФ в соответствии с настоящим Законом программы для ЭВМ или базы данных, ввозимых в РФ из государства, в котором эта программа для ЭВМ или база данных никогда не охранялись или перестали охраняться законом.

Статья 18. Защита прав на программу для ЭВМ и базу данных.

1. Автор программы для ЭВМ или базы данных и иные правообладатели вправе требовать:

— признания прав;

— восстановления положения, существовавшего до нарушения права, и прекращения действий, нарушающих право или создающих угрозу его нарушения;

— возмещения причиненных убытков, в размер которых включается сумма доходов, неправомерно полученных нарушителем;

— выплаты нарушителем компенсации в определяемой по усмотрению суда, арбитражного или третейского суда сумме от 5000-кратного до 50000-кратного установленного законом размера минимальной месячной оплаты труда в случаях нарушения с целью извлечения прибыли вместо возмещения убытков;

— помимо возмещения убытков или выплаты компенсации по усмотрению суда или арбитражного суда может быть взыскан штраф в размере десяти процентов от суммы, присужденной судом или арбитражным судом в пользу истца, в доход республиканского бюджета РФ;

— принятия иных предусмотренных законодательными актами мер, связанных с защитой их прав.

За защитой своего права правообладатели могут обратиться в суд, арбитражный или третейский суд.

Суд или арбитражный суд может вынести решение о конфискации контрафактных экземпляров программы для ЭВМ или базы данных, а также материалов и оборудования, используемых для их воспроизведения, и об их уничтожении либо о передаче их в доход республиканского бюджета РФ либо истцу по его просьбе в счет возмещения убытков.

Статья 19. Арест контрафактных экземпляров программы для ЭВМ или базы данных. На экземпляры программы для ЭВМ или базы данных, изготовленные, воспроизведенные, распространенные, проданные, ввезенные или иным образом использованные либо предназначенные для использования в нарушение прав автором программы для ЭВМ или базы данных и иных правообладателей, может быть наложен арест в порядке, установленном законом.

2. Уголовная ответственность

Уголовная ответственность в этой сфере может наступить в случаях, предусмотренных Уголовным кодексом РФ.

Последствия неправомерного использования информации могут быть самыми разнообразными — это не только нарушение

неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия: отрасли и т.д. Поэтому совершенно оправданно то, что преступления данного вида помещены в раздел IX «Преступления против общественной безопасности и общественного порядка». Таким образом, если исходить из учения о четырехзвенной структуре объекта преступления, общим объектом компьютерных преступлений будет выступать совокупность всех общественных отношений, охраняемых уголовным законом: родовым — общественная безопасность и общественный порядок и видовым — совокупность общественных отношений по правомерному и безопасному использованию информации. Непосредственный объект трактуется исходя из названий и диспозиций конкретных статей. Чаще всего непосредственный объект основного состава компьютерного преступления сформулирован альтернативно, в квалифицированных составах количество их, естественно, увеличивается[1].

Практически все анализируемые преступления относятся к преступлениям средней тяжести, т.е. их максимальная наказуемость в виде лишения свободы не превышает 5 лет. Исключением является лишь создание, использование и распространение вредоносных программ для ЭВМ, повлекшее по неосторожности тяжкое последствие, которое наказывается лишением свободы на срок от 3 до 7 лет и поэтому относится к тяжким преступлениям. При характеристике объективной стороны рассматриваемых составов отмечается, что большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также установление причинной связи между этими двумя признаками. Однако в силу ч. 2 ст. 9 УК РФ вре-

[1] *Симкин Л.* Как остановить компьютерное пиратство // Российская юстиция. 1996. № 10.

менем совершения каждого из этих преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают здесь в форме действий и лишь иногда — как бездействие. В одном случае такой признак объективной стороны состава преступления, как способ его совершения, сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных он, а также время, место, обстановка, орудия, средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств[1].

Из всех признаков субъективной стороны значение будет иметь только один — вина. При этом исходя из ч. 2 ст. 24 УК РФ для всех преступлений данного вида необходимо наличие вины в форме умысла, и лишь два квалифицированных состава предусматривают две ее формы, умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных последствий. Факультативные признаки субъективной стороны так же, как и в вопросе о стороне объективной, не будут иметь значения для квалификации преступления. Так, мотивами совершения таких деяний чаще всего бывают корысть либо хулиганские побуждения, но могут быть и соображения интереса, чувство мести, не исключено совершение их с целью скрыть другое преступление и т.д. Естественно, что особую трудность вызовет проблема отграничения неосторожного и невиновного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в сетях и системах ЭВМ[2].

Субъект нескольких составов является специальным. В остальных случаях им может стать, в принципе, любой че-

[1] *Симкин Л.* Как остановить компьютерное пиратство // Российская юстиция. 1996. № 10.

[2] Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. М.: Юрист, 2001.

ловек, особенно если учесть всевозрастающую компьютерную грамотность населения. Ответственность за преступления против компьютерной безопасности наступает с 16-летнего возраста (ст. 20 УК)[1].

Диспозиции статей 28-й главы описательные, зачастую — бланкетные или отсылочные. Так, для применения ряда их необходимо обратиться к ст. 35 УК, к нормативно-правовому акту об охране компьютерной информации, правилам эксплуатации ЭВМ и т.п.

Санкции — альтернативные, за исключением двух квалифицированных составов, где они — в силу тяжести последствий преступления — «урезаны» до относительно-определенных[2].

Существуют статьи, которые тоже применяются, помимо главы 28, в судебном делопроизводстве при компьютерных преступлениях, а именно статьи главы 21 «Преступления против собственности» Уголовного кодекса РФ.

Статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений». Наказание предусматривает в худшем случае ограничение свободы на срок до трех лет.

Статья 158 «Кража». Наказание предусматривает в худшем случае лишение свободы на срок до десяти лет со штрафом.

Статья 159 «Мошенничество». Наказание предусматривает в худшем случае лишение свободы на срок от пяти до десяти лет со штрафом либо без такового.

Статья 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием». Наказание предусматривает в худшем случае лишение свободы на срок до пяти лет со штрафом или без такового.

Преступления против конституционных прав и свобод человека и гражданина.

---

[1] Уголовный кодекс РФ.

[2] *Гульбин Ю.* Преступления в сфере компьютерной информации // Российская юстиция. 1997. № 10.

Статья 140 УК РФ предусматривает наступление ответственности за отказ в предоставлении гражданину информации. Так как Конституцией РФ закреплена обязанность органов государственной власти и органов местного самоуправления, их должностных лиц предоставить каждому гражданину возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ч. 2 ст. 24), то Уголовный кодекс РФ установил ответственность за отказ в предоставлении гражданину информации.

Предусмотренное ст. 140 УК преступление заключается в следующем: в неправомерном отказе предоставить соответствующую информацию либо в предоставлении неполной или заведомо ложной информации. Отказ является неправомерным, если он противоречит требованиям закона или иного нормативного акта. Отказ может быть выражен в различной форме: устно, письменно, а также путем бездействия. Предоставление неполной информации означает ознакомление гражданина не со всеми документами и материалами, затрагивающими его права и свободы. Под предоставлением заведомо ложной информации имеется в виду сообщение сведений, не соответствующих действительности, должностным лицом, знающим, что сообщаемые сведения являются ложными[1]. Кроме того, обязательными признаками состава преступления здесь являются: во-первых, причинение вреда правам и законным интересам граждан. Во-вторых, субъектом данного преступления может быть только должностное лицо, которое в силу занимаемого им положения располагает или может располагать информацией, затрагивающей права и свободы конкретного гражданина.

Статья 237 Уголовного кодекса РФ предусматривает наступление ответственности за сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей.

---

[1] Комментарий к Уголовному кодексу РФ / Отв. ред. В.М. Лебедев. М, 2003. С. 317.

Под сокрытием имеется в виду утаивание, недоведение до сведения лиц, имеющих право на получение такой информации, либо отказ в ее предоставлении. Под искажением понимается предоставление заведомо ложных либо неполных сведений, вводящих заинтересованные лица в заблуждение относительно наличия и размеров опасности для жизни и здоровья людей либо для окружающей среды[1].

Характерными признаками данного преступления являются: во-первых, совершение его с прямым умыслом, т.е. лицо осознает, что искажает или скрывает информацию, и желает этого. Во-вторых, субъектом преступления может быть как должностное лицо, так и недолжностное (например, владелец или собственник информационных ресурсов и систем), обязанное обеспечивать население соответствующей информацией. В-третьих, скрываемая или искажаемая информация должна быть документированной, т.е. зафиксированной на материальном носителе с реквизитами, позволяющими ее идентифицировать. Очевидно, что сокрытие различных предположений, слухов, чьих-то мнений и т.п. не образует состава преступления.

Статья 287 УК РФ предусматривает ответственность за отказ в предоставлении информации (документов, материалов) Федеральному Собранию РФ или Счетной палате РФ или уклонение от предоставления информации либо предоставление заведомо неполной или ложной информации вышеуказанным органам, если эти деяния совершены должностным лицом, обязанным предоставлять такую информацию. В данной статье не конкретизируется характер той информации (документов, материалов), которая должна быть предоставлена Федеральному Собранию РФ или Счетной палате РФ, таким образом, можно сделать вывод, что требуемая этими органами информация (отчеты, справки, материалы проверок и т.п.) может касаться различных вопросов, решение которых входит в компетенцию запрашиваемых органов. Что же касается запрашиваемых ор-

[1] Комментарий к Уголовному кодексу РФ / Отв. ред. В.М. Лебедев. М., 2003. С. 497.

ганов, то в соответствии со ст. 13 Федерального закона от 11 января 1995 г. «О Счетной палате РФ» все органы государственной власти в РФ, органы местного самоуправления, Центральный Банк РФ, предприятия, учреждения, организации независимо от форм собственности и их должностные лица обязаны предоставлять по запросам Счетной палаты информацию, необходимую для обеспечения ее деятельности[1].

Кроме того, совершение указанных действий в отношении комитетов и комиссий палат Федерального Собрания либо в отношении отдельных членов Совета Федерации, депутатов Государственной Думы или аудиторов Счетной палаты также образуют состав преступления[2].

Отличительным признаком данного состава является то, что субъектом преступления может быть должностное лицо, причем такое, на которое возложена обязанность по предоставлению информации в перечисленные государственные органы.

Выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет за собой уголовную ответственность в соответствии с законом.

3. Гражданско-правовая ответственность

Гражданско-правовая ответственность — ч. 2 ст. 139 Гражданского кодекса: за нарушение нормативно регулирующих информационно-имущественных отношений (исключительные права в авторском праве), а также возмещение морального вреда и имущественного вреда в случае разглашения порочащих сведений.

При предъявлении при регистрации требований, не предусмотренных в Законе о СМИ, нарушителем законодательства о СМИ выступают регистрирующие СМИ органы. Они будут нести гражданскую ответственность в случае причинения вреда в связи с незаконными действиями в соответствии со ст. 1069 ГК РФ.

---

[1] СЗ РФ. 1995. № 3. Ст. 167.

[2] Комментарий к Уголовному кодексу РФ / Отв. ред. В.М. Лебедев. М., 2003. С. 617.

Глава 20. Ответственность в области массовой информации

1. Ответственность за распространение запрещенной рекламы

Все виды запрещенной к распространению рекламы могут повлечь административную ответственность в виде предупреждения антимонопольного органа или штрафа.

Заведомо ложная реклама умышленно вводит потребителя в заблуждение. Другими словами, заранее зная о недостоверности сведений о рекламируемом товаре, рекламодатель (рекламопроизводитель, рекламораспространитель) все же эти сведения дает, производит или, соответственно, распространяет. Такая реклама влечет за собой уголовную ответственность в виде штрафа от 200 до 500 минимальных размеров оплаты труда, либо обязательных работ на срок от 180 до 240 часов, либо ареста на срок от 3 до 6 месяцев, либо лишения свободы на срок до двух лет (ст. 182 УК РФ).

Совершенная повторно в течение года после административного взыскания за те же действия ненадлежащая реклама — в любом из вышеперечисленных проявлений — также должна повлечь за собой уголовную ответственность. Однако Уголовный кодекс подобного состава преступления, увы, не предусматривает, и фактически ответственность не наступает.

Рекламодатель несет ответственность за содержание информации, которая передается в рекламном сообщении. Рекламопроизводитель несет ответственность за этап подготовки рекламы — в том случае, если он совершил какую-то ошибку в этом процессе, скажем, перепутал слова местами, добавил «не» либо, наоборот, убрал «не» в рекламном сообщении.

Рекламораспространитель несет ответственность в той части, которая имеет отношение прежде всего к месту, времени и средству размещения рекламы. Если рекламу определенных товаров нельзя распространять в дневное время, естественно, ответственность за нарушение этого положения несет рекламораспространитель, если рекламу каких-то товаров

нельзя распространять вблизи детских учреждений либо церквей и т.п., то за нарушение этого также несет ответственность рекламораспространитель (ст. 38 Закона о рекламе).

Не отвечая за достоверность содержания рекламы, редакции средств массовой информации тем не менее имеют право требовать от рекламодателя предъявления документальных подтверждений истинности характеристик рекламируемого товара. Однако редакции не нарушают закон и не несут ответственности, если не воспользуются этим правом. Если деятельность рекламодателя подлежит лицензированию, то при рекламе соответствующего товара (будь то недвижимость, оружие, медикаменты или др.), а также при рекламе самого рекламодателя рекламораспространитель обязан потребовать предъявления, а рекламодатель — предоставить лицензию либо ее надлежащим образом заверенную копию. Заметим, что производство и реализация большой части товаров и услуг, которые рекламируются, требуют в нашей стране лицензии — лицензии на сделки с недвижимостью, лицензии на туристические и банковские услуги, лицензии на торговлю табаком и алкоголем и т.д.

Получается, что все, что можно производить, все услуги, которые можно оказывать только после получения лицензии, рекламировать можно только после ее получения. Если вы хотите рекламировать оружие, то сначала нужно получить лицензию на производство оружия, а потом уже рекламировать оружие. На самом деле это не так уж просто, ведь возможна ситуация, когда хотят рекламировать магазин еще до того, как его построят и откроют. Но это невозможно до получения лицензии на право торговли.

Хранить рекламные материалы рекламораспространитель обязан в течение года со дня последнего их распространения. Эти материалы, а также другую информацию, необходимую для осуществления своих полномочий государственными контрольными органами, уполномоченными следить за соблюдением законодательства в сфере рекламы, рекламораспространители обязаны предоставлять по первому их требованию.

Полученные сведения, составляющие коммерческую тайну, контрольные органы разглашать не вправе, причем в законодательстве установлена ответственность за разглашение таких сведений (см., например, ст. 12, 13, 128 и 139 ГК РФ).

В газетах и журналах на последней странице часто публикуют объявления о том, что редакция не несет ответственности за содержание публикуемых в номере рекламных сообщений. На самом деле это объявление от ответственности в качестве рекламораспространителя еще ни одну редакцию не освобождало и не освободит. Редакция обязана, даже при получении уже готовой рекламы от уважаемого рекламодателя, убедиться в соблюдении в этом рекламном сообщении положений закона. Редакция не должна проверять правильность указанного в рекламе телефона, адреса, не должна посылать корреспондента, чтобы проверить, действительно ли товар имеется в продаже, но редакция должна убедиться в наличии у рекламодателя всех необходимых лицензий. Редакция также должна проверить, чтобы рекламные сообщения не нарушали положений Конституции и других законов нашей страны. Например, если в тексте рекламы есть слова, которые подрывают устои государственного строя, то за распространение этой рекламы несет ответственность и редакция распространившего ее СМИ.

Следует особо сказать о такой форме ответственности рекламодателей, как контрреклама. Под ней понимается опровержение ненадлежащей рекламы, распространяемое в целях ликвидации вызванных ею последствий. При этом все расходы по контррекламе несет нарушитель. Здесь обычная мера наказания — штрафы — недостаточно эффективна, поскольку уже введенный недопустимой рекламой в заблуждение потребитель может так и не узнать, что товары, которые он покупает, не обладают обещанными характеристиками или даже опасны для здоровья. Нередки случаи, когда компания, опубликовавшая недостоверную рекламу и заплатившая за это штраф, чувствует себя победителем, поскольку объем ее продаж возрос в несколько раз, даже несмотря на последовавший

запрет Министерства по антимонопольной политике на дальнейшее распространение этой рекламы: люди продолжают покупать ее продукцию по инерции. Воспрепятствовать этому может только контрреклама, хотя случаи ее применения пока редки.

2. Ответственность за иные нарушения законодательства о средствах массовой информации

Например, учреждение СМИ через подставное лицо, получение свидетельства о регистрации обманным путем. В этом случае свидетельство о регистрации может быть признано недействительным только судом в порядке гражданского судопроизводства по заявлению регистрирующего органа. Получение свидетельства через подставное лицо есть один из способов получения свидетельства обманным путем.

При получении лицензии на вещание обманным путем согласно п. 1 ч. 1 ст. 32 Закона о СМИ лицензия аннулируется. Аннулирование лицензии производится решением выдавшего его органа.

Следующий вид нарушения законодательства о СМИ — скрытая уступка лицензии. Согласно п. 3 ч. 1 ст. 32 Закона о СМИ при установлении комиссией по телерадиовещанию факта скрытой уступки лицензии лицензия аннулируется.

Неправомерное получение льгот, установленных для специализированных СМИ, также является нарушением законодательства о СМИ. Льготы установлены для СМИ, специализирующихся на сообщениях и материалах для детей и подростков, инвалидов, а также образовательного и культурно-просветительского назначения. Для них установлен пониженный регистрационный сбор.

Ответственность за этот вид нарушения законодательством о СМИ не установлена.

Незаконное изготовление продукции СМИ без его регистрации либо после решения о прекращении или приостановлении его деятельности влечет административную ответственность, предусмотренную в ст. 13.21 КоАП РФ.

Уклонение от перерегистрации (перерегистрация в соответствии со ст. 11 Закона о СМИ требуется при смене учредителя, изменении состава соучредителей, а равно названия, языка, формы периодического распространения СМИ) противоречит интересам СМИ, поскольку в случае уклонения от перерегистрации они вынуждены будут не изготавливать, не распространять свою продукцию, так как согласно ст. 13.21 КоАП за изготовление и распространение продукции для СМИ, не прошедшего перерегистрацию, предусмотрена административная ответственность.

Воспрепятствование осуществляемому на законном основании распространению продукции СМИ либо установление незаконных ограничений на розничную продажу периодического печатного издания влечет административную ответственность в соответствии со ст. 13.16 КоАП РФ.

Незаконное распространение продукции СМИ без его регистрации либо после решения о прекращении или приостановлении его деятельности влечет административную ответственность, предусмотренную в ст. 13.21 КоАП РФ.

Распространение продукции без разрешения на выход в свет влечет дисциплинарные взыскания, предусмотренные ст. 192 ТК РФ.

Осуществление вещания без лицензии либо с нарушением лицензионных условий влечет административную либо уголовную ответственность.

Предусмотрена административная ответственность за осуществление предпринимательской деятельности без специального разрешения (ст. 14.1 КоАП РФ).

Предпринимательская деятельность с нарушением условий, предусмотренных специальными разрешениями (лицензией), влечет административную ответственность. Однако если в результате этих действий был причинен крупный ущерб гражданам, организациям или государству либо указанная деятельность сопряжена с извлечением дохода в крупном размере, то нарушитель несет уже не административную, а уголовную ответственность, предусмот-

ренную в п. 1 ст. 171 УК РФ. Под доходом в крупном размере признается доход, сумма которого превышает 200 МРОТ.

За нарушение правил распространения обязательных сообщений предусмотрена административная ответственность (ст. 13.17 КоАП РФ).

За нарушение правил распространения рекламы предусмотрена административная ответственность (ст. 14.3 КоАП РФ).

Нарушение порядка объявления выходных данных влечет административную ответственность, предусмотренную ст. 13.22 КоАП РФ.

Создание искусственных помех, препятствующих уверенному приему радио- и телепрограмм, влечет административную ответственность в соответствии со ст. 13.18 КоАП РФ.

3. Основания освобождения от ответственности субъектов права массовой информации

Редакция, главный редактор, журналист не несут ответственности за распространение сведений, не соответствующих действительности и порочащих честь и достоинство граждан и организаций, либо ущемляющих права и законные интересы граждан, либо представляющих собой злоупотребление свободой массовой информации и (или) правами журналиста:

1) если эти сведения присутствуют в обязательных сообщениях;

2) если они получены от информационных агентств;

3) если они содержатся в ответе на запрос информации либо в материалах пресс-служб государственных органов, организаций, учреждений, предприятий, органов общественных объединений;

4) если они являются дословным воспроизведением фрагментов выступлений народных депутатов на съездах и сессиях Советов народных депутатов, делегатов съездов, конференций, пленумов общественных объединений, а также официальных выступлений должностных лиц государственных органов, организаций и общественных объединений;

5) если они содержатся в авторских произведениях, идущих в эфир без предварительной записи, либо в текстах, не подлежащих редактированию в соответствии с настоящим Законом;

6) если они являются дословным воспроизведением сообщений и материалов или их фрагментов, распространенных другим средством массовой информации, которое может быть установлено и привлечено к ответственности за данное нарушение законодательства РФ о средствах массовой информации.

Дословное воспроизведение в средстве массовой информации в период соответствующей избирательной кампании, кампании референдума агитационного материала, распространенного в другом средстве массовой информации, не является основанием для освобождения журналиста, главного редактора, редакции, иной организации, осуществляющей выпуск средства массовой информации, от ответственности за нарушение законодательства РФ о выборах и референдумах, если при дословном воспроизведении такого материала не соблюдены требования указанного законодательства, предъявляемые к опубликованию (обнародованию) агитационных материалов.

4. Ответственность за ущемление свободы массовой информации

Однако следует отметить, что 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 передачи ему информации, за исключением сведений, составляющих государственную, коммерческую или иную специально охраняемую законом тайну;

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

Обнаружение органов, организаций, учреждений или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, влечет немедленное прекращение их финансирования и ликвидацию в порядке, предусмотренном законодательством РФ.

5. Приостановление выпуска СМИ как особый вид ответственности

Следует отметить еще одну особенность привлечения к ответственности СМИ — это приостановление выпуска СМИ за нарушение законодательства РФ о выборах и референдумах. Федеральный закон от 4 июля 2003 г. № 94-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты РФ в связи с принятием Федерального закона "Об основных гарантиях избирательных прав и права на участие в референдуме граждан РФ"» дополнил Закон о СМИ новой ст. 16.1 «Приостановление выпуска средства массовой информации за нарушение законодательства РФ о выборах и референдумах» следующего содержания:

«Если в период избирательной кампании, кампании референдума после вступления в силу решения суда о привлечении главного редактора или редакции радио- и телепрограммы, пе-

риодического печатного издания, иной организации, осуществляющей выпуск средства массовой информации... к административной ответственности за нарушение законодательства РФ о выборах и референдумах этот главный редактор или эта организация допустит повторное нарушение законодательства РФ о выборах и референдумах, Центральная избирательная комиссия РФ... вправе обратиться в федеральный орган исполнительной власти, осуществляющий регистрацию средств массовой информации, с представлением о приостановлении выпуска средства массовой информации, использованного в целях совершения указанных нарушений. Указанный федеральный орган исполнительной власти в пятидневный срок, но не позднее дня, предшествующего дню голосования, а в день, предшествующий дню голосования, и в день голосования немедленно осуществляет с привлечением заинтересованных лиц проверку фактов, изложенных в представлении, и обращается в суд с заявлением о приостановлении выпуска средства массовой информации... Приостановление выпуска средства массовой информации... осуществляется судом на срок до момента окончания голосования на выборах, референдуме, а в случае, если проводится повторное голосование, — до момента окончания повторного голосования».

Рассматриваемая поправка «находится в глубоком противоречии с требованиями российской Конституции и законов», — утверждает М.А. Федотов. Во-первых, она вводит неадекватное ограничение свободы массовой информации. Напомним, что при рассмотрении дел, связанных с проблемой ограничения права человека на информацию, Конституционный Суд РФ придерживается правовой позиции, согласно которой всякое подобное ограничение должно быть соразмерно конституционно признаваемым целям такого ограничения.

Во-вторых, ст. 16.1 Закона о СМИ противоречит основополагающим нормам Кодекса РФ об административных правонарушениях. На это было обращено внимание в заключении Правового управления Государственной Думы по проекту Федерального закона от 4 июля 2003 г. № 94-ФЗ, где указывалось: «В предлагаемой части 5 новой статьи 16.1 Закона фактически раскрыта

объективная сторона некоторых правонарушений законодательства о выборах и референдумах, что может повлечь за собой конкуренцию действующих и проектируемых норм, в том числе и Кодекса РФ об административных правонарушениях. В этой связи также обращаем внимание, что согласно ст. 1.1 и 1.3 КоАП РФ, установление административной ответственности, в том числе за нарушение правил и норм, предусмотренных федеральными законами, а также порядка производства по делам об административных правонарушениях, допускается именно в КоАП РФ, а не в иных законодательных актах».

Если рассматривать приостановление выпуска СМИ как меру пресечения административного правонарушения, то налицо явная коллизия с положениями ст. 27.1 КоАП РФ, которая разрешает в целях пресечения административного правонарушения применять только такие меры, как осмотр принадлежащих юридическому лицу помещений, изъятие вещей и документов, арест товаров и иных вещей и т.д. В КоАП РФ просто нет такой меры пресечения, как приостановление или запрет выпуска средства массовой информации.

Если же рассматривать приостановление выпуска СМИ как административное наказание, то возникает противоречие со ст. 3.2 КоАП РФ, содержащей исчерпывающий перечень видов административных наказаний. Данная статья устанавливает, что в отношении юридических лиц наказания, за исключением предупреждения и штрафа, могут устанавливаться только самим Кодексом, а значит, никак не Законом о СМИ.

Глава 21. Особенности ответственности в сети «Интернети

1. Уголовная ответственность в Интернете

При размещении информации на интернет-сайте уголовная ответственность может возникать в случае, если размещение такой информации связано с распространением заведомо ложных сведений, порочащих честь, достоинство другого лица

или подрывающих его репутацию (ст. 129 Уголовного кодекса РФ от 13 июня 1996 г. № 63-ФЗ[1]). Гражданская ответственность возникает в соответствии со ст. 152 части первой Гражданского кодекса РФ от 30 ноября 1994 г. № 51-ФЗ[2], которая предусматривает, что гражданин вправе требовать *по* суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Правила указанной статьи о защите деловой репутации гражданина соответственно применяются к защите деловой репутации юридического лица.

И.М. Рассолов по этому поводу отмечал, что «став неотъемлемой частью жизни, Интернет вместе с тем зачастую используется для совершения правонарушений, посягающих на конституционные права и законные интересы личности. Он в итоге становится источником противоправных, антиобщественных проявлений»[3].

Деловая репутация юридического лица — одно из условий его успешной деятельности. Деловая репутация гражданина характеризует его как работника (профессионала в какой-либо области), представляет собой оценку его качеств, значимых для востребованности на рынке труда.

Положительная деловая репутация имеет определяющее значение как для крупной, так и маленькой компании, так и для гражданина.

Опорочить деловую репутацию лица в сети «Интернет» несложно. Недобросовестные субъекты могут использовать для этого различные инструменты: многочисленные форумы на интернет-сайтах, доски бесплатных объявлений, ленты средств массовой информации на интернет-сайтах, электронные рассылки, аналитические и сравнительные обзоры и т.д.

---

[1] СЗ РФ. 1996. № 25. Ст. 2954.

[2] СЗ РФ. 1994. № 32. Ст. 3301.

[3] *Рассолов И.М.* Право и Интернет. Теоретические проблемы. М., 2003. С. 200.

На практике часто встречаются ссылки о том, что такой-то товар некачественный, такая-то компания обманывает клиентов и т.д. В результате деловая репутация компании, которая пользуется нелестными отзывами, дискредитируется, отсюда потеря потенциальных клиентов, финансовые потери, падение престижа, курса акций, утрата деловых партнеров и т.д.

Возможно установление ответственности в Интернете, в т.ч. уголовной, в отношении провайдеров, предоставляющих доступ к информации, неуместной для несовершеннолетних, а также иной информации. Этот подход применяется в некоторых австралийских штатах, в США (хотя в США пока нет ни федерального закона, ни закона штата, которые придавали бы этим действиям законную силу). В России также устанавливается уголовная и административная ответственность за злоупотребление свободой массовой информации. Статья 242 УК РФ устанавливает ответственность за незаконное распространение порнографических материалов или предметов, ч. 2 ст. 280 УК РФ — публичные призывы к осуществлению экстремистской деятельности с использованием средств массовой информации.

2. Административная ответственность в Интернете

Статья 13.15 Кодекса РФ об административных правонарушениях устанавливает ответственность за изготовление и (или) распространение относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье. Кроме того, ст. 16 Закона РФ «О средствах массовой информации» устанавливает, что деятельность средства массовой информации может быть прекращена или приостановлена судом в порядке гражданского судопроизводства по иску регистрирующего органа. Основанием для такого прекращения являются неоднократные в течение двенадцати месяцев нарушения редакцией требований закона о недопустимости зло-

употребления массовой информацией, по поводу которых регистрирующим органом или органом государственной власти в сфере печати, телерадиовещания и средств массовых коммуникаций РФ делались письменные предупреждения учредителю и (или) редакции (главному редактору), а равно неисполнение постановления суда о приостановлении деятельности средства массовой информации. Деятельность средства массовой информации может быть также прекращена в порядке и по основаниям, предусмотренным Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»[1]. Статья 12 указанного Закона запрещает использование сетей связи общего пользования для осуществления экстремистской деятельности. В противном случае применяются меры, предусмотренные в данном законе, с учетом законодательства РФ о связи.

Несмотря на законодательное закрепление в России соответствующих мер ответственности за злоупотребление свободой массовой информации, проблема размещения в Интернете нелегальной информации остается актуальной. В связи с чем представляется целесообразным наряду с установлением мер ответственности проводить политику стимулирования добровольного применения пользователями фильтрующих устройств.

3. Гражданская ответственность в Интернете

Использование интернет-сайта может явиться причиной нарушения прав граждан и юридических лиц. Вайшнурс А.А. по этому поводу отмечал, что Интернет сегодня «является ярко выраженным примером произвола в области права человека на доброе имя. Тому есть несколько причин: новизна данного средства распространения массовой информации, скудность специального законодательства в этой области, отсутствие широкой судебной и административной практики, отсутствие значительного числа квалифицированных в обла-

[1] СЗ РФ. 2002. № 30. Ст. 3031.

сти интернет-технологий юристов как в судейском, так и адвокатском корпусе»[1].

Действия граждан и юридических лиц по размещению информации на интернет-сайте могут также нарушать нормы законодательства об авторских и смежных правах.

Большая часть правонарушений в сети «Интернет» связана с нарушением прав на результаты интеллектуальной деятельности. Прежде всего это распространение произведений без разрешения (лицензии) правообладателей.

«Взаимодействие двух систем — авторского права и Интернета — не ограничивается простым "пересечением" их свойств. Интернет оказался технологией, которая способна сыграть для авторского права роль, не менее значимую, чем изобретенная И. Гутенбергом машина для книгопечатания. В свою очередь, авторское право во многом обусловливает пути и степень развития сети Интернет»[2].

Примером незаконного использования объектов интеллектуальной собственности при размещении информации на интернет-сайте могут служить получившие широкое распространение в сети «Интернет» так называемые музыкальные архивы (MP3-архивы), электронные библиотеки, галереи фотографий, видеоархивы. Как правило, размещение информации в данных архивах происходит без ведома автора и правообладателя, без выплаты им вознаграждений за использование их произведений, авторские договоры не заключаются.

Электронно-цифровая форма объектов интеллектуальной собственности в сети «Интернет» имеет несколько отличную от иных возможных форм природу. Но это не причина для того, чтобы ставить под сомнение саму возможность существования этих объектов в Интернете и в подобных ему других информационных сетях. Поэтому не может быть сомнений

[1] *Вайшнурс А.А.* Способы защиты чести, достоинства и деловой репутации в случае публикации ложных порочащих сведений в Интернете // Кодекс-info. 2002. № 11-12. С. 140.

[2] *Кобелев Ю.* Авторское право и Интернет// http://www.russianlaw.net/law/doc/al42.htm.

относительно того, что при использовании произведений автора в Интернете затрагивается его право[1]: существует — значит поддается регулированию.

Размещение (воспроизведение) произведения на интернет-сайте возможно только на основании договора с правообладателем/автором либо его соответствующего разрешения. Если у владельцев интернет-сайта нет такого разрешения (договора), значит, нарушаются авторские права, защищаемые законом (объем нарушения определяется в каждом конкретном случае).

Решением данной проблемы может служить институт коллективного управления имущественными правами, предусмотренный разделом IV Закона «Об авторском и смежных правах». В целях обеспечения имущественных прав авторов, исполнителей, производителей фонограмм и иных обладателей авторских и смежных прав в случаях, когда их практическое осуществление в индивидуальном порядке затруднительно (публичное исполнение, в том числе на радио и телевидении, воспроизведение произведения путем механической, магнитной и иной записи, репродуцирование и другие случаи), могут создаваться организации, управляющие имущественными правами указанных лиц на коллективной основе.

Такие организации создаются непосредственно обладателями авторских и смежных прав и действуют в пределах полученных от них полномочий на основе устава, утверждаемого в порядке, установленном законодательством.

Допускается создание либо отдельных организаций по различным правам и различным категориям обладателей прав, либо организаций, управляющих разными правами в интересах разных категорий обладателей прав, либо одной организации, одновременно управляющей авторскими и смежными правами.

---

[1] *Хромова А.Л.* Интернет и авторские права: симбиоз или антагонизм//http://www.copyright.ru/publ-429.html

Российское общество по коллективному управлению правами авторов и иных правообладателей в сферах мультимедиа, цифровых сетей и визуальных искусств (РОМС) занимается реализацией авторских прав в цифровых сетях, в том числе: 1) в Интернете; 2) при создании и использовании продуктов мультимедиа.

Так, размещение музыкальных произведений на интернет-сайте mp3.sarbc.ru осуществляется на основании Лицензионного соглашения с РОМС, которое предоставляет право при условии выплаты вознаграждения для авторов, правообладателей и субъектов смежных прав использовать музыкальные произведения при осуществлении с помощью цифровых сетей (в том числе Интернета) загрузки файлов, содержащих такие произведения, а также при предоставлении иным лицам возможности осуществлять такую загрузку.

Характерным правонарушением при размещении информации на интернет-сайтах является нарушение норм законодательства о рекламе.

В соответствии со ст. 3 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе» реклама — это информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

Юридические лица или граждане (рекламодатели, рекламопроизводители и рекламораспространители) за нарушение законодательства РФ о рекламе несут гражданско-правовую ответственность в соответствии с законодательством РФ.

Лица, права и интересы которых нарушены в результате ненадлежащей рекламы, вправе обратиться в установленном порядке в суд, арбитражный суд с исками, в том числе с исками о возмещении убытков, включая упущенную выгоду, возмещении вреда, причиненного здоровью и имуществу, компенсации морального вреда, публичном опровержении ненадлежащей рекламы.

4. Ответственность провайдеров в Интернете

Ответственность провайдеров базируется на том, что они имеют организационно-техническую возможность в любой момент времени воздействовать на информационные общественные отношения своих пользователей. Форма воздействия может быть довольно разнообразной: от блокирования информационного обмена до информирования третьих лиц о содержании передаваемой информации[1]. Действительно, оператор связи в любой момент может приостановить доступ пользователя к интернет-сайту, определить сетевые реквизиты пользователя, разместившего информацию. Обязанность по информированию третьих лиц относительно информации и пользователей (потребителей) информации возлагается на операторов связи государством. Условия осуществления деятельности по предоставлению услуг связи, содержащиеся в лицензиях, выдаваемых операторам, предусматривают, что лицензиат при разработке, создании и эксплуатации сети связи обязан в соответствии с законодательством РФ оказывать содействие и предоставлять органам, осуществляющим оперативно-розыскную деятельность, возможность проведения оперативно-розыскных мероприятий на сети связи. Статья 64 Федерального закона о связи указывает на то, что операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

Указанная многомерность отношений, а также тот факт, что оператор связи имеет техническую возможность в любой момент воздействовать на интернет-отношения своих пользо-

[1] *Наумов В. Проблема* ответственности информационных провайдеров//Материалы третьей всероссийской конференции «Право и Интернет: теория и практика» // http://www.russianlaw.net/law/books/book-law-net.htm

вателей, определили появление института ответственности операторов связи.

Существует три подхода к проблеме ответственности оператора связи за информацию, размещенную на интернет-сайте.

Первый подход предполагает, что оператор связи несет ответственность за все действия пользователей вне зависимости от наличия у него как у субъекта права знания о совершаемых действиях.

Второй подход освобождает оператора связи от ответственности за действия пользователей в том случае, если выполняет определенные условия, связанные с характером предоставления услуг и взаимодействием с субъектами информационного обмена и лицами, чьи права нарушаются действиями пользователей.

Согласно третьему подходу оператор связи не отвечает за действия пользователей.

В Китае и странах Ближнего Востока, например, используется первый подход, в Европе — второй. Так, в Европейской директиве по электронной коммерции от 28 февраля 2000 г. (разд. 4, ст. 12—15) проработано наиболее детально решение проблемы указанного вида юридической ответственности.

Директива устанавливает, что провайдер не несет ответственности за передаваемую информацию в случае, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации. При этом допускается временное хранение передаваемой информации для осуществления необходимых технических действий по ее передаче. Утверждается, что провайдер не несет ответственности за действия пользователей при предоставлении услуг хостинга, если он не был осведомлен об их противозаконной информационно-правовой деятельности и после получения информации об этом прекратил размещение или доступ к информации.

В настоящее время в ряде стран мира приняты предметные законы, касающиеся института ответственности провайдеров. В шведском законе, регулирующем ответственность

владельцев досок объявлений (Act (1998 : 112) on Responsibility for Electronic Bulletin Boards), устанавливается, что таковые обязаны удалять сообщения третьих лиц в том случае, если содержащаяся в них информация нарушает ряд норм уголовного и гражданского законодательства (в части авторского права)[1]. Так, в марте 2002 г. шведский суд привлек к ответственности по этому закону редакцию газеты «Aftonbladet» за сообщения нацистского содержания, размещенные на форуме сайта газеты. Форум модерировался, но редакторы сайта в течение некоторого времени не могли удалить сообщения по техническим причинам. Несмотря на то что сообщения в конечном счете были удалены, суд признал редакцию виновной (дело Stockholms tingsratt dom 2002—03—07, me* nr B 7655—00). Такой же принцип был применен в деле Playboy Enterprises, Inc. V. Frena (839 F. Supp. 1552 (1993)). Окружной суд штата Флорида признал владельца сайта, чья доска объявлений содержала размещенные третьими лицами фотоматериалы истца и функционировала в режиме открытого доступа, виновным в нарушении авторских прав[2].

В российском законодательстве на сегодняшний день не определена ответственность операторов связи за размещение информации на обслуживаемых ими интернет-сайтах и не установлена возможность предъявления к ним претензий за качество размещаемой информации.

Волков С. и Булычев В. считают, что этот вопрос об ответственности владельцев интернет-сайтов за информацию, размещенную на них, должен решаться в зависимости от того, можно ли установить автора тех сведений, которые расположены на страницах интернет-сайта. В случае, если автора установить невозможно и сведения являются анонимными (а известно, что именно возможность быть анонимным выступает в качестве ха-

[1] *Рассолов И.М.* Право и Интернет. Теоретические проблемы. М., 2003. С. 231.

[2] *Шириков А.* Кто писал — не знаю, за то и отвечаю // эж-ЮРИСТ. 2005. № 12.

рактерной особенности интернет-коммуникаций), надлежащим ответчиком должен выступать владелец интернет-сайта, на котором расположены сведения[1]. Этой же точки зрения придерживается и А. Шириков, указывая, что ответственность владельца сайта может наступать лишь в том случае, когда нет технической возможности установить личность автора сообщения[2]. По его мнению, привлекать владельца сайта к ответственности за факт размещения на нем противоречащих законодательству сообщений возможно лишь в случаях, если:

— сообщение находится на сайте достаточно долго и размещено так, что к нему имеет реальный доступ неограниченный круг пользователей;

— владелец сайта, имея возможность удалить сообщение, не воспользовался ею в течение разумного времени.

Таким образом, провайдер не несет ответственности в случаях, если:

1) незаконные действия пользователя невозможно достоверно выявить;

2) если действия пользователя нарушают обычаи делового оборота;

3) если провайдер не является отправителем электронного документа;

4) не определял получателя электронного документа;

5) не составлял содержание электронного документа;

6) также провайдер не несет ответственности за сохранность документа и не обязан проверять соответствие электронного документа законодательству РФ.

---

[1] *Волков С, Булычев В.* Защита деловой репутации от порочащих сведений // Российская юстиция. 2003. № 8.

[2] *Шириков А.* Невиноватые мы // Экономика и жизнь. 2005. № 15.

ПРИЛОЖЕНИЯ

Приложение 1. Программа курса ««Информационное право»

Цели и задачи преподавания дисциплины

Формирование у студентов-юристов нового мышления, основанного на использовании новейших информационных и информационно-телекоммуникационных технологий, которые активно способствуют развитию экономики, политики, государства на основе становления информационного общества и принципах современного информационного права России.

Формирование у студентов представления об информационных отношениях; субъектах информационно-правовых отношений; о правовом режиме получения, передачи, хранения и использования информации; о юридических аспектах информационного обмена, информационной безопасности, ответственности в информационной сфере.

Подготовка высококвалифицированных специалистов-юристов для работы в органах государственной власти (в том числе в правоохранительных органах) и в других сферах (юридическое обслуживание предпринимательской деятельности, управление организациями, кадровое дело, правовое образование и тд.), способных представлять интересы в области международного информационного обмена, а также способных ориентироваться в проблемах формирования рынка информационных ресурсов и обеспечивать информационную безопасность государства, общества и личности.

Задачи информационного права России:

— определение места и роли информационного права и информационного законодательства в современном информационном обществе;

— изучение организации в России информационно-правового обеспечения органов государственной власти, юридических и физических лиц;

— изучение зарубежного опыта в области регулирования, упорядочивания и защиты отношений, возникающих в сфере создания, сбора, обработки, накопления, хранения, поиска, получения, распространения и применения информации;

— изучение международного информационного законодательства, информационного законодательства РФ, выработка практических навыков применения информационного законодательства;

— активизация решения проблем юридической науки в области информационных отношений в соответствии с новыми общественными потребностями;

— развитие научного творчества студентов-юристов в области информационного права;

— изучение общих институтов и положений информационного права (право доступа к информации, режимы информации, тайна, информационная безопасность, электронная коммерция, информационные ресурсы, Интернет и др.).

Изучение информационного *права позволит студенту решать следующие задачи:*

— уметь вести поиск необходимых нормативно-правовых актов и информационно-правовых норм в системе действующего законодательства, в том числе с помощью автоматизированных информационно-правовых систем;

— квалифицированно толковать и применять законодательство по информационным правонарушениям, информационному рынку, субъектам информационного права и другим проблемам информации и информационных ресурсов;

— выработать навыки творческого мышления для самостоятельного послевузовского повышения знаний законодательства, уровня своей профессиональной подготовки, умения ориентироваться в обширном и динамично развивающемся информационном законодательстве, разрабатывать и решать новые информационно-правовые проблемы.

Методологические основы формирования информационного права как комплексной отрасли права, с одной стороны, — объективная связь информационного права с государственным управлением как видом социального управления, где информация является особым ресурсом государственного управления и средством управляющего воздействия на социальный процесс, с другой стороны — информация является объектом гражданского оборота, обеспечивая методологическую связь информационного права с гражданским правом.

Эти аспекты определяют структуру и содержание информационного права как учебной дисциплины. Учебные материалы должны выработать у студента понимание специфики общественных отношений, урегулированных нормами и институтами российского информационного права. Необходимо изложить учебные материалы, относящиеся к нормам и институтам информационного права, разграничивающим полномочия и компетенцию субъектов информационного права, в том числе учитывая правоохранительный (юридический) профиль подготовки специалистов, государственному контролю и обеспечению информационной безопасности личности, общества и самого государства, а также вопросам ответственности и гарантиям прав различных субъектов в информационной сфере. Специфика изложения и изучения учебного материала на лекциях и семинарах, структура и содержание подробно определяется ниже.

Преподавание информационного права должно иметь геополитическую и прогрессивную направленность, связанную с реализацией задачи: вхождения России в современное информационное общество и ликвидации некоторого отставания в развитии информационной инфраструктуры страны. Изложение учебных материалов должно увязываться с необходимыми историческими и сравнительно-правовыми их пояснениями, объяснением целей общественной значимости норм и институтов информационного права, должно быть направлено на воспитание у студентов чувства сопричастности к судьбам отечества, формирование созидательного мировоззрения будущих юристов.

РАЗДЕЛ I. ОБЩИЕ ПОЛОЖЕНИЯ

Тема 1. Информационное право как отрасль права.

Понятие информации. Виды информации. Документированная и недокументированная информация. Предмет информационно-правового регулирования. Международный характер информационного права. Комплексный характер информационного права. Соотношение информационного права со смежными отраслями права. Особенности формирования информационного права. Методы информационно-правового регулирования.

(Распределение часов: лекции — 4, семинары — 4.)

Тема 2. Информационно-правовые нормы и отношения. Система и источники информационного права.

Информационная норма: понятие, особенности, виды. Информационно-правовые отношения: понятие, соотношение с правовой нормой, структура, защита информационно-правовых отношений. Система информационного права. Понятие и виды источников информационного права.

(Распределение часов: лекции — 2, самостоятельная работа •—2)

Тема 3. Принципы информационного права.

Понятие принципов информационного права. Виды принципов информационного права. Общеправовые принципы. Специальные принципы информационного права.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 4. Правовое регулирование информационной сферы за рубежом.

Особенности информационно-правового регулирования в США. Государственное регулирование информационного рынка в Японии. Организационная структура защиты персонифицированной информации в Германии.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 5. Понятие и виды субъектов информационного права.

Понятие субъекта информационного права. Виды субъектов информационного права. Российская Федерация как субъект информационного права. Субъекты РФ и муниципальные образования. Граждане и другие физические лица. Общественные объединения граждан. Коммерческие юридические лица.

(Распределение часов: лекции — 2, семинары — 2.)

РАЗДЕЛ II. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ

Тема 6. Система органов государственной власти, регулирующих информационную сферу.

Система и полномочия органов государственной власти, обеспечивающих право доступа к информации. Система и компетенция органов, обеспечивающих охрану государственной тайны. Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 7. Правовые режимы информационных ресурсов.

Понятие и виды конфиденциальной информации. Режимы защиты информации. Государственная тайна как предмет, изъятый из гражданского оборота. Служебная тайна и профессиональная тайна. Тайна частной жизни. Коммерческая и другие виды тайн.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 8. Правовое регулирование создания и применения информационных технологий.

Понятие и виды информационных технологий. Порядок создания информационных технологий. Информационные технологии в применении государственными организациями, коммерческими юридическими лицами и физическими лицами: правила эксплуатации и ограничения применения. Нару-

шения порядка применения информационных технологий информационные войны, несанкционированный мониторинг за активностью потребителя информации.

(Распределение часов: лекции — 2, семинары — 4.)

Тема 9. Правовое регулирование создания и применения информационных систем и их сетей.

Понятие и виды информационных систем и сетей. Порядок создания и применения информационных систем и их сетей. Информационные системы связи: Интернет, электронная почта, цифровая связь, мобильная связь. Множественная юрисдикция субъектов правовых отношений в Интернете (разработчик, провайдер, пользователь). Порядок разработки и официальной регистрации программ для ЭВМ и баз данных.

(Распределение часов: лекции — 2, семинары — 4.)

Тема 10. Правовое регулирование информационных ресурсов.

Понятие и виды информационных ресурсов. Порядок формирования информационных ресурсов. Порядок предоставления информационных услуг. Государственное регулирование библиотечного и архивного дела. Особенности государственного регулирования в условиях сетевой работы и работы с базами данных.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 11. Международный информационный обмен и информационный рынок.

Понятие международного информационного обмена Международное и внутригосударственное правовое регулирование глобализации информационной среды. Субъекть правоотношений информационного обмена. Понятие и струю тура информационного рынка. Понятие электронной коммер' ции, ее элементы. Электронное мошенничество.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 12. Внутриорганизационное управление с использованием информационных систем.

Управление в области защиты информации на предприятиях. Особенности внутриорганизационного управления в условиях сетевой работы и работы с корпоративными базами данных. Правовое регулирование телеработы (виртуальный офис с функционированием удаленного или мобильного персонала). Внутриорганизационное управление с использованием информационных технологий. Электронный документооборот. Юридическое значение электронной подписи.

(Распределение часов: лекции — 2, семинары — 4.)

Тема 13. Государственное регулирование средств массовой информации.

Понятие и виды СМИ: традиционные и сетевые. Правовой статус печатных, электронных и телекоммуникационных СМИ. Компетенция органов государственного управления в отношении СМИ. Правовое регулирование использования информационных технологий в политической и коммерческой рекламе (public relations). Организация издательского дела. Понятие электронной публикации.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 14. Права граждан в информационной сфере.

Право на доступ к информации. Право на защиту персонифицированной информации. Право интеллектуальной собственности. Авторские права. Патентные права. Понятие и правовой статус ноу-хау.

(Распределение часов: лекции — 2, семинары — 2.)

Тема 15. Информационно-правовое обеспечение пользователей информации.

Понятие и виды информационно-правовых систем. Российская автоматизированная система информации о нормативных правовых актах. Справочные правовые системы семейства «Консультант-Плюс». Информационная правовая система «Кодекс».

Универсальная система поддержки правоприменения «Гарант». Юридическая справочно-информационная система.

(Распределение часов: лекции — 2, семинары — 2.)

РАЗДЕЛ III. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Тема 16. Понятие и виды информационной безопасности.

Понятие безопасности личности, общества, государства. Понятие обеспечения безопасности. Понятие и виды информационной безопасности.

Тема 17. Информационная безопасность личности.

Понятие информационной безопасности личности. Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений. Запрет цензуры. Ограничения использования информации о частной жизни. Гарантии информационных прав граждан. Право на судебную защиту. Правовые и этические пределы вмешательства в личную жизнь при использовании интерактивных методов работы с аудиторией.

Тема 18. Информационная безопасность общества.

Понятие информационной безопасности общества. Правовое регулирование средств информатизации, телекоммуникации и связи. Правовое регулирование единого информационного пространства РФ.

Тема 19. Информационная безопасность государства.

Понятие информационной безопасности государства. Обеспечение защиты информационных ресурсов от несанкционированного доступа. Обеспечение безопасности информационных и телекоммуникационных систем.

Тема 20. Обеспечение безопасности в глобальном информационном пространстве.

Понятие безопасности в глобальном информационном пространстве. Информационное обеспечение государственной

политики РФ. Правовое регулирование государственных информационных ресурсов.

(Распределение часов по всем темам раздела: лекции — 2, самостоятельная работа — 4.)

РАЗДЕЛ IV. ОТВЕТСТВЕННОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

Тема 21. Ответственность за правонарушения в информационной сфере.

Общая характеристика и виды ответственности за правонарушения в информационной сфере. Дисциплинарная ответственность в информационной сфере. Административная ответственность в информационной сфере. Уголовная ответственность в информационной сфере. Материальная ответственность в информационной сфере.

(Распределение часов: лекции — 2, самостоятельная работа — 4.)

Приложение 2. Словарь терминов

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения о клиентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

Виды доступа информации — обязательное доведение информации до всеобщего сведения; свободный доступ сообщения информации для всеобщего сведения; предоставление информации по запросу (может быть платным).

Виды информационного оружия — обычное оружие, направляемое по целеуказаниям средств радиотехнической разведки с частичным самонаведением на конечном участке; высокоинтеллектуальное — самонаводящиеся боеприпасы; радиочастотные маскирующие помехи; большие уровни электромагнитных или ионизирующих излучений; воздей-

ствие импульсом высокого напряжения через электрическую сеть; воздействие систем связи на ЭВМ; средства генерации естественной речи конкретного человека (изменение голоса).

Виды информационных правоотношений — а) правоотношения, возникающие в области поиска, получения и потребления информации (например, правоотношения, регулируемые ст. 29 Конституции РФ); б) правоотношения, связанные с производством и распределением исходной и производной информации (например, правоотношения в сфере деятельности СМИ, авторские права в гражданском праве); в) правоотношения в области формирования информационных ресурсов и предоставления информационных услуг (например, правоотношения, регулируемые Законом «Об обязательном экземпляре документов», Законом «О библиотечном деле», Законом «Об архивной службе»); г) правоотношения в области создания и применения информационных технологий, их сетей и средств их обеспечения (право на создание информационных сетей, обязанность на заключение договоров на создание таких объектов для государственных нужд); д) правоотношения в области обеспечения информационной безопасности (право на защиту личной жизни, информации от несанкционированного доступа, защита различных видов тайн).

Виды информационных технологий — высокие интеллектуальные информационные технологии — генерация технических решений, реализующих ситуационное моделирование, позволяющих выявить связь элементов, их динамику и обозначить объективные закономерности среды; вспомогательные информационные технологии — технологии, ориентированные на обеспечение выполнения определенных функций (бухгалтерский учет и статистика, ведение системы кадров, документооборота, ведение финансовых операций, системы для стратегического управления и т.д.); коммуникационные информационные технологии — технологии, обеспечивающие развитие телекоммуникации и ее систем.

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, эконо-

мической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и в пространстве в целях хранения или использования.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к сведениям, составляющим государственную тайну, — процедура оформления права на доступ (санкционированное ознакомление). Состоит из следующих элементов: обязательство нераскрытия данных сведений; временное ограничение прав субъекта государственной тайны; льготы, предоставляемые субъектам государственной тайны; ответственность за разглашение государственной тайны; проверочные мероприятия; решение уполномоченных органов о допуске к сведениям, составляющим государственную тайну.

Доступ к информации — возможность получения информации и ее использования.

Задачи деятельности органов власти в информационной сфере — а) информационное обеспечение деятельности органов (работа по структуризации информации и выбор наиболее правильных легитимных средств обработки информации); б) предоставление каждым органом власти информации другим пользователям.

Закрытый ключ электронно-цифровой подписи — уникальная последовательность символов, известная обладателю электронно-цифровой подписи.

Интернет — универсальная информационная система, включающая в себя два самостоятельных блока: а) глобальное объединение компьютерных и коммуникационных сетей; б) программные средства, обеспечивающие сетевой сервис (электронная почта, мультимедиа и др.).

Информатизация — процесс организации социально-экономических и научно-технических оптимальных условий для удовлетворения информационных потребностей и реализации прав субъектов на основе формирования и использования информационных ресурсов.

Информационная безопасность — состояние защищенности национальных интересов страны (т.е. жизненно важных интересов, основанных на сбалансированной основе) в информационной сфере от внутренних и внешних угроз. Содержание информационной безопасности составляют жизненно важные интересы субъекта в информационной сфере и внутренние и внешние угрозы, возникающие в отношении данных интересов.

Информационная безопасность государства — защита конституционного строя, суверенитета, территориальной целостности с использованием информационных средств. *Жизненно важные интересы государства в информационной сфере:* а) создание условий для реализации интересов личности и общества в информационной сфере; б) формирование институтов общественного контроля за органами государственной власти; в) безусловное обеспечение законности и правопорядка; г) создание условий для развития собственной информационной инфраструктуры; д) формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны; е) защита государственной информационной системы и информационных ресурсов (в том числе: защита государственной тайны); ж) защита единого информационного пространства страны; з) развитие равноправного и взаимного международного сотрудничества. *Угрозы информационной безопасности государства:* размывание единого правового пространства страны из-за принятия субъектами РФ не соответствовавших Конституции РФ правовых актов; разрушение единого информационного пространства России; вытеснение российских информационных агентств и средств массовой информации с внутреннего информационного рынка; монополизация информационного рынка; блокирование деятельности государственных средств массовой информации по информированию российской, зарубеж-

ной аудитории; ослабление роли русского языка как государственного языка РФ; несанкционированное целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем; низкая эффективность информационного обеспечения государственной политики (дефицит кадров, отставание информационных систем от международных стандартов).

Информационная безопасность личности — состояние и условия жизнедеятельности личности, при которых реализуются ее информационные права и свободы. *Жизненно важные интересы личности:,* а) соблюдение и реализация конституционных прав на поиск, получение прав и распространение информации; б) реализация прав гражданина на неприкосновенность частной жизни; в) использование информации в интересах не запрещенной законом деятельности, физического, духовного, интеллектуального развития; г) защита прав на объекты интеллектуальной собственности; д) обеспечение прав гражданина на защиту своего здоровья от неосознаваемой вредной информации. *Угрозы интересам личности:* а) применение нормативных правовых актов, противоречащих конституционным правам граждан; б) противодействие в том числе со стороны криминальных структур реализации гражданами прав на неприкосновенность частной жизни; в) неправомерное ограничение доступа к открытой информации; г) нарушение прав граждан в области массовой информации; д) противоправное применение специальных средств, воздействующих на сознание; е) манипулирование информацией (дезинформация; сокрытие либо искажение информации).

Информационная безопасность общества — защита экономических, социальных, международных и духовных ценностей от внешних и внутренних угроз с использованием информационных средств. *Жизненно важные интересы общества:* а) обеспечение интересов общества; б) построение правового государства; в) построение информационного общества; г) сохранение нравственных ценностей общества; д) предотвращение манипулирования массовым сознанием; е) приоритетное развитие современных информационных технологий. *Угрозы информационной безопасности общества:* а) неисполнение требований закона; б) дезорга-

низация и разрушение системы накопления и сохранения информации; в) усиление зависимости общественной жизни от зарубежных инфраструктур; г) активизация различного рода религиозных сект; д) снижение уровня духовной нравственности, творческого потенциала населения России; е) отток специалистов за рубеж; ж) нарушение прав в сфере оборота информации (утечка, перехват, хищение, навязывание ложной информации); з) нарушение правил в области функционирования информационных систем; и) нарушение правил в области использования средств обеспечения информационной безопасности: воздействие на парольные ключи системы, использование несертифицированных информационных технологий.

Информационная война — действия, направленные на достижение информационного превосходства, поддержку национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственника информации.

Информационная система — технологическая система, представляющая совокупность технических, программных и иных средств, объединяющих структурно и функционально несколько видов информационных процессов, и предоставляющая информационные услуги.

Информационное оружие — средство уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты; ограничения, воспроизведения доступа к ним законных пользователей, дезорганизации работы технических устройств, вывода из строя телекоммуникационных сетей и средств высокотехнологического обеспечения жизни общества и государства.

Информационное право — совокупность правовых норм, охраняемых государством, возникающих в сфере производства, преобразования и потребления информации. Право является информационной системой, следовательно, информационное право изучает и информационную сущность права.

Информационно-правовая норма — норма права, регулирующая обособленную группу общественных отношений при-

менительно к особенностям информационной сферы. Информационно-правовая норма задает содержание прав и обязанностей субъектов, участвующих в правоотношении. Она способствует реализации информационных прав и свобод, а также информационных процессов при обращении информации.

Информационно-правовое правоотношение — явление, в котором абстрактная информационно-правовая норма приобретает свое реальное бытие.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы — отдельные документы и массивы документов, а также документы и массивы документов в информационных системах.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация — сведения (сообщения, данные) независимо от формы их представления. С точки зрения философии информация — это отображение разнообразия. Объектом правового регулирования является только та информация, которую человек извлекает из окружающей среды и отображает в своем сознании.

Информация с ограниченным доступом — сведения, составляющие государственную тайну, служебную тайну, ноу-хау, коммерческую тайну, персональные данные. Информация с ограниченным доступом определяется двумя признаками: а) доступ ограничен в соответствии с законом; б) цель ограничения — защита прав субъектов на тайну.

Информация, не подлежащая засекречиванию, — сведения о чрезвычайных происшествиях, катастрофах, угрожающих безопасности и здоровью граждан; о состоянии экологии, здравоохранения, демографии, образования, культуры, сельского хозяйства и преступности; о привилегиях, компен-

сациях, льготах, предоставляемых всем субъектам; о фактах нарушения прав и свобод человека и гражданина; о ресурсах золотого запаса и государственных валютных резервов; о состоянии здоровья высших должностных лиц; о фактах нарушения законодательства органами государственной власти и должностными лицами.

Коммерческая тайна — научно-техническая, технологическая, коммерческая, организационная, иная используемая в предпринимательской деятельности информация, которая обладает действительной, потенциальной коммерческой ценностью в силу неизвестности ее третьим лицам и к которой нет свободного доступа на законном основании. По отношению к такой информации обладатель принимает адекватные ее ценности правовые, организационные, технические и иные меры охраны.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Крупные информационные системы — информационные системы, имеющие длительный жизненный цикл, масштабные и сложные решаемые задачи, разнообразное программное обеспечение, территориальную распределяемость, возможность миграции в другие информационные системы.

Малые информационные системы — информационные системы, обладающие непродолжительным жизненным циклом, невысокой ценой, для их жизнедеятельности достаточно одного персонального компьютера, практическим отсутствием средств обеспечения безопасности, средств аналитической обработки данных.

Ноу-хау — охраняемые в режиме коммерческой тайны результаты интеллектуальной деятельности, которые могут быть переданы другому лицу и использованы на законном основании только по усмотрению лица, обладающего такой информацией на законном основании, и которые не обеспечены патентной защитой.

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.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности

Общеправовые информационно-правовые принципы — а) приоритетности прав личности; б) законности; в) ответственности (за нарушение прав и обязанностей).

Объекты информации, составляющей профессиональную тайну, —- а) врачебная тайна; б) тайна связи; в) нотариальная тайна; г) адвокатская тайна; д) тайна усыновления; е) тайна страхования; ж) тайна исповеди.

Объекты отношений в Интернете — а) информационные ресурсы, продукты, услуги; б) информационные права и свободы (например, права на доменное имя); в) информационная целостность; г) информационный суверенитет; д) информационная безопасность.

Объекты персональных данных — а) биографические и опознавательные данные; б) личные характеристики; в) семейное положение; г) имущественное, финансовое положение; д) состояние здоровья.

Объекты служебной тайны — а) военная тайна; б) тайна следствия; в) судебная тайна; г) налоговая тайна; д) охраноспособная конфиденциальная информация, составляющая коммерческую, банковскую, профессиональную тайну, тайну частной жизни.

Обязательный экземпляр документа — ресурсная база национальной информационной инфраструктуры. Не подлежат обязательному предоставлению документы личного характера (письма), документы секретного характера, документы, содержащиеся в единичном исполнении, архивные документы и управленческая информация. Обязательному представлению подлежат: издания со значком «С»; издания для слепых;

официальные документы, подлежащие опубликованию; аудиовизуальная продукция; электронные издания; неопубликованные издания (диссертации, научные исследования).

Ограничения в применении информационных технологий — разработка и распространение программ, нарушающих нормативное функционирование информационной и телекоммуникационной систем; внедрение в апробированные программы изделий и компонентов, реализующих функции, не предусмотренные документацией на эти программы; компрометация ключей и средств криптографической защиты информации; воздействие на параллельно-ключевые системы защиты автоматизирующих систем обработки и передачи информации; внедрение электронных устройств для перехвата информации в технических устройствах обработки, хранения и передачи информации.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Основания для ограничения информационных прав — а) защита основ конституционного строя; б) защита нравственности; в) защита здоровья; г) защита прав и законных интересов других лиц; д) обеспечение обороны страны и безопасности государства. Необходимо создать единый перечень оснований для ограничений и перечень случаев прямого ограничения прав на информацию.

Основания рассекречивания сведений, составляющих государственную тайну, — а) взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими государственную тайну; б) истечение установленного срока засекречивания (общий срок — 30 лет, но возможно установление большего срока межведомственной комиссией по защите государственной тайны); в) изменение объективных обстоятельств.

Основные направления деятельности органов власти — а) отбор информации, необходимый для обеспечения деятельно-

сти; б) систематизация информации; в) подготовка и ведение банков информационных данных; г) ответственность за неадекватность информационных ресурсов задачам органов власти, а также ответственность за неполноту и несвоевременность сведений за использование информации не по назначению; д) организация информационной системы; е) обеспечение безопасности.

Основные направления защиты информационной сферы — а) защита интересов личности, общества и государства от воздействия вредной, недоброкачественной информации; б) защита информации, информационных ресурсов и информационной системы от неправомерного воздействия различных субъектов; в) защита информационных прав.

Основные направления правового регулирования отношений в Интернете — а) защита от вредной, незаконной информации; б) соблюдение авторских и смежных прав в условиях распространения информации в электронном виде; в) вопросы электронного документооборота; в) вопросы киберэкономики; г) информационная безопасность; д) правонарушения в Интернете.

Основные требования к информационной системе — а) эффективность; б) качество функционирования (точность; защищенность; согласованность со стандартами); в) надежность — те пороги, когда система отказывает (по качеству информации; по времени доступа; по производительности); г) безопасность.

Особенности информационного общества — а) наличие информационной инфраструктуры (трансграничные информационно-телекоммуникационные сети и информационные ресурсы в них); б) массовое применение персональных компьютеров и подключение их к трансграничным информационно-телекоммуникационным сетям; в) подготовка членов общества к работе на компьютерах в трансграничных информационно-телекоммуникационных сетях; г) новые формы и виды работы в трансграничных информационно-телекоммуникационных сетях и виртуальном пространстве; д) возможность практически мгновенно получать из трансграничных информационно-телекоммуникационных сетей информацию; е) возможность мгновенно общать-

ся; ж) интеграция СМИ и трансграничных информационно-телекоммуникационных сетей; з) отсутствие географических и геополитических границ государств, участвующих в трансграничных информационно-телекоммуникационных сетях.

Особенности информационной войны. Объект воздействия — все виды информации и информационной системы. Объект воздействия может выступать как оружие и как объект защиты. Расширяется территория и пространство ведения войны. Информационная война ведется как при объявлении войны, так и в кризисных ситуациях. Информационная война ведется как военными, так и гражданскими структурами.

Ответственность в информационной сфере. Юридическая ответственность реализуется с учетом специфических методов информационного права при возникновении конфликтных противоправных ситуаций. Дисциплинарная ответственность наступает за противоправные действия, совершаемые субъектами информационного права в связи с исполнением своих прав и обязанностей (п. 6 ст. 9 Закона «О правовой охране топологий интегральных микросхем», ст. 46 Конституции РФ — ответственность служащих за предоставление недоброкачественной информации). Административная ответственность устанавливается в гл. 13 КоАП РФ — за использование несертифицированных услуг связи, нарушение правил защиты информации, разглашение информации с ограниченным доступом, злоупотребление свободой массовой информации. Гражданско-правовая ответственность предусматривается ч. 2 ст. 139 ГК РФ: за нарушение норм, регулирующих информационно-имущественные отношения (исключительные права в авторском праве), а также возмещение морального вреда и имущественного вреда в случае разглашения порочащих сведений. Уголовная ответственность устанавливается УК РФ: ст. 237 «Сокрытие, искажение информации, касающиеся здоровья, жизни населения»; ст. 283 и 284 — правонарушения, связанные с разглашением государственной тайны; глава о правонарушениях в компьютерной сфере (ст. 272, 273 и 274). Ответственность средств массовой информации предусмотрена за злоупотребления

правами журналиста; нарушение неприкосновенности частной жизни; клевету и оскорбление; нарушение более 2 раз в год ст. 4 Закона «О средствах массовой информации» (о публикации различного рода запрещенной информации).

Открытая информация — вся неправовая информация, информация о выборах и референдуме; официальные документы.

Открытый ключ электронно-цифровой подписи — уникальная последовательность символов, доступная любому пользователю для подтверждения подписи.

Отличие информационного оружия от обычного оружия — скрытность (возможность применения без видимой подготовки); масштабность (применяется без учета геополитических границ); универсальность (применяется военными, гражданскими организациями).

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Право на информацию — нормативно определенный порядок реализации полномочий различных субъектов в области производства (создания, получения, доступа, сбора, хранения, использования и распространения) информации в целях, не противоречащих свободам, правам и интересам личности, общества и государства. В Конституции РФ закреплены следующие информационные права: а) право на неприкосновенность частной жизни; б) право переписки и иных сообщений; в) свобода мысли и слова; г) свобода массовой информации; д) право свободно искать, получать, передавать и производить информацию любым законным способом; е) право на образование; ж) право на достоверную информацию о состоянии окружающей среды; з) свобода всех видов творчества; и) свобода преподавания; к) право на доступ к культурным ценностям.

Правовой статус журналиста — совокупность специальных прав и обязанностей журналистов и приравненных к ним лиц (работающих в штате редакции, но не собирающих информацию, внештатных работников). Правовой статус журналиста включает в себя следующие элементы: а) трудовые отношения, иные договорные отношения лица с зарегистрированным СМИ; б) функции журналиста (поиск, распространение, выпуск информации), в том числе право журналиста на запрос, доступ к информации о работе государственных органов; в) аккредитацию; г) защиту источника информации.

Правовой статус средств массовой информации состоит из следующих элементов: а) обязательная государственная регистрация, которая носит не разрешительный, а уведомительный характер; б) лицензирование (является обязательным только для TV и радиовещания); аннулирование лицензии производится при систематическом нарушении законодательства о порядке лицензирования; в) порядок выпуска средств массовой информации; г) обязательное наличие устава редакции и устава юридического лица (устав редакции — фактический договор между редакцией и учредителем); д) обеспечение государством самостоятельности СМИ; е) экономическая государственная поддержка (налоговые льготы, государственные дотации при определенных условиях); ж) регулирование государством рекламы в средствах массовой информации.

Правовой статус субъектов информационного права включает в себя: информационную правоспособность; информационную дееспособность, права и обязанности субъектов, а также ответственность, гарантии осуществления их прав. По отношению к информации все субъекты можно разделить на три группы: производители, обладатели, собственники информации, потребители.

Предмет информационного права — часть общественных отношений, которые связаны с созданием, оформлением, хранением и обработкой, распространением, использованием информационных ресурсов, связывается с развитием в области формирования и управления информационными ресурсами,

с развитием и использованием новых технологических работ, с информацией и технологиями ее передачи в системах и сетях коммуникаций с установлением мер по обеспечению безопасности в информационных сферах, включающая в себя юридическую ответственность в названных областях.

Предметы правоотношений в сети «Интернет» — сайт, страница, сервер, домен, электронная почта и др.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Признаки информационной системы — а) выполнение одной, нескольких функций в отношении информации; б) единство системы (наличие общей файловой базы, единых стандартов и протоколов, единого управления); в) возможность композиции и декомпозиции объектов системы при выполнении заданных функций (выдержки из законов в «Гаранте», закладки — все в одном файле).

Признаки отнесения сведений к служебной тайне — а) сведения, содержащие служебную информацию о деятельности государственных органов или подведомственных им предприятий, организаций, запрет на распространение которых установлен законом или диктуется служебной необходимостью; б) сведения, являющиеся конфиденциальной информацией для других лиц, но ставшие известными представителям государственных органов в силу исполнения ими служебных обязанностей.

Признаки охраноспособности информации — а) охране подлежит только документированная информация; б) информация должна соответствовать ограничениям, установленным законом; в) защита информации устанавливается законом.

Принципы засекречивания информации — а) принцип законности: конкретная информация должна соответствовать перечню сведений, составляющих государственную тайну; б) принцип обоснованности: целесообразность отнесения указанных сведений к государственной тайне устанавливается путем экспертной оценки вероятного ущерба интересам го-

сударства и общества и на основании баланса жизненно важных интересов личности, общества и государства; в) принцип своевременности: засекречивание с момента получения сведений или заблаговременное засекречивание; г) принцип обязательной защиты: сведения защищаются органами, обладающими соответствующей компетенцией.

Принципы информационного права — зафиксированные в правовых нормах основные начала, определяющие сущность и содержание данной отрасли права, придающие ей системный характер и позволяющие ей говорить о целостности механизма правового регулирования, базирующиеся на Конституции РФ, федеральных законах и других нормативных актах.

Профессиональная тайна — защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой. Распространение этой информации может нанести ущерб доверителю, но при этом информация не является иной тайной.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Режим защиты информации — установленная законом процедура доступа к соответствующим сведениям и ответственность за разглашение этих сведений. Режим защиты информации устанавливается в отношении трех групп сведений: а) сведения, относящиеся к государственной тайне: режим устанавливается уполномоченным государственным органом на основании Закона «О государственной тайне»; б) конфиденциальная информация, режим защиты которой устанавливается собственником информационных ресурсов или уполномоченным им лицом на основании Закона «Об информации»; в) персональные данные; режим защиты таких данных должен устанавливаться специальным федеральным законом, который не принят.

Режимы коммерческой тайны — а) конфиденциальные отношения по контракту — с момента трудоустройства между сотрудником и юридическим лицом оформляются в трудовом договоре (контракте) или в приложении к нему; б) конфиденциальные отношения по служебным функциям, возникающие между сотрудниками одной фирмы, определяющиеся должностными инструкциями; в) конфиденциальные отношения по условиям договора — между заказчиком и исполнителем — оформляются в гражданском договоре.

Система информационного права включает в себя четыре раздела: а) общие положения; б) государственное регулирование информационной сферы (правовые режимы информационных ресурсов, порядок создания и применения информационных технологий, международный информационный обмен, информационный рынок (электронная коммерция), внутриорганизационное управление с использованием информационных систем, регулирование средств массовой информации, права граждан в информационной сфере, архивное и библиотечное дело); в) информационная безопасность (обеспечение безопасности личности, государства, общества и глобального информационного пространства); г) ответственность в информационной сфере: уголовная, административная, дисциплинарная, гражданско-правовая.

Система органов государственной власти, обеспечивающих право доступа к информации. Конституция РФ закрепляет право свободного доступа к информации, поэтому государственное управление в информационной сфере осуществляется всеми ветвями власти. Общее управление осуществляют: Федеральное Собрание РФ, Президент РФ, Правительство, суды, Совет Безопасности.

Служебная **тайна** — защищаемая законом конфиденциальная информация, ставшая известной в государственных органах или ОМС на закрытых основаниях в силу исполнения ими служебных обязанностей, а также служебная информация о деятельности самого органа.

Специальные информационно-правовые принципы — 1) принципы, обеспечивающиеся Конституцией РФ, но имею-

щие свою специфику в информационном праве: а) принцип свободного производства, распределения, доступа к информации; б) принцип запрещения производства и распространения информации, вредной и опасной для развития личности, общества и государства. Он реализуется через нормы безопасности государства; 2) принципы, которые формулируются на основе свойств информации: а) принцип «отчуждения» информации от ее создателя; б) принцип оборотоспособности информации; в) принцип информационного объекта (двуединство информации и ее носителя); г) принцип распространяемости и экземплярности информации.

Средние информационные системы — информационные системы, имеющие длительный жизненный цикл, наличие аналитической обработки данных, наличие средств обеспечения безопасности, необходим штат сотрудников и есть взаимодействие с фирмой-разработчиком.

Средства массовой информации — результат интеллектуальной деятельности, имеющий форму периодического распространения информации.

Степени секретности — а) особая важность — такой гриф имеют сведения, разглашение которых может нанести ущерб интересам РФ; б) совершенно секретно — такой гриф имеют сведения, разглашение которых может причинить ущерб министерствам и ведомствам; в) секретно — такой гриф имеют сведения, разглашение которых может причинить ущерб предприятиям, учреждениям, организациям (до 1991 г. сведения такого рода относились к служебной тайне).

Субъекты банковской тайны — владелец банковской тайны — клиент; пользователь банковской тайны — банк.

Субъекты государственной тайны — лица, допущенные к сведениям, составляющим государственную тайну.

Субъекты коммерческой тайны — а) обладатели коммерческой тайны — сама организация и сотрудники, работающие в ней; б) правопреемники — лица, которым информация, составляющая коммерческую тайну, стала известна в силу служебного положения, исполнения профессиональ-

ных обязанностей, в силу договора, на ином законном основании.

Субъекты персональных данных — лица, к которым относятся данные, их наследники. Ограничение права на охрану персональных данных существует для субъектов, допущенных к государственной тайне; а также подозреваемых в совершении преступлений. Режим конфиденциальности снимается в случае обезличивания персональных данных или по желанию субъекта персональных данных.

Субъекты права массовой информации — учредитель, редакция, издатель, распространитель и собственник имущества редакции.

Субъекты правоотношений в Интернете — а) создатели программных технологий (частей информационной инфраструктуры); б) производители и распространители информации в Интернете, в том числе оказывающие услуги по подключению (провайдеры); в) потребители.

Субъекты профессиональной тайны — а) доверитель; б) держатель; в) пользователь (государственные органы, которым становится известна государственная тайна в связи с использованием служебных обязанностей).

Субъекты электронно-цифровой подписи — пользователи информационной системы; обладатели электронно-цифровой подписи; удостоверяющие центры; уполномоченные федеральные органы исполнительной власти.

Тайна частной жизни — составной элемент права на неприкосновенность частной жизни. Тайна частной жизни включает в себя личную, семейную тайну и охрану персональных данных. Правовая охрана права на неприкосновенность частной жизни осуществляется установлением конституционных гарантий. Информация, затрагивающая неприкосновенность частной жизни и ставшая известной на законных основаниях другим лицам, должна охраняться в режиме профессиональной или служебной тайны.

Цели защиты информации — а) предотвращение хищения, утечки, искажения, утраты и подделки информации; б) предотвращение несанкционированных действий по унич-

тожению, модификации, копированию и блокированию информации; в) реализация права на государственную тайну и конфиденциальную информацию.

Электронно-цифровая подпись — реквизит электронного документа, полученный в результате преобразования информации с использованием закрытого ключа электронно-цифровой подписи, и позволяющий установить подлинность и целостность содержащейся в электронном документе информации, а также обладателя электронно-цифровой подписи. Электронно-цифровая подпись в электронном документе становится равнозначной собственноручной подписи при следующих условиях (одновременно) — а) сертификат ключа электронно-цифровой подписи не утратил силу; б) подтверждена подлинность электронно-цифровой подписи в электронном документе; в) электронно-цифровая подпись используется в отношениях, имеющих юридическое значение.

Электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронный документ — документ на цифровом носителе, состоящий из трех элементов: содержание информации; форма предоставления содержания; носитель информации.

Юридические свойства информации — свойства информации, позволяющие осуществлять правовое регулирование в отношении информации: а) физическая неотчуждаемость (отчуждение информации заменяется передачей прав на ее использование); б) обособленность информации — для включения в оборот информация используется в виде символов, знаков, таким образом обособляется от производителя и существует отдельно; в) двуединство информации и носителя; г) распространяемость (тиражируемость) информации — возможность распространения неограниченного количества экземпляров без изменения содержания информации; д) организационная форма информации — документ; е) экземплярность информации — существование информации на отдельном материальном носителе, отсюда учет количества экземпляров через учет количества носителей.

Приложение 3. Список рекомендуемой литературы

1. *Агапов А.Б.* Организационно-правовые проблемы информационного обеспечения государственных органов: Автореф. дис. ... доктора юрид. наук. — М., 1995.

2. *Агапов А.Б.* Основы государственного управления в сфере информатизации в РФ: Учеб. пособие. — М., 1997.

3. *Агапов А.Б.* Основы федерального информационного права России. — М.: Экономика, 1995.

4. *Батурин ЮМ.* Проблемы компьютерного права. — М., 1991.

5. *Бачило И.Л.* Информационное право: роль и место в системе права // Государство и право. 2001. № 2.

6. *Бачило И.Л.* Информационное право: Учеб. пособие. — М., 2001.

7. *Бачило И.Л.* Правовое регулирование процессов информатизации // Государство и право. 1994. № 12.

8. *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право: учебник. — СПб., 2005.

9. *Боер В.М.* Информационно-правовая политика и безопасность России (теоретико-правовой аспект): Автореф. дис.... доктора юрид. наук. — СПб., 1998.

10. *Ващекин Н.П., Абрамов Ю.Ф.* Информационная деятельность и мировоззрение. — Иркутск: Изд-во Иркутского университета, 1990.

11. *Гаврилов М.В.* Компьютер. Персональное дело. — Саратов: Изд-во Саратовской академии права, 1999.

12. *Гаврилов О.А.* Курс правовой информатики. — М., 2000.

13. *Дмитриев В.В.* Диалектика содержания и формы в информационных процессах. — Минск: Наука и техника, 1973.

14. Институты административного права России: Сборник статей / Под ред. И.Л. Бачило и Н.Ю. Хаманевой. — М., 1999.

15. Информационная цивилизация: пространства, культура, человек. — Саратов, 2000.

16. Информационное общество: информационные войны, информационная безопасность / Под ред. М.А. Вуса. — СПб., 1999.

17. Информационные системы в управлении производством / Под ред. Ю.П. Васильева. — М.: Прогресс, 1973.

18. *Колосков ЮМ.* Массовая информация и международное право. — М.: Международные отношения, 1974.

19. Комментарий к Федеральному закону «Об информации, информатизации и защите информации» / Под ред. И.Л. Бачило, А.В. Волокитина, В.А. Копылова и др. — М.: ИГП РАН, 1996.

20. Концепция информационной безопасности / Под ред. Д.С. Черешкина. — М.: ИСА РАН, 1994.

21. *Копылов В.А.* О структуре и составе информационного законодательства // Государство и право. 1996. № 6.

22. *Корченкова Н.Ю.* Становление теоретико-правовой концепции права на информацию: Автореф. дис.... канд. юрид. наук. — Нижний Новгород: Нижегородский госуниверситет,, 2000.

23. *Крылов В.В.* Информационные компьютерные преступления. — М.: ИНФРА-М; Норма, 1997.

24. *Крылов В.В.* Информация как элемент криминальной деятельности // Вестник Московского университета. Серия 11. Право. 1998. № 4.

25. Перспективные информационные технологии в правовой сфере: Монография / Под ред. В.А. Копылова. — М., 1993.

26. *Полевой Н., Крылов В.* Компьютерные технологии в юридической деятельности. — М.: БЕК, 1994.

27. *Рассолов ММ.* Информационное право: Учеб. пособие. — М., 1999.

28. *Рассолов ММ.* Информационное право: анализ и решение практических задач. — М., 1998.

29. *Рассолов ММ.* Проблемы управления и информации в области права. — М., 1991.

30. *Рассолов М.М., Элькин В.Д., Рассолов ИМ.* Правовая информатика и управление в сфере предпринимательства. — М, 1996.

31. *Снытников А.А.* Информация как объект гражданских правовых отношений: Автореф. дис. ... доктора юрид. наук. — СПб., 2000.

32. *Тихомиров Ю.А.* Информационный статус субъектов права//Труды ИЗ и СП. 1992. № 52.

33. *Тихомиров Ю.А.* Публичное право. — М.: БЕК, 1995.

34. *Федотов М.* Законодательство о средствах массовой информации. — М.: Гардарика, 1996.

35. *Шверский А.А.* Защита информации: проблемы теории и практики. — М.: Юристъ, 1996.

36. *Юрченко И.А.* Информация конфиденциального характера как предмет уголовно-правовой охраны: Автореф. дис.... канд. юрид. наук. — М., 2000.

Наталия Николаевна Ковалева

Информационное право России

Учебное пособие

Санитарно-эпидемиологическое заключение
№ 77.99.02.953.Д.004609.07.04 от 13.07.2004 г.

Лицензия № 06473 от 19 декабря 2001 г.
Подписано в печать 25.10.2006. Формат 60x84 1/16.
Печать офсетная. Бумага газетная. Печ. л. 22,5.
Тираж 2500 экз. Заказ № 6902.

Издательско-торговая корпорация «Дашков и К°»
129347, Москва, Ярославское шоссе, д. 142, к. 732.
Для писем: 129347, Москва, п/о И-347
Тел./факс: (495) 182-01-58,182-11-79,183-93-01
E-mail: sales@dashkov.ru — отдел продаж
office@dashkov.ru — офис;
http://www.dashkov.ru

Отпечатано в соответствии с качеством предоставленных диапозитивов
в ФГУП «Производственно-издательский комбинат ВИНИТИ»,
140010, г. Люберцы Московской обл., Октябрьский пр-т, 403. Тел.: 554-21-86