Саратовский государственный университет им. Н.Г. Чернышевского

С.А. Куликова

ИНФОРМАЦИОННОЕ ПРАВО РОССИИ

Учебное пособие для студентов,
обучающихся по специальностям (направлениям)
«Юриспруденция» и «Прикладная информатика в юриспруденции»

Саратов
Издательство Саратовского университета
2010

УДК 349(075.8)
ББК 67.404.3я73
К90

Куликова С.А.

К90 Информационное право России: Учеб. пособие для студентов, обучающихся по специальностям (направлениям) «Юриспруденция» и «Прикладная информатика в юриспруденции». – Саратов: Изд-во Сарат. ун-та, 2010. – 196 с.
ISBN 978-5-292-03922-8

Учебное пособие подготовлено в соответствии с государственным образовательным стандартом и программой учебного курса «Информационное право».

Автором рассматриваются как общие понятия информационного права, так и проблемы развития основных правовых институтов. В частности, анализируется право на доступ к информации о деятельности органов государственной власти, правовые режимы общедоступной информации и информации ограниченного доступа, вопросы электронного документооборота, создания и эксплуатации информационных систем, особенности информационных правонарушений и ответственности за их совершение.

Для студентов, обучающихся по специальностям (направлениям) «Юриспруденция» и «Прикладная информатика в юриспруденции».

Рекомендуют к печати:

Кафедра конституционного и муниципального права юридического факультета
Саратовского государственного университета
Кандидат юридических наук *Н.Н. Ковалева*
(Саратовская государственная академия права)
Кандидат юридических наук *С.Е. Чаннов*
(Саратовский государственный университет)

УДК 349(075.8)
ББК 67.404.3я73

ISBN 978-5-292-03922-8

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Информационное право является относительно новой комплексной отраслью права и находится на стадии своего становления. Возникновение отрасли связано с возрастающей ролью информации в современном постиндустриальном обществе.

Наше время характеризуется широким распространением информационно-компьютерных технологий и глобальных телекоммуникационных сетей. Это создает принципиально новые возможности и стимулы для поиска, получения и распространения идей, мнений, знаний, демократизации общественных отношений и формирования экономики нового типа.

Информационные процессы развиваются стремительными темпами, что сказывается на характере общественных отношений, складывающихся между членами данного общества, а также гражданами и государством. Внедрение информационных систем и технологий требует новых личностных качеств: например, все чаще говорят об информационной компетентности государственных служащих, которая включает в себя компьютерную грамотность, умение работать с информацией, оперативно принимать управленческие решения на основе ее обработки. Появилось новое понятие «информационный капитал личности». Именно этот капитал значительно повышает конкурентоспособность современного человека.

В то же время растет количество правонарушений в информационной среде, повышается их латентность. Обеспечение информационной безопасности личности, общества и государства является одним из приоритетов современной государственной политики.

В этих условиях роль права возрастает. Право как универсальный социальный регулятор должно определять и поддерживать те направления, которые становятся приоритетными в информационном обществе, воздействовать непосредственным образом на ход информационных процессов.

В то же время применение информационно-коммуникационных технологий порождает ряд правовых проблем, которые требуют дальнейшего совершенствования национального законодательства. Необходимы уточнение и систематизация терминологии, разработка новых нормативных правовых актов, корректировка уже действующих и отмена тех актов, которые препятствуют применению электронных документов в частноправовой и публичной сферах, эффективной эксплуатации информационных систем и внедрению информационных технологий в деятельность государственных органов.

Настоящее пособие построено по модульной системе и состоит из четырех разделов. В первом даются общие теоретические понятия, характеризуются особенности информационного права как отрасли права Российской Федерации, приводятся основные нормативные правовые источники. Во втором рассматривается институт права на информацию, объясняется понятие правового режима информационных ресурсов, исследуется правовое регулирование в области массовой информации. Третий раздел целиком посвящен изучению информационных процессов в электронной среде. Здесь исследуются наиболее сложные вопросы информационного права, в правовом регулировании которых много «белых пятен». В четвертом разделе особое внимание уделено актуальным проблемам информационной безопасности и ответственности за правонарушения в информационной сфере.

Сегодня весь спектр отношений по поиску, получению, передаче и распространению информации представлен в сети Интернет. В пособии проводится анализ особенностей поведения субъектов и осуществления информационных правоотношений в сети Интернет. Рассматриваются основные правовые проблемы регулирования информационных отношений в Интернете: решение доменных споров, возможность защиты от вредной информации, установление правового режима электронных средств массовой информации, защита авторских прав, обеспечение информационной безопасности и др.

Современное информационное право включает в себя большое количество законов и иных нормативных актов. В предлагаемом пособии очерчиваются основные правовые подходы к той или иной проблеме и называются основные акты, регулирующие соответствующие отношения. Более подробное их изучение предполагается на практических занятиях.

Учебное пособие дополнено одноименным учебно-методическим пособием, в котором даются вопросы к семинарским занятиям, тематические списки литературы, практические задания, темы рефератов и вопросы к зачету.

Модуль 1
ОБЩАЯ ЧАСТЬ. ИНФОРМАЦИОННОЕ ПРАВО КАК ОТРАСЛЬ ПРАВА РФ

Тема 1. ПОНЯТИЕ И ВИДЫ ИНФОРМАЦИИ

Понятие информации

Понятие информации относится к таким базовым онтологическим понятиям, как «материя» и «энергия».

В то же время понятие информации продолжает оставаться одним из самых сложных и противоречивых. Оно стало привлекать к себе внимание в начале XX века в результате совершенствования теории связи и возрастания роли обмена различными сведениями в общественной и политической жизни. Каждая наука рассматривала свои, важные именно для нее аспекты информации и давала свое понятие информации.

В книге И.В. Мелик-Гайказян собрана коллекция определений слова «информация»[1]. Приведем некоторые из них:

1) Информация есть *знания,* переданные кем-то другим или приобретенные путем собственного исследования или изучения (Ф. Махлуп).

2) Информация есть *отражение* в сознании людей объективных причинно-следственных связей в окружающем нас реальном мире (А. Берг, Ю. Черняк).

3) Информация – не энергия и не материя, а сообщение (сигнал, команда) и обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств (Н. Винер).

---

[1] Цит. по: *Чернавский Д.С.* Синергетика и информация: Динамическая теория информации. М., 2009. С. 16–17.

4) Информация – оригинальность, новизна, мера сложности структур (А. Моль).

5) Информация – это *совокупность приемов, правил* или сведений, необходимых оператору для построения (В. Корогодин).

6) Информация есть запомненный *выбор* одного варианта из нескольких возможных и равноправных (Д. Чернавский).

Такого рода определения неприменимы в праве.

Юридическое определение информации дается в Федеральном законе **«Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ**. Статья 2 этого Закона определяет информацию как **«сведения (сообщения, данные) независимо от формы их представления».** В данном определении законодатель связал понятие информации с двумя признаками.

1. Содержательность. Этот признак проявляется через отождествление информации со сведениями (сообщениями). Сведения – некие символы лиц, предметов, фактов, событий, явлений и процессов, т.е. некое содержание, полученное из внешнего мира.

2. Независимость от формы представления сведений. Сведения могут передаваться в любой воспринимаемой форме: устной, письменной, визуальной, акустической и т.п. Сведения, выраженные в знаках, обычно называют данными.

В юридической науке информация рассматривается с точки зрения ее ценности, полезности для общества. Именно в этом аспекте информация может выступать как объект правоотношений.

Объектом правоотношений выступает материальное или нематериальное благо, с помощью которого удовлетворяются публичные или частные интересы. Особенность информации состоит в том, что она **является благом особого рода**. Оно материально в том смысле, что материя способна переносить, отражать и содержать информацию. В то же время само содержание информации носит идеальный характер.

Материальная и нематериальная стороны информации, делающие ее благом особого рода, проявляют себя в ее связи с материальными носителями. Информация не может существовать без некоторого материального носителя, но она не связана с определенным материальным носителем. Одна и та же информация может переноситься (и при этом перекодироваться) с одного носителя на другой. В этом случае информация остается инвариантной (неизменяющейся) тому носителю, на котором она находится в данный момент. Например, лекция по информационному праву, записанная на диске, может быть перенесена на бумажный носитель. В процессе воспроизведения информация проходит соответствующие последовательные преобразования, считываясь в устройстве компьютера, и выводится на принтер в виде печатного текста. Таким образом, она меняет целый ряд материальных носителей, оставаясь той же самой в содержательном плане.

Юридические особенности и свойства информации

Информации любого вида присущи некоторые свойства, которые отличают ее от других объектов правоотношений и влекут определенные особенности ее правовой охраны. В юридической доктрине сложилась стройная система описания **основных юридических свойств информации**. Обычно выделяют следующие[2].

1. Свойство **физической неотчуждаемости** информации. Оно основано на том, что знания не отчуждаемы от человека – их носителя. (В отличие от вещи информацию обратно не отнимешь, человека не заставишь ее забыть). При передаче информации от одного лица к другому и юридическом закреплении этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование.

2. Свойство **информационной вещи**. Сама информация носит нематериальный характер и лишь будучи воплощенной в материальную форму (текст, символ, графический знак) может распространяться и быть включена в гражданско-правовой оборот. Информация передается и распространяется только на материальных носителях, в этом проявляется двуединство информации (ее содержания) и носителя, на котором она закреплена. Поэтому на информационную вещь распространяется действие двух правовых институтов – института авторского права и института вещной собственности. К информационным вещам мы можем относить как отдельные документы, так и сложные организационные информационные структуры (базы данных, библиотеки, архивы).

3. Свойство **организационной формы**. Информация, находящаяся в обороте, как правило, предоставляется в документированном виде.

4. Свойство **обособляемости** информации. Для включения в оборот информация всегда овеществляется в виде символов, благодаря чему обособляется от ее производителя и существует независимо от него. Это делает возможным оборотоспособность информации как самостоятельного отдельного объекта правоотношений.

5. Свойство **тиражируемости** информации. Информация может иметь неограниченное число пользователей, использоваться неограниченное число раз и при этом оставаться неизменной. Сообщение может быть записано на материальном носителе. Таким образом, оно является формой передачи информации и может распространяться в каналах общественной коммуникации, воспроизводиться без участия автора, быть доступным для неограниченного круга субъектов. Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания. Отсюда следует, что необходимо юридически закреплять объем прав по использованию информации ли-

[2] См., например: *Копылов В.А.* Информационное право: Учебник. М., 2004. С. 49–50.

цами, обладающими такой информацией, т.е. обладающими знаниями о содержании информации.

6. Свойство **экземплярности** информации. Это свойство заключается в том, что информация распространяется не сама по себе, а на материальном носителе. Следовательно, возможен учет экземпляров информации через учет носителей, содержащих ее. Понятие экземплярности информации дает возможность учитывать обращение, прежде всего, документированной информации, а также учитывать и регистрировать документы.

Существует ряд понятий, которые дают **дополнительную характеристику информации**. Наиболее употребляемые из них:

– **достоверность** – соответствие данных объективной реальности;

– **адекватность** – способность информации создавать у получателя соответствующее представление об объекте, процессе или явлении. Нельзя смешивать понятия «достоверность» и «адекватность» информации. Под адекватностью понимают степень соответствия информации, полученной потребителем, тому, что поставщик вложил в ее содержание;

– **полнота** – достаточность данных для понимания сути явления и принятия решения. При распространении информации действует закон искажения информации по мере ее движения. Данный закон связан с различной способностью и готовностью субъектов к ее восприятию. Именно поэтому в тех случаях, когда важны достоверность и полнота информации, встает вопрос о ее фиксации на материальном носителе и соблюдении определенных требований к процедуре и способу фиксации;

– **новизна** – не все данные могут быть востребованы, а только те, которые содержат новизну. Абстрактные или общеизвестные сведения не обладают потребительскими свойствами и не могут быть объектом правоотношений, следовательно, не имеют юридической сущности;

– **оптимальность** – сочетание полноты и краткости данных. Их должно быть достаточно для принятия решения, слишком большой объем информации ведет к дополнительным затратам времени в процессе ее сбора, хранения, передачи и обработки;

– **своевременность** – актуальность в момент принятия решений;

– **объективность и субъективность информации** – степень выражения в предоставляемых данных мировоззрения поставщика информации. Понятие объективности информации является относительным;

– **доступность** – мера возможности получить ту или иную информацию;

– **неисчерпаемость** – информация не подвержена физическому износу в процессе ее использования и обладает такой особенностью, как возможность неограниченного тиражирования;

– **ценность** – способность расширять возможности потребителя информации.

Неисчерпаемость и ценность информации во многом способствуют прогрессу человечества поскольку именно благодаря этим ее качествам

происходят накопление знаний и передача их от поколения к поколению. Однако данные качества информации приводят к тому, что одни и те же сведения могут использоваться различными субъектами, в том числе и преследующими противоположные цели.

Кроме того, для целей правового регулирования информационных отношений большое значение имеют такие ее характеристики, как **конфиденциальность** – защищенность информации от несанкционированного доступа, и **целостность** – свойство, при наличии которого информация сохраняет заранее определенные системой вид и качество[3].

Типы классификации информации

Учеными предлагаются различные способы деления информации в зависимости от оснований классификации.

1. В соответствии с основными видами отражения:

1)элементарная – на уровне атомов (в неживой природе);

2)биологическая – создается живыми существами;

3)социальная – область человеческих отношений;

4)технико-кибернетическая – производная, созданная в результате деятельности машин.

2. По связи с материальным носителем.

Вся информация делится на свободную (идеальную) и связанную (материальную). Под **свободной (идеальной)** понимают такую информацию, которая ассоциируется с процессом познания и свободно циркулирует между различными материальными носителями. Примерами свободной информации могут служить передаваемое по радио сообщение и живая человеческая речь. Свободная информация представляет собой наиболее распространенное как в науке, так и в обыденном применении значение термина «информация», поскольку именно оно отождествляет собой содержательный аспект, фигурируя чаще всего в качестве сведений.

Связанная (материальная, внутренняя, структурная) информация характеризует организованность, упорядоченность какой-либо системы. Говоря другими словами, это информация, прошедшая стадию опредмечивания. Примерами связанной информации является информация ДНК или информация, зафиксированная в техническом устройстве в виде определенного сочетания его конструктивных элементов, а также эстетическая информация, которую несут в себе скульптура, живопись и архитектура. Связанная информация может существовать в природе, а также являться рукотворной. Связанная информация как застывшая структура фиксирует конфигурацию или количественный либо каче-

[3] См.: *Годин В.В., Корнеев И.К.* Информационное обеспечение управленческой деятельности. М., 2001.

ственный состав самого материального носителя, например сплава или технического изделия[4].

Хотя связанная и свободная информация рассматриваются как два качественно различных типа, они взаимно предполагают друг друга и могут переходить один в другой.

***3. По форме выражения*:**

По степени организованности информация делится на **документированную и недокументированную.**

Документ – особая организационная форма выражения информации, основанная на двуединстве информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения.

Недокументированная информация остается за пределами правового регулирования.

4. По роли в системе права. Информацию делят на правовую и неправовую**.**

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

– нормативную (содержит нормы права, например закон, подзаконный акт);

– ненормативную.

Неправовая создается не как результат правовой деятельности, однако обращается в обществе в соответствии с предписаниями правовых норм.

5. По степени доступа. Информация подразделяется на **общедоступную** и информацию **ограниченного доступа**, распространение которой возможно в условиях конфиденциальности или секретности.

Проблема разграничения информации на открытую и ограниченного доступа имеет большое значение, поскольку Конституция РФ и ряд международных соглашений, участницей которых является Россия, закрепляют презумпцию доступности информации и предусматривают право свободно искать, получать, передавать, производить и распространять ее любым законным способом. Право на информацию является личным правом гражданина. В то же время сохранение личной, коммерческой и государственной тайн входит в число интересов граждан, организаций и государства в целом.

К **общедоступной** относится информация, которая может выступать как ***объект гражданских прав*** (научная и художественная литература, географические карты, фотографии, другая информация, создаваемая с целью извлечения прибыли), а также информация, содержащаяся в документах, закрепляющих авторские права на изобретения, полезные модели, промышленные образцы (патенты, свидетельства).

---

[4] См.: *Городов О.А.* Информационное право: Учебник. М., 2007. С. 12–13.

К общедоступной принадлежит и ***массовая информация***: сообщения информационного характера, подготавливаемые и распространяемые СМИ, в том числе и ***реклама*** физических и юридических лиц, производимых продуктов, предоставляемых услуг.

К этой же группе относятся ***информация о выборах, референдуме, официальные документы, законы и подзаконные акты***.

Информация ограниченного доступа включает в себя, во-первых, ***государственную тайну*** – защищаемые государством сведения, создаваемые в условиях секретности в соответствии с законом; и, во-вторых, ***конфиденциальную информацию***.

К **конфиденциальной информации** относятся ***служебная*** тайна, ***профессиональные*** тайны (врачебная, адвокатская, нотариальная и т.д.). Кроме того, к конфиденциальной информации относится ***коммерческая тайна*** – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, включая ноу-хау. К этой же группе относятся ***персональные данные*** (в порядке защиты ***личной тайны***) – информация о гражданах, которая создается самими гражданами в их повседневной деятельности и представляется как сведения о себе (анкета, карточка учета, история болезни, декларация о доходах, банковская запись и т.д.).

В Федеральном законе «Об информации, информационных технологиях и о защите информации» кроме классификации по доступу прибавляется еще и по порядку распространения, порядку предоставления, а также указывается возможность использования таких оснований деления, как содержание и обладатель (но последнее закон не расшифровывает).

6. По порядку распространения:

1) информация, распространяемая свободно (такая общедоступная информация, как нормативные правовые акты, массовая информация);

2) информация, распространяемая ограниченно (например, информация о выборах и референдумах (ограничена по сроку действия), реклама, порядок распространения которой зависит как от формы, так и от содержания (ограничение времени трансляции рекламы на канале или печатной площади, ограничение рекламы пива, спиртного, сигарет)).

3) информация, запрещенная к распространению (призывы к межнациональной и межрелигиозной розни, подрыву конституционного строя, порнография, оскорбление, клевета).

7. По порядку предоставления.

1) информация, предоставляемая в обязательном порядке (предусматривается Конституцией и федеральными законами, за отказ в ее предоставлении наступает правовая ответственность. Примером может служить информация, затрагивающая конституционные права и свободы граждан: об экологических бедствиях, техногенных катастрофах, несущих опасность жизни и здоровью людей, о деятельности государственных органов и т.д.);

2) информация, предоставляемая добровольно (на основе соглашения) (компьютерная программа, написанная на заказ, проведение маркетинговых исследований с целью лучшего сбыта продукции и т.д.)***;***

3) информация, которую запрещено предоставлять (государственная тайна, персональные данные).

Следует отметить, что Закон разделяет понятия **«распространение»** и **«предоставление»** информации. При этом под распространением понимается ***передача информации неопределенному кругу лиц***; под предоставлением – ***определенному кругу лиц*** (п. 8, 9 ст. 2). Следовательно, обязанность предоставить информацию не тождественна обязанности ее распространить. Обязательное распространение (в законодательстве обычно применяется термин «опубликование» или «обнародование») предполагает общедоступный характер информации. Например, обязательное опубликование предусмотрено для нормативных правовых актов.

Обязанность по предоставлению информации может касаться как открытой информации, так и информации ограниченного доступа. Примером обязанности предоставления открытой информации является ответ должностного лица на журналистский запрос. Примером обязанности по предоставлению информации ограниченного доступа могут быть нормы Федерального закона «Об обществах с ограниченной ответственностью» (ст. 8 и 9), которые предусматривают право участника на получение информации о деятельности общества и одновременно возлагают на него обязанность по соблюдению ее конфиденциальности. Федеральный закон «О персональных данных» также предусматривает обязанность предоставления персональных данных лицу, чьи персональные данные обрабатываются.

Обязанность распространить информацию относится к конкретному лицу в конкретном правоотношении. Такая обязанность носит однократный характер. После того как информация была в соответствии с законом обнародована, она переходит в режим свободного, неограниченного распространения.

К особой группе относится информация, предоставленная в виде ***объектов авторского права***. Эта информация по общему правилу общедоступная, а вот режим ее распространения характеризуется следующими принципами. Распространение произведения составляет исключительное право его автора. Из этого можно сделать вывод о том, что данная информация относится к ограниченно распространяемой. Однако специфика объектов авторского права (охрана формы произведения), принцип исчерпания авторских прав, а также целый ряд изъятий (журналистские статьи, идеи, концепции и т.д.) из исключительных прав автора делают данный вывод не столь однозначным (т.е. информация может переходить из одной группы в другую)[5].

[5] См.: *Антопольский А.А.* Доступ к информации и его ограничение // Информационное право: Актуальные проблемы теории и практики / Под общ. ред. И.Л. Бачило. М., 2009. С. 450.

Тема 2. ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОГО ПРАВА КАК ОТРАСЛИ ПРАВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Понятие информационного права

Информационного право – молодая отрасль права. Развитие информационных отношений в начале 90-х годов XX века повлекло за собой необходимость принятия значительного количества нормативных актов, направленных на их регулирование. Один за другим принимаются законы «О средствах массовой информации», «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О связи», «О федеральных органах правительственной связи и информации» и др.

Наличие обширной нормативной базы позволило многим ученым поставить вопрос о формировании новой отрасли российского права – информационного.

До сих пор многие понятия информационного права являются дискуссионными, в том числе и понятие самого информационного права.

Информационное право как отрасль права – это система правовых норм, регулирующих общественные отношения по поиску, получению, передаче, производству и распространению информации и производных от нее продуктов (информационных ресурсов, технологий, систем).

В сферу регулирования информационного права включаются отношения по поводу информации довольно широкого спектра. Это и право граждан на информацию о деятельности государственных органов, и деятельность СМИ, и библиотечное, архивное дело, различные виды тайн: государственная, коммерческая, личная. В настоящее время на наших глазах происходит формирование совершенно новых общественных отношений в глобальной информационной сети – возможная мера и способы их правового регулирования являются одним из перспективных направлений развития информационного права.

Отрасль информационное право входит в семейство административного права.

Информационное право как наука изучает закономерности формирования и функционирования общественных отношений, возникающих и протекающих в информационной сфере, и вырабатывает юридические модели, позволяющие осуществлять адекватное правовое регулирование этих отношений.

Можно выделить несколько наиболее важных научных направлений:

– изучение специфики информации как объекта правового регулировании;

– формирование принципов и методов правового регулирования деятельности в области создания и использования информационных ресурсов, технологий, коммуникаций и их сетей;

– изучение правовых режимов информации;

– исследование роли информационного права в процессе глобализации;

– анализ правовых проблем глобальной сети Интернет и способов их решения;

– разработка способов обеспечения информационной безопасности личности, государства и общества.

Комплексный характер информационного права

Информационное право является комплексной отраслью, объединяет в предметной области регулирования однородную группу общественных отношений, тесно взаимодействует с профилирующими отраслями права, и прежде всего конституционным, гражданским, уголовным и административным правом.

Эта взаимосвязь, в частности, прослеживается на следующих примерах. Конституционное право оперирует понятиями, непосредственно связанными с предметом регулирования информационного права. Нормы Конституции РФ провозглашают свободу информации, закрепляют содержание права на информацию, гарантируют защиту информации, находящейся в режиме личной, семейной и государственной тайны.

Гражданский кодекс РФ предусматривает правила оказания информационных услуг (ст. 779), обязанности продавца по предоставлению покупателю информации о товаре (ст. 495); гарантирует сохранение некоторых видов тайн: банковской (ст. 852), тайны завещания (ст. 1123), конфиденциальность информации, полученной сторонами по договору (ст. 727), исключительное право на секрет производства (ст. 1467). Часть четвертая Гражданского кодекса, посвященная авторскому праву, теснейшим образом соприкасается с нормами информационного права.

УК РФ содержит значительное количество норм, в соответствии с которыми деяния, совершенные в информационной сфере, признаются уголовно наказуемыми. Например, клевета (ст. 129), оскорбление (ст. 130), нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), заведомо ложное сообщение об акте терроризма (ст. 207), сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей (с. 237), преступления в сфере компьютерной информации (ст. 272–274), разглашение государственной тайны (ст. 283), а также данных предварительного расследования (ст. 310) и т.д.

Значителен перечень мер административного характера, применяемого к правонарушителям. КоАП содержит специальную гл. 13 «Административные правонарушения в области связи и информации». В ней, в частности, определены санкции за нарушение установленного законом порядка, сбора, хранения, использования или распространения информации о гражданах (персональных данных) – ст. 13.11; нарушение правил защиты информации – ст. 13.12; разглашение информации с ограниченным доступом – ст. 13.14; злоупотребление свободой массовой информации – ст. 13.15; воспрепятствование распространению продукции средства массовой информации – ст. 13.16; нарушение правил хранения, комплектования, учета или использования архивных документов.

Иные составы действий, квалифицируемых в качестве административных правонарушений в информационной сфере, содержатся в разрозненном виде практически во всей Особенной части КоАП. Административно-правовые санкции установлены, в частности, в отношении нарушения права гражданина на ознакомление со списком избирателей, участников референдума (ст. 5.1); изготовление или распространение анонимных агитационных материалов (ст. 5.12), нарушение законодательства о рекламе (ст. 14.3); предоставление ложных сведений для получения удостоверения личности гражданина (паспорта) либо других документов, удостоверяющих личность или гражданство (ст. 19.18).

Практика правового регулирования информации позволяет сделать вывод о том, что отношения по поводу информационного оборота регулируются многими отраслями права. Однако формирующееся информационное право имеет следующие выделяющие его признаки:

1)значительный массив законодательства;

2)наличие самостоятельного предмета правового регулирования;

3)социальная и экономическая заинтересованность государства в развитии информационных отношений;

4)возникновение и бурное развитие общественных отношений в информационной среде, влекущее за собой необходимость их правового регулирования[6].

Многие специалисты считают, что комплексность информационного права – явление временное, обусловленное первоначальным этапом накопления нормативного материала. Когда информационное законодательство сформируется в более системном виде, информационное право перестанет быть комплексной отраслью.

Предмет правового регулирования в информационном праве

Регулируя поведение людей в какой-либо сфере, государство воздействует на отдельные, как правило, однородные группы общественных

[6] См.: *Ковалева Н.Н.* Информационное право России: Учеб. пособие. М., 2009. С. 25.

отношений. По мнению большинства исследователей, то, на что направлено воздействие определенной отрасли права, является ее предметом. Специфика предмета, т.е. характерные особенности и реальное содержание регулируемых отношений, определяется качественным своеобразием той или иной области общественных отношений.

Предмет информационного права – отношения по поиску, получению, передаче, производству и распространению информации. Эти отношения являются ядром предметной области информационного права. К ним тесно примыкают так называемые смежные отношения, а именно отношения по поводу:

1)обеспечения прав граждан на информацию;

2)создания, преобразования и потребления информации;

3)разработки и использования информационных технологий, телекоммуникационных сетей;

4)сохранения конфиденциальности информации, в случаях, предусмотренных законодательством;

5)обеспечения информационной безопасности.

Сама **информация выступает объектом отношений**, урегулированных нормами информационного права, но не является его предметом, поскольку в структуру предмета любой отрасли права входят только общественные отношения. В то же время особенности общественных отношений предопределены спецификой самого объекта, т.е. информации. Отличие информации от других объектов права состоит в том, что она является благом особого рода, которое проявляет себя не только в объектах материального мира, но и в идеальных продуктах интеллектуальной деятельности человека.

Можно предположить, что со временем предметная область информационного права будет изменяться путем включения в нее новых групп общественных отношений, которые возникнут в информационной сфере. Включение этих отношений в предмет информационного права будет зависеть, прежде всего, от содержания и смысла норм информационного законодательства, отличающегося сегодня некоторой неупорядоченностью и противоречивостью.

Методы правового регулирования

Под методом правового регулирования в информационном праве будем понимать правовые приемы и способы воздействия на информационные отношения. Являясь комплексной отраслью права, информационное право использует методы, характерные для различных отраслей.

Все методы правового регулирования делятся на императивные и диспозитивные.

К **императивным методам** относятся:

1) **повеление** – возложение на участников информационных правоотношений обязанности совершать какие-либо действия. Этот способ чаще

всего используется в административном праве, где большая часть норм имеет повелительный, императивный характер. Примером повеления может служить содержащееся в КоАП указание на то, что должностное лицо должно в установленный законом срок предоставить информацию;

2) **запрет** – возложение на участников информационных правоотношений обязанности воздерживаться от совершения каких-либо действий. Цель запретов – предотвращение информационных правонарушений. Чаще всего этот способ применяется в уголовном праве. Например, гл. 28 УК РФ «Преступления в сфере компьютерной информации» содержит запреты на «неправомерный доступ к компьютерной информации» (ст. 272), «создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273), «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Диспозитивные методы, основанные на равенстве участников правоотношений и их возможности самостоятельно выбирать модель поведения, включают в себя:

1) **дозволение** – предоставление участникам информационных правоотношений права совершать какие-либо действия либо не совершать их по своему выбору, например, в сфере библиотечного дела, гражданско-правовых отношениях;

2) **согласование** – достижение согласия между субъектами. Метод согласования широко применяется в сфере регулирования интеллектуальной собственности;

3) **рекомендации** – указание на предпочтительную модель поведения участников информационных правоотношений, например, при регулировании деятельности СМИ.

В информационном праве могут использоваться и иные методы правового регулирования. В целом можно отметить, что информационное право использует в равной степени как императивные методы, характерные для публичного права, так и диспозитивные, присущие частному праву.

Принципы информационного права

Принципы – основные исходные положения, юридически объясняющие и закрепляющие объективные закономерности общественных отношений, проявляющихся в информационной сфере.

Принципы информационного права базируются на положениях основных конституционных норм, закрепляющих информационные права и свободы и гарантирующих их осуществление, а также на особенностях и юридических свойствах информации как объекта правоотношений.

Выделяют следующие **основные принципы:**

1. Принцип приоритетности прав личности. Статья 2 Конституции РФ утверждает, что признание, соблюдение и защита прав и свобод

человека и гражданина – обязанность государства. Отсюда следует, что органы государственной власти обязаны защищать права и свободы человека и гражданина в информационной сфере.

2. Принцип свободного производства и распространения любой информации, не ограниченной федеральным законом. Свобода мысли и слова, свобода творчества и волеизъявления являются базовыми демократическими ценностями. Однако свобода мысли, мнений, убеждений не может быть реализована, если невозможно их свободно высказать, донести до других свои знания или продукты творческого труда.

3. Принцип запрещения производства и распространения информации, вредной и опасной для развития личности, общества, государства. Запрет направлен на защиту интересов и свобод личности и общества от воздействия такой информации, распространение которой может привести к нарушению информационных прав и свобод, дестабилизации общества и нарушению целостности государства.

4. Принцип свободного доступа (открытости) информации, или принцип гласности. Ни одна государственная структура не может вводить ограничений по доступу потребителей к информации, которой она обладает в соответствии с установленной для нее компетенцией, затрагивающей права и свободы человека и гражданина и представляющей общественный интерес.

5. Принцип полноты обработки и оперативности предоставления информации. Только имея полную, достоверную и своевременно предоставленную информацию субъекты социальной и экономической деятельности могут принимать адекватные ситуации решения.

6. Принцип законности. Субъекты информационного права обязаны строго соблюдать Конституцию РФ и законодательство Российской Федерации.

7. Принцип ответственности. За нарушение информационных прав граждан предусмотрена дисциплинарная, административная и уголовная ответственность.

8. Принцип оборотоспособности информации основан на юридическом свойстве обособляемости информации от ее создателя (обладателя) на основе ее овеществляемости. Информация, будучи обнародованной, превращается в объект, существующий независимо от ее создателя, и поэтому может быть включена в общественный оборот.

9. Принцип информационного объекта (информационной вещи), или принцип двуединства информации и ее носителя, основан на свойстве двуединства материального носителя и содержания информации, отображенной на нем.

Система информационного права

Внутри отрасли информационного права нормы группируются в подотрасли и институты.

Структурно система информационного права подразделяется на две части – Общую и Особенную.

В Общей части сосредоточиваются нормы, устанавливающие основные понятия, общие принципы, правовые формы и методы правового регулирования информационных отношений. Дается характеристика источников информационного права. Определяется специфика информационных правоотношений, субъектов и объектов информационного права.

Особенная часть включает в себя отдельные институты информационного права, в которых сгруппированы близкие по смысловому содержанию информационно-правовые нормы. Таких институтов довольно много. Можно выделить несколько групп:

1) правовое регулирование отношений по поводу обращения общедоступной информации. Право на информацию, информационные функции государства. Правовое регулирование деятельности средств массовой информации, рекламы, функционирования общедоступных информационных ресурсов (библиотек, архивов и т.д.);

2) режим документированной информации, электронный документооборот, формирование электронного правительства;

3) порядок создания и применения информационных технологий и информационных систем;

4) правовой режим информации ограниченного доступа. Виды тайн;

5) информационная безопасность личности, общества и государства.

Тема 3. ИНФОРМАЦИОННЫЕ ПРАВООТНОШЕНИЯ

Понятие и виды информационных правоотношений

Информационные правоотношения возникают, изменяются и прекращаются в информационной сфере и регулируются информационно-правовыми нормами. Являясь разновидностью правовых отношений, они выражают все основные признаки правовых отношений.

Нормы информационного права регулируют далеко не все, лишь наиболее важные группы общественных отношений, которые имеют существенное значение для интересов личности, общества и государства. Не любое отношение, сложившееся в информационной сфере, может быть подвергнуто правовому регулированию. Причинами этого являются нецелесообразность правового вмешательства в отдельные сферы жизни граждан и невозможность внешнего контроля за исполнением тех или иных нормативных предписаний в силу специфики объекта регули-

рования. Например, невозможно урегулировать нормами права процесс творчества, установить порядок создания произведения или запретить распространение анекдотов. Таким образом, не всякое общественное отношение, сложившееся в связи с поиском, получением передачей, производством, распространением, преобразованием и потреблением информации, выступает в форме информационного правоотношения.

Выделим основные виды информационных правоотношений.

Различаются ***регулятивные*** и ***охранительные*** правоотношения. Регулятивные связаны с дозволенной деятельностью по поиску, получению передаче, производству и распространению информации. Данные отношения возникают из правомерных действий участников. Охранительные правоотношения возникают с связи с совершенными правонарушениями. Так, за воспрепятствование распространению продукции средства массовой информации виновные несут ответственность согласно ст. 13.16 КоАП.

Помимо этого проводится деление на ***материальные*** и ***процедурные***. Материальные информационные правоотношения складываются по поводу реализации прав и обязанностей субъектов данных отношений. Примером подобного рода правоотношений могут служить отношения, возникшие в результате реализации журналистом права быть принятым должностными лицами в связи с запросом информации (ст. 47 закона РФ «О СМИ»). Процедурные информационные правоотношения складываются по поводу процедуры их возникновения, изменения или прекращения. Например, при оформлении граждан на допуск к сведениям особой важности.

В зависимости от вида связи между субъектами информационных правоотношений они делятся на ***абсолютные*** и ***относительные***. В абсолютных информационных правоотношениях управомоченному субъекту противостоит неопределенное количество пассивно обязанных лиц, которые не должны нарушать его права и чинить препятствия в реализации его юридических возможностей. Примером абсолютного правоотношения может служить правоотношение между автором/правообладателем и читателями зрителями, слушателями его произведения, которые должны соблюдать его авторские права.

В относительных информационных правоотношениях управомоченному субъекту в качестве обязанных противостоят точно поименованные лица. Таковы, например, отношения между работодателем и работниками, складывающиеся по поводу охраны коммерческой тайны.

Очень важным и присущим именно информационному праву представляется деление правоотношений на ***целевые*** и ***обеспечивающие.***

Информационно-правовой характер носят многие нормы различных отраслей права (например, нормы Налогового кодекса РФ о декларировании и отчетности, нормы Земельного кодекса РФ о мониторинге земли, нормы Уголовно-процессуального кодекса РФ о процессуальных

действиях со свидетелем и другими лицами и т.п.). В данных случаях получение или предоставление информации являются не самостоятельной целью деятельности, а только способом достичь желаемую цель. Поэтому подобные отношения называют обеспечивающими[7].

Вместе с тем можно выделить информационные отношения, представляющие собой одновременно и средство для достижения конкретных целей, и определенный результат именно информационной деятельности (например, отношения, возникающие при производстве и распространении печатного издания, при применении механизмов информационной безопасности, создании и функционировании ГАС «Выборы», ГАС «Правосудие» и др.). В данном случае и средства достижения определенных целей, и результат этих действий находятся в информационной сфере и носят информационно-правовой характер. Такие отношения будут называться целевыми.

Классификация информационных правоотношений может быть проведена в соответствии с тем, какие информационные процессы осуществляются:

1) информационные правоотношения, возникающие при осуществлении поиска, получения и потребления информации. В данном случае на первый план выходят фигуры потребителей информации, т.е. тех лиц, которые реализуют свое конституционное право на поиск и получение информации. В этот круг входят граждане, организации, пользователи библиотек, журналисты, потребители рекламы и т.д. В то же время участниками таких правоотношений являются обладатели информации;

2) информационные правоотношения, возникающие при производстве, передаче и распространении информации, информационных ресурсов, информационных продуктов, информационных услуг. Здесь ведущую роль играют производители информации: издательства, редакции, рекламодатели, рекламопроизводители, журналисты, авторы произведений, органы государственной власти. При передаче и распространении информации правоотношения складываются преимущественно в области связи, международного информационного обмена. Соответственно участниками этих отношений выступают организации связи, операторы связи, пользователи услуг связи рекламораспространители;

3) информационные правоотношения, возникающие при создании и применении информационных систем, их сетей и средств обеспечения. Фактически, это отношения по проектированию и эксплуатации указанных информационных объектов. Следовательно, правоотношения будут складываться между авторами (разработчиками), собственниками, потребителями и такими органами, как Министерство информационных технологий и связи РФ, Федеральная служба по надзору в сфере связи,

[7] Подробнее об этом см.: *Ловцов Д.А.* Информационные правоотношения: особенности и продуктивная классификация // Информационное право. 2009. № 1. С. 3.

Федеральное агентство по информационным технологиям, органы по сертификации и испытательные центры;

4) информационные правоотношения, возникающие при создании и применении средств и механизмов информационной безопасности. Осуществление безопасности государства, в том числе и информационной, – дело специальных служб, поэтому основную роль здесь будут играть Правительство РФ, Совет безопасности РФ, Федеральная служба безопасности РФ, служба специальной связи и информации при Федеральной службе охраны РФ, Федеральная служба по техническому и экспортному контролю РФ, Межведомственная комиссия по защите государственной тайны.

Характеристика основных объектов информационных правоотношений

Согласно ст. 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (далее – закон «Об информации») **информация может являться объектом публичных, гражданских и иных правовых отношений**. Она может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

В то же время информация (в ее идеальном, содержательном аспекте) как объект правоотношений изучена мало. Она создается и воспринимается субъектом в соответствии с его потребностями, интересами и целями. Перенос информации на материальный носитель не материализует ее. Материален лишь носитель информации. Идеальный характер информации усложняет процесс правового регулирования информационных отношений, ограничивает возможность распространения на информацию института вещной собственности. Несмотря на то что носитель информации является вещью, информация в правовом смысле не может рассматриваться как вещь. Когда мы передаем вещь, мы зачастую передаем весь объем прав (владения, пользования, распоряжения). Но когда мы передаем зафиксированную на материальном носителе информацию, мы в правовом смысле передаем сам носитель и сумму каких-то прав по распоряжению содержащейся на нем информации (например, право ее дальнейшего распространения)[8]. Одна и та же информация может находиться у неограниченного круга лиц, а с вещью это невозможно. Информация может быть мгновенно скопирована и воспроизведена большое число раз, а вещь – нет. Поэтому информация как объект права относится

[8] Подробнее см.: *Кузьмин В.П.* Понятие и юридическая сущность информации // Информационное право. 2009. № 2. С. 4–8.

к особым объектам исключительных прав, требующим своего законодательного закрепления[9].

Получение информации не может обеспечить полный объем вещных прав на нее. Право собственности распространяется только на материальный носитель информации. В то же время ценность информации не зависит от стоимости ее носителя. Она определяется теми последствиями, которые следуют за получением информации.

Конструирование абсолютного субъективного права на информацию затруднено еще и тем обстоятельством, что правом возможно урегулировать лишь такие отношения, объект которых поддается внешнему контролю и тем самым попадает в правовое поле. Информация, если ее и рассматривать в качестве сведений, такому контролю поддается слабо (поскольку сведения регенерируются актами их передачи и обладают мультиплицирующими свойствами, которые юридической наукой изучены в недостаточной мере) в силу ее особенностей.

Видимо, поэтому **с 1 января 2008 года информация исключена из перечня объектов гражданских прав (ст. 128 ГК РФ).**

На современном этапе **законодатель предпочитает регулировать отношения, объектом которых выступает не информация, а производные от нее продукты и деятельность, связанная с ними.** Подобный подход законодателя объясняется как раз отсутствием юридической модели специального права на информацию, которое бы выполняло функции, аналогичные функциям вещного права собственности.

В.А. Копылов предлагает ввести понятие «информационная собственность», т.е. «право собственности на исключительное право использования содержания информация, отображенной в конкретном экземпляре информационного объекта, подтверждающее это исключительное право»[10]. Тем самым он пытается соединить вещную и интеллектуальную собственность. Но пока это одна из научных гипотез.

Важно отметить, что в законе «Об информации» нет понятий «собственность на информацию» и «собственник информации». В ст. 2 вводится понятие «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.

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами

---

9 См.: *Семилетов С.И.* Информация как особый объект права //Проблемы информатизации. 1999. № 3. С. 58.

10 *Копылов В.А.* Информационное право: вопросы теории и практики. М., 2003.

местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации, 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 и 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.

Обладатель информации 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.

Другим важным объектом информационных правоотношений является **документ**. Легальное определение документированной информации мы встречаем в трех федеральных законах.

Согласно ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» **«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».** В данном определении законодатель указывает, во-первых, на неразрывную связь содержания с материальным носителем и, во-вторых, на особый элемент документированной информации, а именно ее реквизиты, подлежащие закреплению на том же материальном носителе.

В Федеральном законе «О библиотечном деле» от 29 декабря 1994 г. документ определен как «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).

Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 года определяет документ как «материальный носитель с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, предназначенный для передачи во времени и пространстве в целях общественного использования и хранения» (ст. 1).

Таким образом, в перечисленных федеральных законах были актуализированы два противоположных подхода к документированной информации. В федеральных законах 1994 года при определении документа акцент был сделан на **материальный носитель** с зафиксированными на нем сведениями. В Законе об информации смысловой акцент переносится на **информацию**, особым образом зафиксированную на материальном носителе.

С понятием документа тесно связано понятие **«информационные ресурсы»**. В широком смысле информационные ресурсы – это совокупность сведений, отражающих накопленные знания в той или иной области человеческой деятельности, представленных в какой-либо объективной форме и систематизированных определенным образом. Действующий закон «Об информации» такого термина не содержит. Обычно под информационными ресурсами понимают документы и массивы документов, а также документы и массивы документов (библиотеки, архивы, фонды, банки данных), подготовленные и систематизированные в удобной и пригодной для использования форме.

Информационные ресурсы (в отличие от всех других видов ресурсов – трудовых, энергетических, минеральных и т.д.) тем быстрее растут, чем больше их расходуют.

Информационные технологии проникли практически во все сферы государственного и муниципального управления, экономики, политики, социальной жизни и используются для решения самых разнообразных задач. Повышая эффективность государственного управления и бизнес-процессов, информационные технологии в то же время способны качественно изменять само содержание этих процессов, оказывая тем самым существенное влияние на государство и общество. Именно на таком, широком, понимании информационных технологий базируется их определение, данное в законе «Об информации»: **информационные технологии –** процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

В последнее время под информационными чаще всего понимают компьютерные технологии, с помощью которых осуществляются хранение, преобразование, защита, обработка, передача и получение информации.

Основные черты современных информационных технологий:

– компьютерная обработка информации по заданным алгоритмам;

– хранение больших объёмов информации на машинных носителях;

– передача информации на любые расстояния в ограниченное время.

В законе «Об информации» перечислены следующие объекты информационных правоотношений:

– 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.

Информационная система включает в себя следующие объекты:

– средства вычислительной техники, информационно-вычислительные системы, комплексы и сети;

– программные средства – операционные системы, системы управления, прикладные программы, программные средства телекоммуникации и др.;

– базы и банки данных, т.е. представленная в объективной форме информация, систематизированная таким образом, чтобы она могла быть найдена и обработана с помощью компьютера.

Выделяют следующие требования к информационным системам:

– эффективность – соотношение затрат и получаемых результатов;

– качество функционирования – степень приспособленности системы к выполнению заданных функций;

– надежность – безотказность работы системы (отказ системы может выражаться в снижении производительности, появлении большого количества ошибок и др.);

– безопасность – защищенность информации (ее целостности, конфиденциальности, доступности) и объектов самой системы.

Основные цели внедрения информационных систем:

– автоматизация применения математических методов к решению управленческих задач;

– частичное освобождение сотрудников от рутинного труда;

– минимизация вероятности появления ошибок в ходе передачи либо обработки информации;

– снижение объема бумажных документов и совершенствование документооборота;

– ускорение подготовки решений и передачи документов.

В последнее время важными целями применения информационных систем называют возможность общественного контроля за деятельностью органов власти и их должностных лиц и снижение коррупциогенности принятия управленческих решений.

Более подробный анализ правового режима отдельных объектов информационных правоотношений будет дан в соответствующих главах учебного пособия.

Система источников информационного права

Система информационного законодательства – это совокупность законов и издаваемых в соответствии с ними иных нормативных правовых актов, посвященных прямому или опосредованному ре-

гулированию отношений, объектом которых является информация, информационные продукты и связанная с ними деятельность.

Система информационного законодательства включает в себя:

1)международные правовые акты;

2)конституционные нормы;

3)правовые акты федеральных органов:

– акты, регулирующие собственно информационные отношения,

– акты других отраслей права,

4) акты органов субъектов Российской Федерации.

Международные правовые акты

Значение международных правовых актов для регулирования правоотношений, протекающих в информационной сфере, обусловлено рядом обстоятельств. Распространение информации носит трансграничный характер. Международная сеть телекоммуникаций дает возможность донести сведения, знания, идеи до мировой общественности. С развитием Интернета, независимых СМИ удержать распространение информации все сложнее. Происходит рост глобальной электронной торговли и международных финансовых институтов. Развивается многостороннее сотрудничество в области образования, развития науки, культуры. Правонарушения с использованием информационных технологий и средств обеспечения также носят международный характер. При этом зачастую происходит «сшибка» национальных законодательств, отсутствуют единые нормы, единое понимание глобальных угроз, которые ведут к неэффективности отдельных запретов либо иных попыток регулирования в сфере информационных отношений. Все это делает необходимым развитие именно международного сотрудничества в области информационного права.

Впервые «право на свободу информации» на международном уровне было закреплено **ст. 19 Всеобщей декларации прав человека 1948 года:** «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами независимо от государственных границ».

Совершенствование механизмов обеспечения этого права граждан привело к формированию **концепции права универсального доступа или универсальной услуги.** Иными словами, речь идет об обеспечении государством определенных стандартов доступа возможно большего числа граждан к мировому информационному наследию.

Сегодня право универсального доступа к информации или право на универсальное информационное обслуживание рассматривается как новое социально-экономическое право в системе прав и свобод.

Это положение нашло свое развитие и в **Окинавской хартии глобального информационного общества 2000 г**., где указывалось, в частности, на необходимость преодоления «цифрового разрыва» внутри государств и между ними, стратегию развития людских ресурсов, возможности которых соответствовали бы требованиям информационного века.

Женевская декларация принципов универсального и недискриминационного доступа к ИКТ 2003 г. устанавливает, что необходимым фундаментом построения информационного общества являются развитие информационной и коммуникационной инфраструктуры, устранение барьеров на пути достижения равноправного доступа к информации, формирование глобальной культуры кибербезопасности.

Продолжением идей Женевской декларации стали положения **Тунисского обязательства 2005 г.** о том, что для информационного общества существенное значение имеет реализация принципа **свободного потока информации, идей и знаний**. В связи с этим нужно оказывать содействие в обеспечении повсеместного, равноправного и приемлемого в ценовом отношении доступа к ИКТ, включая универсальные концепции и ассистивные технологии, для людей во всем мире, в особенности для лиц с физическими и умственными недостатками, пожилых людей, мигрантов, беженцев, безработных, представителей маргинализированных и уязвимых групп общества.

Другим важным аспектом права на информацию является **право на доступ к официальной информации или «право знать».** Советом Европы была принята рекомендация No R (81) 19 от **25 ноября 1981 г. «О доступе к информации, находящейся в ведении государственных ведомств»,** в которой говорится: «Каждый человек, находящийся под юрисдикцией государства-члена, имеет право получения по запросу информации, находящейся в распоряжении государственных ведомств, за исключением законодательных органов и органов судебной власти. При этом допускаются лишь четко определенные ограничения и исключения, связанные с обеспечением конфиденциальности охраняемых видов информации, разглашение которой в соответствии с законом не может быть осуществлено в обычном порядке».

Получение официальной информации является способом увеличения прозрачности деятельности органов власти и потому на государствах лежит долг обеспечить систематический доступ граждан через электронные средства коммуникации ко всем документам, которые по закону являются общественным достоянием.

Параллельно с развитием права на информацию развивалось и **право на защиту информации о частной жизни граждан**. Начало этого направления соотносится с принятием важнейших международно-правовых актов: **Всеобщей декларации прав человека 1948 года, Европейской конвенции о защите прав человека и основных свобод**

1950 года, Международного пакта о гражданских и политических правах 1966 года, закрепивших общеобязательные нормы о правах человека, в частности право на защиту неприкосновенности частной жизни.

В 70–80-е годы XX века с развитием информационных отношений, технологий обработки и хранения информации и процессов глобализации о гражданах эта проблема стала рассматриваться через призму защиты персональных данных. Важным международным актом в данной области является **Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 года,** закрепившая норму о том, что каждое государство, ратифицировавшее Конвенцию, должно принять необходимые меры для того, чтобы основные принципы защиты данных, предусмотренные Конвенцией, были реализованы в национальном законодательстве. Фактически, принятие Конвенции установило единые требования защиты личной жизни в случае передачи персональных данных через границы государств, имеющих разное законодательство о персональных данных.

Формирование международно-правовой базы в сфере информационных отношений связано с **запретом на распространение вредной информации**. Международный пакт о гражданских и политических правах от 16 декабря 1966 года В ст. 1 определяет, что вся информация должна быть свободно обращающейся, но ст. 19 вводит ограничения свободы обращения информации, а ст. 20 исключает из сферы информационного обмена информацию, относящуюся к пропаганде войны, национальной, расовой или религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию. Распространение непристойной информации запрещается Международной конвенцией о пресечении обращения порнографических изданий и торговли ими от 12 сентября 1923 года. На предотвращение распространения информации незаконного содержания, в том числе и детской порнографии, направлена и резолюция Совета по телекоммуникациям Европейской комиссии от 27 сентября 1996 года.

23 ноября 2001 года была заключена **Конвенция Совета Европы «О киберпреступности».** На сегодняшний день ее участницами являются 42 страны, в том числе и Армения, Великобритания, Венгрия, Германия, Греция, Дания, Испания, Италия, Канада, Латвия, Литва, Польша, Словения, США, Украина, Финляндия, Франция, Швеция, Эстония, Япония и др. Конвенция вступила в силу 1 июля 2004 года.

Россия подписала эту Конвенцию с заявлением (распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп). В заявлении говорилось, что Россия определится в вопросе о своем участии в Конвенции при условии возможного пересмотра п. «b» ст. 32 этого документа.

Статья 32 Конвенции посвящена трансграничному доступу к общедоступным и компьютерным данным, хранящимся на территории страны-участницы. Ставший камнем преткновения п. «b» предусматривает воз-

можность «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему»[11].

Представители Российской Федерации посчитали, что данная норма может нанести ущерб суверенитету и национальной безопасности нашей страны, правам и законным интересам граждан и юридических лиц.

Поскольку данное положение пересмотрено не было, в марте 2008 года Россия отозвала свою подпись (распоряжение Президента РФ от 22 марта № 144-рп).

Рост глобальной электронной торговли, развитие международных финансовых институтов, двустороннее и многосторонне сотрудничество в области образования, развития науки, международная сеть телекоммуникаций – все это отражается в международных актах (существуют международные документы, посвященные электронной торговле, охране авторских прав и т.д.). Мы будем их рассматривать в соответствующих разделах.

Конституционная основа информационного права Российской Федерации

Право на информацию относится к важнейшим конституционным правам и свободам граждан. В соответствии с п. 4 ст. 29 Конституции РФ «каждый имеет право искать, получать, передавать, производить и распространять информацию любым законным способом».

Формулировка, данная в Конституции РФ, отличается от формулировки ст. 19 Всеобщей декларации прав человека и включает в себя 5 правомочий.

Из содержания конституционной нормы вытекает ряд юридических возможностей:

во-первых, возможность доступа к информации через право «искать» и «получать»;

во-вторых, возможность выражения своих идей, мнений и знаний через право «передавать» и «распространять»;

в-третьих, возможность создавать некий информационный продукт, результат собственной интеллектуальной деятельности через право «производить».

Одной из особенностей права на информацию в теоретическом аспекте является то, что оно одновременно может быть отнесено и к группе политических, и к группе личных прав граждан.

[11] Конвенция официально опубликована не была. Перевод на русский язык предоставлен Аппаратом Государственной Думы Федерального Собрания РФ. URL: http://www.medialow.ru (дата последнего обращения: 25 апреля 2010).

Отнесение этого права к личным правам необходимо, поскольку, во-первых, право на информацию, как и любое из личных прав, тесно связано непосредственно с личностью своего обладателя, во-вторых, оно неотчуждаемо и принадлежит каждому человеку от рождения.

Политическую направленность это право приобрело в связи с возникновением нормы о свободе именно массовой информации. Здесь важным является то, что получение и распространение массовой информации могут быть важным политическим инструментом, средством достижения политических целей.

Право на информацию ценно не только само по себе. Информационные права личности, помимо удовлетворения потребностей человека в образовании, культуре и общении, являются гарантией реализации других прав и свобод. Так, возможность доступа к общественно значимой информации является фундаментом для участия граждан в управлении делами государства, позволяет контролировать деятельность органов власти и общественных организаций. Поэтому в Конституции предусматривается определенная система гарантий права граждан на информацию, традиционно выражаемая в форме прямых конституционных запретов. Это следующие нормы:

1. «Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина не могут применяться, если они не опубликованы официально для всеобщего сведения»; «законы подлежат обязательному опубликованию, неопубликованные законы не действуют» – ст. 15.

2. «Каждый имеет право на личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» – ст. 23.

3. «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» – ст. 24.

4. «Перечень сведений, составляющих государственную тайну, определяется федеральным законом» – ст. 29.

5. «Органы государственной власти и органы местного самоуправления, должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом» – ч. 2 ст. 24.

Конституция РФ устанавливает также принцип ответственности за нарушение права граждан на информацию: «Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом» – ч. 3 ст. 41.

Считается, что право на информацию представляет собой четвертое, самое «молодое» поколение субъективных прав и свобод человека[12].

---

12 См.: *Головистикова А.Н., Грудцына Л.Ю.* Права человека: Учебник. М., 2008. С. 144.

Фактически, право на информацию может быть реализовано различными способами: посредством межличностного общения (в том числе и на собраниях и митингах, сходах граждан), обращения в органы государственной власти Российской Федерации и субъектов Российской Федерации, в процессе обучения, при помощи средств массовой информации.

Информационное законодательство – основной источник информационного права

Среди правовых актов федеральных органов главное место занимают **федеральные законы.** Они обладают высшей юридической силой, регулируют наиболее важные, основополагающие отношения.

Несмотря на то что информационное законодательство находится на этапе своего становления, уже сегодня можно говорить о системе информационного законодательства.

Среди законов выделяется базовый для информационной сферы **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** (далее – закон «Об информации»), пришедший на смену Федеральному закону от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации».

Новым законом регулируются три группы взаимосвязанных между собой отношений, складывающихся при:

– осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

В законе «Об информации» 2006 года получили закрепление вопросы, связанные с правомочиями обладателя информации (ст. 6), правом на доступ к информации (ст. 8), ограничением доступа к информации (ст. 9), государственным регулированием отношений в сфере применения информационных технологий (ст. 12), структурой и построением информационных систем (ст. 13, 14) и т.д. Классификация информации (см. тему 1) дана по этому же закону.

К актам информационного законодательства федерального уровня относится и **Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 г. № 77-ФЗ.** Данный нормативный акт определяет политику государства в области формирования обязательного экземпляра документов как ресурсной базы комплектования библиотечно-информационного фонда России и развития системы государственной библиографии, предусматривает обеспечение сохранности обязательного экземпляра документов, его общественное использование. Федеральный закон «Об обязательном экземпляре документов» отличает сугубо административно-правовой характер регулирования.

Важную роль в реализации информационных функций государства, повышении открытости органов госвласти призваны сыграть недавно принятый **Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»,** вступивший в силу 1 января 2010 года, а также **Федеральный закон от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».**

Механизм реализации конституционного права граждан на обращение с заявлениями, предложениями, жалобами в государственные органы власти предусмотрен **Федеральным законом «О порядке рассмотрения обращений граждан» от 2 мая 2006 года № 59-ФЗ.**

Видное место среди источников информационного права занимает **закон РФ «О средствах массовой информации» от 27 декабря 1991 года № 2124-I,** представляющий собой комплексный нормативный акт, регламентирующий отношения, возникающие в процессе организации и функционирования средств массовой информации. В основных разделах закона нашли свое правовое регулирование вопросы организации деятельности средств массовой информации, распространения массовой информации, отношения СМИ с гражданами и организациями, прав и обязанностей журналиста, ответственности за нарушение законодательства о СМИ.

Ряд законов регулируют правовой режим информации ограниченного доступа. Особое место здесь принадлежит **закону РФ «О государственной тайне»** от **21 июля 1993 года № 5485–1**. Данным нормативным актом регламентируются отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием, рассекречиванием и защитой в интересах безопасности Российской Федерации. Принципы охраны конфиденциальной информации устанавливают также **Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ, Федеральный закон «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ,** Перечень сведений конфиденциального характера (утвержден указом Президента РФ от 6 марта 1997 года № 188).

На современном этапе большое значение приобретает развитие электронного документооборота. В связи с этим был принят **Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ,** целью которого является обеспечение правовых условий использования электронной цифровой подписи в электронных документах.

Формирование информационного общества невозможно без обеспечения информационной безопасности граждан, общества и государства. Этому призваны способствовать **закон РФ «О безопасности» от 5 марта 1992 года № 2446-I, Доктрина информационной безопасности Российской Федерации** (утверждена Президентом РФ 9 сентября 2000 года

№ Пр-1895), **Концепция национальной безопасности Российской Федерации** (утверждена Президентом РФ 10 января 2000 года № 24).

Система информационного законодательства включает в себя не только правовые акты федеральных органов, но и **акты органов субъектов Российской Федерации**. Это обусловлено, в частности, тем обстоятельством, что Конституция РФ в п. «и» ст. 71 относит информацию и связь к ведению Российской Федерации и в то же время защиту прав и свобод человека и гражданина в информационной сфере к совместному ведению Российской Федерации и субъектов Федерации (п. «б» части первой ст. 72 Конституции РФ).

Например, ряд статей Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» предусматривает принятие нормативных актов субъектов Федерации. Поэтому конец 2009 – начало 2010 года ознаменовались принятием законов субъектов Российской Федерации об обеспечении доступа к информации о деятельности государственных органов субъектов Российской Федерации и соответствующих постановлений правительств, изменением регламентов и утверждением перечней информации, размещаемой в сети Интернет. Так, в регламенте Саратовской областной думы появилась новая ст. 36.1, которая устанавливает порядок присутствия граждан на открытых заседаниях областной думы, был принят закон Саратовской области «Об обеспечении доступа к информации о деятельности государственных органов Саратовской области» от 25 декабря 2009 года № 217-ЗСО (ст. 4). Аналогичные нормативные акты были приняты в Читинской, Рязанской и других областях.

В условиях, когда российские регионы характеризуются большими различиями в уровне информатизации, особое значение приобретает опыт передовых регионов, одним из которых является Ханты-Мансийский автономный округ. Он устойчиво входит в пятерку лидеров по уровню развития информационных технологий и он имеет самое большое количество пунктов общественного доступа в Интернет по сравнению с другими субъектами Российской Федерации. Округ стал первым российским регионом, в котором на государственном уровне стала решаться задача обучения взрослых граждан навыкам пользования современными информационно-коммуникационными технологиями. Эти успехи были достигнуты благодаря системному развитию регионального законодательства. Всего с 1996 году в округе было принято 175 постановлений, распоряжений губернатора и правительства по вопросам использования и защиты информационных ресурсов, а также формирования правового поля в области реализации мероприятий федеральной целевой программы «Электронная Россия»[13].

[13] См.: *Маслова Н.Р.* Состояние и проблемы формирования правовой основы реализации «Стратегии развития информационного общества в России» на федеральном и региональном уровне // Информационное право. 2009. № 2. С. 16.

Тема 4. СУБЪЕКТЫ ИНФОРМАЦИОННОГО ПРАВА

Личность – основной субъект информационных правоотношений

Круг субъектов информационного права весьма разнообразен. Участниками информационных правоотношений выступают физические и юридические лица, а также публичные образования, являющиеся носителями предусмотренных информационным законодательством прав и обязанностей.

Субъекты информационных правоотношений имеют определенный правовой статус. Общий правовой статус связан с наличием или отсутствием правоспособности и дееспособности субъекта в этой области. Правоспособность в данной сфере – способность лица иметь информационные права и обязанности. Дееспособность – способность реализовывать эти права и обязанности в практической деятельности.

Начнем с определения **информационного правового статуса физических лиц.** Категория субъектов может быть представлена в правовых актах как «гражданин», «индивид», «человек», личность», «лицо». Глава 2 Конституции «Права и свободы человека и гражданина» признает и гарантирует закрепленные в ней права согласно общепризнанным принципам и нормам международного права. Субъекты, на которых распространяется действие данной главы Конституции, названы термином «каждый». Статья 62 Конституции устанавливает, что «иностранные граждане и лица без гражданства пользуются в Российской Федерации правами и несут обязанности наравне с гражданами Российской Федерации, кроме случаев, установленных федеральным законом или международным договором Российской Федерации».

Общий правовой статус в области права на информацию зафиксирован ст. 29 Конституции, где говорится, что «каждому гарантируется свобода мысли и слова» (п. 1), «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (п. 4). Таким образом, общим правовым статусом в информационном праве будут обладать и граждане Российской Федерации, и иностранцы, и лица без гражданства.

Правоспособность может быть ограничена. Например, согласно ст. 7 закона РФ «О средствах массовой информации» учредителем СМИ не может выступать гражданин, не достигший восемнадцатилетнего возраста либо отбывающий наказание в местах лишения свободы по приговору суда, либо душевнобольной, признанный судом недееспособным, а также гражданин другого государства или лицо без гражданства, не проживающее постоянно в Российской Федерации.

В последнее время активно обсуждается правовой статус детей в информационной сфере. В информационном праве правоспособность

возникает еще до рождения ребенка: например, право на доступ к завещанию, которое было составлено на имя ребенка, не родившегося к моменту составления и вступления в силу документа. Право на защиту от вредного, в том числе и информационного, воздействия на плод пока не отражено в праве, но должно стать гарантией права на здоровье матери и ребенка. Ребенок может сам реализовать право на доступ к информации в период дошкольного и школьного воспитания и образования. Книги, аудио- и телепередачи, доступные для него с согласия или без согласия родителей формируют его информационное поле. Задача права – создать такие гарантии, которые оградят ребенка от нежелательного информационного воздействия и обяжут ответственных лиц (родителей, воспитателей, учителей) обеспечить необходимые условия для здорового информационного развития ребенка.

Говоря о дееспособности, т.е. способности реализовывать свои информационные права, надо иметь в виду п. 2 ст. 26 ГК РФ, согласно которому несовершеннолетние в возрасте от 14 до 18 лет вправе самостоятельно, без согласия родителей, усыновителей и попечителей распоряжаться своим заработком, стипендией или иными доходами (в том числе и приобретать печатные издания, аудиопродукцию, иные объекты информационных ресурсов); осуществлять права автора произведения науки, литературы или искусства, изобретения или иного результата интеллектуальной деятельности, т.е. создавать информационную продукцию; иметь электронную карту при распоряжении своим вкладом в кредитном учреждении. Малолетние в возрасте от 6 до 14 лет могут совершать мелкие бытовые сделки: например, получать телефонные услуги, выходить в Интернет, совершать иные действия, за последствия которых ответственность несут их родители.

Как отмечает Н.Н. Ковалева, «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»[14]. Например, согласно ст. 2 закона «О СМИ» «под главным редактором понимается лицо, возглавляющее редакцию и принимающее окончательные решения в отношении производства и выпуска средства массовой информации». Таким образом, дееспособность главного редактора возникает с момента назначения его на должность и возложения соответствующих обязанностей. В соответствии со ст. 1228 ГК РФ «автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат», т.е. способность реализовывать авторские права возникает только после создания произведения или иного результата творческой деятельности.

---

14 *Ковалева Н.Н.* Указ. соч. С. 61.

Если гражданин принадлежит к какой-то определенной категории и на него возложены специальные обязанности, он обладает **специальным правовым статусом.** Например, специальным правовым статусом в информационном праве обладает судья, на которого возлагается обязанность не разглашать суждения, имевшие место при обсуждении и постановлении приговора (ст. 298 УПК). Специальным правовым статусом обладает журналист, имеющий целый ряд прав и обязанностей. Специальный правовой статус в области информации будет реализовываться также субъектами, заключающими трудовой договор: гражданин обязан предоставить свои документы в составе, определенном государством для конкретного места работы, а наниматель – обеспечить полноту и достоверность получаемой работником информации для заключения договора. В данном случае мы видим тесную связь трудового правоотношения (само заключение договора) и информационного. Информационное правоотношение предшествует трудовому и сопутствует ему.

Органы государственной власти и должностные лица как субъекты информационных правоотношений

Правовой статус органов государственной власти, служащих государственной службы устанавливается Конституцией РФ, федеральными законами и нормативно-правовыми актами субъектов Российской Федерации. В этих актах в определенной степени затрагиваются вопросы информационного характера. Применительно к органу, его подразделениям и должностям служащих устанавливаются структура информационного ресурса, способы получения и использования информации в процессе служебной деятельности. При этом информационная деятельность носит обеспечительный характер. Вся информационная работа подчинена роли и обязанностям органа государственной власти. Определяющими являются статус органа государственной власти, его место в системе государственной власти, но, кроме того, действуют нормы, устанавливающие порядок работы с документами, который определен специальными актами в области документирования и установления режима информации. Как отмечает И.Л. Бачило, «гражданин с момента своего рождения находится в различных формах контакта с информационным пространством своего местопребывания. И в связи с этим важно установить, кто призван гарантировать его право на информацию и кто обязан обеспечить защиту его интересов в рассматриваемой области. Наиболее тесные связи у гражданина возникают с органами исполнительной власти и местного самоуправления. Регистрация рождения, получение паспорта, регистрация по месту постоянного жительства и месту пребывания, оформление жилищно-коммунальных услуг, прикрепление к учреждениям здравоохранения и получение страхового полиса, решение вопросов пенсионного обеспечения и т.д. – все это действия, которые порождают определенные

документы и создают блоки документированной информации, определяющей статус гражданина»[15].

Правовое регулирование перечисленных правовых вопросов устанавливается различными нормативными правовыми актами.

Правовой статус организаций и учреждений (юридических лиц) в информационной сфере

Различают общий информационно-правовой статус организаций, обладающих правом юридического лица, и специальный информационно-правовой статус организаций, которые осуществляют функциональную деятельность в области сбора, хранения, обработки, передачи информации, ее распространения, т.е. деятельность на профессиональной основе.

В порядке осуществления **общего правового статуса** юридическое лицо реализует свои права, обязательства и обязанности в соответствии с ГК РФ, уставом конкретных организаций и учреждений, а также законодательством России, касающимся того или иного вида организаций. В рамках общего статуса будут решаться проблемы создания и приобретения информационных ресурсов, информационных технологий, формирования и поддержки систем информационной безопасности, развития информационного потенциала сотрудников.

Специальный статус организации, которая ориентирована исключительно на работу с информацией, осуществление информационных, коммуникационных услуг, получает обязательное оформление в федеральных законах и иных нормативных правовых актах Российской Федерации. Например, архивы, библиотеки, операторы связи и т.д.

В процессе формирования и использования государственных информационных ресурсов специализированными организациями используется особый правовой институт – лицензирование. Отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и юридическими лицами, индивидуальными предпринимателями в связи с осуществлением лицензирования своей деятельности, регулируются Федеральным законом «О лицензировании отдельных видов деятельности» № 128-ФЗ.

В этом случае информационная правосубъектность коммерческой организации связывается законодателем с двумя моментами – получением статуса юридического лица или индивидуального предпринимателя и лицензии. Например, ст. 2 Федерального закона «О связи» определяет оператора связи как юридическое лицо или индивидуального предпринимателя, оказывающее услуги на основании соответствующей лицензии.

---

15 *Бачило И.Л.* Информационное право: Учебник для вузов. М., 2009. С. 57.

Субъекты информационного права в публичных и гражданско-правовых отношениях

Один и тот же субъект может выступать участником информационных правоотношений, складывающихся в различных областях общественной жизни.

Для информационных отношений **публично-правового** характера свойственно деление субъектов на **две** группы:

1)потребители информации;

2)производители информации.

К **потребителям** относится широкий круг субъектов, испытывающих потребность в получении информации разного вида и назначения, необходимой им, прежде всего, для принятия соответствующих решений в повседневной деятельности. Это могут быть граждане, юридические лица, общественные объединения, фирмы, учреждения и предприятия, органы государственной власти и другие структуры, запрашивающие информацию. Они обладают равными правами на доступ к государственным информационным ресурсам. Информация, полученная гражданами и организациями на законных основаниях из государственных информационных ресурсов, может быть использована ими для создания производной информации.

Производителями информации в публично-правовых отношениях выступают **органы государственной власти и местного самоуправления**, исполняющие обязанности по информационному обеспечению физических и юридических лиц.

В **частноправовой сфере** информационного права (гражданский оборот информации) выделяется **три** категории субъектов**.**

1) производители информации, информационных ресурсов, информационных продуктов, информационных услуг, а также информационных систем, технологий и средств их обеспечения;

2) обладатели (держатели) информации, информационных ресурсов, информационных продуктов, информационных услуг, которые являются своего рода посредниками между производителями и потребителями информации;

3) потребители информации, информационных ресурсов, информационных продуктов, информационных услуг, т.е конечные получатели информации.

Каждый из них выступает в качестве собственника определенного информационного объекта.

Производитель информации является собственником **оригинала** информационного объекта, на котором произведенная им информация содержится. Информационные правомочия и право собственности на оригинал объекта он приобретает по факту создания информации.

Он обладает всеми информационными правомочиями, т.е. круг его правомочий самый широкий.

Обладатель (держатель) информации обладает определенным объемом полномочий в соответствии с условиями договора, заключенного им с производителем информации на тиражирование и распространение информации с учетом удовлетворения имущественных прав производителя информации. Одновременно он по условиям того же договора является собственником либо оригинала произведения (при передаче ему всех информационных правомочий), либо учтенной копии информационного объекта (при передаче части таких правомочий).

Потребитель информации обладает правомочиями только **в объеме права знать и применять в личной деятельности** содержание информации, отображенной в приобретенном им информационном объекте на условиях договора купли-продажи, в том числе и договора оферты. Ему запрещается тиражирование и распространение информации в коммерческих целях или нарушение имущественных прав производителя информации другими способами.

Модуль 2
ПРАВОВОЙ РЕЖИМ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ

Тема 5. ПРАВО НА ИНФОРМАЦИЮ

Институт права на информацию

Право на информацию является важнейшим институтом отрасли информационного права.

Институт права на информацию – это совокупность правовых актов и отдельных норм, определяющих порядок реализации прав субъектов информационного права в области поиска, получения передачи, производства и распространения информации в целях, не противоречащих правам и интересам человека, государства, общества, в соответствии с законодательством Российской Федерацией и нормами международного права.

Правовое закрепление права на информацию граждан в Российской Федерации имеет свою историю. В Конституции СССР 1977 года и в Конституции РСФСР 1978 года это право самостоятельно не выделялось. Оно было включено в систему политических прав и свобод. Конституция РСФСР закрепляла свободы слова, печати, собраний, митингов, уличных шествий и демонстраций. Косвенно право на информацию конституцион-

но фиксировалось в связи с гарантиями прав на образование, пользование достижениями культуры, участие в государственном управлении, внесение предложений в государственные и общественные органы об улучшении их деятельности. Кроме того, конституционно охранялись права на тайну переписки, телефонные переговоры и телеграфные сообщения. На самом деле в стране официально существовала цензура, правозащитники, деятели культуры, не согласные с режимом, отправлялись в ссылки, лишались гражданства и высылались из страны. Существовало большое количество «закрытой» информации: служебная тайна входила в систему государственных секретов, был ограничен доступ к значительному количеству книг и архивных материалов.

В полном объеме право на информацию было зафиксировано конституционно после принятия Верховным советом РСФСР в 1991 году Декларации прав и свобод человека и гражданина. Ныне действующая Конституция РФ содержит специальную норму о праве на информацию (ч. 4 ст. 29): «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Здесь же зафиксировано ограничение свободы относительно сведений, отнесенных к государственной тайне: «Перечень сведений, составляющих государственную тайну, определяется федеральным законом». В данной статье содержится еще одна норма – ч. 5 гарантирует свободу массовой информации и запрещает цензуру.

Проблема права на информацию очень важна, прежде всего, в плане практического применения. Исследование процесса включения данного права человека и гражданина в систему национального и международного права касается места, связей, зависимостей этого права в системе других прав человека. Необходимо уяснить содержание указанного права и правовые механизмы его реализации.

В связи с этим специалисты говорят о том, что необходим закон «О праве на информацию», а также развитие всех сопутствующих ему нормативных правовых актов, позволяющих сформировать полноценный институт информационного права.

Известный специалист в области информационного права И.Л. Бачило отмечает, что закрепление права на информацию должно иметь 3 аспекта:

1) **формально-правовой**, связанный с **признанием определенного права** и его реализацией в пределах действия позитивного права определенного государства и международного сообщества;

2) **сущностный**, связанный с нормативно закрепленным **содержанием** данного права, реализуемого через определенные полномочия одних субъектов и корреспондирующие ему правовые обязанности других субъектов;

3) **процессуальный,** регулирующий **порядок реализации** права[16].

[16] См.: *Бачило И.Л.* Информационное право. С. 135.

Формально-правовое признание права на информацию закреплено в Конституции РФ и Федеральном законе «Об информации». Субъектом этого права, согласно конституционной норме, является каждый человек независимо от возраста, пола и гражданства. Тем самым признается, что право на информацию носит глобальный, межтерриториальный характер. В то же время существуют особенности обеспечения права на информацию разнородных субъектов: например, детей, право на информацию для которых должно обеспечиваться наряду с их защитой от вредной информации; мигрантов, прибывших в нашу страну из чужого информационного пространства, плохо знающих язык и потому испытывающих проблемы в получении информации; пожилых людей, которые в силу доверчивости, некритичности восприятия получаемых сведений, неумения пользоваться современными информационными технологиями становятся жертвами недостоверной рекламы или заведомо ложной информации, распространяемой мошенниками.

Статья 8 закона «Об информации» делит всех субъектов на 2 группы – это граждане (физические лица) и организации (юридические лица). Они вправе осуществлять поиск, получать любую информацию в любых формах и из любых источников при условии соблюдения требований, установленных законодательством Российской Федерации.

На практике право на информацию сводится к **праву на доступ к информации**, т.е. реализации правомочий *искать и получать* информацию, которые являются основой для осуществления других правомочий: передавать, распространять можно уже полученную информацию, производить собственную информацию можно на основе уже полученной.

Содержательная сторона права на информацию связана с тем, что оно реализуется в разных сферах человеческой жизни: политической, гражданско-правовой, социальной, поэтому информация нужна разнородная. В части 2 ст. 8 Федерального закона «Об информации» «Право на доступ к информации» установлено, что гражданин имеет право на получение от государственных органов, органов местного самоуправления информации, *непосредственно затрагивающей его права и свободы.* Неопределенность этой нормы проявляется в неясности критериев отнесения сведений к «затрагивающим права и свободы граждан».

Поэтому **во многих федеральных законах и постановлениях Правительства РФ, регулирующих различные сферы человеческой жизни и деятельности, существуют специальные нормы о праве на информацию.**

Возможность получать информацию о состоянии окружающей среды – одно из основных конституционных прав граждан. Поэтому целый ряд законов определяет, какая именно экологическая информация и каким способом может быть получена.

Например, Основы законодательства РФ об охране здоровья граждан в ст. 19 закрепляют, что «граждане имеют право на регулярное получение

достоверной и своевременной информации о факторах, способствующих сохранению здоровья или оказывающих на него вредное влияние, включая информацию о санитарно-эпидемиологическом благополучии района проживания, рациональных нормах питания, о продукции, работах, услугах, их соответствии санитарным нормам и правилам, о других факторах. Эта информация предоставляется органами государственной власти и органами местного самоуправления в соответствии с их полномочиями через средства массовой информации или непосредственно гражданам».

В соответствии со ст. 6 Федерального закона «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21 декабря 1994 года № 68-ФЗ федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления обязаны оперативно и достоверно информировать население о возникновении чрезвычайных ситуациях, приемах и способах защиты населения от них, состоянии защиты населения и территорий от чрезвычайных ситуаций и принятых мерах по обеспечению безопасности. Понятно, что такие ситуации порождают у людей тревогу, страхи, могут вызвать панику, поэтому информирование населения должно осуществляться всеми возможными средствами: через средства массовой информации, с использованием специализированных технических средств оповещения и информирования населения в местах массового пребывания людей, по иным каналам.

Достаточно подробно право на информацию регламентируется законом РФ «О защите прав потребителей» от 7 февраля 1992 года № 2300-1, в котором данному праву посвящено пять статей. Информация, право на получение которой имеет потребитель, включает в себя сведения об изготовителе (исполнителе, продавце), режиме его работы, товарах (работах, услугах). В Законе подробно оговариваются состав, качество предоставляемой информации, момент ее доведения до потребителя, язык, а также лица, обязанные предоставлять соответствующую информацию. Закон предъявляет требования к характеру предоставляемой информации – это должны быть полные исчерпывающие сведения, позволяющие потребителю составить точное представление об изготовителе (исполнителе, продавце) и о товарах (работах, услугах). Способы доведения информации до потребителя определяются спецификой отдельных сфер обслуживания, но она должна быть доведена в наглядной и доступной форме.

Потребители, как правило, демонстрируют слабое знание своих прав, поэтому законом закреплено право на просвещение в области защиты прав потребителей, которое реализуется общественными объединениями и союзами потребителей, средствами массовой информации и т.д.

Отдельную сферу информации, правом на доступ к которой обладают граждане Российской Федерации, составляет официальная информация. Особенности ее предоставления будут рассмотрены далее.

Право на информацию в различных сферах человеческой жизни и деятельности юридически закреплено. Тем не менее основной правовой проблемой в этой области является то, что законы принимались в разное время, целью их принятия было регулирование общественных отношений в определенной сфере, а защита права на информацию обеспечивалась как бы «по касательной», в разных законодательных актах мы встречаем концептуальные отличия в наполнении самого понятия «право на информацию», в объеме его предоставления и способах регулирования.

Третий аспект правового оформления права на информацию – **процессуальный.**

Граждане могут получать информацию различными способами, все их перечислить невозможно. Отметим те из них, которые получили правовую регламентацию в российском законодательстве.

1. **Непосредственное участие в мероприятиях, затрагивающих права и свободы граждан.** Формы такого участия могут быть различны. Например, согласно Федеральному закону «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 года № 8-ФЗ государственные органы и органы местного самоуправления обязаны обеспечить возможность присутствия граждан (физических лиц), в том числе и представителей организаций, общественных объединений, на своих коллегиальных заседаниях. Это делает работу органов государственной власти и органов местного самоуправления гласной и открытой.

Относительно новой формой является проведение публичных слушаний по общественно значимым вопросам. Проведение публичных слушаний предусматривается Федеральным законом «Об общих принципах организации и деятельности законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации», согласно которому по проекту бюджета субъекта Российской Федерации и проекта годового отчета об исполнении бюджета субъекта Российской Федерации проводятся публичные слушания. Проведение публичных слушаний предусмотрено также законодательством субъектов Российской Федерации. Например, в Уставе Нижегородской области содержится положение о том, что по проектам законов, имеющих особую социальную значимость, могут проводиться публичные слушания, в которых вправе принимать участие граждане, представители общественных организаций, средств массовой информации, ученые и специалисты. В Красноярском крае принят специальный закон «О публичных слушаниях в Законодательном Собрании Красноярского края». Можно отметить ряд недостатков в правовом регулировании публичных слушаний. Прежде всего это отсутствие перечня проблем, по которым проведение публичных слушаний должно быть обязательным. Инициатива проведения таких слушаний принадлежит органам власти – граждане, общественные организации не могут заставить их провести слушания по

тем вопросам, которые действительно волнуют общество. Мнения, высказанные гражданами, не носят обязывающего характера. Все это свидетельствует о необходимости серьезной доработки законодательства о публичных слушаниях по общественно значимым вопросам[17].

2. **Информирование с помощью средств массовой информации.** Целый ряд законов предусматривает обязательное **обнародование (опубликование**) официальной информации: нормативных правовых актов, информации о деятельности государственных органов в СМИ. Существуют государственные СМИ, которые освещают работу руководителей страны, высших должностных лиц, выражают официальную точку зрения по общественно значимым вопросам. Их деятельность регулируется Федеральным законом «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» от 13 января 1995 года № 7-ФЗ. Большую роль в создании многомерного информационного пространства играют средства массовой информации оппозиционных политических партий, общественных движений и независимые СМИ. Деятельность СМИ регламентируется законом РФ «О средствах массовой информации» от 27 декабря 1991 года № 2124-I.

3. **Представление информации на официальных сайтах в сети Интернет.** В последнее время органы государственной власти и общественные организации все активнее осваивают Интернет, открывают свои сайты, где выкладывают информацию о своей деятельности. Перечень информации, которая должна быть представлена на сайтах органов государственной власти, установлен Федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 года № 8-ФЗ.

4. **Ознакомление с библиотечными и архивными фондами.** Принципы деятельности библиотек устанавливаются Федеральным законом «О библиотечном деле» от 29 декабря 1994 года № 78-ФЗ. Закон гарантирует право каждого человека на свободный доступ к информации, свободное духовное развитие, приобщение к ценностям национальной и мировой культуры, а также на культурную, научную и образовательную деятельность. Статья 24 Федерального закона «Об архивном деле» от 22 октября 2004 года № 125-ФЗ предусматривает, что граждане Российской Федерации имеют право свободно искать и получать для изучения архивные документы. Доступ к архивным документам обеспечивается путем предоставления пользователю архивными документами справочно-поисковых средств и информации об этих средствах, а также подлинников и (или) копий необходимых ему документов.

---

[17] См.: *Бердникова Е.В.* Обеспечение открытости органов законодательной власти // Конституционно-правовое регулирование транспарентности органов государственной власти в Российской Федерации и Канаде. М., 2009. С. 44–46.

5. **Обращение в органы государственной власти с запросом информации, заявлениями, жалобами и предложениями.** Этот способ реализуется с помощью Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» от 2 мая 2006 года № 59-ФЗ. Ответ на запрос о получении информации и на обращение должен быть дан в возможно короткий срок, но не позднее, чем через **30 дней** после дня получения запроса. Если запрашиваемая информация не может быть выдана в указанный срок, обратившемуся направляется письменное уведомление об отсрочке ее предоставления. В уведомлении должны быть указаны **срок и причины отсрочки.**

Если орган **не обладает запрашиваемой информацией**, он сообщает об этом **в 7-дневный срок.**

Отказ в предоставлении информации должен содержать указание причин, по которым запрос не может быть удовлетворен, дату принятия решения об отказе, а также порядок его обжалования.

Гражданин вправе избрать любую форму запроса, предусмотренную федеральным законом, **не обосновывать необходимость получения запрашиваемой информации**, в случае предоставления ответа в устной форме, требовать письменного ответа, обжаловать в установленном порядке действия органов, их должностных лиц, нарушивших право на доступ к информации и порядок его реализации.

Законом специально предусматриваются гарантии безопасности гражданина в связи с его обращением, а именно:

– запрещается преследование гражданина в связи с его обращением;

– при рассмотрении обращения не допускается разглашение сведений, содержащихся в нем, а также сведений, касающихся частной жизни гражданина без его согласия;

– запрещается направлять жалобу на рассмотрение в государственный орган, орган местного самоуправления или должностному лицу, решение или действие (бездействие) которых обжалуется.

Важное значение имеет **возможность судебной защиты права на информацию.** Примеры практики такой защиты уже есть. Так, согласно постановлению Правительства РФ от 12 февраля 2003 году, каждый федеральный орган исполнительной власти обязан создать свой официальный сайт в Интернете, на котором своевременно и регулярно будет размещать сведения о своей деятельности в соответствии с Перечнем, утвержденным этим постановлением. Отсутствие у федерального органа исполнительной власти своего официального сайта в Интернете должно рассматриваться как существенное препятствие на пути реализации права граждан на доступ к информации о деятельности этого органа и может быть обжаловано в судебном порядке.

В 2005 году группа юристов, сотрудничающих с Институтом развития свободы информации, инициировала серию судебных процессов по оспариванию бездействия ряда федеральных органов исполнительной

власти, которые либо не создавали в Интернете свои официальные сайты, либо не размещали на них подлежащие опубликованию сведения[18].

В жалобе оспаривалось бездействие Министерства здравоохранения и социального развития РФ, Федеральной службы по труду и занятости, Федеральной службы по техническому и экспортному контролю, Федеральной службы в сфере природопользования, Федеральной регистрационной службы.

В итоге споров по вопросу принятия дела к производству суд признал отсутствие официального сайта достаточным поводом для обращения гражданина в суд. Предвидя неблагоприятную для себя перспективу, федеральные органы исполнительной власти мобилизовали свои усилия и в августе 2005 года открыли собственные сайты.

Ограничение права на информацию

Право на информацию относится к личным правам граждан, поэтому его ограничение может осуществляться только на основе конституционных норм в следующих целях:

– соблюдения прав и свобод других лиц (ст. 17);

– защиты неприкосновенности частной жизни, личной, семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. ст. 23, 24);

– защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (ст. 55);

– обеспечения безопасности граждан (в условиях чрезвычайного положения) (ст. 56).

Ограничение доступа к информации устанавливается Федеральным законом «Об информации». Дается **закрытый перечень,** т.е. он не может быть дополнен ведомственными инструкциями и распоряжениями.

1. Ограничение доступа к информации устанавливается федеральными законами **в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.**

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей **государственную тайну,** осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим **коммерческую тайну, служеб-**

[18] См.: *Павлов И.П.* Право граждан на доступ к информации о деятельности органов государственной власти и судебная практика его защиты // Теоретические проблемы информационного права. М., 2006. С. 135.

ную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (**профессиональная тайна**), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления **информации о его частной жизни**, в том числе и информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к **персональным данным** граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В то же время в ряде федеральных законов установлены категории информации, доступ к которой не может быть ограничен.

Согласно Закону об информации **не может быть ограничен доступ к:**

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжа-

лованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

Если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

Правовой проблемой является получение информации от юридических лиц – коммерческих фирм, управляющих организаций, товариществ собственников жилья, жилищно-строительных кооперативов и т.д., которые не входят в число субъектов, обязанных отвечать на обращения граждан.

Доступ к информации о деятельности органов государственной власти

Полноценное социальное взаимодействие между человеком, институтами гражданского общества и государством возможно только на основе информационной открытости органов власти. «Важными условиями формирования гражданского общества являются: расширение участия граждан в управлении государством, усиление контроля за деятельностью всех ветвей власти, включение граждан в процесс принятия важных государственных решений… Определяющим условием общественной контрольной деятельности выступает открытость органов власти, поскольку информация об их деятельности является предметом анализа и оценки общественности»[19].

Статья 24 Конституции РФ закрепляет **обязанность органов государственной власти и органов местного самоуправления, их должностных лиц обеспечивать каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы.**

Эта конституционная норма была конкретизирована Федеральным законом «Об информации». В частности, устанавливается **принцип открытости информации о деятельности государственных органов и свободного доступа к такой информации**, кроме случаев, установленных федеральными законами, прямо говорится о **невозможности ограничения доступа к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств.**

Требование открытости власти в равной степени относится к трем ее ветвям.

---

19 *Володин В.В., Комкова Г.Н.* Общественный контроль как механизм обеспечения открытости органов публичной власти //Конституционно-правовое регулирование транспарентности органов государственной власти в Российской Федерации и Канаде. М., 2009. С. 88.

На федеральном уровне открытость **законодательной власти** обеспечивается обязанностью опубликования принятых законов. Это положение гарантируется ч. 3 ст. 15 Конституции РФ и Федеральным законом «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания». Кроме того, законодательная власть в своей деятельности активно использует информационные технологии: на сайте http://www.duma.gov.ru/ размещаются поступившие законопроекты, довольно подробно освещается процесс подготовки и принятия нормативных правовых актов.

Согласно Регламенту Государственной Думы Федерального Собрания РФ на заседаниях комитета, комиссии, палаты могут присутствовать представители СМИ.

Для выяснения общественного мнения по вопросам законопроектной деятельности комитеты и комиссии могут организовывать парламентские слушания, проводить конференции, совещания, круглые столы, семинары. Наиболее социально значимые законопроекты обсуждаются в СМИ, комментируются депутатами и разработчиками.

Согласно Федеральному закону «О статусе члена Совета Федерации и статусе депутата Государственной Думы Федерального Собрания Российской Федерации» от 8 мая 1994 года № 3-ФЗ члены Совета Федерации депутаты Государственной думы организуют свои приемные, где ведут прием граждан, проводят встречи с избирателями. Депутаты выступают в средствах массовой информации, рассказывают о своей деятельности, деятельности фракции и партии.

Однако, как отмечают исследователи, все же большая часть работы, связанной с подготовкой и принятем политических решений, остается закрытой для общественности. Например, одним из этапов законодательного процесса является так называемый предзаконодательный процесс, который включает в себя появление идеи, обоснование предложений о необходимости разработки нового законопроекта и подготовку самого законопроекта. Именно на этом этапе сталкиваются интересы многочисленных лоббистов, способствующих принятию или отклонению законопроекта, поэтому данный этап является наиболее закрытым для общественности[20].

Законодательные собрания субъектов Федерации в своих регламентах устанавливают различные формы информирования граждан о своей деятельности. Например, регламентом Саратовской областной думы устанавливается порядок присутствия граждан на ее открытых заседаниях непосредственно в зале заседаний.

Наибольшей критике по поводу доступности информации о своей деятельности подвергаются **органы исполнительной власти**. Именно

---

20 См.: *Малько А.В., Исаков Н.В., Субочев В.В.* Правовая политика в урегулировании лоббизма. Саратов, 2003. С. 56.

эта информация особенно необходима социальным и экономическим субъектам для адекватной оценки обстановки и своевременного принятия решений.

Первым нормативным правовым актом, регулирующим вопросы доступа к государственной информации, стало **постановление Правительства РФ от 12 февраля 2003 года № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»**. Согласно этому документу федеральные органы исполнительной власти обязаны своевременно и регулярно размещать указанные информационные ресурсы в информационных системах общего пользования, в том числе и сети Интернет.

Для государственных органов исполнительной власти субъектов Российской Федерации, а также для органов местного самоуправления в отношении создания собственных интернет-представительств и обеспечения ими доступа граждан к информации о своей деятельности указанное выше постановление носило рекомендательный характер. Тем не менее в большинстве субъектов Российской Федерации были приняты региональные подзаконные акты, касающиеся возможности обеспечения права граждан на доступ к соответствующим информационным ресурсам.

С 1 января 2010 года вступил в силу Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 года № 8-ФЗ.

Закон устанавливает **основные принципы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления:**

1) открытость и доступность информации о деятельности государственных органов и органов местного самоуправления, за исключением случаев, предусмотренных федеральным законом;

2) достоверность информации о деятельности государственных органов и органов местного самоуправления и своевременность ее предоставления;

3) свобода поиска, получения, передачи и распространения информации о деятельности государственных органов и органов местного самоуправления любым законным способом;

4) соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права организаций на защиту их деловой репутации при предоставлении информации о деятельности государственных органов и органов местного самоуправления.

Статья 10 данного Закона **впервые обязывает государственные органы и органы местного самоуправления создавать в сети Интернет официальные сайты**, где должна размещаться информация об их деятельности. Кроме того, на сайте указываются адреса электронной почты,

по которым пользователем информацией может быть направлен запрос и получена запрашиваемая информация.

Другим важным положительным моментом является то, что в законе прямо указывается, какую именно информацию должны сообщать о своей деятельности органы государственной власти и местного самоуправления. Вся информация, размещаемая на сайтах, делится на **две** большие группы.

1. **Обязательно размещаемая информация,** ее перечень содержится в тексте самого закона. В том числе:

– общая информация о государственном органе, об органе местного самоуправления;

– информация о нормотворческой деятельности органа власти, в том числе изданные им нормативные правовые акты, включая сведения о внесении в них изменений, признании их утратившими силу, признании их судом недействующими;

– информация о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд;

– административные регламенты, стандарты государственных и муниципальных услуг;

– установленные формы обращений, заявлений и иных документов, принимаемых государственным органом к рассмотрению;

– порядок обжалования нормативных правовых актов и иных решений, принятых государственным органом, его территориальными органами, муниципальных правовых актов;

– информация о состоянии защиты населения и территорий от чрезвычайных ситуаций и принятых мерах по обеспечению их безопасности, о прогнозируемых и возникших чрезвычайных ситуациях, о приемах и способах защиты населения от них;

– информация о результатах проверок, проведенных государственным органом, его территориальными органами, органом местного самоуправления, подведомственными организациями в пределах их полномочий, а также о результатах проверок, проведенных в государственном органе, его территориальных органах, органе местного самоуправления, подведомственных организациях и др.

Должны также размещаться обзоры обращений пользователей, а также обобщенная информация о результатах рассмотрения этих обращений и принятых мерах.

2. **Иная информация** в соответствии со специальными перечнями. Эта информация должна распространяться на официальных сайтах указанных органов дополнительно к обязательно размещаемой. Фактически, данная норма обязывает федеральные органы власти и органы власти субъектов Федерации, органы местного самоуправления принять собственные нормативные акты, в которых будут представлены необходимые перечни информации о их деятельности.

В целом данное требование следует признать чрезвычайно актуальным, поскольку в современной науке Интернет рассматривается как один из методов повышения участия граждан в управлении на всех уровнях. Предполагается, что с помощью Интернета можно будет реализовать обратную связь между государственными органами и населением на качественно новом уровне, приблизить органы государственного управления к гражданам, улучшить работу с населением. «Общественно-политическая деятельность обретает новую глубину с развитием Интернета»[21].

В то же время можно указать на некоторые недостатки данного Закона, например на то, что граждане и общественные организации исключены из субъектов, определяющих объем и содержание распространяемой в Интернете информации. Не предусмотрены механизмы реализации удовлетворения общественного интереса, которые заставили бы органы власти опубликовать в Интернете интересующую граждан информацию. Это может привести к тому, что на сайтах будет распространяться информация справочного характера, официальные отчеты, официальные статистические данные, а не те сведения, которые действительно востребованы обществом.

Для **официальных сайтов федеральных органов исполнительной власти** Минэкономразвития РФ в соответствии с Постановлением Правительства РФ от 22 июня 2009 года № 514 «О внесении изменений в Положение о Министерстве экономического развития Российской Федерации» устанавливаются **единые требования к технологическим, программным и лингвистическим средствам обеспечения пользования** сайтами.

Эти требования были утверждены приказом Министерства экономического развития РФ от 16 ноября 2009 года № 470. К ним относятся:

1) круглосуточная доступность и бесплатность информации, независимость доступа от проприетарного программного обеспечения (для ознакомления с информацией должно быть достаточно веб-обозревателя), предоставление информации без процедур регистрации пользователей или заключения ими лицензионных или иных соглашений;

2) программное обеспечение официального сайта должно обеспечивать: а) возможность поиска всей текстовой информации, размещенной на официальном сайте, включая поиск документа по его реквизитам, содержанию, а также по фрагментам текста, содержащегося в нем (при этом данная информация должна быть также доступна посредством средств автоматизированного сбора данных в сети Интернет, в том числе и глобальных поисковых систем); б) возможность определения даты и времени размещения информации; в) учет посещаемости всех страниц официального сайта (и бесплатное раскрытие в сети Интернет сводных данных

[21] *Жарова А.К.* Гражданское общество: системный подход // Информационное право: актуальные проблемы теории и практики. С. 48.

о посещаемости, доступность данных за последние три года); г) размещение отдельных категорий документов – нормативных правовых и иных актов, проектов актов, судебных актов, докладов, отчетов, договоров, обзоров, прогнозов, протоколов, заключений, статистической информации, образцов форм и иных документов – дополнительно к обычному гипертекстовому формату в виде файлов с возможностью сохранения на технических средствах пользователей;

3) применение средств электронной цифровой подписи при размещении, изменении или удалении информации; ведение электронных журналов учета соответствующих операций; ежедневное резервное копирование всей информации и электронных журналов учета операций;

4) требования к структуре сайта и удобству пользования включают: а) возможность навигации, поиска и использования текстовой информации, размещенной на официальном сайте, при выключенной функции отображения графических элементов страниц в веб-обозревателе; б) вся размещенная на официальном сайте информация должна быть доступна путем последовательного перехода по гиперссылкам, начиная с главной страницы официального сайта не более чем за пять переходов (по кратчайшей последовательности); в) предоставление наглядной информации о структуре сайта и о местонахождении отображаемой страницы в этой структуре; г) обязательное размещение на каждой странице главного меню, явно обозначенной ссылки на главную страницу, ссылки на карту сайта, наименования органа; д) URL каждой страницы должен отображать ее положение в логической структуре сайта и соответствовать ее назначению и т.д.

5) информация размещается на официальном сайте на русском языке, однако по решению руководителя федерального органа исполнительной власти (территориального органа федерального органа исполнительной власти) отдельная информация может быть также размещена на других языках.

Таким образом, **впервые в российском законодательстве закреплены требования к структуре сайта и удобству его использования**.

Данные требования следовало бы распространить и на официальные сайты иных органов исполнительной и законодательной власти, пока же, согласно законодательству, сами эти органами должны принять соответствующие технические, программные, лингвистические требования для обеспечения пользования своими официальными сайтами.

Конституционная основа **информационной открытости судов** заложена Конституцией, в которой закреплено: «Разбирательство дел во всех делах открытое. Слушание дела в закрытом заседании допускается в случаях, предусмотренных федеральным законом» (ч. 1 ст. 123).

Федеральный конституционный закон «О судебной системе» от 31 декабря 1996 года № 1-ФКЗ полностью повторяет конституционную формулировку: «Разбирательство дел во всех судах открытое. Слуша-

ние дела в закрытом заседании допускается в случаях, предусмотренных федеральным законом» (ст. 9). На практике возможность присутствия граждан, представителей СМИ на судебных заседаниях далеко не всегда может быть реализована. «Вопросы доступа в здания судов в России находятся практически вне правового регулирования. Проблема доступности в здание суда связана с обеспечением порядка и безопасности, которое находится в ведении службы судебных приставов… Особых правил доступа в здание суда не существует. При решении этих вопросов необходимо сохранение баланса прозрачности и доступности судопроизводства с обеспечением порядка в судебных заседаниях и уважения к суду»[22].

Кроме того, осуществление гласности и обнародование судебных решений регулируются внутренними регламентами судебных органов. Например, Регламентом Конституционного Суда в целях обеспечения оперативности и полноты информации предусмотрено создание информационной системы, содержащей, в частности, банки данных:

– о законах и иных нормативных актах Российской Федерации и субъектов Российской Федерации;

– о решениях Конституционного Суда;

– о решениях зарубежных конституционных судов;

– о конституционной юстиции в субъектах Российской Федерации.

Кроме того, в отношении информационного наполнения интернет-сайтов арбитражных судов на данный момент применяется информационное письмо № ВАС-С01/УИС-984 от 12 июля 2007 года, по поводу судов общей юрисдикции действует положение по созданию и сопровождению официальных интернет-сайтов судов общей юрисдикции Российской Федерации, утвержденное постановлением Президиума Верховного Суда РФ от 24 ноября 2004 года. В соответствии с этим постановлением все суды общей юрисдикции и органы Судебного департамента сформировали свои интернет-сайты. После этого началось внедрение государственной автоматизированной системы (ГАС) «Правосудие». Для создания единого информационного пространства судов и органов Судебного департамента был открыт единый интернет-портал ГАС «Правосудие» (http://www.sudrf.ru).

Внедрение ГАС «Правосудие» – одно из центральных направлений федеральной целевой программы «Развитие судебной системы России на 2007–2011 годы», которая также исходит из того, что повышение качества правосудия и уровня судебной защиты прав и законных интересов граждан, наряду с гарантиями независимости судей, созданием надлежащих условий для судебной деятельности и повышением роли исполнения судебных актов невозможно без обеспечения гласности и открытости судопроизводства.

---

[22] *Апарина О.Ю., Липчанская М.А.* Особенности транспарентности органов судебной власти в Российской Федерации // Конституционно-правовое регулирование транспарентности органов государственной власти в Российской Федерации и Канаде. М., 2009. С. 73.

1 июля 2010 г. вступает в силу **Федеральный закон «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22 декабря 2008 года № 262.**

Во многом положения этого закона сходны с положениями Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», например устанавливаются те же принципы и способы организации доступа к информации.

Устанавливается перечень информации, обязательно размещаемой в сети Интернет: общая информация о суде; информация, связанная с рассмотрением дел в суде; требования, предъявляемые к форме и содержанию документов, используемых при обращении в суд, и (или) образцы этих документов, порядок представления указанных документов в суд; сведения о размере и порядке уплаты государственной пошлины по категориям дел, подлежащих рассмотрению в суде; сведения о находящихся в суде делах; регистрационные номера данных дел, информация о прохождении дел в суде, а также сведения о вынесении судебных актов по результатам рассмотрения дел (назначено к слушанию с указанием даты, времени и места проведения судебного заседания, а также с пометками: рассмотрено, отложено, приостановлено, прекращено, заключено мировое соглашение, заявление оставлено без рассмотрения, иное с учетом особенностей соответствующего судопроизводства); тексты судебных актов, сведения об их обжаловании и о результатах такого обжалования, а при опубликовании судебных актов – сведения об источниках их опубликования; порядок обжалования судебных актов; разъяснения, обобщения и обзоры по вопросам судебной практики рассмотрения судами дел; порядок ознакомления с материалами дела лиц, участвующих в деле и т.д.

В то же время закон учитывает специфику судебных дел и устанавливает **особые требования к размещению в сети интернет-текстов судебных актов:**

– в целях обеспечения безопасности участников судебного процесса из указанных актов исключаются персональные данные, кроме фамилий и инициалов судей (судьи), рассматривавших (рассматривавшего) дело, а также прокурора и адвоката, если они участвовали в судебном разбирательстве. Вместо исключенных персональных данных используются инициалы, псевдонимы или другие обозначения, не позволяющие идентифицировать участников судебного процесса.

– не подлежат размещению в сети Интернет тексты судебных актов, вынесенных по делам, затрагивающим безопасность государства, возникающим из семейно-правовых отношений, в том числе и по делам об усыновлении (удочерении) ребенка, другим делам, затрагивающим права и законные интересы несовершеннолетних, о преступлениях против половой неприкосновенности и половой свободы личности, об ограничении дееспособности гражданина или о признании его недееспособным,

о принудительной госпитализации гражданина в психиатрический стационар и принудительном психиатрическом освидетельствовании и т.д.

В целом надо сказать, что принятие двух федеральных законов – «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» и «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», несмотря на их некоторые недостатки, должно способствовать выведению судов и органов государственной власти, органов местного самоуправления на качественно новый уровень информационного обеспечения своей деятельности и содействовать развитию гражданского общества в России.

Тема 6. ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Понятие информационных ресурсов

Информационные ресурсы – документы и массивы документов, а также документы и массивы документов (библиотеки, архивы, фонды, банки данных), подготовленные и систематизированные в удобной и пригодной для использования форме.

Ныне действующий закон «Об информации» не дает определения информационных ресурсов, хотя в ряде нормативных актов данный термин используется. Например, согласно ст. 2 Федерального закона «О Государственной автоматизированной системе РФ «Выборы» «информационные ресурсы ГАС «Выборы» – отдельные документы, отдельные массивы документов, документы и массивы документов, формируемые, хранимые и используемые в ГАС «Выборы»; согласно ст. 425 Таможенного кодекса РФ «информационные ресурсы таможенных органов составляют документы и сведения, представляемые лицами при совершении таможенных операций в соответствии с настоящим Кодексом, а также иные документы и сведения, имеющиеся в распоряжении таможенных органов в соответствии с настоящим Кодексом и другими федеральными законами».

Понятие «информационные ресурсы» тесно связано с понятием «документ».

Документ является необходимой формой выражения информационного ресурса, его элементарной единицей.

Возрастающая роль информационных ресурсов в развитии страны нашла отражение в Концепции государственной информационной политики, одобренной на заседании Комитета Государственной Думы по информационной политике и связи 15 октября 1998 года.

В Стратегии развития информационного общества в Российской Федерации, утвержденной Президентом РФ 7 февраля 2008 года, в число пяти слагаемых, необходимых для того, чтобы Россия стала частью глобального информационного общества, наряду с некоторыми технологическими условиями входит и «информационное наполнение сети (контент)»[23].

Основные правовые режимы информационных ресурсов

Характеристику правового режима информационных ресурсов следует начать с определения категории «правовой режим» в юридической науке. Существуют различные определения данной категории. Н.И. Матузов и А.В. Малько правовой режим определяют как функциональную характеристику права, особый порядок правового регулирования; С.С. Алексеев пишет, что правовой режим – это комплекс правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создающих особую направленность регулирования.

В состав правового режима информационных ресурсов включаются 4 обязательных требования, без которых такие ресурсы не могут быть включены в систему правовых отношений и не могут получить полноценной правовой защиты.

Итак, в состав правового режима входят:

1)категория информации по доступу к ней;

2)порядок документирования информации;

3)право собственности на отдельные документы, массивы документов, а также документы и массивы в составе информационных систем;

4)порядок правовой защиты информации.

Ведущую роль играет классификация информационного ресурса по принадлежности к режиму свободного доступа или ограниченного доступа к информации.

Обычно выделяют 3 вида режимов:

1)режим свободного доступа;

2)режим ограниченного доступа;

3)режим документированной информации.

Это самое общее деление. Общие режимы делятся на частные, которые характеризуют специфику правового регулирования поиска, получения, передачи, производства и распространения информации в отдельных сферах общественных отношений.

Режим свободного доступа включает в себя следующие правовые режимы:

1)режим информационных ресурсов, отнесенных к общественному достоянию;

[23] Российская газета. 2008. 16 февр.

2)режим массовой информации;

3)режим исключительных прав.

Режим ограниченного доступа включает в себя режим информации, отнесенной к государственной тайне, и режим конфиденциальной информации.

Специальной оговорки требует правовой **режим документированной информации**. Этот режим как бы выпадает из классификации по доступности сведений. Он отражает форму представления информации и ее связь с материальным носителем. Данный режим не исключает деления информации на общедоступную и ограниченного доступа и является вторичным по отношению к ним.

Правовое регулирование в области обязательного экземпляра документов, архивного и библиотечного дела

Правовое регулирование формирования, хранения и использования информационных ресурсов Российской Федерации осуществляется целым рядом законодательных актов. Рассмотрим основные из них.

Федеральный закон «Об обязательном экземпляре документов» от 29 декабря 1994 года № 77-ФЗ определяет политику государства в области формирования обязательного экземпляра документов как ресурсной базы комплектования библиотечно-информационного фонда России и развития системы государственной библиографии, предусматривает обеспечение сохранности обязательного экземпляра документов, его общественное использование. Закон «Об обязательном экземпляре документов» отличает **сугубо административно-правовой характер регулирования.**

Обязательный экземпляр документов – это экземпляры различных видов тиражированных документов, подлежащие передаче производителями в соответствующие организации в порядке и количестве, установленном федеральным законом.

Важное место в системе формирования обязательного экземпляра документов занимает фигура производителя указанных документов. Поэтому закон детально регламентирует круг отношений, субъектами которых являются лица, вовлеченные в процесс производства документированной информации.

В соответствии со ст. 1 Федерального закона «Об обязательном экземпляре документов» **производитель документов** – юридическое лицо, независимо от его организационно-правовой формы и формы собственности, или физическое лицо, осуществляющее предпринимательскую деятельность без образования юридического лица, осуществляющее подготовку, публикацию (выпуск) и рассылку (передачу, доставку) обязательного экземпляра. Таким образом, это могут быть издатель, редакция СМИ, производитель фонограммы, аудиовизуальной продукции, организация по производству телерадиопродукции, организации, осуществляющие научно-исследовательские, опытно-конструкторские и технологи-

ческие работы. Из приведенного определения следует, что законодатель включил в круг производителей максимально возможный перечень лиц, сделав исключение для граждан, не являющихся предпринимателями, и для общественных объединений до их государственной регистрации.

Действующее законодательство гарантирует производителю ряд прав. Но эти право возникают при условии полной и оперативной доставки обязательного бесплатного экземпляра.

В числе **гарантируемых прав** ст. 16 называет:

– бесплатное опубликование библиографической информации в изданиях государственной библиографии и централизованной каталогизации;

– постоянное хранение производимых документов всех видов в национальных фондохранилищах;

– включение библиографической информации в отечественные и зарубежные автоматизированные банки данных;

– бесплатное предоставление по запросам субъектов фактографических и статистических данных, касающихся их продукции;

– соблюдение получателями прав производителей в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

Основной обязанностью производителя документа является доставка обязательного бесплатного экземпляра. Он передается получателям безвозмездно. Затраты на подготовку (публикацию), выпуск и рассылку (передачу, доставку) обязательных бесплатных экземпляров производители документов должны относить на себестоимость производимых документов.

Не все документы публикуются, тем не менее они тоже должны рассылаться: например, отчеты о научно-исследовательских работах, диссертации и т.д. во Всероссийский научно-технический информационный центр.

Игровые и документальные фильмы, мультфильмы, радиопрограммы доставляются в Госфильмофонд, Государственный архив кинофотодокументов, Государственный фонд телевизионных и радиопрограмм.

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

Согласно **Федеральному закону «О библиотечном деле» от 29 декабря 1994 года № 78-ФЗ библиотека – это информационное, культурное, образовательное учреждение, располагающее организованным фондом тиражированных документов и представляющее их во временное пользование физическим и юридическим лицам** (ст. 1).

На территории Российской Федерации могут учреждаться и действовать библиотеки разных видов и форм собственности. Их классификация дается в ст. 4 Федерального закона «О библиотечном деле»: федеральные библиотеки, библиотеки субъектов Федерации, муниципальные, предпри-

ятий, Российской академии наук, научно-исследовательских учреждений, образовательных учреждений, общественных объединений и частные.

В целях создания особых условий для сохранения и использования культурного достояния народов Российской Федерации некоторые федеральные библиотеки наделяются статусом национальных библиотек Российской Федерации. Таких библиотек 2 – Российская государственная библиотека и Российская национальная библиотека.

Государственные и муниципальные библиотеки должны иметь статус юридического лица и существовать в организационно-правовой форме учреждений. Иные библиотеки могут не являться юридическими лицами и их нельзя рассматривать в качестве правосубъектных образований, обладающих обособленным имуществом.

Библиотеки обладают специальной правоспособностью, поскольку они вправе утверждать правила пользования библиотеками, конкретные формы своей деятельности, определять сумму залога, источники комплектования своих фондов и т.д.

Основными обязанностями библиотек являются:

– обслуживание читателей;

– обеспечение сохранности особо значимых изданий и коллекций, отнесенных к памятникам истории и культуры;

– предоставление отчетов о своей деятельности в соответствии с законодательством.

В законе закреплены права граждан в области библиотечного дела:

– **право на библиотечное обслуживание** – независимо от пола, возраста, национальности, образования, социального положения, политических убеждений, отношения к религии каждый гражданин имеет право на библиотечное обслуживание;

– **право на библиотечную деятельность** – возможность участия в деятельности попечительских советов и иных объединений читателей;

– **право на частные библиотечные собрания** – возможность иметь в частной собственности собрание документов, в том числе тех, которые включают особо ценные издания и коллекции, отнесенные к памятникам культуры. В этом случае граждане имеют право на поддержку со стороны государства для обеспечения сохранности своих собраний при условии их регистрации в качестве памятников истории и культуры в органах федеральной власти.

Организация хранения, учета и использования архивных документов выступает одним из важнейших направлений формирования государственных информационных ресурсов. Основой архивного законодательства является **Федеральный закон «Об архивном деле в Российской Федерации» от 22 октября 2004 года № 125-ФЗ.**

Архив – это учреждение или структурное подразделение организации, осуществляющие хранение, комплектование, учет и использование архивных документов (ст. 3).

Архивный фонд РФ представляет собой исторически сложившуюся и постоянно пополняющуюся 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 Российской Федерации, подлежащих постоянному хранению.

Архивные документы включаются в состав Архивного фонда РФ на основании экспертизы ценности документов. Экспертиза осуществляется Центральной экспертно-проверочной комиссией Федерального архивного агентства.

Архивные документы могут находиться в государственной собственности, муниципальной и частной.

Устанавливается несколько видов хранения документов:

– постоянное хранение (бессрочное);

– временное хранение до их передачи на постоянное хранение;

– депозитарное хранение (органы государственной власти и местного самоуправления, Академии наук РФ, кроме РАН, хранят в Архивном фонде РФ свои документы временно, на его условиях, т.е. кладут на депозит);

– временное хранение до их уничтожения.

Согласно п. 3 ст. 10 архивные документы, находящиеся в государственной или муниципальной собственности, не подлежат приватизации, не могут быть объектом продажи, мены, дарения, а также иных сделок, которые могут привести к их отчуждению, если иное не предусмотрено международным договором Российской Федерации или федеральными законами. В случае приватизации государственных или муниципальных предприятий образовавшиеся в процессе их деятельности архивные документы, в том числе и документы по личному составу, остаются соответственно в федеральной собственности, собственности субъекта Российской Федерации и муниципальной собственности.

Порядок ввоза и вывоза архивных документов устанавливается таможенным законодательством Российской Федерации, законом РФ «О вывозе и ввозе культурных ценностей» от 15 апреля 1993 г. № 4804-1 и др.

Пользователь архивными документами имеет **право свободно искать и получать для изучения архивные документы**. Доступ к архивным документам обеспечивается путем предоставления гражданам справочно-поисковых средств, подлинников и (или) копий необходимых документов.

При этом государственные и муниципальные музеи, архивы, библиотеки, организации Российской академии наук обеспечивают необходимые условия для поиска и изучения документов. Условия доступа к архивным документам, находящимся в частной собственности, за исключением тех,

доступ к которым регламентируется законодательством Российской Федерации, устанавливаются их собственником или владельцем[24].

Пользователь архивными документами имеет право передавать, распространять информацию, содержащуюся в них, использовать ее для создания собственного произведения, т.е. реализовывать все свои информационные правомочия.

Тема 7. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ МАССОВОЙ ИНФОРМАЦИИ

Понятие средств массовой информации

СМИ часто называют четвертой властью, действующей наряду с законодательной, исполнительной и судебной, имея в виду их огромное влияние на общественное мнение и государственную политику. Значение информационной функции СМИ особенно вырастает в условиях глобализации[25]. В то же время сфера отношений, связанных с производством и распространением массовой информации, является одной из самых конфликтных. Появление в Интернете новых способов распространения информации только добавило вопросов.

Базовым в сфере правового регулирования отношений, возникающих по поводу организации деятельности средств массовой информации, их взаимодействия с гражданами и организациями, порядка распространения массовой информации, является **Закон РФ «О средствах массовой информации» от 27 декабря 1991 г. № 2124-I.**

Статья 2 данного закона определяет СМИ **как «периодические печатные издания, радио-, теле- и видеопрограммы, кинохроникальные программы, иные формы распространения массовой информации».** Под **массовой информацией** законодатель понимает **предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.**

Из данного определения следует, что средство массовой информации в его легальной интерпретации есть не что иное, как **одна из форм распространения информации**. Таких форм может существовать много, но наиболее значимые законодатель выделил в отдельный перечень.

---

[24] См.: *Попов Л.Л., Мигачев Ю.И., Тихомиров С.В.* Доступ к архивным документам и их использование // Информационное право: Учебник. М., 2010. С. 265.

[25] См.: *Лукашук И.И.* Средства массовой информации, государство, право. М., 2001. С. 7.

Многие ученые-юристы критикуют данное определение средства массовой информации и указывают, что понятие «формы» не может являться основным (наряду с периодичностью выпуска) признаком СМИ.

Кроме того, определение СМИ как формы распространения массовой информации не позволяет отнести их ни к объектам, ни к субъектам правоотношений.

Действительно, смешение субъекта с объектом – весьма типичная ошибка для законодательства о СМИ. В некоторых статьях Закона РФ «О средствах массовой информации» СМИ рассматриваются как объект права, а 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» говорится о предъявлении иска «к средству массовой информации» (п. 5) и о «возложении на средство массовой информации обязанности» (п. 7), тем самым СМИ отождествляется с юридическим лицом и рассматривается как субъект права.

Исследуя особенности правовой природы СМИ, крупнейший специалист в этой области М.А. Федотов приходит к выводу, что «в случае со СМИ мы имеем дело **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»[26].

Для российского законодательства не ново понятие фикции, когда объект существует только в правовом поле и может быть признан вещью (объектом) исключительно в юридическом смысле слова.

Федотов предлагает собственное определение средства массовой информации: это **результат интеллектуальной деятельности, имеющий название в качестве средства индивидуализации и форму периодического печатного издания, радио-, теле- и видеопрограммы, кинохроникальной программы или иную форму периодического распространения массовой информации.**

Такое определение представляется наиболее удачным, поскольку в нем содержится 4 характеристики СМИ:

1) результат интеллектуальной деятельности, который включает в себя особенности отбора и интерпретации информации в зависимости от целей издания, его политической и иной определенности и т.д.;

2) название в качестве средства индивидуализации, что позволит воспринимать печатное издание или телепередачу как обобщенный объект;

3) форма издания;

4) его периодичность.

---

[26] См.: *Федотов М.А.* Право массовой информации в Российской Федерации. М., 2002. С. 176.

Через СМИ реализуются все информационные права граждан: сбор, создание, получение, передача и обработка и распространение информации. Субъектами отношений в данной сфере являются, с одной стороны, учредители СМИ, редакторы, журналисты, авторы, т. е. те, кто участвует в создании, формировании содержания в определенной форме СМИ. С другой стороны, субъектами отношений в области массовой информации являются читатели, зрители, слушатели, т.е. те, кто воспринимает и использует информацию, исходящую от конкретного СМИ.

СМИ являются важнейшим источником информирования населения о фактах, явлениях, событиях, совершающихся в мире в самое короткое время, формируют общественное мнение по важнейшим общественно-политическим вопросам, создают и разрушают авторитеты. В связи с этим правовое регулирование СМИ является важнейшим институтом информационного права после права на информацию.

В российской Конституции проводится обособление массовой информации как информации особого рода. В части 1 ст. 29 закреплено право на свободное выражение мысли и слова, ч. 3 этой статьи устанавливает, что никто не может быть принужден к выражению своих мнений и отказу от них, ч. 5 запрещает цензуру.

Закон РФ «О СМИ» определяет **принцип свободы массовой информации**, в соответствии с которым поиск, получение, производство и распространение массовой информации, учреждение средств массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации не подлежат ограничениям, за исключением случаев, предусмотренных законодательством Российской Федерации.

Не допускаются **цензура массовой информации** (ст. 3 Закона РФ «О СМИ»), т.е. требование к редакции СМИ со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а также наложение запрета на распространение сообщений и материалов, их отдельных частей. Создание и финансирование организации учреждений, органов или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, также не допускаются.

В то же время существует ряд запретов и ограничений на использование массовой информации.

В ч. 2 ст. 29 Конституции РФ говорится о том, что «не допускается пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть или вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства».

Кроме того, на недопустимость злоупотребления свободой массовой информации указано в ст. 4 Закона РФ «О СМИ». Из нее следует, что не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости.

Запрещается использование в радио-, теле-, видео- и кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье, а равно распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена.

Запрещается распространение в средствах массовой информации, а также в компьютерных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также распространение иной информации, запрещенной федеральными законами.

При освещении контртеррористической операции запрещается распространение в средствах массовой информации сведений о специальных средствах, технических приемах и тактике проведения такой операции, если это может препятствовать ее проведению или поставить под угрозу жизнь и здоровье людей.

Принцип недопустимости злоупотребления свободой массовой информации используется также и в законодательстве о выборах и референдуме. Пункт 1.1 ст. 56 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12 июня 2002 г. № 67-ФЗ закрепляет принцип недопустимости злоупотребления правом на ведение агитации, называя в качестве одного из его видов – злоупотребление свободой массовой информации.

Правовое регулирование деятельности средств массовой информации

Деятельность средств массовой информации осуществляется после приобретения ими соответствующего правового статуса, обладание которым выступает необходимым условием их функционирования. Прежде чем распространять свою продукцию СМИ должно пройти стадии учреждения и регистрации (а в некоторых случаях – лицензирования).

Учреждение СМИ. Правом на учреждение СМИ обладают граждане, объединения граждан, организации и государственные органы, органы самоуправления.

Не могут выступать учредителями граждане, не достигшие 18 лет, отбывающие наказание в местах лишения свободы по приговору суда, душевнобольные, признанные судом недееспособными, объединения граждан и организации, деятельность которых запрещена законом. Не могут быть учредителями средств массовой информации граждане другого государства и лица без гражданства.

Устав редакции и устав юридического лица. Институт редакционного устава исходит из необходимости нахождения баланса интересов между журналистским коллективом и учредителем СМИ. По сути, редакционный устав является договором между этими субъектами.

Согласно Закону о СМИ в уставе редакции должны быть определены: взаимные права и обязанности учредителя, редакции, главного редактора; полномочия коллектива журналистов; порядок назначения (избрания) главного редактора, редакционной коллегии и (или) иных органов управления редакцией; основания и порядок прекращения и приостановления деятельности средства массовой информации; передача и (или) сохранение права на название, иные юридические последствия смены учредителя: изменение состава соучредителей, прекращение деятельности СМИ, ликвидация или реорганизация редакции, изменение ее организационно-правовой формы; порядок утверждения и изменения устава редакции и т.д. Можно дополнить устав и иными положениями, если они не противоречат законодательству.

На практике редакционные уставы заключаются редко, что нарушает права журналистов и редакционных коллективов.

Обеспечение редакционной самостоятельности. В действующем Законе о СМИ закреплен принцип профессиональной самостоятельности редакций и журналистов. Так, ч.3 ст.18 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)».

На практике редко можно встретить цензуру в том виде, как ее определяет Закон. Чаще приходится говорить о внутренней цензуре: существует понятие редакционной политики, идеологической направленности

издания, и если журналистский материал не будет им соответствовать, его просто не опубликуют.

Средства массовой информации могут переходить от одного владельца к другому и в конце концов концентрироваться в руках немногих. Эта проблема имеет не столько экономическое, сколько политическое значение – ведь чем выше уровень монополизации СМИ, тем меньше информационного разнообразия они смогут предложить обществу. Процессы концентрации СМИ необходимо поставить в разумные рамки, иначе за сравнительно короткий срок может произойти тотальная монополизация их рынка.

Процедура регистрации СМИ. Как следует из текста Закона о СМИ, процедура регистрации начинается с подачи заявления учредителем или лицом, действующим по его уполномочию. Оно подается в регистрирующий орган в зависимости от территории распространения продукции регистрируемого СМИ. Если продукция СМИ предназначается для распространения на всей территории России, в нескольких субъектах Федерации или за рубежом, то регистрация осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Постановление Правительства РФ от 16.03.2009 г. № 228).

При этом сам учредитель решает, на какой территории он собирается распространять продукцию своего СМИ. Заявление о регистрации подается в письменной форме.

В нем указываются название регистрируемого СМИ, язык, на котором оно будет выходить, адрес редакции, форма периодического распространения массовой информации, примерная тематика и (или) специализация, источники финансирования, предполагаемые периодичность выпуска и его максимальный объем. Причем регистрирующий орган вправе в отведенный ему законом месячный срок провести проверку представленных сведений, но не может потребовать от заявителя представления каких-либо дополнительных документов.

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 в следующих случаях:

1) если заявление подано от имени субъекта, не обладающего правом на учреждение СМИ (например, иностранца);

2) 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 понятно, что на большинство вопросов заявитель может отвечать в предположительном ключе;

3) если название, примерная тематика или специализация СМИ представляет собой злоупотребление свободой массовой информации;

4) если ранее было зарегистрировано СМИ с тем же названием и той же формой распространения информации. Практически все случаи отказа в регистрации имели место именно по этой причине.

Регистрация не является обязательной для тех СМИ, которые создаются органами власти исключительно для издания официальных материалов, нормативных и иных актов или выпускаются тиражом менее 1 000 экземпляров. Поэтому, например, подавляющее число ведомственных многотиражных газет издаются тиражом 999 экземпляров. Однако освобождение от регистрации не означает запрета на регистрацию таких СМИ. Исходя из анализа особенностей процедуры регистрации можно сделать вывод о том, что государственная регистрация СМИ носит ***уведомительный*** характер.

Процедура лицензирования деятельности аудиовизуальных СМИ. Для телевидения и радиовещания регистрация СМИ является необходимым, но не достаточным условием для начала деятельности по производству и выпуску средства массовой информации. Эта категория СМИ использует для передачи информации естественным образом ограниченный ресурс (эфирные частоты), в связи с чем государство ввело систему лицензирования в данной сфере. Лицензирование деятельности, в том числе и контроль за соблюдением лицензиатами лицензионных условий и требований, осуществляется также Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Аннулирование лицензии возможно в судебном порядке по искам заинтересованных лиц или лицензирующего органа в следующих случаях:

– обнаружение недостоверных данных в документах, послуживших основанием для принятия решения о выдаче лицензии;

– неустранение в установленный срок обстоятельств, послуживших основанием для приостановления действия лицензии;

– невыполнение лицензиатом обязательств, принятых им в процессе участия в торгах (если лицензия выдана по результатам проведенных торгов).

Правовой статус журналиста

В статусе журналиста реализуются те особые профессиональные интересы, которые производны от специфики его социальной роли. Речь идет о важнейших свойствах, которые в своей совокупности отличают журналистику от других профессий, и прежде всего о ее творческом характере и элементах публичной службы (public service). Отсюда следует обязанность законодателя, с одной стороны, установить гарантии свободы творчества и создать условия для эффективного выполнения журналистом социальной функции, а с другой – обеспечить ему повышенную правовую защиту при исполнении профессиональных обязанностей как

лицу, выполняющему общественный долг и ответственному перед своей аудиторией.

Согласно Закону о СМИ существуют правовое состояние журналиста и правовое состояние лица, приравненного к журналисту.

Согласно ст. 2 Закона о СМИ **журналистом признается лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию.** Как мы видим, в определении правового статуса журналиста соединены три компонента: характер работы журналиста, наличие обязательной регистрации СМИ и правовых отношений между журналистом и редакцией.

Лицами, приравненными к журналистам, признаются, во-первых, **штатные сотрудники редакций**, занимающиеся редактированием, созданием, сбором или подготовкой сообщений и материалов для **многотиражных газет** и других СМИ, продукция которых распространяется в пределах одной организации; а во-вторых, **авторы**, не связанные с редакцией СМИ трудовыми или иными договорными отношениями, но **признаваемые ею своими внештатными авторами или корреспондентами** при выполнении ими поручений редакции.

Права и обязанности журналиста определяются нормами гл. V Закона о СМИ. Зафиксированные здесь права и обязанности можно разделить на три группы:

1)права и обязанности, связанные **с получением** информации;

2)права и обязанности, связанные **с распространением** информации;

3)права и обязанности, связанные **с производством и выпуском** средств массовой информации.

Итак, в ходе ***поиска и сбора*** информации журналист реализует следующие права и обязанности: право искать, запрашивать и получать информацию (п. 1 ч. 1 ст. 47 Закона о СМИ); право посещать органы государственной власти и местного самоуправления, государственные и муниципальные организации и учреждения, унитарные предприятия, органы общественных объединений либо их пресс-службы (п. 2); право быть принятым должностными лицами в связи с запросом информации (п. 3); право получать доступ к документам и материалам, за исключением их фрагментов, содержащих сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну (п. 4); право копировать документы и материалы при условии соблюдения авторских прав и других исключительных прав (интеллектуальной собственности) (п. 5); право производить записи, в том числе и с использованием средств аудио- и видеотехники, кино- и фотосъемки, за исключением случаев, когда это запрещено законом (п. 6); право посещать специально охраняемые места стихийных бедствий, аварий и катастроф,

массовых беспорядков и массовых скоплений граждан, а также местности, в которых объявлено чрезвычайное положение; право присутствовать на митингах и демонстрациях (п. 7); право проверять достоверность сообщаемой ему информации (п. 8).

К сожалению, на практике эти права нередко нарушаются. Чаще всего речь идет о недопущении представителей прессы на место события, имеющего общественно важное значение, а также об «отсечении» журналистов от источников информации.

Упорядочению контактов власти и журналистов призван служить **институт аккредитации**. Согласно ст. 48 Закона о СМИ правила аккредитации не являются едиными для всех. Они устанавливаются самими органами государственной власти и местного самоуправления, организациями, учреждениями, органами общественных объединений, аккредитующими работников прессы. Редакции имеют право подавать заявки на аккредитацию своих журналистов, однако их удовлетворение зависит от того, соответствуют ли они установленным правилам. Сами эти правила должны соответствовать законодательству:

1) не должны ущемлять свободу массовой информации или права журналиста, поскольку поиск, получение, производство и распространение массовой информации **не подлежат ограничениям**, за исключением установленных федеральным законом;

2) не должны ущемлять права неаккредитованных журналистов (которые, например, должны иметь такой же доступ к информации о работе органов государственной власти);

3) должны гарантировать, что аккредитовавшие журналиста органы и организации будут предварительно извещать его о заседаниях, совещаниях и других мероприятиях, обеспечивать стенограммами, протоколами и другими документами, создавать благоприятные условия для аудио- и видеозаписи, фото- и киносъемки.

Но зачастую местные власти стремятся всячески оградить себя от прессы. Для этого вводят большое количество дополнительных условий, правил и ограничений на аккредитацию журналистов.

Другую группу составляют права журналиста, которые реализуются в процессе ***передачи информации*** от него к аудитории СМИ: а) право распространять информацию (п. 1 ч. 1 ст. 47); право публиковать, оглашать или иным способом воспроизводить документы и материалы при условии соблюдения авторских прав и других исключительных прав (интеллектуальной собственности) (п. 5); в) право излагать свои личные суждения и давать оценку в сообщениях и материалах, предназначенных для распространения в СМИ за его подписью (п. 9); г) право снять свою подпись под сообщением и 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 требованиями права

интеллектуальной собственности (п. 11); д) право распространять подготовленные им сообщения и материалы за своей подписью, под псевдонимом или без подписи (п. 12); е) право распространять сообщения и материалы, подготовленные с использованием скрытой аудио- и видеозаписи, кино- и фотосъемки только при наличии условий, перечисленных в ст. 51.

Именно на этапе передачи полученной информации от журналиста к аудитории СМИ возможны попытки возрождения цензуры. Чиновники разных рангов дают редактору или журналисту рекомендации как освещать интересные для власть имущих темы или вовсе отказаться от публикаций, посвященных острым проблемам.

Что же касается прав, связанных с **производством и выпуском СМИ**, то здесь к наиболее значимым фактам ограничения профессиональной деятельности редакций следует отнести попытки изъятия тиражей оппозиционных изданий, прекращения работы редакций, которые находятся в оппозиции к местным органам исполнительной власти в период выборных кампаний.

Наряду с правами у журналиста есть **обязанности,** они перечислены в ст. 49 Закона о СМИ. Журналист должен соблюдать устав редакции, с которой он состоит в трудовых отношениях, проверять достоверность, сообщаемой им информации, удовлетворять просьбы лиц, предоставивших информацию, об указании на ее источник, а также об авторизации цитируемого высказывания, если оно оглашается впервые, сохранять конфиденциальность информации и (или) ее источника, при получении информации от граждан и должностных лиц ставить их в известность о проведении аудио- и видеозаписи, кино- и фотосъемки, обязан предъявлять при осуществлении профессиональной деятельности по первому требованию редакционное удостоверение или иной документ, удостоверяющий его личность и полномочия.

Заслушивает внимания вопрос о соотношении права журналиста проверять достоверность сообщаемой **ему** информации (п. 8 ч. 1 ст. 47) и его обязанности проверять достоверность сообщаемой **им** информации (п. 2 ч. 1 ст. 49). Когда журналист является непосредственным очевидцем события, он обязан точно и добросовестно передать аудитории то, что сам видел и слышал. Именно так говорится в Декларации принципов поведения журналистов, утвержденной Международной федерацией журналистов (МФЖ): «Освещая события, журналист обязан оперировать только фактами, которые установлены лично им». Отсюда следует, что журналист обязан проверить, насколько достоверно в его сообщении будет изложено то, чему он сам был свидетелем.

Однако в большинстве случаев журналист не является непосредственным очевидцем событий и получает необходимые ему сведения из разных источников информации. В таком случае он **имеет право** проверить достоверность полученной информации. Например, должностное лицо прислало ответ на запрос информации. Журналист вправе не по-

верить тому, что содержится в ответе, и проверить, насколько он соответствует действительности. Это его, журналиста, право, но не обязанность.

Проверка достоверности информации становится **обязанностью** лишь в том случае, если журналист сообщает аудитории то, что стало ему известно от источника, **не указывая при этом сам источник.** В таком случае он как бы берет на себя роль очевидца, хотя таковым не является, и как очевидец обязан отвечать за достоверность сообщаемой ему информации.

Журналист обладает правом на **запрос информации**, т.е. на обращение редакции или журналиста к государственным органам и организациям, общественным объединениям и должностным лицам с целью получения сведений об их деятельности. Закон о СМИ допускает запрос информации как в устной, так и письменной форме. Это означает, что устное обращение журналиста, например, к губернатору с просьбой дать интервью есть не что иное, как запрос информации в устной форме. Следовательно, ответы интервьюируемого на вопросы журналиста следует рассматривать как ответ на запрос информации. При этом п. 3 ст. 57 освобождает журналиста от ответственности за содержание информации, если она получена в ответ на запрос.

На практике журналисты часто встречаются с волокитой и бюрократическими ухищрениями, направленными на то, чтобы не предоставлять информацию.

Заслуживает внимания вопрос о **защите источника информации.** Закон гарантирует свободу обмена корреспонденцией: никто не вправе вскрывать письма и телеграммы, поступающих в редакцию, знакомиться с их содержанием и оглашать его, подслушивать телефонные разговоры сотрудников, иначе как на основании судебного решения. Кроме того, Закон обязывает редакции СМИ и их сотрудников сохранять в тайне поступающую к ним от граждан доверительную информацию. Согласно ч. 2 ст. 41 и п. 4. ч. 1 ст. 49 Закона о СМИ редакции и журналисты обязаны не разглашать персональные данные, позволяющие идентифицировать личность автора письма или иного сообщения в редакцию, если тот оговорил сохранение их в тайне.

Профессия предоставляет журналисту право и обязанность вершить от имени общества публичный моральный суд над явлениями, привлекающими общественный интерес. Поэтому законодательством предусмотрены правовые гарантии журналистам для осуществления их правовой деятельности – статьи 140 (отказ в предоставлении информации) и 144 (воспрепятствование законной деятельности журналиста) УК РФ.

Проблемы правового регулирования электронных СМИ

Электронные СМИ занимают все более значительную долю рынка информационных услуг. Согласно исследованиям компании «Яндекс» крупное российское интернет-издание предлагает своим посетите-

лям 161 новость в день, каждый год в Рунете появляются сотни новых интернет-изданий[27]. Возрастает значимость интернет-СМИ практически во всех сферах. При этом развитие технических и технологических средств распространения массовой информации значительно опережает развитие правовых средств регулирования в этой сфере отношений.

Источники информации, существующие в Интернете, можно разделить на несколько видов.

1. Сайт официально существующего и зарегистрированного печатного издания, теле-, радиокомпании. Например, на сайтах «Российской газеты», «Комсомольской правды», «Эхо Москвы», как правило, представлены электронная версия печатного издания, архивы, где можно найти все прошлые выпуски. От бумажного или аудиоварианта они отличаются большим объемом представленных материалов, оперативностью, наличием гипертекстовых ссылок, возможностью обсуждения материалов в интерактивном режиме.

2. Издания, официально зарегистрированные как СМИ, но существующие только в электронной версии. Газета РУ, Четвертая власть.

3. Официальные сайты государственных органов, содержащие информацию о деятельности государственных органов и органов местного самоуправления.

4. Сайты, блоги, чаты, живые журналы, иные общедоступные информационные ресурсы, не зарегистрированные в качестве СМИ.

Именно эта четвертая группа источников информации вызывает больше всего вопросов. Указанные информационные объекты являются относительно новыми, правовой статус их до сих пор не определен, необходимость включения их в орбиту правового регулирования очевидна.

На сайтах публикуется большое количество различной информации, в том числе и порнографической, недостоверной или откровенно клеветнической, способствующей разжиганию национальной розни, имеющей отношение к терроризму и содержащей призывы к свержению власти. Тем самым происходит злоупотребление свободой массовой информации по смыслу ст. 4 Закона о СМИ. Содержание ресурсов противоречит интересам личности, общества и государства.

В ряде случаев деяния, нарушающие интересы личности, общества и государства и производимые через Интернет, рассматриваются как противоправные и противозаконные, но иногда, несмотря на очевидный социальный вред, однозначной юридической квалификации осуществляемым действиям дать нельзя.

Это связано с тем, что Закон РФ «О СМИ» не дает конечного перечня средств массовой информации, данный перечень заканчивается дефиницией «иные средства массовой информации». Закон не относит сайт

[27] Яндекс исследовал СМИ российского Интернета URL: http://gtmarket.ru/nevs/media-advertising-marceting/2006/11/23/408 (дата последнего обращения: 20 апреля 2010).

к перечню СМИ. Статья 24 Закона как будто бы предполагает возможность отнесения сайта к иным средствам массовой информации: «Правила, установленные настоящим Законом для периодических печатных изданий, применяются в отношении периодического распространения тиражом тысяча и более экземпляров текстов, созданных с помощью компьютеров и (или) хранящихся в их банках и базах данных, а равно в отношении иных средств массовой информации, продукция которых распространяется в виде печатных сообщений, материалов, изображений.

Правила, установленные настоящим Законом для радио- и телепрограмм, применяются в отношении периодического распространения массовой информации через системы телетекста, видеотекста и иные телекоммуникационные сети, если законодательством Российской Федерации не установлено иное».

Но не понятно, как и кто определит тираж сайта и что считать периодичностью? Ведь обновление информации на интернет-странице может производиться не сразу, а постепенно. Любые рассуждения о том, можно или нельзя относить к СМИ информационные источники Интернета, будут весьма спорными, и в настоящий момент однозначного и адекватного ответа на этот вопрос не существует.

Дело в том, что в момент разработки и создания Закона «О СМИ» никто не предполагал, что через несколько лет возникнет сеть Интернет – абсолютно новый механизм распространения информации, с помощью которого любое лицо, не имея никаких особых профессиональных навыков и организационно-технических возможностей, сможет распространять массовую информацию.

Приходится согласиться с Ю.М. Батуриным, одним из авторов Закона «О СМИ»: «Все эти интерпретации норм действующего закона “О средствах массовой информации” не имеют и не могут иметь однозначного толкования, поскольку уровень развития правоотношений в области распространения информации изменился с 1991 г. настолько, что нет никаких сомнений в необходимости изменять сами основы подходов к регулированию»[28]. В связи с развитием цифровых технологий необходимо совершенствование законодательства, которое оперирует устаревшим понятийным аппаратом и ориентировано на устаревшие модели правового регулирования.

На практике подавляющее большинство сайтов в сети Интернет не регистрируется в качестве средств массовой информации, поэтому проблема законности распространения массовой информации того или иного содержания остается открытой.

Существует несколько проектов изменения Закона «О СМИ» с учетом электронной формы их распространения. Однако единого мнения об определении правового статуса электронных СМИ пока не сложилось.

---

[28] Журналистика и право. Вып. 26. URL: http://www.medialaw.ru (дата последнего обращения: 20 апреля 2010).

В.Б. Наумов определяет возможные способы ликвидации этого пробела. Он считает, что возможно три варианта действий:

1) внесение в норму, характеризующую признак распространения массовой информации, дополнительных уточнений, отражающих особенности такого источника массовой информации, как сайт;

2) включение понятия «сайт» в категорию средств массовой информации;

3) создание в сфере информационного обмена новой системы категорий и понятий, вообще не ставящей во главу угла понятие «средство массовой информации»[29].

Первый и второй варианты можно реализовать путем принятия поправок в действующий Закон «О СМИ». Именно таким путем пошли некоторые западно-европейские страны. Например, в Финляндии соответствующим законом закреплен правовой статус интернет-СМИ, которые называются «сетевыми изданиями». Закон упоминает и иные источники массовой информации, существующие в Сети: порталы, чаты, блоги, закрепляя за ними более мягкий правовой режим.

Австрийское законодательство оперирует понятием «периодическое электронное средство массовой информации». Их владельцы, подобно владельцам прочих СМИ, будут обязаны публиковать о себе определенный набор идентифицирующих сведений. Данный закон дифференцирует интернет-СМИ по критерию публичности. Для тех из них, что предназначены исключительно для самовыражения, предусмотрен более мягкий правовой режим функционирования. И финский и австрийский законы предусматривают право на ответ, т.е. возможность лица, которое считает, что в сетевом издании была дана оскорбительная для него информация, разместить в этом же издании свой ответ.

В последнее время все популярнее становятся формы так называемой «горизонтальной» коммуникации, когда информация распространяется не профессиональными журналистами, СМИ или правительственными органами, а непосредственно самими пользователями. Блоги и чаты превращаются в живое пространство общественного мнения. Многие интернет-издания и медиахолдинги выделяют площадки для размещения интернет-блогов и разрешают читателям публиковать собственные новости. Фактически идет распространение массовой информации людьми-непрофессионалами, не имеющими элементарных навыков работы с информацией, не обладающими определенным правовым статусом в информационной сфере. Нередки случаи, когда российская блогосфера становится объектом манипуляций, когда вдруг происходит вброс «сенсационных фактов», пользователи, не имеющие работать с информацией, не проверяют ее, не могут критично осмыслить появившиеся сведения, мгновенно передают их друг другу, способствуя тем самым распространению заведомо ложной информации.

---

[29] См.: *Наумов В.Б.* Право и Интернет: Очерки теории и практики. М., 2002. С. 81.

Еще одной новой формой реализации свободы слова становится создание информации на основе вики-технологий, которые представляют собой гипертекстовую среду, позволяющую пользователям легко добавлять свои новости, сведения, знания в контент вики-сайта. «Вики-технология призвана решать простую и естественную задачу – дать возможность каждому посетителю сетевого ресурса участвовать в разработке сетевого контента. Причем участвовать не только в качестве комментатора, но и в качестве полноценного автора и редактора»[30]. Знаменитой эта технология стала после создания Wikipedia (Википедии) – онлайн-энциклопедии, создаваемой трудом неограниченного коллектива добровольных авторов. Популярность Википедии огромна, на сегодняшний день количество сведений, представленных на ее электронных страницах, составляет более 15 млн статей (на русском – 497 786), что превышает объем любой из энциклопедий, когда-либо созданных людьми. Отношения между авторами=пользователями Википедии строятся на основе саморегулирования: в случае появления недостоверной, ошибочной или заведомо ложной информации она критикуется, исправляется, дополняется другими авторами. В то же время надежность и точность Википедии все же часто становятся объектом критики.

Можно выделить два подхода к правовому регулированию распространения массовой информации в Интернете. Первая позиция заключается в том, что к интернет-источникам необходимо применять инструментарий правового регулирования, действующий с сфере массовой информации, сами интернет-источники признать средствами массовой информации, их авторам придать правовой статус журналистов и редакторов. Такой точки зрения придерживается, например, А.Г. Арешев: «Такие формы коммуникации, как блоги, форумы, электронные версии прессы являются публичной информацией, которая должна регулироваться теми же законами, что и телерадиовещание и печатные издания. Вряд ли в этом случае уместно говорить о цензуре – речь идет просто о создании единой законодательной среды для всех источников информации»[31].

Другой подход представлен в работах В.Н. Монахова, который говорит о необходимости переноса акцента в регулировании СМИ с форм распространения информации на требования к контенту – содержанию информации. Ученый указывает, что в ближайшем будущем должна произойти смена векторов правового регулирования: от правового ответа на вопрос «как?» к ответу на вопрос «что?».

На этапе развития «как?» главным было регулирование технологических и организационно-правовых форм, с помощью которых инфор-

---

30 *Монахов В.Н.* Средства массовой информации в новых условиях // Информационное право: актуальные проблемы теории и практики. С. 356.

31 *Арешев А.Г.* Новые средства массовой информации: в поисках оптимального баланса // Конфликты в информационной сфере: Материалы теоретического семинара Сектора информационного права ИГП РАН. М., 2009. С. 121.

мация доставляется потребителю. Этап развития «что?» формулирует содержательные вопросы, прежде всего о качественной стороне информации (контенте), механизме реализации права на свободу слова, защите от злоупотребления этой свободой[32].

Тема 8. ПРАВОВОЕ РЕГУЛИРОВАНИЕ РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

Особенности рекламной информации

Реклама является одним из наиболее распространенных и распространяемых видов информации, в то же время в науке информационного права она исследована недостаточно.

Понятие рекламы дано в ст. 3 Федерального закона «О рекламе» от 13 марта 2006 г. № 38-ФЗ.

Реклама – 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.

Из этого определения следует, что понятие рекламы дается через понятие информации. Однако реклама – не всякая информация. Она обладает определенными признаками:

1)она должна быть распространена;

2)она адресована неопределенному кругу лиц;

3)это информация, которая создается с четко определенной целью: привлечь внимание к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

Специфика рекламы состоит в том, что она обладает ***двойственной природой***. С одной стороны, реклама является формой распространения массовой информации, и в таком случае должна пользоваться конституционной защитой свободы информации. Стало быть, ее можно ограничивать только федеральным законом и только в той мере, в какой это необходимо в целях защиты конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, для обеспечения обороны и безопасности нашего государства.

С другой стороны, реклама отличается от простых объявлений и сообщений тем, что создает привлекательный образ товара или услуги.

---

32 *Монахов В.Н.* СМИ – что день грядущий им готовит? // Теоретические проблемы информационного права. М., 2006. С. 67.

Реклама всегда идет навстречу иллюзиям, вкусам, ожиданиям потребителей, но, как правило, информирование зачастую заменяется внушением и манипуляцией сознанием. Это достигается при помощи вербальных средств, а также за счет применения новейших технологий.

Нужно согласиться с А.В. Минбалеевым, что «с позиции информационного права реклама является специализированной разновидностью массовой информации, обладающей определенными признаками, которая предназначена для реализации конкретных целей, предусмотренных в том или ином законе»[33].

«Правовой подход, который сложился в большинстве стран мира, – отмечает А. Рихтер, – свидетельствует о том, что хотя реклама и признается формой свободы слова, степень ее правовой защищенности не столь велика, как у других форм этой свободы. Другими словами, реклама подлежит ограничениям, непривычным для иной информации»[34]. Не исключением здесь является и правовое регулирование рекламы в нашей стране.

Реклама, будучи одной из форм распространения массовой информации, является мощным стимулирующим фактором, определяющим поведение потребителя на рынке товаров, работ и услуг. Реклама влияет на колебание рыночной стоимости товара, формирует покупательский спрос, мотивацию поведения субъектов предпринимательской деятельности, создает стиль фирмы либо коммерческой организации и ее деловую репутацию. Именно на основе рекламы потребители зачастую делают свой выбор в пользу того или иного товара, отдают предпочтение тому или иному производителю.

В то же время сама рекламная индустрия стала развиваться в России в полноценном формате лишь в последние полтора десятилетия. Как следствие, к настоящему моменту еще не до конца сложилось адекватное отношение потребителей к рекламе (особенно это касается лиц пожилого возраста, которые в основной своей массе привыкли безоговорочно верить телевизору и печатному слову), а также и этические составляющие деятельности рекламодателей и рекламопроизводителей. Следовательно, можно говорить об объективной необходимости защитить потребителя информации от недостоверной рекламы.

В Законе о рекламе определена **сфера действия** законодательства о рекламе.

Новый закон, как и прежний, устанавливает, что его действие **не распространяется** на:

1) политическую рекламу;

2) объявления физических лиц или юридических лиц, не связанные с осуществлением предпринимательской деятельности;

---

33 *Минбалеев А.В.* Реклама как объект информационных правоотношений. Челябинск, 2009. С. 203.

34 *Рихтер А.* Правовое регулирование рекламы в СМИ //Законодательство и практика СМИ. 1999. № 5. С. 89.

3) упоминания о товаре, средствах его индивидуализации, об изготовителе или о продавце товара, которые органично интегрированы в произведения науки, литературы или искусства и сами по себе не являются сведениями рекламного характера (п. 9 ч. 2 ст. 2 Закона). Ярким примером данного способа продвижения товара является скрытая реклама известных брэндов, размещенная в самых известных российских блокбастерах, вышедших в прокат в последнее время. Ранее Закон о рекламе никак не регулировал данные правоотношения, поэтому возникали спорные ситуации: считать или не считать показ в фильме того или иного товара со всеми полагающимися ему логотипами рекламой или нет. Теперь на этот вопрос дается относительно понятный ответ: такие материалы рекламой не являются.

4) информацию, раскрытие или распространение либо доведение до потребителя которой является обязательным в соответствии с федеральным законом, – справочно-информационные и аналитические материалы (обзоры внутреннего и внешнего рынков, результаты научных исследований и испытаний), не имеющие в качестве основной цели продвижение товара на рынке и не являющиеся социальной рекламой;

5) сообщения органов государственной власти, иных государственных органов, органов местного самоуправления, муниципальных органов, которые не входят в структуру органов местного самоуправления, если такие сообщения не содержат сведений рекламного характера и не являются социальной рекламой;

6) вывески и указатели, не содержащие сведений рекламного характера;

7) информацию о товаре, его изготовителе, об импортере или экспортере, размещенную на товаре или его упаковке;

8) любые элементы оформления товара, помещенные на товаре или его упаковке и не относящиеся к другому товару.

Отграничение рекламы от иных видов информации имеет большое практическое значение. Ю.Ю. Горячева под рекламой понимает «исключительно информацию, способствующую предпринимательской деятельности, носящую добровольный характер, могущую побудить потребителя к действиям, связанным с реализацией или приобретением объектов как товаров на рынке»[35]. Схожую позицию занимает и правоприменитель[36].

Закон дает определение основных субъектов рекламных правоотношений:

1) **«рекламодатель»** – изготовитель или продавец товара, либо иное определившее объект рекламирования и (или) **содержание** рекламы лицо;

2) **«рекламопроизводитель»** – лицо, осуществляющее полностью или частично приведение информации в готовую для распространения в виде рекламы **форму**;

---

35 *Горячева Ю.Ю.* Разграничение рекламы и информации нерекламного характера // Законодательство. 2000. № 5. С. 12.

36 См.: Постановление Президиума Высшего Арбитражного Суда РФ от 19.10. 1999 г. № 3331/99 // Вестн. ВАС РФ. 2000. № 1. С. 45.

3) **«рекламораспространитель»** – лицо, осуществляющее распространение рекламы любым **способом**, в любой **форме** и с использованием любых **средств**;

4) **«потребители рекламы»** – лица, на привлечение внимания которых к объекту рекламирования направлена реклама.

Новый закон вводит понятия новых субъекта и объекта рекламной деятельности – спонсор и спонсорская реклама.

Основные ограничения в рекламе

Реклама, не соответствующая требованиям законодательства Российской Федерации, определяется Законом как **ненадлежащая,** которая включает в себя три вида: **недобросовестную, недостоверную, скрытую**.

Недобросовестной признается реклама, которая:

1)содержит некорректные сравнения рекламируемого товара с находящимися в обороте товарами;

2)порочит честь, достоинство или деловую репутацию лица, в том числе и конкурентов;

3)представляет собой рекламу товара, которая запрещена данным способом, в данное время или в данном месте, если она осуществляется под видом рекламы другого товара, товарный знак или знак обслуживания которого тождествен или сходен до степени смешения с товарным знаком или знаком обслуживания товара, в отношении рекламы которого установлены соответствующие требования и ограничения, а также под видом рекламы изготовителя или продавца такого товара.

Впервые в российском законодательстве вводится запрет на использование так называемых «зонтичных» брэндов. Их применение представляет собой рекламу товаров, рекламирование которых жестко ограничено тем или иным законом, посредством другого товара, имеющего с ним тождественные или сходные до степени смешения средства индивидуализации: название, логотип, форму упаковки или тары и т.п. Потребитель в большинстве случаев, видя или слыша подобную рекламу, относит ее не к формально рекламируемому товару, а к тому, реклама которого данным способом, в данное время или в данном месте запрещена и прорекламировать который фактически и хотел рекламодатель.

Наибольшее распространение использование «зонтичных» брэндов получило в сфере рекламы алкогольной продукции. Почти все компании, производящие или импортирующие алкогольную продукцию под широко известными товарными знаками, были замечены в рекламе товаров, услуг, конкурсов, лотерей или иных мероприятий, имеющих похожее или одинаковое название с алкогольными брэндами. Ограничения, накладываемые на рекламу алкоголя, закрывают для нее самые мощные СМИ и средства распространения рекламы: телевидение, радио, печатные издания (за небольшим исключением), средства размещения наружной ре-

кламы. Производители спиртного, не желая, чтобы потребитель попросту забыл, как выглядит их продукция, шли на хитрость и использовали «зонтичные» брэнды. Видя растущее число случаев обхода ограничений, наложенных на рекламу алкоголя и иных подобных товаров, законодатель попытался поставить на их пути серьезный заслон;

4) нарушает антимонопольное законодательство.

Часть 3 ст. 5 Закона содержит в себе перечень признаков **недостоверной** рекламы. Недостоверной признается реклама, которая **содержит несоответствующие сведения** об ассортименте, комплектации, потребительских качествах товаров и т.д.

В предыдущем Законе о рекламе устанавливался запрет на использование терминов в превосходной степени, в частности, путем употребления слов «самый», «только», «лучший», «абсолютный», «единственный» и тому подобных, если их невозможно подтвердить документально. В настоящее время непосредственно запрет на использование этих слов исчез, но появился запрет на недостоверную информацию о преимуществах рекламируемого товара перед находящимися в обороте, которые произведены другими изготовителями или реализуются другими продавцами.

В отдельную категорию выделена реклама, содержащая недостоверные сведения о правах на использование официальных государственных символов и символов международных организаций. Это связано с получившей распространение практикой неправомерного использования в рекламе тех или иных товаров, работ или услуг в качестве визуального ряда и (или) звукового сопровождения государственной символики и атрибутики. В резуьтате у потребителей создавалось впечатление о том, что деятельность по продаже рекламируемого товара (выполнению работ или оказанию услуг) проводится под эгидой, с ведома или при поддержке государства. Как известно, степень доверия населения к государству в России достаточно высока, в силу чего подобные товары, работы или услуги получали неоправданное преимущество перед аналогичными товарами, работами и услугами других производителей за счет введения потребителя в заблуждение.

Это же касается недостоверных сведений об официальном и общественном признании, получении медалей, призов, дипломов и иных наград.

Отметим также, что прежний Закон о рекламе разграничивал недостоверную и заведомо ложную рекламу. Такая реклама определялась как «реклама, с помощью которой рекламодатель (рекламопроизводитель, рекламораспространитель) умышленно вводит в заблуждение потребителя рекламы».

Специалисты по-разному относятся к исчезновению понятия «ложная реклама» из Закона о рекламе. Практическое значение такого разграничения объяснялось присутствием в Уголовном кодексе РФ ст. 182, устанавливавшей ответственность за использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей

(исполнителей, продавцов) в корыстных целях, которое причинило значительный ущерб. Федеральным законом от 8 декабря 2003 года № 162-ФЗ «О внесении изменений и дополнений в Уголовный кодекс Российской Федерации» данная статья была исключена из УК РФ. Таким образом, поскольку заведомо ложная реклама была декриминализирована, необходимость в разграничении заведомо ложной и недостоверной рекламы отпала. Многие ученые-юристы считают декриминализацию ст. 182 УК РФ и исчезновение понятия «ложная реклама» из закона о рекламе негативным фактом.

В целом появился целый ряд новых **общих ограничений на рекламу**. Она не должна побуждать к совершению противоправных действий, призывать к насилию и жестокости, формировать негативное отношение к лицам, не пользующимся рекламируемыми товарами, или осуждать таких лиц.

В настоящее время в рекламе не допускается:

– использование иностранных слов и выражений, которые могут привести к искажению смысла информации;

– использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений, в том числе и 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;

– демонстрация процессов курения и потребления алкогольной продукции, а также пива и напитков, изготавливаемых на его основе, ранее такое ограничение существовало только для рекламы алкогольной и табачной продукции, теперь запрет охватывает любую рекламу;

– использование образов медицинских и фармацевтических работников, за исключением использования в рекламе медицинских услуг, средств личной гигиены, в рекламе, потребителями которой являются исключительно медицинские и фармацевтические работники, а также распространяемой в местах проведения медицинских или фармацевтических выставок, семинаров, конференций и иных подобных мероприятий, размещенной в печатных изданиях, предназначенных для медицинских и фармацевтических работников;

– реклама, в которой отсутствует часть существенной информации о рекламируемом товаре, об условиях его приобретения или использования, если при этом искажается смысл информации и вводятся в заблуждение потребители рекламы.

Отдельная статья Закона посвящена **защите несовершеннолетних в реклам**е. В данном случае запреты связаны с тем, что недостаточность жизненного опыта, ранимость, доверчивость, эмоциональная открытость делают несовершеннолетних наиболее уязвимыми от рекламного воздействия.

Не допускается следующая реклама:

1) наркотических средств, психотропных веществ и их прекурсоров;

2) взрывчатых веществ и материалов, за исключением пиротехнических изделий;

3) органов и (или) тканей человека в качестве объектов купли-продажи;

4) товаров, подлежащих государственной регистрации в случае отсутствия такой регистрации;

5) товаров, подлежащих обязательной сертификации или иному обязательному подтверждению соответствия требованиям технических регламентов в случае отсутствия такой сертификации или подтверждения такого соответствия;

6) товаров, на производство и (или) реализацию которых требуется получение лицензий или иных специальных разрешений в случае отсутствия таких разрешений.

Особенности рекламы отдельных видов товаров

Реклама некоторых товаров и услуг подлежит разнообразным ограничениям. Прежде всего, это ограничения по содержанию и форме. Например, установлено, что реклама алкогольной продукции, пива и табака не должна содержать утверждения о том, что употребление этой продукции имеет важное значение для достижения общественного признания, спортивного или личного успеха, способствует улучшению физического или эмоционального состояния, а также осуждать неупотребление этой продукции и обращаться к несовершеннолетним и использовать их образы. В рекламе пива запрещено использовать образы людей и животных. Кроме того, установлены ограничения по месту ее распространения: реклама данных продуктов не должна размещаться на первой и последней полосах газет, обложках журналов, в предназначенных для несовершеннолетних печатных изданиях, а также рядом с детскими, образовательными, медицинскими, оздоровительными организациями, театрами, музеями, библиотеками, лекториями, планетариями, физкультурно-оздоровительными и спортивными сооружениями (т.е. не ближе чем 100 м от них). В то же время реклама алкогольной продукции и табака в принципе запрещена в теле-, радиопрограммах и на рекламных конструкциях, а реклама пива не должна размещаться в телепрограммах с 7 до 22 часов и в радиопрограммах с 9 до 24 часов, но может размещаться на рекламных конструкциях. Реклама всех этих видов товаров должна сопровождаться предупреждением о вреде чрезмерного потребления. Предупреждения для алкогольной продукции и табачных изделий должно занимать не менее 10% площади рекламного сообщения, пива – не менее 7%.

Реклама лекарственных средств, методов лечения, биологических добавок не должна содержать ссылки на конкретные случаи излечения, выражение благодарности якобы излечившихся, утверждение или предположение о наличии у потребителей тех или иных заболеваний, создавать впечатление ненужности обращения к врачу.

Очень подробно прописаны ограничения рекламы финансовых услуг и ценных бумаг. Это связано с распространением финансовых пирамид, для которых реклама является необходимым условием деятельности.

Закон о рекламе также запрещает **скрытую рекламу**, т.е. рекламу, которая оказывает неосознаваемое потребителями воздействие на их сознание, в частности, путем использования видеовставок (двойной звукозаписи) и иными способами.

Правовое регулирование распространения рекламы в электронной среде

Основные положения Закона о рекламе применяются и по отношению к рекламе, распространяемой в Интернете. Это касается запрета недостоверной и недобросовестной рекламы, общих ограничений на рекламу у отдельных видов товаров.

Одним из способов распространения рекламы в электронной среде является спам – навязанное пользователю электронное послание.

Количество массовых рассылок, получаемых в виде незапрашиваемой корреспонденции, увеличивается и наносит большой ущерб и пользователям, и интернет-провайдерам, вынужденным наращивать мощности только для того, чтобы быть в состоянии обработать огромный объем незапрошенных сообщений.

Главная опасность спама состоит в том, что таким способом распространяется не только реклама, но и вредоносные программы – вирусы.

В Федеральном законе «О рекламе» от 13 марта 2006 г. № 38-ФЗ в ч. 1 ст. 18 впервые запрещены несанкционированные пользователем электронные рассылки.

Распространение рекламы по сетям электросвязи, в частности, посредством использования телефонной, факсимильной, подвижной радиотелефонной связи допускается только **при условии предварительного согласия абонента или адресата на получение рекламы**. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено. Рекламораспространитель обязан немедленно **прекратить свои действия в адрес лица, обратившегося к нему**.

Не допускается использование сетей электросвязи для распространения рекламы с применением средств выбора и (или) набора абонентского номера без участия человека (автоматического дозванивания, автоматической рассылки).

Таким образом, рассылка незапрошенных сообщений является одним из нарушений Закона о рекламе и соответственно влечет административную ответственность.

Кроме того, ст. 10 Федерального закона «Об информации» устанавливает два важных требования:

– информация, распространяемая без использования средств массовой информации, **должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица**;

– при использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, **распространяющее информацию, обязано обеспечить ее получателю возможность отказа от нее**.

Таким образом, для всех рассылок вне зависимости от их содержания устанавливается режим обязательного обеспечения возможности отказа от рассылаемой информации, что, безусловно, является положительным моментом.

Важный шаг в борьбе против спама можно назвать постановление Правительства РФ от 10 сентября 2007 г. № 575 «Правила оказания телематических услуг связи», в котором было дано определение спама и введен запрет на него.

Согласно п. 2 Правил спам – «телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя».

В этом же документе устанавливается, что абонент вправе:

а) отказаться от оплаты телематических услуг связи, не предусмотренных договором и предоставленных ему без его согласия;

в) требовать от оператора связи исключения возможности доступа к информационным системам, сетевые адреса или унифицированные указатели которых абонент сообщает этому оператору в предусмотренном договором виде.

В свою очередь, оператор связи обязан:

а) предпринимать меры по защите абонентского терминала от воздействия вредоносного программного обеспечения;

б) препятствовать распространению спама и вредоносного программного обеспечения с его абонентского терминала.

Таким образом, указанным нормативным актом применительно к рассылкам закрепляется механизм «opt-in» (режим, в котором рассылка осуществляется исключительно по предварительной подписке) и устанавливается запрет фальсификации сведений об авторе сообщения.

Государственный контроль в сфере рекламы

Государственный контроль в сфере рекламы возложен на Антимонопольный орган и его территориальные органы (Федеральная антимонопольная служба – ФАС).

Антимонопольный орган вправе:

1) выдавать рекламодателям, рекламопроизводителям, рекламораспространителям обязательные для исполнения предписания о **прекращении нарушения** законодательства Российской Федерации о рекламе;

2) выдавать федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации и МСУ обязательные для исполнения предписания **об отмене или изменении актов, изданных ими и противоречащих законодательству о рекламе**;

3) предъявлять в суд или арбитражный суд иски **о запрете распространения рекламы**, осуществляемого с нарушением законодательства РФ;

4) предъявлять в суд или арбитражный суд иски о публичном **опровержении недостоверной рекламы (контррекламе)** за счет рекламодателя.

За недостоверную рекламу предусмотрена административная ответственность. Не указан конкретный состав правонарушений, поэтому можно сделать вывод, что весь спектр нарушений законодательства о рекламе является административным правонарушением: распространение ненадлежащей рекламы (недобросовестной, недостоверной, в неположенное время, в неположенном месте, с нарушением ограничений, предусмотренных для отдельных видов товаров, отказ от контррекламы и др.).

К сожалению, на сегодняшний день эффективных методов защиты от недостоверной рекламы на стадии, когда она еще не дошла до конечного потребителя, практически не существует. Штрафы, предусмотренные законодательством об административных правонарушениях, несопоставимы с потенциальной прибылью от недостоверной рекламы, а такие меры, как запрет (прекращение размещения) недостоверной рекламы и контрреклама недостаточно оперативны и не обеспечивают гарантированную защиту потребителей.

Закон о рекламе устанавливает, что любой факт ненадлежащей рекламы является основанием для принятия антимонопольным органом решения об опубликовании контррекламы. Особенностью данного вида наказания для рекламодателя является то, что контрреклама должна быть опубликована в тех же средствах массовой информации, в то же время (если это телевидение или радио) или на том же месте той же полосы (в печатных СМИ) и, самое главное, в том же объеме, что и первоначальная реклама. Все расходы, связанные с опубликованием контррекламы, должен нести нарушитель.

Важно отметить, что федеральный орган не вправе заниматься цензурой: он контролирует рекламу не с момента ее изготовления, а лишь после распространения.

Модуль 3

ПРАВОВЫЕ РЕЖИМЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, СИСТЕМ И КОММУНИКАЦИОННЫХ СЕТЕЙ

Тема 9. ПРАВОВЫЕ ОСНОВЫ ДОКУМЕНТИРОВАНИЯ ИНФОРМАЦИИ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ

Понятие и признаки документированной информации

Согласно ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» **«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».** В данном определении законодатель указывает, во-первых, на неразрывную связь содержания с материальным носителем и, во-вторых, на особый элемент документированной информации, а именно ее реквизиты, подлежащие закреплению на том же материальном носителе.

Роль документа в праве состоит в том, что он является письменным свидетельством, удостоверяющим факты, данные, сведения, имеющие определенное правовое значение. При этом сам документ остается искусственной формой существования информации, которая включает выделенные по цели сведения и через определенные реквизиты позволяет донести информацию о создателе, содержании, источнике, адресате информации и других обстоятельствах ее использования.

Основными требованиями, обеспечивающими юридическую силу документа, являются:

– соблюдение письменной формы;

– соответствие нормативно-правовым актам, определяющим сферу регулирования и цели создания;

– обеспечение необходимой степени защищенности информации от подделки и несанкционированных изменений;

– удостоверение информации должностным лицом в пределах его полномочий и компетенции собственноручной подписью;

– соблюдение порядка ведения и приобщения документа к делу.

Особую роль в документе выполняют **реквизиты**, т.е. такие атрибуты документа, которые предусмотрены законом или действующим порядком оформления (правилами), их наличие делает документ до-

стоверным, действительным, отсутствие одного или нескольких реквизитов влечет ничтожность или оспоримость документа. При возникновении правовых коллизий их участников интересуют, прежде всего, такие реквизиты, которые обеспечивают юридическую силу и значимость документа. Одним из таких реквизитов является подпись. Подпись – это реквизит, устанавливаемый в соответствии с требованиями нормативно-правовых актов, стандартов или обычаев делового оборота. Наличие подписи в документе означает, что человек, ее поставивший, ознакомился с содержанием документа, согласен с ним, принимает на себя определенные обязательства или несет ответственность за действия, вытекающие из его содержания. Целями юридической процедуры подписания является подтверждение идентичности подписывающей стороны. При этом предполагается, что подписант, во-первых, дееспособен, во-вторых, обладает соответствующими полномочиями, в-третьих, свободен в своем волеизъявлении. Кроме того, содержание документа не может измениться после его подписания.

Информационный ресурс, выраженный документом, представляет собой материальный объект и одновременно является результатом интеллектуальной деятельности. Если форма документа будет соответствовать требованиям произведения, он является объектом авторского права.

Особенности электронного документа

Относительно новой формой организации и представления документированной информации является электронный документ, представляющий собой модификацию базового родового понятия «документ». Электронные документы получили широкое применение во многих сферах деятельности, причем последние используются не только наряду с традиционными бумажными документами, но и вместо них. «Переход на новые формы представления информации и работы с этим ресурсом, скорость доступа к информации и обмена ею в режиме он-лайн способствуют расширению информационного пространства каждого пользователя, облегчают контакты обладателей информацией и всех, кто нуждается в ее получении и использовании. И все это совершается через документ – основную форму представления информации»[37].

Считается, что использование систем электронного документооборота позволяет добиться огромного экономического эффекта, а применительно к России с учетом ее территориальной протяженности такое снижение издержек может быть особенно значительным.

В связи с этим особенно актуальным является правовое регулирование отношений в области электронного документооборота и придание юридической силы электронным документам.

Легальное определение электронного документа мы находим в Федеральном законе «Об электронной цифровой подписи» от 10 января

---

37 *Бачило И.Л.* Информационное право. С. 166.

2002 г. № 1-ФЗ. Согласно этому Закону «**электронный документ – документ, в котором информация представлена в электронно-цифровой форме**». Законодатель в данном определении обратил внимание лишь на форму предоставления информации данного класса, отличающую ее от других документов. В юридической литературе отмечалось, что указанное определение слишком широкое, в чем и состоит его недостаток.

Выделяют три элемента электронного документа:

1)само содержание информации;

2)форма предоставления содержания;

3)носитель информации.

Для электронных документов характерны некоторые особенности, создающие проблемы их использования. При характеристике электронного документа надо иметь в виду следующее:

1. Электронный документ определяется через понятие «документ» в его классическом значении. Отличие электронного документа от традиционного бумажного состоит в том, что **его содержание может восприниматься исключительно с помощью специальных инструментально-технических и программно-аппаратных средств**. В то же время не стоит жестко разделять бумажные и электронные документы, более эффективным будет применение двойных технологий, которые гармонично сочетают бумажные и электронные способы документирования информации.

2. Основной формой электронного документа является **электронный файл**[38]. Иными словами, объектом права может быть запись именного цифрового файла или запись в файле, запись в файле базы данных как объективно существующая статическая форма материального представления информации. Носителями электронных файлов могут выступать магнитный жесткий диск, дискета, флеш-карта, оптический CD-диск и др.

3. Электронный документ обязательно должен быть доступен для восприятия человека. Поэтому статус электронных документов не может быть распространен на информацию, создаваемую средствами вычислительной техники в процессе их работы, которая не имеет аналоговых отображений и, соответственно, не может быть воспринята человеком[39]. Но в отличие от традиционного документа, который облечен в единую (единственную) форму представления, электронный документ может объективироваться, выражаться и восприниматься в разных формах.

4. Содержание электронного документа связано с формой его организации, реквизитами, характеризующими составителя документа, получателя, сведения о времени и месте его составления и др.

---

38 См.: *Семилетов С.И.* Документирование информации и организация документооборота в условиях информатизации // Информационные ресурсы развития Российской Федерации. Правовые проблемы. М., 2003. С. 121–122.

39 См.: *Чаннов С.Е.* Информационное право России. М., 2006. С. 56.

Специалисты выделяют так называемые **сводные электронные документы**, к которым относятся базы данных, информационные ресурсы сервера и банки данных. Сложную структуру имеют электронные регистрационно-учетные документы: регистры, реестры, классификаторы.

В целом электронный документ должен иметь правовой режим, уравнивающий его с традиционными документами.

Юридическая сила электронного документа определяется теми же требованиями, что и юридическая сила традиционного документа, т.е. наличием необходимых реквизитов и выполнением установленных юридических процедур. Но электронный документ обладает специфическими особенностями: он легко копируется, может быть изменен без ведома его создателя, а также подделан.

Придать электронному документу юридическую силу и защитить его от несанкционированного изменения призвана электронная цифровая подпись (ЭЦП). Условия и порядок ее применения призван был решить Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ.

Электронная цифровая подпись (ЭЦП)

Электронно-цифровая подпись – 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.

С юридической точки зрения **ЭЦП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе** (ст. 3 Федерального закона «Об электронной цифровой подписи»).

В данном определении законодатель устанавливает триединую цель введения электронной цифровой подписи:

– защита от подделки;
– способ идентификации;
– гарантия от искажения информации.

Субъектами электронно-цифровой подписи выступают:

– пользователи информационной системы;
– обладатели электронно-цифровой подписи;
– удостоверяющие центры;
– уполномоченные федеральные органы исполнительной власти.

ЭЦП основана на так называемой **технологии асимметричных ключей подписи**. Для автора документа генерируется **закрытый ключ**

– последовательность цифр определенной длины. Электронный документ с технической точки зрения также представляет собой последовательность цифр. На базе закрытого ключа создается **открытый ключ**, доступный каждому. Открытый и закрытый ключи однозначно связаны между собой, однако вычислить закрытый ключ по открытому практически невозможно.

Общая схема использования ЭЦП заключается в следующем. Отправитель электронного документа, являющийся владельцем сертификата ключа, создает с применением известного только ему закрытого ключа свою электронную подпись, т.е. специальную программу кодирования, и направляет электронный документ с реквизитом в виде этой программы по электронной почте адресату. Тот, кому адресован данный документ с ЭЦП, имеет возможность прочесть электронный документ и подтвердить правильность ЭЦП с помощью открытого ключа.

Закрытый ключ содержится в тайне и известен только владельцу, чтобы никто кроме него не смог сформировать ЭЦП под документом. В то же время любое заинтересованное лицо может проверить с помощью опубликованного открытого ключа, что документ подписал именно владелец и не искажен (иначе меняется производная величина). В результате запуска программы открытого ключа пользователь получает результаты проверки в наглядном виде как сообщение о том, что документ подписан таким-то лицом, некоторые другие дополнительные данные, или получает отрицательный результат.

Таким образом, подделать электронный документ, подписанный ЭЦП, значительно 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.

Важно, чтобы информация о принадлежности открытого ключа определенному пользователю была документально оформлена, причем такое оформление должно быть выполнено соответствующим ответственным органом – удостоверяющим центром. Соответствующий документ получил название сертификата ключа подписи. Требования к сертификату ключа подписи изложены в ст. 6 Закона об ЭЦП. 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 удостоверяющих центров, но доказательная сила такой подписи резко падает.

Удостоверяющий центр изготавливает сертификаты ключей подписей, создает ключи ЭЦП с гарантией сохранения в тайне закрытого клю-

ча, приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их, ведет реестр сертификатов ключей подписей и архива удостоверяющего центра, осуществляет подтверждение подлинности электронной цифровой подписи в электронном документе.

Электронно-цифровая подпись в электронном документе становится равнозначной собственноручной подписи при следующих условиях:

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.

Выделяются следующие **правовые проблемы, связанные с использованием ЭЦП**[40]**.** Собственноручная подпись не отделима от человека, а наиболее важный компонент ЭЦП – секретный закрытый ключ – отделим. Поэтому если третьему лицу станет известен закрытый ключ, отличить подлог подписи до аннулирования ключей будет невозможно. В результате этого возникает необходимость в установлении правомерности владения секретным ключом лица, подписавшего документ.

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 сохранности 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 электронной 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 причинены в результате несанкционированного взлома сертифицированных средств цифровой подписи или наличия в них разного рода программных или аппаратных закладок. Не определен также порядок хранения и доступа к закрытым ключам ЭЦП в удостоверяющих центрах.

---

40 См.: *Ковалева Н.Н.* Указ.соч. С. 202.

К недостаткам Федерального закона «Об электронной цифровой подписи» можно отнести следующее:

– допускается использование единственной технологии электронной цифровой подписи;

– единая иерархическая система удостоверяющих центров и обязательная сертификация средств электронной цифровой подписи делают ее применение чрезвычайно сложным и довольно дорогим;

– его положения не соответствуют основным принципам, реализуемым в иностранном законодательстве и международном праве при осуществлении правового регулирования электронных подписей;

– не допускается электронная цифровая подпись юридических лиц.

Указанные недостатки не позволяют широко использовать положения Федерального закона «Об электронной цифровой подписи» в правоприменительной практике. По информации Государственно-правового управления Президента РФ, по состоянию на февраль 2007 г., количество действующих в России сертификатов ключа подписи составляет 200 тыс. ед. Таким образом, процент лиц, использующих ЭЦП в России, не превышает 0,2%. В то же время, по данным Института Фраунхофера по открытым коммуникационным системам, по состоянию на 2005 г. (т.е. через 5 лет после принятия соответствующей Директивы), в Европе использовали усиленные электронные подписи до 70% населения.

В настоящее время в Государственной Думе Федерального Собрания РФ рассматривается законопроект «Об электронной подписи», призванный устранить недостатки действующего закона.

В законопроекте предлагается использовать три вида электронной подписи: простую, усиленную и квалифицированную электронную подпись.

Простая электронная подпись только указывает на лицо, подписавшее сообщение, и не позволяет установить неизменность подписи и подписанной информации после подписания. Случаи равнозначности простой электронной подписи должны предусматриваться соглашениями участников отношений или нормативными правовыми актами.

Усиленная электронная подпись отвечает одновременно трем условиям (однозначная связь с подписывающим лицом; использование средств, которые подписывающее лицо способно сохранять под своим контролем; обеспечение неизменности подписанного электронного документа или возможности обнаружить факт внесения изменений в электронный документ после его подписания). Информация в электронно-цифровой форме, подписанная усиленной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью. Усиленная электронная подпись соответствует электронно-цифровой подписи, предусмотренной действующим законодательством.

Квалифицированной электронной подписью признается усиленная электронная подпись, имеющая квалифицированный сертификат. Предполагается, что степень ее защиты будет выше.

Электронное государство и электронное управление: понятие и сущность

В начале 1990-х годов одной из наиболее популярных концепций формирования информационного общества в основных зарубежных странах (США, Япония, Южная Корея, Европейский союз) стала теория компьютеризации государственных (публичных) функций.

Первоначально она появилась в теориях американских ученых-управленцев Нью-Йоркского университета, где говорилось о неминуемой трансформации государства как управленческого механизма общества в условиях глобализации. Эта теория получила название «Электронное управление» или «Электронное правительство».

Первые попытки реализовать концепцию электронного управления государством были предприняты в 1992 году в США. В настоящее время подобные программы реализуются и на общеевропейском, и национальном уровне. Под электронным управлением подразумевается использование правительственными структурами информационных и коммуникационных технологий для выполнения своих функций.

Первые шаги носили локальный характер, каждый орган и организация запасались вычислительной техникой, создавали свои базы данных. Но очень скоро стало понятно, что этого явно недостаточно.

В России принята **Концепция формирования в Российской Федерации электронного правительства до 2010 года** (распоряжение Правительства РФ от 6 мая 2008 г. № 632-р). В этой Концепции впервые в Росси дается официальное определение данного термина. «**Под электронным правительством в Концепции понимается новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения информационно-коммуникационных технологий качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов».**

Принят целый ряд важных документов:

1) **федеральная целевая программа** «**Электронная Россия (2002–2010 годы)»** (постановление Правительства РФ от 28 января 2002 г. № 65);

2) **федеральная целевая программа «Развитие судебной системы России на 2007–2011 годы»** (постановление Правительства РФ от 21 сентября 2006 года № 583);

3) **концепция региональной информатизации до 2010 г.** (распоряжение Правительства РФ от 17 июля 2006 г.);

4) **концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года** (распоряжение Правительства РФ от 27 сентября 2004 г. № 1244-р);

5) **положение о системе межведомственного электронного документооборота** (постановление Правительства РФ от 22 сентября 2009 г. № 754).

Этими документами определяются основные приоритеты, принципы и направления реализации единой государственной политики в сфере использования информационных технологий в деятельности федеральных органов государственной власти в соответствии с задачами модернизации государственного управления и административной реформы.

Использование современных информационных технологий при осуществлении работы федеральных органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления должно сократить издержки на управление, в частности, за счет высвобождения части технического персонала данных органов. Долю электронного документооборота в данных органах предполагается довести до 65% внутри ведомств и до 40% в межведомственном документообороте. Создание системы электронных закупок продукции для федеральных государственных нужд может помочь сэкономить от 20 до 40 % средств соответствующих бюджетов, выделяемых на подготовку и проведение торгов и организацию закупок.

В результате создания системы электронного управления фактически сформируется единый порядок сбора, обработки, накопления, хранения, поиска и распространения информации, что существенно повысит возможности координации действий силовых структур и будет способствовать росту безопасности и обороноспособности страны.

Важную роль в обеспечении права граждан на доступ к информации о деятельности органов государственной власти играет федеральная целевая программа «Электронная Россия».

Целями формирования в Российской Федерации электронного правительства являются:

– повышение качества и доступности предоставляемых организациям и гражданам государственных услуг, упрощение процедуры и сокращение сроков их оказания, снижение административных издержек со стороны граждан и организаций, связанных с получением государственных услуг, а также внедрение единых стандартов обслуживания граждан;

– повышение открытости информации о деятельности органов государственной власти и расширение возможности доступа к ней и непосредственного участия организаций, граждан и институтов гражданского общества в процедурах формирования и экспертизы решений, принимаемых на всех уровнях государственного управления;

– повышение качества административно-управленческих процессов;

– обеспечение оперативности и полноты контроля за результативностью деятельности органов государственной власти и обеспечение тре-

буемого уровня информационной безопасности электронного правительства при его функционировании.

Для достижения указанных целей необходимо обеспечить:

1) развитие **ведомственных сайтов** в сети Интернет, полноту и своевременность размещения на них соответствующей информации, удобство использования, а также доступ через них к данным, содержащимся в ведомственных информационных системах. Предполагается доступ пользователей к сайтам государственных органов в сети Интернет и интерактивным сервисам. Электронные платежи осуществляются пользователями с различных программно-аппаратных платформ, **включая мобильные электронные устройства**. При этом существенную долю составляют граждане, имеющие различные физические недостатки (плохие слух и зрение, ограничения в подвижности и др.) и для которых электронные формы взаимодействия зачастую оказываются наиболее удобным или даже единственным способом доступа к государственным сервисам.

Необходимо предусмотреть применение механизмов, обеспечивающих достоверность размещаемой информации и исключающих нерегламентированные и неконтролируемые публикации и изменение размещаемых сведений;

2) формирование **инфраструктуры общественного доступа** к размещаемой в сети Интернет информации о деятельности органов государственной власти и предоставляемых государственных услугах организациям и гражданам. Для обеспечения доступа граждан к информации о деятельности государственных органов и предоставляемым ими государственных услугах предусмотрено создание **центров общественного доступа** на базе отделений федеральной почтовой связи, региональных и муниципальных библиотек, пунктов коллективного доступа, организуемых в рамках реализации механизма оказания универсальных услуг связи. Кроме того, центры общественного доступа или **информационные терминалы** могут устанавливаться в органах исполнительной власти, оказывающих государственные услуги организациям и гражданам;

3) внедрение в практику **центров обработки телефонных обращений граждан.** В случае обращения граждан в федеральный орган исполнительной власти запрос в центр телефонного обслуживания осуществляется по единому федеральному номеру, в региональные органы власти – по единому региональному номеру.

На уровне субъекта Российской Федерации предусматривается создание **единого регионального центра телефонного обслуживания**;

4) создание **единой системы информационно-справочной поддержки** граждан по вопросам предоставления государственных услуг и взаимодействия граждан с государственными органами.

В целях обеспечения комплексной справочной поддержки граждан по вопросам взаимодействия с государственными органами предполагается также создание **единой информационно-справочной системы.**

Основой справочной системы **станет единый реестр государственных услуг,** предоставляемых организациям и гражданам. Он включает информацию об условиях их получения, а также общий справочник общественных приемных, центров приема и обслуживания граждан государственными органами с указанием телефонов, времени приема и ответственных должностных лиц и порядка обжалования действий (бездействий) сотрудников государственных органов при выполнении ими обязанностей по предоставлению государственных услуг.

В целях повышения удобства при **очном** взаимодействии организаций и граждан с государственными органами предполагается создание многофункциональных центров предоставления государственных и муниципальных услуг (далее – многофункциональные центры).

Многофункциональные центры создаются для обеспечения предоставления комплекса взаимосвязанных между собой государственных услуг федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления по принципу **«одного окна».** При этом межведомственное взаимодействие, необходимое для оказания государственной услуги (включая различные согласования, получение выписок, справок и др.), происходит без участия заявителя.

Взаимодействие органов государственной власти с получателями государственных и муниципальных услуг производится лично, по телефону, с помощью электронной почты, а также посредством сети Интернет (в том числе и через интернет-портал государственных услуг) и через информационные киоски (инфоматы), расположенные в многофункциональном центре.

Предусматривается обеспечить возможность **регистрации** поступивших обращений заявителей в системе электронного документооборота соответствующего федерального органа исполнительной власти, органа исполнительной власти субъектов Российской Федерации и органа местного самоуправления непосредственно с автоматизированного рабочего места оператора многофункционального центра и автоматического формирования выписки из электронного журнала регистрации и **контроля** за обращениями заявителей в многофункциональный центр, а также передачи в соответствии с правилами документооборота заявления и представленного заявителем пакета документов в органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления, участвующие в предоставлении государственных и муниципальных услуг.

При этом можно выделить следующие **приоритетные группы государственных услуг** для внедрения электронных средств коммуникации в процессы их предоставления:

– государственные услуги в сфере учета объектов недвижимости, а также регистрации прав на них и сделок с ними;

– государственные услуги в сфере обеспечения социальной помощи и социальных выплат;

– государственные услуги по оформлению правового состояния граждан;

– государственные услуги в сфере получения разрешений для предпринимательской деятельности.

Распоряжением Правительства РФ от 25 июня 2009 г. № 872-р утвержден **Перечень государственных услуг и функций, осуществляемых в электронной форме**. В этот перечень входят, например, государственная регистрация юридических лиц, физических лиц в качестве индивидуальных предпринимателей, регистрация автотранспортных средств, содействие занятости безработных граждан, лицензирование отдельных видов деятельности и др. Перечень является ограниченным. Не все государственные органы имеют право на осуществление таких услуг.

Можно выделить ряд **правовых проблем внедрения электронного управления**.

Прежде всего надо отметить **несовершенство нормативно-правовой базы**, обеспечивающей соединение традиционных приемов и технологий административного управления и информационно-коммуникационных технологий, наличие противоречий в нормативных правовых актах, нечеткость и неоднозначность используемых понятий, наличие пробелов в правовом регулировании. Необходимы уточнение и систематизация терминологии, разработка новых нормативных правовых актов, корректировка уже действующих и отмена правовых актов, которые препятствуют применению ИКТ в деятельности государственных органов по предоставлению государственных услуг в электронном виде.

Реализация положений Концепции формирования в Российской Федерации электронного правительства, ФЦП «Электронная Россия», Концепции региональной информатизации приведет к значительному росту электронного документооборота.

В связи с этим особенно актуальным является **правовое регулирование отношений в области электронного документооборота и придание юридической силы этого вида документам.**

Как отмечают специалисты, «в настоящее время электронный документооборот не сопровождается законодательными гарантиями, которые в полной мере обеспечивали бы законность и действительность разнообразных юридических действий, совершаемых в сети Интернет. Не установлены оптимальные юридические критерии, предъявляемые к электронному обмену данными. Законодательство не регламентирует порядок передачи, получения, хранения электронных документов»[41].

[41] *Филатова Л.В.* Актуальные вопросы правового регулирования предоставления государственных услуг в электронной форме // Условия реализации прав граждан и организаций на основе информационных технологий. М., 2010. С. 197.

Участникам электронного документооборота часто предъявляются требования о предоставлении в подтверждение сделки бумажных документов, подписанных собственноручными подписями сторон, или фотокопий, сканированных изображений бумажных документов с подписью. В этих случаях электронные документы не выполняют самостоятельных функций, а только дублируют традиционные документы.

Неразвитость электронного документооборота, недоверие к электронному документу тормозят развитие электронных услуг населению. Например, одна из таких услуг – заполнение гражданами налоговых деклараций в электронной форме. На сайтах территориальных управлений налоговых служб представлены образцы таких деклараций и пошаговая инструкция, помогающая заполнить декларацию, например, на домашнем компьютере. Однако последним пунктом этой инструкции является требование распечатать ее (т.е. перевести в традиционный бумажный вид) и затем принести в налоговое управление по месту жительства.

Таким образом, для повышения эффективности государственного управления уже сейчас требуются разработка и принятие правового обеспечения, включающего основы регулирования электронного документооборота, общего порядка применения электронных документов, а также регламент внедрения в деловой оборот простых и понятных процедур электронного взаимодействия между различными субъектами. Прежде всего это касается отношений между органами государственной власти и гражданами, общественными организациями, юридическими лицами.

Еще одна проблема внедрения ИКТ в деятельность органов власти связана с тем, что система электронного управления включает в себя три звена:

1) систему государственного электронного управления – «электронное правительство»;

2) систему электронного управления субъектов Федерации – «электронный регион»;

3) многочисленные системы электронного муниципального управления – «электронный город» и «электронный район».

В связи с этим большой проблемой является информационное неравенство регионов. В ряде экономически развитых субъектов Федерации уже внедрены и успешно действуют программы «Электронный регион», «Электронный город», «Электронный путеводитель», «Информационный киоск», развернута сеть центров общественного доступа к сети Интернет, развивается система предоставления государственных услуг в электронной форме. В большинстве регионов формирование систем субфедерального электронного управления идет очень медленными темпами.

«Решение проблем информационного неравенства в России (в условиях гигантского разрыва экономического развития между группой богатых регионов и всеми остальными) невозможно принятием специальных программ сугубо на региональном или городском уровне, без федераль-

ного координирования и финансовой поддержки», – справедливо отмечает А.А. Тедеев[42].

Следует сказать, что возможности, предоставляемые современными информационными технологиями, доступны далеко не всем. В 1997 году Программой развития ООН было введено новое понятие «информационная бедность». Это понятие отражает рост социальной дифференциации населения по принципу возможностей доступа к информационно-коммуникационным технологиям. Информационное неравенство как новый вид социального неравенства выступает одной из серьезнейших угроз реализации прав человека в условиях глобализации информационной среды. Основными причинами «цифрового разрыва» в нашей стране можно назвать следующие: неразвитость информационной инфраструктуры, относительно высокая стоимость доступа к ней, неспособность основной массы людей извлекать преимущества из информационной деятельности, отсутствие навыков использования ИКТ в повседневной деятельности у людей старшего поколения, оставшихся «за бортом информационного общества».

В настоящее время необходимым является изменение характера информационного взаимодействия общества и государства, выражающееся в расширении прав граждан путем предоставления доступа к разнообразной информации, увеличении возможностей людей участвовать в процессе принятия решений. При этом важна не информатизация органов власти сама по себе, в центре этих процессов должен быть человек как источник, потребитель информации и субъект гражданского общества, его интересы и потребности.

Тема 10. ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Порядок разработки и внедрения информационных технологий

Согласно ст. 2 Закона об информации **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

В широком понимании термин «информационные технологии» охватывает все области передачи, хранения и восприятия информации. На практике информационные технологии часто отождествляются с компьютерными технологиями, и это неслучайно: появление компьютеров

[42] *Тедеев А.А.* Информационное право: Учебник. М., 2005. С. 108.

вывело информационные технологии на новый уровень. В российском законодательстве в частности, Гражданском и Уголовном кодексах, не говорится о компьютерных технологиях, в нем употребляется термин «программы для ЭВМ».

Порядок разработки и внедрения информационных технологий регулируется нормами гражданского законодательства, в первую очередь ГК РФ (гл. 38 «Выполнение научно-исследовательских, опытно-конструкторских и технологических работ»).

Правовое регулирование должно охватывать:

1)вид продукции;

2)авторство;

3)сферу применения продукта, его назначение;

4)опытное, серийное или массовое изготовление;

5)включение в сферу обмена и использования.

Исходя из этого, сферы правового регламентирования можно разделить на два блока:

1) порядок создания этого информационного продукта;

2) порядок его применения.

Порядок создания информационных технологий предполагает наличие двух субъектов:

1-й субъект – исполнитель, который обязан выполнить работу, передать заказчику ее результаты, согласовать необходимость использования охраняемых результатов интеллектуальной деятельности, принадлежащих третьим лицам, незамедлительно информировать заказчика о невозможности получить ожидаемые результаты или нецелесообразности продолжения работы;

2-й субъект – собственник, должен передать исполнителю необходимую для выполнения работы информацию, принять результаты и оплатить их.

Для права в области создания и использования программ и программного обеспечения важно решение следующих задач:

1)защита прав создателя программы как продукта интеллектуальной деятельности;

2)включение их в рыночные отношения;

3)регулирование сферы непосредственного использования в процессе их функционирования.

В последнее время часто говорится о необходимости создания условий для наращивания потенциала информационных технологий и их использования в интересах общества.

Окинавская хартия глобального информационного общества определяет информационные технологии в качестве одного из наиболее важных факторов, влияющих на формирование общества в XXI веке, образ жизни людей, их образование, работу, взаимодействие правительства и гражданского общества. В хартии также обозначены проблемы борьбы

с компьютерными преступлениями. В Стратегии развития информационного общества Российской Федерации указывается на необходимость стимулирования применения информационных и телекоммуникационных технологий, создания условий для развития соответствующей инфраструктуры (средств вычислительной техники, радиоэлектроники, телекоммуникационного оборудования и программного обеспечения) и др.

В современной России складывается практика применения технологий в основном зарубежного производства, а затем адаптации этих продуктов к российским условиям использования. В связи с этим особенно актуальным представляется налаживание отечественного производства информационных технологий.

Законодатель устанавливает лишь ограничения в порядке применения ИТ:

1)внедрение в апробированное программное изделие компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

2) разработка и распространение программ, нарушающих нормальное функционирование информационных и телекоммуникационных систем;

3)воздействие на парольно-ключевые системы защиты автоматизированных систем, обработки и передачи информации;

4)компрометация ключей и средств криптографической информации;

5)внедрение электронных устройств для перехвата информации.

В целом государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных Законом об информации;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе и сети Интернет и иных подобных информационно-телекоммуникационных сетей.

Государственные органы и органы местного самоуправления в соответствии со своими полномочиями осуществляют следующую деятельность:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Правовая охрана программ для ЭВМ и баз данных

Гражданский кодекс дает следующие определения этих понятий:

1) **базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ст. 1260);**

2) **программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения (ст. 1261).**

Базы данных охраняются как **составное произведение** (так же, как и сборники, антологии, энциклопедии). Автору составного произведения принадлежат авторские права на осуществленные им подбор или расположение материалов.

Согласно статьям 1259, 1261 авторские права на все виды **программ для ЭВМ** (в том числе и на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как и авторские права на **произведения литературы**. Аналогичное правило предусмотрено п. 1 ст. 10 Соглашения по торговым аспектам прав интеллектуальной собственности (Соглашение TRIPS), в соответствии с которым компьютерные программы (в форме исходного текста и объектного кода) подлежат авторско-правовой охране как литературные произведения. В то же время следует учитывать, что по своей природе программы для ЭВМ отличаются значительной спецификой, которая вытекает непосредственно из их предназначения – обеспечивать функционирование компьютерных устройств, осуществление определенных алгоритмов и процессов, достижение результатов, по своей сущности имеющих технический характер. Перед литературными произведениями подобные задачи не ставятся.

На протяжении длительного времени правовая охрана программ ЭВМ осуществлялась Законом РФ «О правовой охране программ для электронных вычислительных машин и баз данных». Одновременно применению подлежали положения Закона РФ «Об авторском праве и смежных правах». **Оба закона перестали действовать** с момента вступления в силу Четвертой части ГК РФ – 1 января 2008 года.

Программы для ЭВМ и базы данных включены в перечень охраняемых результатов интеллектуальной деятельности наряду с произведениями литературы и искусства, фонограммами, изобретениями, полезными

моделями, промышленными образцами, типологиями интегральных микросхем и др. (ст. 1225 ГК РФ). Поэтому автору принадлежат личные неимущественные и исключительные имущественные права.

Однако есть некоторые особенности реализации авторских прав в отношении программ ЭВМ и баз данных, обусловленные их природой. Например, к исключительным имущественным правам относится право на воспроизведение, т.е. изготовление одного и более экземпляров произведения или его части в любой материальной форме. При этом запись произведения на электронном носителе, в том числе и запись в память ЭВМ, также считается воспроизведением, кроме случая, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего своей единственной целью правомерное использование записи.

Автор программы для ЭВМ, базы данных вправе распространять их любым способом, например путем продажи, а также импортировать в целях распространения.

Автору принадлежит право на переработку произведения. Под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе и перевод программы или базы данных с одного языка на другой, за исключением адаптации, т.е. внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Специально регулируются отношения, возникающие при **создании программы** для ЭВМ или базы данных по договору заказа. Согласно ст. 1296 исключительное право на такую программу или базу данных принадлежит заказчику. Возможны другие варианты определения режима исключительного права на программу или базу данных, но эти варианты должны определяться соглашением между заказчиком и исполнителем.

В случае когда по общему правилу исключительное право принадлежит заказчику, исполнитель вправе в течение всего срока действия этого права использовать созданную им программу или базу данных для собственных нужд на условиях безвозмездной простой (неисключительной) лицензии (это значит, что заказчик сможет выдавать такие лицензии и другим лицам).

Если же исключительное право по договору заказа на программу ЭВМ или базу данных принадлежит исполнителю, заказчик имеет право использовать программу или базу данных для собственных нужд на условиях той же безвозмездной простой (неисключительной) лицензии.

Если исполнитель не является автором, а выступает в качестве работодателя для автора программы или базы данных, создание программы для ЭВМ или базы данных будет считаться служебным произведением. В определенных законом случаях (работодатель в установленный срок на-

чинает использование служебного произведения, передает исключительное право на него другому лицу, принимает решение о сохранении данного произведения в тайне) автор имеет право на вознаграждение. Размер, условия и порядок выплаты авторского вознаграждения оговариваются работодателем и автором в договорном порядке.

Гражданским кодексом допускается свободное воспроизведение многих объектов авторского права без согласия автора и без выплаты дополнительного вознаграждения. Однако такое **«свободное воспроизведение в личных целях» баз данных или их существенных частей, а также программ для ЭВМ прямо запрещается действующим законодательством**.

Из этого общего запрета есть исключения: лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных, может производить следующие действия:

1) осуществлять запись программы, базы данных и их сохранение в памяти ЭВМ исключительно в том случае, если это необходимо в целях функционирования программы или базы данных;

2) изготавливать копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или замены правомерно приобретенного экземпляра в случаях, когда данный экземпляр был утерян, уничтожен или стал непригоден для использования;

3) вносить в программу для ЭВМ или базу данных изменения, необходимые для их функционирования на технических средствах пользователя, а также исправлять явные ошибки;

4) изучать, исследовать, испытывать функционирование программы для ЭВМ в целях определения идей и принципов, лежащих в основе любого элемента программы.

Кроме того, законный обладатель программы для ЭВМ вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу). Условием проведения таких действий является их необходимость для достижения способности к взаимодействию программы для ЭВМ, независимо разработанной данным лицом, с другими программами, которые могут взаимодействовать с декомпилируемой программой.

Для осуществления указанных действий необходимо соблюдение как минимум трех важных условий: 1) информация, необходимая для достижения способности к взаимодействию, не была раньше доступна этому лицу из других источников; 2) указанные действия осуществляются в отношении не всей декомпилируемой программы, а только тех ее частей, которые необходимы для достижения способности к взаимодействию; 3) важно, чтобы информация, полученная в результате декомпилирования, могла использоваться только для достижения способности к взаи-

модействию независимо разработанной программы для ЭВМ с другими программами.

Более того, информация, полученная в результате декомпилирования, не может использоваться для разработки программы, существенно схожей с декомпилированной программой или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

Важное значение имеет п. 4 ст. 1280 ГК РФ, в силу которого действия владельца экземпляра программы не должны наносить неоправданный ущерб нормальному использованию программы для ЭВМ или базы данных и необоснованным образом ущемлять законные интересы автора или иного правообладателя. Несмотря на полезность данной нормы, следует признать, что содержание ее категорий «неоправданный ущерб» и «необоснованным образом» нуждаются в дополнительном толковании.

Гражданским кодексом предусматривается возможность предоставления права использовать произведение по лицензионному договору. Такой договор заключает автор или иной правообладатель (лицензиар) и лицо, которое получает право использования произведения в установленных договором пределах (лицензиат).

Форма лицензионного договора о предоставлении права использования программы для ЭВМ или базы данных отличается значительным своеобразием.

Заключение договоров о предоставлении права использования программы для ЭВМ или базы данных допускается путем заключения каждым пользователем с соответствующим правообладателем так называемого договора присоединения (ст. 428 ГК РФ), условия которого изложены на приобретаемом экземпляре такой программы или базы данных либо на упаковке данного экземпляра. Такие договоры получили название «оберточных лицензий». Покупатель предупреждается о том, что, вскрыв упаковку, он вступает в договорные отношения с правообладателем на изложенных на ней условиях. Одним из этих условий является обязательство пользователя не воспроизводить и не распространять программный продукт без согласия правообладателя. Начало использования такой программы или базы данных означает его согласие на заключение договора. Однако проконтролировать соблюдение пользователем данного обязательства очень трудно, вследствие чего проблема договорного регулирования отношений по использованию авторских прав на программы для ЭВМ и базы данных продолжает оставаться чрезвычайно актуальной.

Государственная регистрация программ для ЭВМ

Специфика правового регулирования вопросов охраны программ для ЭВМ и баз данных получила отражение, в частности, в установлении возможности **добровольной,** осуществляемой по усмотрению правооб-

ладателей, государственной **регистрации** программ для ЭВМ и баз данных (ст. 1262 ГК РФ).

Правообладатель в течение срока действия исключительного права на программу для ЭВМ или базу данных может по своему желанию зарегистрировать такую программу или базу данных в федеральном органе исполнительной власти по интеллектуальной собственности. На сегодняшний день регистрация осуществляется в **Российском агентстве по правовой охране программ для ЭВМ, баз данных и топологий интегральных микросхем (РОСАПО),** которое является структурным подразделением Роспатента, регистрацию также можно пройти в Федеральном институте промышленной собственности (ФИПС).

Регистрация программы для ЭВМ или базы данных начинается с подачи заявки. В число обязательных документов входят:

– заявление о государственной регистрации программы для ЭВМ или базы данных, где указываются правообладатель и автор, место жительства или место нахождения каждого из них. При этом автор может отказаться от упоминания его в заявке;

– депонируемые материалы, идентифицирующие программу для ЭВМ или базу данных, включая реферат;

– документ, подтверждающий уплату государственной пошлины в установленном размере. Если заявитель освобожден от уплаты пошлины или имеет право на уменьшение ее размера, отсрочку уплаты, он должен предоставить документ о наличии у него соответствующих оснований. Согласно ст. 333[30] Налогового кодекса РФ госпошлина на регистрацию программ для ЭВМ и баз данных составляет для организаций 2600 руб., для физических лиц 1700 руб.

Любая заявка должна относиться только к одной программе либо к одной базе данных.

На основании поданной заявки РОСАПО проверяет наличие необходимых документов и материалов и соответствие их легальным требованиям. Никаких специальных экспертиз не проводится. После этого программа для ЭВМ или база данных вносится соответственно в Реестр программ для ЭВМ и в Реестр баз данных. Заявителю выдается свидетельство о государственной регистрации, сведения о регистрации публикуются в официальном бюллетене данного органа.

Для того чтобы избежать возможных неточностей или неполноты сведений, допускаются дополнение, уточнение, исправление информации, содержащейся в заявке. Это можно осуществить только до публикации сведений в официальном бюллетене.

Важное требование закона – программы для ЭВМ или базы данных **не должны содержать сведения, составляющие государственную или иную охраняемую законом тайну**.

Несмотря на то что государственная регистрация программ для ЭВМ и баз данных является факультативной, договоры об отчуждении

исключительного права или переходе исключительного права на зарегистрированную программу ЭВМ или базу данных другим лицам должны регистрироваться **в обязательном порядке**. Затем эти (уже измененные сведения) будут внесены в соответствующие реестры.

Несоблюдение требования о государственной регистрации может повлечь для правообладателя негативные последствия, поскольку существует презумпция достоверности сведений, внесенных в Реестр (пока не доказано иное, данные сведения считаются достоверными).

Можно сделать вывод, что регистрация программ для ЭВМ и баз данных, во-первых, не обязательна, а факультативна, во-вторых, носит не разрешительный, а уведомительный характер, в-третьих, предоставляет лицу, осуществившему такую регистрацию, ряд прав, например право на публикацию в официальном бюллетене РОСАПО, служит дополнительным доказательством авторства в случае возникновения конфликтов.

Тема 11. ИНФОРМАЦИОННЫЕ СИСТЕМЫ КАК ОБЪЕКТЫ ПРАВОГО РЕГУЛИРОВАНИЯ

Понятие информационной системы

Под **информационной системой** законодатель понимает «совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» (ст. 2 Закона об информации).

Сложность данного понятия обусловлена соединением разнородных элементов (информация, базы данных, информационные технологии, технические средства), каждый из которых является объектом права. О.А. Городов отметил, что «юридическая конструкция информационной системы напоминает юридическую конструкцию предприятия»[43]. Аналогия в данном случае состоит в том, что и информационная система в целом и отдельные ее составляющие могут выступать самостоятельными объектами права.

В состав основных объектов информационной системы могут быть включены технические и программные средства, комплексы, сети и системы, которые можно объединить в одну структуру для создания, преобразования, хранения, распространения, приема (передачи) и представления информации. К ним, в частности, относятся программные, технические, лингвистические, правовые и организационные средства, используемые

[43] *Городов О.А.* Информационное право. С. 50.

или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

В ранее действовавшем Законе об информации, информатизации и защите информации под информационной системой понималась организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в частности, с использованием средств вычислительной техники и связи, реализующих информационные процессы. Таким образом, ранее действовавший закон включал в понятие следующие информационные системы:

– неавтоматизированные (библиотеки, архивы);

– смешанные, когда одна часть информационных ресурсов обрабатывалась вручную, а другая с использованием вычислительной техники и связи,

– автоматизированные, которых в это время (1995 г.) было еще чрезвычайно мало, но они тоже подходили под это определение.

В ныне действующем Законе об информации определение информационной системы дается через понятие базы данных (а не массива документов), технические средства являются одним из трех обязательных (а не факультативных, как раньше) признаков информационной системы. Поэтому если ранее к информационным системам относились библиотеки, архивы и т.д., теперь они перестали соответствовать легальному определению.

Понятие информационных систем стало включать в себя:

– автоматизированные;

– смешанные, поскольку информационные технологии и технические средства могут быть предназначены для ручной и механизированной обработки информации.

Например, Федеральный закон «О персональных данных» от 27 июля 2006 № 151-ФЗ, принятый в один день с Законом об информации, допускает обработку персональных данных как с использованием средств автоматизации, так и без него.

С 1 января 2008 года вступила в силу Четвертая часть ГК РФ, в которой появилось определение базы данных. В нем указывается, что все материалы, составляющие базу данных, должны быть систематизированы таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ. Следовательно, понятие «базы данных» однозначно было связано законодателем с возможностью их обработки с помощью ЭВМ.

Тем самым законодатель вывел из-под действия Закона об информации информационные системы, в которых обработка информации ведется без использования средств автоматизации или не только с их использованием. На практике же такие системы продолжают существовать. По сути, в результате изменения Гражданского кодекса произошло отождествление понятий информационной системы и автоматизированной информационной системы.

В то же время считается, что автоматизированные информационные системы, например ГАС «Выборы», ГАС «Правосудие», составляют отдельную категорию информационных систем.

Приходится констатировать, что в данном случае мы имеем дело с коллизией в праве, сложившейся в результате столкновения двух расходящихся по содержанию норм различных действующих нормативных актов, в которых рассматривается один и тот же вопрос. Указанная коллизия порождает неоднозначность в определении объема термина «информационные системы».

Эта правовая коллизия нашла свое отражение в действующем законодательстве. Например, в ст. 56 Градостроительного кодекса РФ от 29 декабря 2004 года № 190-ФЗ информационная система обеспечения градостроительной деятельности определяется как «систематизированный *свод документированных сведений* о развитии территорий, об их застройке, о земельных участках, об объектах капитального строительства и иных сведений». Это определение дано в соответствии с устаревшей формулировкой утратившего действие Закона об информатизации. На практике используются и неавтоматизированные информационные системы, включающие в себя материалы в текстовой форме, в виде карт и схем, и автоматизированные информационные системы (которые вышеприведенному определению не соответствуют). Подобная путаница в определении информационной системы, обеспечивающей какой-либо род деятельности, характерна для многих нормативных актов.

Виды информационных систем

Согласно ст. 13 Федерального закона «Об информации» различаются:

1) **государственные информационные системы** – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов и законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) **муниципальные информационные системы**, созданные на основе решения органа местного самоуправления;

3) **иные информационные системы**.

Закон не содержит каких-либо норм, которые определяли бы отличия в правовом режиме федеральных, региональных и муниципальных систем.

Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между ними. Данный вид информационных систем создается и эксплуатируется на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами и органами местного самоуправления.

Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе и программно-технические средства и средства защиты информации, должны соответствовать требованиям Федерального закона от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании».

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Для **негосударственных информационных систем** установлено, что оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

В законе об информатизации признавалось право собственности на информационные системы. Это положение подвергалось критике[44], отмечалось, что информационные технологии, которые являются неотъемлемой частью информационных систем, имеют информационно-правовую, а не вещно-правовую природу, и в ряде случаев могут являться объектами интеллектуальных прав. В новом Законе об информации говорится о **собственности на технические средства** и **правомерности владения базами данных**. Поэтому нужно согласиться с А.В. Туликовым, который называет информационные системы «квазиправовым объектом информационных правоотношений, поскольку … какие-либо определенные права на информационные системы законодательство не содержит»[45].

Кроме того, информационные системы бывают **фактографическими** и документальными. К первым относятся информационные системы, предназначенные для поиска однозначного ответа на запрос и однознач-

---

44 См., например: *Городов О.А.* Комментарий к Федеральному закону «Об информации, информатизации и защите информации». СПб., 2003. С. 151.

45 *Туликов А.В.* Особенности правового обеспечения «жизненного цикла» государственных и муниципальных информационных систем // Конфликты в информационной сфере: Материалы теоретического семинара Сектора информационного права ИГП РАН. М., 2009. С. 96.

ного решения поставленных задач. Фактографические информационные системы делят, в свою очередь, на информационно-справочные системы, информационно-поисковые системы и системы оперативной обработки данных. Системы оперативной обработки данных решают такие задачи, как управление производством, бухгалтерский учет и т.п.

Документальные информационные системы предназначены для решения задач, не предусматривающих однозначного ответа на вопрос. Некоторые системы представляют собой смешанный тип фактографической и документальной информационной системы.

Распространено мнение, что особенности правового режима тех или иных информационных систем сводятся к особенностям правового режима содержащейся в таких системах информации. Как пишет Г.Л. Акопов, «основное назначение информационной системы – реализовать информационные процессы в той области деятельности, где данная система функционирует»[46].

Законодатель также, по-видимому, считает, что правовой режим государственных и муниципальных информационных систем различной отраслевой и ведомственной принадлежности очень сильно отличается и поэтому требует особенного подхода и принятия отдельных нормативных актов, в которых устанавливается структура, состав информационного, программного, технического и правового обеспечения информационной системы, обусловленные целями ее функционирования.

В связи с этим создание и использование **ведомственных информационных систем** предусматриваются большим количеством нормативных актов. Перечислим некоторые из них, где эти вопросы наиболее разработаны: Налоговый и Таможенный кодексы, федеральные законы «О персональных данных», «О Государственной автоматизированной системе “Выборы”», «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» и постановления Правительства РФ «О государственной информационной системе миграционного учета», «О мерах по созданию автоматизированной системы обязательного страхования гражданской ответственности владельцев транспортных средств», приказ федеральной службы по надзору в сфере образования и науки об использовании автоматизированной информационной системы «Экзамен» во время проведения ЕГЭ в 2005 году, распоряжение Правительства РФ «О Концепции создания государственной автоматизированной системы информационного обеспечения управления приоритетными национальными проектами» и др.

О масштабах применения информационных систем в государственном и муниципальном управлении позволяет судить перечень информационных систем и ресурсов Москвы, составленный А.П. Жихаревым в 2006 году: данный перечень включает 236 наименований[47].

---

46 *Акопов Г.Л.* Информационное право: Учеб.пособие. Ростов н/Д, 2008. С. 73.

47 См.: *Жихарев А.П.* Автоматизированные информационные системы и ресурсы г. Москвы. М., 2006. С. 22.

В ряде правовых актов получили нормативное закрепление принципы использования, эксплуатации и развития информационных систем, правовой статус участников и вопросы ответственности, юридическая сила документов, подготовленных с использованием этих систем. Рассмотрим некоторые из них.

В Федеральном законе от 10 января 2003 г. № 20-ФЗ «О государственной автоматизированной системе "Выборы"» указаны принципы использования, эксплуатации и развития соответствующей системы:

1) соблюдение конституционных прав граждан при автоматизированной обработке информации о них;

2) обеспечение гласности деятельности избирательных комиссий, комиссий референдума при использовании ГАС «Выборы»;

3) оперативное информирование избирателей, участников референдума о ходе и результатах выборов и референдума;

4) недопустимость вмешательства в информационные процессы в ГАС «Выборы» органов государственной власти, государственных органов, органов местного самоуправления, их должностных лиц, других лиц и организаций, которые в соответствии с федеральными законами не могут вмешиваться в данные процессы;

5) обязательное применение ГАС «Выборы» при подготовке и проведении выборов и референдума, недопустимость использования для этих целей вместо ГАС «Выборы» других автоматизированных систем и информационных технологий;

6) обеспечение безопасности информации в ГАС «Выборы» в сочетании с открытостью системы и доступностью информации, содержащейся в информационных ресурсах ГАС «Выборы»;

7) обеспечение достоверности информации, получаемой с использованием ГАС «Выборы»;

8) применение лицензионных программных средств общего назначения, сертифицированных специализированных программно-технических средств и средств связи ГАС «Выборы».

Государственным заказчиком ГАС «Выборы» является Центральная избирательная комиссия РФ.

Законом определяются условия придания юридической силы документам, подготовленным с использованием ГАС «Выборы». Документ на бумажном носителе, подготовленный с использованием ГАС «Выборы», приобретает юридическую силу после его подписания соответствующими должностными лицами. Электронный документ, подготовленный с ее использованием, приобретает юридическую силу после его подписания электронными цифровыми подписями соответствующих должностных лиц. Протокол, сводная таблица об итогах голосования, иные сводные документы, подготовленные в электронном виде с использованием ГАС «Выборы», приобретают юридическую силу после подписания электронными цифровыми подписями соответствующих должностных лиц после

обязательной проверки в установленном порядке с помощью открытых ключей электронных цифровых подписей подлинности всех исходных электронных документов, на основе которых готовится сводный электронный документ.

Согласно ст. 3 Федерального закона «О персональных данных» от 27 июля 2006 года «информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств». Большинство автоматизированных информационных систем попадают именно под эту категорию, их основное назначение – систематизация персонального учета населения.

Особенности обработки персональных данных в государственных или муниципальных системах персональных данных регламентируются ст. 13 Закона о персональных данных. В ней, в частности, предусматривается, что государственные органы и муниципальные органы создают в пределах своих полномочий государственные или муниципальные информационные системы персональных данных, также может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Важно отметить положение Закона о персональных данных, согласно которому права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

Не допускается обработка персональных данных, избыточных по отношении к целям, заявленным при их сборе, а также объединение баз данных, если они создавались в целях, не совместимых друг с другом.

В отношении персональных данных установлен режим конфиденциальности со стороны оператора и третьих лиц, получивших доступ к таким данным. Исключение составляет доступ к обезличенным и общедоступным персональным данным.

В положении «О Государственной информационной системе миграционного учета», разработанном в соответствии с Федеральным законом «О миграционном учете иностранных граждан и лиц без гражданства в

Российской Федерации», четко устанавливаются участники информационного обмена – оператор, поставщики и пользователи.

Оператором информационной системы является Федеральная миграционная служба.

Поставщиками сведений в информационную систему являются МВД, МИД, ФСБ, ФНС, а также иные органы государственной власти и органы местного самоуправления, если на них возложены обязанности по учету информации об иностранных гражданах и ее представлению в соответствующие миграционные органы.

Пользователями информационной системы являются заинтересованные федеральные органы государственной власти, их структурные подразделения, территориальные органы федеральных органов исполнительной власти, органы государственной власти субъектов Российской Федерации. Пользователями информационной системы могут являться также иные организации, которым федеральным законом предоставлено право доступа к сведениям.

При этом установлено, что обладателем сведений, размещенных в информационной системе, является Федеральная миграционная служба, а также поставщик сведений.

В качестве специализированной автоматизированной информационной подсистемы создается Центральный банк данных по учету иностранных граждан, временно пребывающих, временно или постоянно проживающих в России, в том числе и участников государственной программы по оказанию содействия добровольному переселению в Российской Федерации соотечественников, проживающих за рубежом.

Одними из основных принципов, на основе которых формируется и функционирует информационная система, являются:

а) использование информационных систем, созданных в установленном порядке для автоматизации учетной деятельности;

б) применение современных информационных технологий для обеспечения автоматизированной обработки сведений и их передачи по цифровым линиям связи;

в) однократный ввод и многократное использование сведений;

г) персональная ответственность должностных лиц участников информационного обмена за полноту и достоверность сведений, их своевременную передачу и изменение, а также хранение и уничтожение в установленном порядке;

д) защита сведений путем использования разрешенных к применению в Российской Федерации средств криптографической и технической защиты, включая средства защиты от несанкционированного доступа;

е) применение средств электронной цифровой подписи. При их использовании электронный документ, содержащий сведения, имеет юридическое значение, они также обеспечивают невозможность отрицания факта направления и (или) получения сведений.

Данным документом установлен также порядок внесения изменений в базы данных: оператор информационной системы в случае установления недостоверности сведений обеспечивает их изменение, при необходимости информирует об этом поставщиков сведений и пользователей информационной системы.

Участники информационного обмена (их должностные лица) несут ответственность за ущерб, возникший по их вине в результате:

а) неправильного или ненадлежащего составления электронного документа;

б) разглашения и (или) передачи третьим лицам сведений, паролей доступа к сведениям (включая компрометацию криптографических ключей и ключей электронной цифровой подписи);

в) утраты, несанкционированного уничтожения, изменения, исправления сведений, утери носителей сведений;

г) совершения иных действий (бездействия), повлекших причинение ущерба.

В целом можно сделать вывод, что в каждом из перечисленных правовых актов по-своему определяются принципы использования информационных систем, правовой статус ее участников и вопросы их ответственности, юридическая сила документов, подготовленных с использованием этих систем. Не хватает унификации правового регулирования отношений по использованию информационных систем. Нормативное правовое обеспечение характеризуется фрагментарностью, противоречивостью, акцент делается на локальных, процедурных вопросах, решение которых полностью зависит от органов и организаций, ответственных за их эксплуатацию.

Правовые проблемы, связанные с созданием и эксплуатацией информационных систем

Наиболее острой сейчас является проблема обеспечения безопасности информации, содержащейся в базах данных. Привычными стали масштабные хищения персональных данных, в результате которых на черном рынке продаются базы данных налогоплательщиков, ВИЧ-инфицированных, лиц, имеющих судимости, абонентов сотовых сетей. Целый ряд сайтов предлагает подробную информацию по жителям Москвы и регионов: адреса, телефоны, автотранспорт, налоги, криминал. Тем самым нарушается право на частную жизнь, личную тайну, человек становится уязвимой мишенью для преступных группировок разного толка. Повышенная общественная опасность нарушения конфиденциальности персональных данных, которые хранятся и обрабатываются в соответствующих информационных системах, должна учитываться законодателем на всех этапах их создания и эксплуатации.

В последнее время особенностям функционирования информационных систем персональных данных было посвящено несколько норма-

тивных документов: Постановления Правительства РФ «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17 ноября 2008 года № 781, «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 6 июля 2008 года, «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 года № 687.

В то же время недостатком указанных положений является то, что они направлены на защиту информационных систем от лиц, внешних по отношению к системе, и слабо затрагивают ее непосредственных пользователей – сотрудников, имеющих доступ к персональным данным в силу служебных обязанностей и профессиональной деятельности.

Другим недостатком информационных систем персональных данных, как отмечают специалисты, является отсутствие общественно-правовой экспертизы на предмет того, насколько внедрение такой АИС может угрожать правам и законным интересам граждан. Р.В. Амелин приводит показательный пример: когда создается система для обработки данных в какой-то конкретной области (например, учет призывников, ВИЧ-инфицированных и др.), то основной базовой возможностью такой системы оказывается запрос на выборку данных, удовлетворяющих определенному критерию. Впоследствии такая выборка может являться объектом незаконного распространения. Когда несколько таких систем интегрируются в одну, базовой возможностью новой системы является получение исчерпывающей информации о конкретном лице. «Между тем эти возможности вообще не должны присутствовать в системе… Назначение системы – отвечать на конкретные запросы», – заключает исследователь[48]. Дело в том, что программисты, разрабатывающие такую систему, кладут в ее основу традиционную базу данных и включают стандартную функцию выборки всей хранящейся в системе информации. При этом они не обладают правовыми знаниями и не подозревают, что создают возможность для грубого нарушения прав большого количества людей.

Выходом из данной ситуации (и других подобных) могут стать проведение общественно-правовой экспертизы, которая обеспечит контроль за соблюдением прав граждан при автоматической обработке.

На разных этапах жизненного цикла информационной системы могут возникать разнородные правовые проблемы. Следует отметить, что понятие «жизненный цикл информационной системы» является техническим, а не правовым, определяющим период, начинающийся с момента

[48] *Амелин Р.В.* О правовых принципах разработки государственных АИС, обрабатывающих персональные данные // Информационное право. 2009. № 2. С. 33.

принятия решения о необходимости создания информационной системы и заканчивающийся в момент ее полного изъятия из эксплуатации.

А.В. Туликов выделяет следующие этапы: разработку концепции системы, проектирование и разработку системы, эксплуатацию, сопровождение и списание системы. На каждом из этих этапов складывается комплекс взаимоотношений, урегулированный различными отраслями права (публичные – режим обработки, безопасность информации, частные – договорные отношения, интеллектуальные права).

Анализ статей 13 и 14 Закона об информации позволяет сделать вывод, что законодатель выделяет только два этапа жизненного цикла информационной системы – создание и эксплуатацию.

На этапе создания главными являются правоотношения между заказчиком и разработчиком АИС – в соответствии с требованиями данного закона заказчик объявляет конкурс на разработку АИС, отражая требования к ней в конкурсной документации. Именно здесь могут появиться ошибки анализа и проектирования. Зачастую они связаны с тем, что заказчик, который определяет цель и задачи создания информационной системы, не всегда четко представляет, что он хочет получить в результате деятельности этой системы, и потому составляет очень приблизительное техническое задание. Разработчик, не являющийся специалистом в той области, где будет функционировать система, может способствовать реализации ею заведомо неправильных действий.

Наиболее ярким примером служит ситуация с ЕГАИС (единая государственная автоматизированная информационная система), предназначенной для автоматизации государственного контроля за объемом производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции.

Целью использования ЕГАИС называлось обеспечение полноты и достоверности учета производства и оборота соответствующей продукции с возможностью детализации до производителя, вида, наименования, крепости, объема и правильности начисления акциза.

Ее внедрение (планировалось в 2005 году) сопровождалось техническими неполадками, значительным финансовым ущербом для участников рынка. На начальном этапе заказчик (Федеральная налоговая служба) не сумел разработать полноценное техническое задание, не были подготовлены нормативно-правовые акты, контролирующие разработку и внедрение ЕГАИС, программно-техническое обеспечение не соответствовало заявленным требованиям. В результате введения в действие данной системы с прилавков магазинов почти полностью исчезла алкогольная продукция, большие убытки терпели производители парфюмерии (поскольку в своем производстве они применяют спиртосодержащие элементы, то их тоже пытались учесть в ЕГАИС). Работа системы была остановлена, введен альтернативный режим передачи данных через файлы. В результате неоднократных доработок ЕГАИС работала стабильно,

но из-за отсутствия некоторых функций и необходимых отчетов система не позволяла получать информацию об объемах поставленной и отпущенной в розничную сеть продукции и осуществлять мониторинг рынка. В ноябре 2007 года было начато внедрение новой версии ЕГАИС, созданной другими разработчиками. И только 1 июля 2009 года на официальном сайте ФНС появилось сообщение о завершении внедрения ЕГАИС учета объема производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции.

Причиной возникновения подобной ситуации стало отсутствие нормативной базы, регламентирующей процесс создания государственных и муниципальных АИС.

На каждом этапе формирования такой системы – при формировании требований к ней, разработке ее концепции и, наконец, техническом создании – необходимо осуществлять контроль за соответствием автоматизированной системы заявленным целям.

Не решенным остается вопрос об ответственности за создание некорректно функционирующей системы. В случаях умышленного причинения вреда, грубых ошибок, допущенных разработчиками, ответственность несут производители программ. Если ошибки допущены при анализе и проектировании или на стадии согласования проекта между заказчиком и разработчиком, субъект ответственности действующим законодательством не определен.

Отсутствуют законодательно закрепленные обязанности лиц, обеспечивающих эффективную эксплуатацию системы. В некоторых актах закреплены требования к обеспечению безопасности информации, содержащейся в базах данных, и обязанности по изъятию недостоверной информации. Но не хватает норм, регулирующих изменения в информационной системе, исправление возможных ошибок программирования, необходимую доработку, модернизацию.

Такой этап, как списание информационной системы по каким-либо основаниям (параметрам) в действующем законодательстве отсутствует.

Внедрение информационных систем способствует повышению эффективности исполнения функций органов власти за счет получения более оперативной, полной и точной информации. Использование информационных технологий и внедрение автоматизированных систем позволяет существенно повысить прозрачность взаимодействия бизнес-структур и государственных органов, способствует формированию активного гражданского общества. Но для решения этих задач необходимо обеспечить полноценное правовое регулирование в данной области. Ближайшими задачами являются уточнение и систематизация терминологии, разработка новых нормативных правовых актов и унификация и корректировка уже действующих.

Тема 12. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ

Правовые подходы к понятию «Интернет»

Современное информационное пространство основано на широком применении компьютерной техники, информационных технологий и Интернета. К середине 2008 года число пользователей Интернета составило около 1,5 млрд человек, или примерно четверть населения планеты. Развивается российский сегмент Интернета: по итогам 2008 года число интернет-пользователей в России составило более 40 млн человек, что на 10–15% больше, чем в предыдущем году; среднее время пребывания в Интернете в расчете на каждого пользователя – 1 час в сутки. Количество почтовых ящиков в бесплатных почтовых службах приближается к 120 млн. Активно используются поисковые системы: за год пользователи получили 17,6 млрд ответов, или 1300 поисковых ответов в секунду[49]. Человечество впервые столкнулось с ситуацией, когда циркуляция информации приобрела столь масштабный характер и осуществляется в электронно-цифровой форме. При этом, как отмечают практически все исследователи, существующее законодательство плохо приспособлено к правовому регулированию данных отношений.

Легального определения «Интернет» в российском законодательстве нет. Не сложилось пока и единого понимания, что это такое.

Обычно при характеристике Интернета указывают, что эта всемирная информационная паутина сформирована на базе бесчисленного множества компьютеров разных типов и назначения, программных средств, информационных ресурсов, средств связи и телекоммуникаций, по которым передается и получается информация. Совокупность информационных массивов как бы пронизывается многочисленными гипертекстовыми связями. Каждая такая связь соединяет между собой любые точки текстовых или графических документов. Все это создает возможность доступа отдельного пользователя к практически неограниченным информационным массивам. Тем самым создается единое электронное информационное пространство.

Что такое Интернет с юридической точки зрения? Можно выделить различные подходы к его пониманию. Например, в проекте модельного закона «Об Интернете», рассмотренном Комиссией Совета Федерации по информационной политике, Интернет понимается как «глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посред-

[49] Пленарный доклад на объединенной конференции Российского интернет-форума и Конференции Интернет и бизнес (РИФ+КИБ). 29.04.2009. URL: http://ok2009/ru (дата последнего обращения: 25 апреля 2010).

ством глобального адресного пространства, основанного на использовании интернет-протокола (Internet protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP)»[50]. Таким образом, в данном документе превалируют **технические и технологические характеристики** Интернета и мало учитываются его социальные составляющие. Интернет понимается только как высокотехнологичный инструмент.

Другую позицию демонстрируют теоретики информационного права. В.А. Копылов дает следующее определение: «Интернет – это распределенная всемирная база данных, включающая в себя множество различных информационных массивов, информационных ресурсов, баз данных, состоящих из документов, данных текстов, объединенных между собой трансграничной телекоммуникационной информационной паутиной или сетью»[51]. Тем самым, он акцентирует внимание на **информационных ресурсах**, базах данных и документах.

В.Б. Наумов определяет Интернет как «… глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого, общеобязательного свода правил (законов) пользования сетью Интернет не установлено. Существуют, однако, общепризнанные нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов, и только они»[52]. Этот исследователь выделяет социальный аспект: децентрализованное сообщество, признающее **общепризнанные правила и нормы** работы в сети.

А.К. Жарова указывает на то, что «Интернет – пространственно-распределенная глобальная сеть компьютерных технологий и инфраструктур пользователей, позволяющих осуществлять операции по обращению информации и предоставлять (получать) информационные услуги в целях удовлетворения потребностей физических, юридических лиц, органов власти и других субъектов в информации, обеспечивать их контакты в режиме реального времени, функционирующая на основе технических стандартов, а также норм национального и международного права»[53]. Можно сказать, что в своем определении исследовательница стремится соединить **техническое, человеческое и правовое** измерение.

---

[50] О разработке этого документа договорились власти государств-участников СНГ на Межпарламентской ассамблее, если он будет одобрен, то станет образцом для законодательства об Интернете России и целого ряда стран ближнего зарубежья. http//:www.rmob.ru/?news_id=2610.

[51] *Копылов В.А.* Информационное право. С. 232.

[52] *Наумов В.Б.* Право и Интернет: Очерки теории и практики. С. 31.

[53] *Жарова А.К.* Информация. Правовое регулирование обращения информации в Интернет. М., 2006. С. 16.

И.Л. Бачило представляет такое определение: «Интернет – это сфера непрерывного информационно-коммуникационного процесса, обеспечивающего обращение информации (сведений) в цифровой форме в неограниченном пространстве через пункты связи, и реализации двух или многостороннего обмена информационным ресурсом пользователей в целях получения, накопления знаний или осуществления электронных операций субъектов в разных областях реализации их интересов, прав и обязанностей»[54]. Тем самым, исследовательница уходит от технических моментов и определяет Интернет как **новую сферу** человеческой деятельности.

На сегодняшний день к основным информационным ресурсам (службам) Интернета можно отнести собственно World Wide Web (WWW или Web), электронную почту (E-mail), службы FTP-хранения файлов и их предоставления пользователям; телеконференции и службы интерактивного общения пользователей; дискуссионные группы Usenet, Fidonet. В Интернете сосредоточены деловая, образовательная, развлекательная информация, электронные газеты и журналы, базы данных практически по всем областям жизнедеятельности общества, доступ к разнообразным информационным ресурсам библиотек, государственных учреждений.

Интернет не только способствует развитию электронной коммерции и развитию человеческого потенциала, но и воспроизводит всевозможные виды девиантного и делинквентного поведения. Предоставляя огромные возможности доступа к информации, Интернет выступает не просто идеальным инструментом коммуникации, но и катализатором негативных социальных явлений, общественная опасность которых увеличивается. По оценкам экспертов британской компании «1871LTD», исследовавших уровень преступности в глобальной паутине, только в 2006 году в Интернете было совершено около 3 млн правонарушений, включая 207 000 случаев финансовых махинаций, 144 500 случаев взломов компьютеров и 850 000 преступлений в сексуальной сфере, включая скачивание порнографии.

При обсуждении вопросов правового регулирования возникает вопрос: как распространить действие уже существующих законов на новые социальные отношения, чтобы они действовали в интересах общества? При этом необходимо соблюдение баланса между свободой развития информационных отношений и необходимостью их регламентации в интересах общества.

Субъекты правоотношений в сети Интернет

Для правового регулирования необходимо уяснить круг основных субъектов – участников правоотношений и определить их статус. Только

---

54 *Бачило И.Л.* Информационное право. М., 2009. С. 254.

человек может вступать в правоотношения, принимать решения, нести ответственность. Функционирование Интернета обеспечивают провайдеры, владельцы серверов, а также пользователи услугами и потребители информации. Все они – реальные лица (физические или юридические), которые имеют определенное расположение в сети, юридический адрес, инфраструктуру и банковские счета.

В проекте модельного закона «Об Интернете» выделяются следующие субъекты правоотношений:

1) **государство в лице его органов власти**, осуществляющее регулирование Интернета;

2) **пользователи** Интернета – юридические и физические лица, которым предоставляются услуги Интернета;

3) **операторы** услуг Интернета;

4) **саморегулируемые организации**, участвующие в процессе регулирования Интернета.

А.К. Жарова называет следующих субъектов – участников правоотношений в сети:

1. Государство.

2. Юридические лица.

2.1. Операторы (провайдеры) – организации, специализирующиеся на предоставлении доступа к информации посредством каналов связи и удаленного доступа. В свою очередь, по предоставляемым услугам и выполняемым функциям провайдеры могут классифицироваться как:

– *провайдер содержания (контент);*

– *хост-провайдеры;*

– *провайдер доступа.*

Отдельный сервис-провайдер, исполняющий несколько функций, может относиться к нескольким типам провайдеров.

Провайдеры содержания (контент-провайдеры) предоставляют собственное содержание и обеспечивают его доступность посредством хост-провайдера. Пример провайдера содержания – информационное агентство, которое не выпускает собственных газет и журналов, имеет сеть корреспондентов по всей стране, которые передают информацию. Агентство торгует информацией, поскольку другие газеты и журналы не имеют возможности содержать корреспондентскую сеть.

Хост-провайдеры сдают в аренду часть своего серверного пространства, оказывают услуги по размещению чужого сайта на своем сервере, поддерживают работоспособность пользовательского сайта.

Провайдеры доступа обеспечивают доступ к сети, например доступ к Интернету. Их услуга заключается главным образом в перемещении данных без их постоянного хранения.

2.2. Организации, пользующиеся услугами любых категорий провайдеров, – пользователи услуг, которые предоставляют через провайдера доступ к сети Интернет своим пользователям (например, сотрудникам).

3. Физические лица.
3.1. Автор.
3.2. Собственник информации или информационного ресурса.
3.3. Владелец информации или информационного ресурса.
3.4. Поставщики содержания.
3.5. Конечные пользователи.

Ответственность за содержание размещаемой в сети информации должен нести автор сообщения, поэтому в законодательствах ряда стран автор обязан отождествлять себя. Пользователи идентифицируют себя, осуществляя процедуру регистрации, указывая адрес электронной почты. Но эта практика распространена не везде.

Одним из наиболее сложных правовых вопросов является проблема ответственности информационных провайдеров, которая в законодательстве ряда стран мира решается по-разному. Дело в том, что в Интернете, в отличие от материального мира, особую роль играют организации и лица, обеспечивающие технологическую поддержку информационным отношениям – интернет-компании, операторы связи, владельцы ресурсов и систем, которые дают возможность желающим пользоваться их услугами и средствами, за счет чего последние участвуют в отношениях, создают и распространяют информацию. Эти лица (провайдеры, информационные посредники, операторы информационных систем) могут оказывать влияние на регулирование отношений, используя свои технические возможности и отключая или блокируя пользователей и их ресурсы. Как совершенно верно замечает В.Н. Наумов, «пределы реализации прав или обязанностей информационных провайдеров по контролю за отношениями упираются, с одной стороны, в запрет цензуры, с другой – на ситуацию оказывает влияние тот факт, что никто, кроме них, прекратить правонарушение, совершаемое их пользователями (или клиентами), технически не может. Так же важно и то, что именно информационные провайдеры при расследовании правонарушений имеют возможность предоставлять техническую информацию об обстоятельствах, имевших место в сети Интернет»[55].

Государство в соответствии с принципами и нормами международного права регулирует общественные отношения, возникающие с развитием информационных технологий, формирует нормативную базу, способствующую включению России в мировое информационное пространство, осуществляет контроль за содержанием распространяемой в сети информации, обеспечивает эффективную защиту граждан и общества от вредной и незаконной информации.

---

55 *Наумов В.Б.* О современных процессах в сфере правовой защиты свободы слова в сети Интернет. URL:2007, Виктор Наумов, nau@mail.iias.spb.su

Правовое регулирование проблем, связанных с развитием Интернета

Процесс развития Интернета опережает процесс его формально-правового регламентирования. В силу экстерриториальности данной информационной сети основные интернет-проблемы обеспечения прав и свобод человека в информационной среде одинаково актуальны для всех развитых стран. Обозначим некоторые из них.

1. **Проблема защищенности личных данных физических лиц**. В современном (информационном) обществе человек постоянно оставляет электронные следы своего пребывания: его личные данные используются большим количеством субъектов экономической и социальной деятельности: работодателями, страховыми компаниями, пенсионными фондами, финансово-кредитными организациями и т.д. Это делает возможным осуществление тотальной слежки за гражданами со стороны государственных структур или неправомерное использование личных данных криминальными сообществами.

Государствами-членами Совета Европы 28 января 1981 года подписана Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера, введен запрет на обработку данных о расе, политических взглядах, здоровье и религии. Россия присоединилась к Европейской конвенции в ноябре 2001 года, а в 2006 году был принят Федеральный закон «О персональных данных», который вступил в силу 25 января 2007 года Положения этого нормативного акта затрагивают всех граждан России (как субъектов персональных данных) и все предприятия, организации, учреждения, которые как операторы ведут обработку персональных данных о своих сотрудниках и клиентах.

2. **Проблема защиты средств индивидуализации** (товарный знак, фирменное наименование, знак обслуживания) от незаконного использования в глобальной компьютерной сети Интернет. В частности, правового разрешения требует вопрос об отнесении к средствам индивидуализации **доменного имени**.

3. Юридические проблемы, связанные с **неопределенностью правового статуса электронных сетевых СМИ**, распространяемых (размещаемых на сайтах) в глобальной компьютерной сети Интернет. В связи с этим невозможна однозначная юридическая квалификация правонарушений, связанных со злоупотреблением свободой слова.

4. Реализация информационно-правового режима **авторских отношений**. В частности, правовые проблемы защиты исключительных прав на программы для ЭВМ в сети Интернет, прав авторов и прав владельцев сайта. На практике реализация авторских и смежных прав осуществляется недостаточно. Жертвам данного вида преступления сложно доказать факт нарушения их прав, когда незаконное размещение объектов авторского права имеет место в компьютерных системах или сетях

общего доступа. Увеличение количества мультимедийных произведений в Интернете, простота копирования, массовая распространенность такого правонарушения, как пиратство заставляют по-новому осмыслить понятия «автор», «соавтор», «объем исключительных прав» в электронной среде. По вопросу защиты интеллектуальной собственности следует найти справедливое решение, удовлетворяющее законные запросы авторов, права которых должны быть обеспечены в сетевой среде, экономические интересы корпораций и прав на поиск, получение и распространение информации (информационных продуктов) пользователей. В последнее время говорится о возможности сочетания правовых и программных средств для защиты исключительных прав авторов, например наделении электронных документов возможностью саморазрушения в случае их незаконного использования.

5. Проблема **подсудности споров**, возникающих в процессе осуществления электронной деятельности. В силу экстерриториальности Интернета правонарушители и жертвы могут быть гражданами разных государств, правонарушения совершаться на территории разных государств и не понятно, что считать «местом правонарушения» в классическом смысле слова: место загрузки информации, место расположения сервера, место ознакомления с информацией? В связи с этим возникает конкуренция юрисдикции, другими словами, не понятно, в суд какой страны следует обращаться с иском. Согласно Рекомендациям представителя ОБСЕ по вопросам свободы СМИ, «весь контент в Интернете должен регулироваться законами страны его происхождения (“правило загрузки”). Любое законодательство, возлагающее ответственность за контент – куда бы он ни перекачивался – на автора или издателя, является чрезмерным ограничением свободы выражения мнений»[56]. Нужно также иметь в виду, что чаще всего за уголовные преступления, совершенные в виртуальной среде или с помощью аппаратно-технических средств, применяется норма национального законодательства (Уголовный кодекс РФ), а по гражданским делам – нормы международного частного права. В случае нарушения права интеллектуальной собственности международная юридическая практика исходит из того, что в зависимости от доли ущерба применяются закон и суд страны наиболее пострадавшей стороны (т.е. право той страны, которой нанесен больший ущерб). В расчет должны приниматься законы и размер ущерба других стран[57]. Говорится также о возможности заключения международного соглашения о применении правовых норм той страны, где расположен сервер.

---

56 Рекомендации представителя ОБСЕ по вопросам свободы СМИ: Справ. по свободе массовой информации в Интернете. Вена, 2004. С. 15.

57 См.: *Рассолов И.М.* Право и киберпространство: решения и рекомендации // Конфликты в информационной сфере: Материалы теоретического семинара Сектора информационного права Института государства и права РАН 2008 г. М., 2009. С. 35.

Реальностью становится выдача преступников иностранному государству. Россией ратифицирован ряд международных документов: Европейская конвенция о выдаче от 13 декабря 1957 года и Европейская конвенция о взаимной правовой помощи по уголовным делам от 20 апреля 1959 года. Обе конвенции были ратифицированы Россией 25 октября 1999 года и вступили в силу 9 марта 2000 года. Кроме того, 17 июня 1999 года был подписан договор между Российской Федерацией и США о взаимной правовой помощи по уголовным делам, который затем был ратифицирован 3 ноября 2000 года.

6. Вопросы по **формированию доказательной базы**: фиксация, сбор, представление доказательств и их допустимость и достоверность. Сложность расследования правонарушений в сети Интернет связана с отсутствием материальных носителей с закрепленной на них информацией (в отличие, например, от газет и журналов), а также с тем, что спорные сведения легко уничтожить или изменить. Поэтому для доказательства в суде факта распространения порочащих сведений в сети конкретными лицами необходимо осуществить сложные процессуальные действия: просмотр протоколов доступа, проверку учетных записей провайдеров, просмотр содержимого серверов, установление владельцев серверов (которые могут находиться в разных странах).

В настоящее время используется такой способ доказывания юридического факта распространения информации в сети, как заверение у нотариуса интернет-страниц. В соответствии с гражданско-процессуальным законодательством (ст. 71 ГПК) такие доказательства принимаются судами в качестве письменных. Не решенными остаются и вопросы использования электронных документов в качестве доказательств в суде.

Острые дискуссии вызывает вопрос о **направлениях правового регулирования отношений в сети Интернет.** Здесь надо выделить три важных аспекта.

1. Одни ученые говорят о необходимости масштабного пересмотра действующего законодательства, чтобы отношения, протекающие в электронной среде, подпадали под его действие. Для этого предлагается внести изменения в Гражданский, Гражданско-процессуальный, Налоговый, Административный, Уголовный, Уголовно-процессуальный (а, возможно, и другие) кодексы, а также в ряд федеральных законов.

Другие настаивают на принятии национального кодекса по поддержанию правовых стандартов в Интернете. «Отношения, формирующиеся в информационной среде сети Интернет, выступают самостоятельными (новыми) правоотношениями, существенно отличающимися от традиционных, поэтому для их урегулирования необходимо формировать принципиально новую систему нормативных правовых актов, и проблема их регулирования принципиально не может быть решена путем внесения изменений в уже существующие акты различной отраслевой направленности. В самом общем виде целью формирования системы информационно-

правового регулирования общественных отношений, формирующихся в информационной среде, является создание правовых предпосылок для широкого использования новейших информационных технологий во всех сферах общественной жизни, в экономике, во взаимоотношениях органов государственной власти и местного самоуправления с гражданами и организациями. Такая задача может решаться либо путем принятия интернет-кодекса, либо комплексного федерального закона, который бы хоть и не именовался кодексом, но во многом исполнял его функции»[58].

2. Сложность регулирования информации в системе Интернет заключается в том, что глобальная сеть состоит из сетей, которые одновременно являются уникальными государственными сетями и составными частями мировой сети Интернет. Происходит размывание государственных информационных границ, которое требует унификации национальных норм информационного регулирования. В связи с этим проблемы, возникающие при обращении информации в сети, необходимо рассматривать в совокупности национальных и международных норм.

Попытки отдельного государства установить правила обмена информацией в сети представляются безуспешными. Происходят столкновение и ломка национального законодательства этих стран в виртуальном пространстве. Отсюда возникает вопрос: можно ли рассматривать Интернет в качестве целостного предмета правового регулирования и возможно ли определить основы правового регулирования отношений в системе Интернет на универсальном уровне? Видимо, нет и не может быть какого-либо единственно правильного ответа национального законодательства на проблемы интернет-пространства. Очерченные проблемы должны обсуждаться и решаться международным сообществом в целом.

3. Соблюдение прав и интересов лиц, вступающих в различные виды отношений в сети Интернет, возможно в случае последовательного проведения принципа сорегулирования, правового и этического. Это обусловлено тем, что государство и его контролирующие органы объективно не успевают за стремительно развивающимися технологиями, существующие правовые регуляторы и система государственного управления недостаточно эффективны применительно к целому ряду интернет-отношений. В то же время лица, добровольно согласившиеся пользоваться теми или иными сервисами и ресурсами информационного пространства, также добровольно принимают на себя локальные самоограничения, устанавливают определенные правила и модели поведения. Первым неформальным кодексом поведения, разработанным не законодателями или представителями отрасли, а пользователями, которые хотели сами цивилизованно использовать сеть, был Нетикет. Саморегули-

[58] *Тедеев А.А.* Проблемы и условия формирования системы информационно-правового регулирования общественных отношений, возникающих в информационной среде глобальных компьютерных сетей. URL: http://rniiis.ru/articlesip409/tevdeev.doc (дата последнего обращения: 28 апреля 2010)

руемые организации в Интернете доказали возможность эффективного решения ряда проблем[59].

Модель сорегулирования предполагает, что государство, операторы услуг, саморегулируемые организации являются равноправными участниками регулирования Интернета.

Государство в этом процессе осуществляет:

1)разработку, координацию и реализацию государственной политики на национальном, региональном и международном уровнях;

2)создание благоприятных условий для развития распространения и широкого применения Интернета и интернет-технологий;

3)разработку законов, иных нормативных правовых актов;

4)надзор за соблюдением законодательства;

5)борьбу с преступлениями, совершаемыми с помощью Интернета;

6)поощрение языкового и культурного разнообразия;

7)содействие урегулированию споров.

Операторы услуг в процессе регулирования Интернета осуществляют:

1)разработку стратегических предложений, руководящих принципов и инструментария для заинтересованных сторон;

2)участие в разработке национального законодательства и национальной и международной политики в сфере использования Интернета;

3)разработку стандартов, применяемых при развитии Интернета.

Саморегулируемые организации в Интернете осуществляют:

1)общественный контроль за мерами, предлагаемыми и применяемыми государством;

2)общественную экспертизу разрабатываемых и (или) принимаемых законов и иных нормативных актов;

3)разработку стандартов, применяемых при развитии Интернета;

4)организацию функционирования системы национальных доменных имен;

5)контроль качества услуг, оказываемых операторами Интернета;

6)содействие решению задачи обеспечения равноправного доступа граждан к Интернету.

Таким образом, нормативные правовые акты, направленные на регулирование правоотношений, связанных с использованием Интернета, подлежат обязательному предварительному обсуждению саморегулируемыми организациями пользователей и операторов и должны учитывать мнение указанных организаций, высказанные по результатам такого обсуждения.

Необходимо исходить из того, что любые принятые решения по управлению и саморегулированию отношений не должны противоречить закону.

---

59 См.: *Хиббард Л.* Интернет с человеческим лицом – общая ответственность: Справочник по свободе массовой информации в Интернете. Вена, 2004; Настольная книга по медийному саморегулированию / Под ред. д-ра юрид. наук, проф. М.А. Федотова. М., 2009.

Экономическая деятельность в электронной среде

Современное экономическое развитие стран и регионов во многом зависит от того, насколько эффективно применяются высокие технологии. В большинстве развитых стран производственные затраты на них значительно выросли. В настоящее время обосновывается концепция «информационной экономики», в которой информация рассматривается как производственный ресурс и товар.

Электронная экономическая деятельность охватывает все виды отношений, опосредуемых электронным обменом информацией и связанных с заключением международных и внутренних сделок: куплю-продажу, поставку, соглашение о распределении продукции, торговое представительство, факторинг, лизинг, проектирование, консалтинг, инвестиционные контракты, страхование, соглашения об эксплуатации и концессии, банковские услуги и др.

Другими словами, это такая экономическая деятельность, которая представляет собой совокупность процессов, совершаемых в электронной форме с использованием современных информационных технологий и направленных на перераспределение товаров, работ и услуг в ходе предпринимательской деятельности хозяйствующих субъектов. В качестве основного инструмента осуществления указанных экономических процессов выступает глобальная компьютерная сеть Интернет.

Виды электронной коммерческой деятельности можно классифицировать по различным основаниям.

При классификации по **функционально-производственным** признакам различают два вида электронной экономической деятельности, связанной с перераспределением товаров и перераспределением работ и услуг. Рассмотрим названные категории экономической деятельности подробнее.

1. **Электронная экономическая деятельность, связанная с перераспределением товаров, или электронная торговля.** Как отмечает А.А. Тедеев, применительно к экономическим отношениям, формирующимся в процессе использования глобальной компьютерной сети Интернет, зарубежные авторы выделяют два вида товаров – «мягкие» (soft) и «жесткие» (hard). Под «мягкими» понимаются товары, перераспределение (поставка) которых возможно в электронной форме: информационные и звуковые файлы, программные продукты, представленные в электронной форме ценные бумаги, безналичные финансовые средства («электронные деньги»). А под «жесткими» – все остальные движимые и недвижимые вещи[60].

2. **Электронная экономическая деятельность, связанная с перераспределением работ и услуг**. Здесь в качестве основных подвидов выделяются:

---

[60] См.: *Тедеев А.А.* Информационное право. С. 218.

– **электронная финансовая деятельность** (финансовое посредничество), т.е. электронные расчеты с использованием банковских карт и электронных денег и т.д.;

– **электронная страховая деятельность;**

– **электронная консультативная деятельность**, в частности, по вопросам правового регулирования, налогообложения бухгалтерского учета и др.;

– **электронная маркетинговая деятельность,** в том числе и исследование конъюнктуры рынка, деятельность в области рекламы, а также по выявлению общественного мнения;

– **электронная образовательная деятельность**, в частности, в области осуществления программ дистанционного образования с использованием глобальной компьютерной сети Интернет;

– **электронная издательская деятельность**, в частности, в области издания средств массовой информации в глобальной компьютерной сети Интернет (электронных сетевых газет);

– **деятельность по предоставлению услуг электронной связи**, в том числе и по предоставлению услуг доступа к Интернету, осуществляемая юридическими лицами – провайдерами.

Перенесение экономических процессов в электронную среду ставит перед юридической наукой особые задачи в сфере правового регулирования экономики. Объем совершаемых международных и внутренних сделок требует таких правовых норм, которые способствовали бы развитию глобального рынка путем унификации законодательства, правил и процедур, применяемых в различных странах.

Например, согласно одному из принципов современной электронной коммерции сто́роны, заключившие сделку, не вправе ставить под сомнение ее законность и действительность только на том основании, что она заключена электронным способом. Этот принцип закреплен в законодательстве далеко не всех стран, правовой режим электронного документа и электронной подписи, его удостоверяющей, существенно различается в национальных законодательствах. Это позволяет оспаривать законность заключения того или иного соглашения на том основании, что невозможно предоставить традиционный документ в письменной форме на бумажном носителе, заверенный собственноручными подписями сторон.

Значительно усложняется структура отношений, возникающих в процессе электронной внешнеэкономической деятельности, а следовательно, и процесс их правового регулирования. Сдерживающим фактором развития данного процесса является сложность регулирования вопросов правового, таможенного, налогового и иного характера в отношении таких сделок.

В целях преодоления названных правовых препятствий Комиссией ООН по праву международной торговли (ЮНСИТРАЛ) в 1996 году был разработан модельный закон «Об электронной торговле». Предполагает-

ся, что на основе этого закона страны могут в национальном законодательстве решить основные проблемы, связанные с правовым режимом электронных документов, определением ответственности при несоблюдении сторонами обязательств, возникших при заключении договоров в электронной форме и т.д. Позже были разработаны американский проект «Рамочных условий для глобальной электронной коммерции» и «Европейская инициатива в области электронной коммерции».

Все перечисленные документы в большей степени указывают направление разработки правового обеспечения, а не устанавливают конкретные нормы.

Общим для всех этих документов является положение о том, что на действия в информационном пространстве не должны накладываться более жесткие ограничения, чем на аналогичную деятельность, осуществляемую традиционными средствами, а также, о том, что электронная коммерция не должна облагаться дополнительными налогами.

В перечисленных документах отмечается также, что ключевую роль в содействии развитию электронной коммерции должно играть национальное законодательство, в частности, необходимо придание юридической значимости электронным документам, признание электронной подписи судом, обеспечение защиты персональных данных третьих лиц.

И.М. Рассолов отмечает, что в нашей стране электронная торговля остается второстепенной и экономически малоприбыльной для физических лиц в силу ряда причин. Необходимо «гарантировать и обеспечить юридические рамки безопасности для потребителей, предлагая им соответствующий уровень защиты, сравнимый с тем, который установлен для “классической” купли-продажи в нашей стране и в других государствах»[61]. Для этого, считает автор, необходимо принять российский закон «Об электронной торговле», который закрепил бы основные правила для рынка электронной торговли; при этом следует «формализовать» кодексы профессиональной этики, которые давно используются в Интернете. Кроме того, необходимо активнее внедрять в практику разрешение конфликтов третейскими судами в указанной среде; электронная торговля в скором времени станет «торговлей троих», что уже сегодня ведет к появлению новых юридических услуг и профессий, таких как кибер-нотариусы, кибер-юрисконсульты, кибер-адвокаты и т.д. Следует также приспособиться к уже существующим международным стандартам удостоверения и регламентации электронных обменов, гармонизовать свои отношения по поводу системы удостоверения электронных сделок хотя бы в рамках СНГ. В связи с этим важно также внести существенные изменения в действующий Федеральный закон «Об электронной цифровой подписи» и принять международное согла-

---

61 *Рассолов И.М.* Право и Интернет: теоретические проблемы: Автореф. дис. … д-ра юрид. наук. М., 2008. С. 31–32.

шение, касающееся электронных сделок, фиксирующее налог с продаж, взимаемый в стране назначения. Такая система уже применяется в Европе для торговли готовыми изделиями и в сфере услуг; было бы также целесообразно создать совещательный орган, например структурное подразделение при Минэкономразвития России, который мог бы следить за динамикой развития этой среды и вырабатывать необходимые рекомендации.

Одним из условий развития электронной торговли является обеспечение безопасности при передаче коммерчески значимой информации (и персональных данных) через Интернет. При заключении сделок, производстве расчетов и платежей стороны, разделенные пространством, должны иметь возможность идентифицировать друг друга, быть уверенными в целостности информации и конфиденциальности сеанса связи.

Хотя Закон об электронной торговле в нашей стране не принят, специальных правовых моделей, адресованных участникам электронной коммерции, российское законодательство не содержит. Однако не правильной представляется точка зрения, согласно которой отношения в сети Интернет находятся вне юрисдикции Российской Федерации и вне правового регулирования вообще.

На экономические отношения, формирующиеся и протекающие в сети Интернет, распространяются нормы действующего российского законодательства. В частности, следует разделять правомерную (законную), неправомерную и преступную экономическую деятельность.

Под **правомерной, законной экономической деятельностью** хозяйствующих субъектов в электронной сфере понимается любая экономическая деятельность, не запрещенная российским законодательством, осуществляемая надлежащим лицом, при наличии необходимого для этого государственного разрешения (лицензии), в случаях, когда наличие такой лицензии установлено законом.

Неправомерной считается электронная коммерческая деятельность, осуществляемая с нарушением требований закона, как то:

1)электронная экономическая деятельность лиц, **не зарегистрированных в установленном порядке** (например, физических лиц, не зарегистрированных в качестве индивидуальных предпринимателей);

2)электронная коммерческая деятельность без специального разрешения (например, ведение банковской деятельности юридическим лицом, не имеющим соответствующей лицензии)[62].

Преступная экономическая деятельность – виновное совершение с использованием Интернета общественно опасных деяний, запрещенных действующим уголовным законом под угрозой наказания. И.Н. Соловьев приводит следующую типологию преступной экономической деятельности в Интернете:

---

62 См.: *Тедеев А.А.* Информационное право: Учебник. М., 2005. С. 220-221.

1)мошенничество при совершении сделок через Интернет, хищение из виртуальных магазинов, денежных средств с банковских счетов и коммерческой информации физических и юридических лиц – пользователей сети, а также создание виртуальных финансовых пирамид;

2)совершение сделок и операций, скрытых от налоговых органов;

3)нарушение авторских и патентных прав, а также незаконное использование различных информационных баз данных правоохранительных и контролирующих органов;

4)совершение уголовных преступлений в сфере компьютерной информации (статьи 272–274 УК РФ), совершение в электронной форме сделок с объектами, изъятыми из оборота, а также с ограниченно оборотоспособными объектами (нахождение которых в обороте допускается по специальному разрешению), когда такие сделки совершаются в нарушение норм Уголовного кодекса[63].

Правовая проблема выбора механизмов регулирования электронной экономической деятельности (наряду с другими информационными отношениями, возникающими и протекающими в сети Интернет) становится все более актуальной. Развитие глобальной компьютерной сети достигло высокого уровня и способно оказывать значимое воздействие на различные сферы жизни общества. Поэтому государственное регулирование информационных отношений в сети представляется неизбежным. В первую очередь в этом нуждаются экономические отношения.

Защита прав на объекты интеллектуальной собственности в сети Интернет

Самые нарушаемые права в сети Интернет – это права на объекты интеллектуальной собственности. Особенность интернет-ресурсов состоит в том, что все объекты авторского права – текстовые, аудио- и видеоматериалы, графические объекты, базы данных, программы – существуют в форме электронных документов и потому могут быть легко скопированы, модифицированы, переправлены от одного пользователя другому (другим).

Основными правонарушениями в данной области являются:

1)плагиат, когда электронные документы копируются, модифицируются и выдаются за собственное творчество;

2)размещение материалов на интернет-сайтах и предоставление открытого доступа к ним, которое происходит без разрешения правообладателя. В результате автор не получает ту прибыль, на которую он рассчитывал в случае продажи произведения через торговую сеть.

---

63 См.: *Соловьев И.Н.* Криминогенные аспекты глобальной сети Интернет // Налоговый вестн. 2001. № 4

В отношении плагиата надо учитывать, что на произведения, размещенные в Интернете, распространяются нормы Гражданского кодекса, в частности статьи 1225, 1259, согласно которым **к объектам авторских прав относятся литературные произведения, музыкальные произведения с текстом или без текста, аудиовизуальные произведения, произведения живописи, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства, фотографические и другие произведения**.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы решения технических, организационных или иных задач, открытия, факты и языки программирования.

Существует и особый объект авторского права, обязанный своим появлением Интернету, – сайт. Он представляет собой определенную систему, которая включает в себя концепцию, структуру, совокупность интернет-страниц (на которых, в свою очередь, располагаются тексты, дизайн, фотографии, графика) и программный код. Каждый из этих элементов является объектом авторского права.

Согласно нормам Гражданского кодекса **интеллектуальные права не зависят от права собственности на материальный носитель**, в котором выражен результат интеллектуальной деятельности. Переход права собственности на вещь не влечет переход или предоставление прав на результат интеллектуальной деятельности. Несмотря на то что результаты интеллектуальной деятельности должны быть обязательно выражены в объективной форме и зачастую существуют на определенных материальных носителях, от этого они не перестают быть идеальными объектами. Они не подвержены износу, амортизации и могут устаревать только морально.

Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в его создание, в том числе и оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь, те, кто только способствовал оформлению прав на этот результат или контролировал выполнение работ.

Автору принадлежат личные неимущественные и исключительные имущественные права: право авторства; право на имя, т.е. право обнародовать произведение под собственным именем, псевдонимом или анонимно; право использовать или разрешать использовать свое произведение; право обнародовать или разрешать обнародовать свое произведение; право на защиту произведения от искажения; право на воспроизведение, распространение, переработку и т.д.

Любое самостоятельное авторское произведение автоматически, по умолчанию, попадает под защиту авторского права, обязательной регистрации авторского права не требуется.

В то же время согласно нормам Гражданско-процессуального кодекса каждая сторона обязана доказать те обстоятельства, на которые она ссылается в споре. Поэтому автору в случае защиты своих прав придется доказывать факт авторства и факт нарушения его прав. Сложность состоит в том, что произведение создается в электронной форме (процесс создания, творческих поисков не закрепляется на бумажном или ином носителе), существенно сокращается время, в течение которого произведение может быть скопировано и воспроизведено в другом месте и под другим именем.

С развитием Интернета появляются новые способы защиты авторских прав, например депонирование объекта авторского права (в цифровой форме) в веб-депозитарии, при этом автору выдается свидетельство о принятии произведения на депонирование. Эта процедура позволяет подтвердить факт и время публикации и в случае судебного спора решить вопрос о спорном авторстве. Можно депонировать произведение в печатном виде, в таком случае автору тоже выдается свидетельство о депонировании и регистрации.

Возможно нотариальное удостоверение времени размещения материалов, применение фото- и видеосъемки объектов авторских прав с фиксацией времени съемки, привлечение свидетельских показаний.

Правообладатель для оповещения о принадлежащем ему исключительном праве на произведение вправе использовать **знак охраны авторского права**, который помещается на каждом экземпляре произведения и состоит из следующих элементов:

– латинской буквы «С» в окружности;
– имени или наименования правообладателя;
– года первого опубликования произведения.

Никто не вправе изменять или удалять из произведений информацию об авторских и смежных правах, которая идентифицирует произведение или объект авторских прав, автора, обладателя авторских прав, а также информацию об условиях их использования. Умышленное изъятие или искажение такой информации будет считаться противозаконным.

Наиболее современным способом является размещение в теле произведения специальных электронных меток, которые устойчивы к сжатию, изменению размеров и формата. Для их нанесения требуется специальное программное обеспечение, которое наносит скрытый код определенного формата в файлы. Таким образом, файл произведения содержит дополнительную информацию об авторе. Можно использовать программный продукт, который приводит к частичному разрушению электронного документа в случае его несанкционированного копирования.

Применяемые на практике технические средства защиты авторских прав получили свое легальное закрепление и регламентацию в ст. 1299 ГК РФ. В ней разрешается использование любых технологий, технических устройств или их компонентов с целью контроля доступа

к произведению, предотвращения или ограничения действий, не разрешенных в отношении произведения самим автором или иным правообладателем. Одновременно налагается запрет на осуществление действий, направленных на нейтрализацию указанных технических средств охраны авторских прав третьими лицами.

Второй проблемой, как уже указывалось, является размещение на интернет-сайтах объектов авторского права и предоставление открытого доступа к ним без разрешения правообладателя. Технологии построения файлообменных сетей позволяют конечным пользователям беспрепятственно воспроизводить и распространять охраняемые произведения в неограниченном количестве.

Файлообменные сети различаются по техническим возможностям, но основные принципы их работы едины. Применение технологий peer-to-peer (P2P) позволяет пользователям транслировать контент напрямую и горизонтально, в отличие от обычных сетей, строящихся по иерархическому принципу, когда нужно запрашивать содержимое у вышестоящего по рангу сервера. На практике эти технологии позволяют обладателям цифровых копий объектов авторского права (например, музыкальных композиций, фильмов, видеоигр, компьютерных программ) обмениваться этими копиями друг с другом, избегая необходимости получать их от издательства или дистрибьютора[64].

Можно привести ставший широко известным пример использования этих технологий. Около 40 млн подписчиков по всему миру зарегистрировались на сайте napster.com и, используя поисковые средства веб-сайта, идентифицировали компьютеры, содержащие файлы опубликованных музыкальных произведений. Затем музыкальный файл копировался и пересылался с одного компьютера на другие (без всяких отчислений правообладателям). По иску звукозаписывающих компаний существование сайта было прекращено.

Как утверждает американский исследователь Арнольд Луцкер, происходит столкновение культур и мировоззрений сообщества обладателей авторских прав и поколения Интернета (Internet Generation). Поколение I-Gen считает, что доступ к произведениям в Интернете должен быть всемирным и свободным, автор, размещая свои произведения в свободном доступе, приобретает дополнительную популярность, что принесет ему в дальнейшем финансовое вознаграждение. Сообщество обладателей авторских прав полагает, что доступ должен быть контролируемым, а копирование – оплачиваемым[65].

По данным социологов, бесплатными онлайн-ресурсами пользуется 69% россиян-пользователей Интернета. Из оставшегося 31% только 10%

---

64 Подробнее см.: *Жвалов К.А.* Файлообменные сети и добросовестное использование: опыт США // Информационное право. 2009. № 1. С. 18.

65 См.: *Луцкер А.П.* Авторское право в цифровых технологиях и СМИ. М., 2005. С. 286.

считает скачивание бесплатных фильмов и музыки преступлением, остальные либо не умеют этого делать, либо не хотят тратить на это время[66].

В России также имеется опыт борьбы с подобными правонарушениями. В феврале 2010 года. Следственный комитет при прокуратуре РФ возбудил уголовное дело за незаконное использование объектов авторского права, совершенное в крупном размере, против владельцев файлообменного сервиса torrents.ru. В ходе расследования было установлено, что посредством этого сайта копировались и неоднократно распространялись контрафактные компьютерные программы. Сайт был закрыт.

Основной российской организацией, защищающей права авторов, является Российское авторское общество (РАО), существует также специализированная организация Российское общество по мультимедиа и цифровым сетям.

Российское законодательство предоставляет автору (правообладателю) широкие возможности для восстановления нарушенных прав:

– признание права;

– пресечение действий, нарушающих право или создающих угрозу его нарушения;

– возмещение причиненных убытков или компенсацию в размере от 10 тыс. до 5 млн руб.;

– изъятие материального носителя;

– публикацию решения суда о допущенном нарушении с указанием действительного правообладателя.

Автор или правообладатель может подать иск о компенсации морального вреда. Ответственность за нарушение авторских прав предусматривается Уголовным кодексом (ст. 146 УК РФ) и Кодексом об административных правонарушениях (ст. 7.12).

Правовые проблемы регистрации доменных имен

Для того чтобы пользователь мог попасть на нужный ему сайт, необходима эффективная система адресации. Каждому компьютеру присваивается IP-адрес, состоящий из набора цифр, но цифры запоминать неудобно, поэтому используются доменные имена, состоящие из букв и цифр и имеющие смысловое значение. Воспроизводя на компьютере доменное имя, пользователь попадает на искомый сайт, благодаря системе DNS (Domain Name System), которая производит сопоставление IP-адресов и доменных имен.

Обычно под доменным именем понимают символьное обозначение, зарегистрированное для сетевой адресации, в которой используется система доменных имен DNS.

---

66 См.: Исследовательский центр портала superjob.ru. URL: http://www.superjob.ru/research/news/1388/ (дата последнего обращения: 28 апреля 2010).

В.Б. Наумов указывает, что «доменное имя – это, по сути, средство индивидуализации в широком смысле, которое позволяет потребителям просто и эффективно находить в виртуальном пространстве известные им в хозяйственном обороте наименования»[67].

К средствам индивидуализации (согласно ст. 1225 ГК РФ) относятся фирменные наименования, товарные знаки и знаки обслуживания, наименование мест происхождения товаров, коммерческие обозначения. Они используются участниками гражданского оборота в целях идентификации самих субъектов экономической деятельности, их продукции, работ или услуг.

Особенность доменных имен состоит в том, что они служат для индивидуализации информационных ресурсов, принадлежащих физическим или юридическим лицам.

Общий порядок присвоения адресов и доменных имен определяет международная организация ICANN. Она разработала два нормативных документа: «Единая политика рассмотрения споров о доменных именах» (Uniform Domain Name Dispute Resolution Policy), сокращенно UDRP и «Правила для Единой политики рассмотрения споров о доменных именах», сокращенно Правила UDRP. Эти документы устанавливают систему внесудебного урегулирования доменных споров.

В России функции по учету и контролю в данной сфере осуществляются РосНИИРОС.

Для того чтобы избежать совпадения доменных наименований, производится их регистрация. Два одинаковых имени не могут быть зарегистрированы. Регистрация осуществляется в соответствии с Правилами регистрации доменных имен в домене RU, утвержденными Координационным центром национального домена в сети Интернет.

Регистрация доменного имени – это внесение в Реестр доменных имен информации о доменном имени и его администраторе. Срок действия регистрации, в течение которого осуществляется хранение в Реестре информации о доменном имени, составляет один год, но срок может быть продлен еще на год необходимое число раз.

Пробелы в законодательстве способствуют распространению различного рода правонарушений в этой сфере. Конфликты, связанные с доменными именами, почти всегда происходят вокруг широко известных фирменных наименований, товарных знаков, фамилий людей и других средств индивидуализации физических и юридических лиц. Многие адреса, содержащие наименования известных фирм, на самом деле принадлежат не им, а лицам, которые не имеют к этим фирмам никакого отношения, но успели зарегистрировать такое доменное имя с целью его последующей перепродажи. Такая деятельность именуется термином

[67] См.: *Наумов В.Б.* Российская судебная практика по спорам, связанным с использованием сети Интернет. URL: http://www.russianlaw.net/law/doc/a23.htm (дата последнего обращения: 28 апреля 2010)..

«кибersквоттинг» и носит международный характер. Например, компания NetNames провела исследование доменных имен в зонах COM, NET, ORG и CO.UK, имеющих отношение к футболу. В этих четырех доменных зонах было найдено 68 доменных имен, которые содержат имя и фамилию Дэвида Бекхэма. Однако не все домены используются. Лишь 3 из них зарегистрированы юристами Дэвида Бекхэма и указывают на его сайты. Большинство принадлежит третьим лицам – кибersквоттерам, которые надеятся заработать на популярности футболиста.

Согласно UDRP недобросовестность использования доменного имени определяется следующими показателями:

1)регистрацией или приобретением ответчиком доменного имени главным образом с целью продажи, сдачи в аренду или передачи иным образом заявителю, который является владельцем товарного знака, или его конкуренту за деньги или иные ценности, превышающие подтвержденные расходы ответчика, прямо относящиеся к доменному имени;

2)регистрацией доменного имени в с целью помешать владельцу товарного знака использовать знак в соответствующем доменном имени, при условии, что ответчик заинтересован в такой модели поведения;

3)регистрацией с целью помешать деятельности конкурента;

4)стремлением ответчика привлечь с коммерческой целью пользователей Интернета к своему сайту путем создания вероятности восприятия принадлежащего заявителю знака как источника существования, финансирования, организационной принадлежности или поддержки своего сайта и предоставляемых с его помощью продукции или услуг[68].

В целях защиты интересов частноправовых интересов экономических субъектов в Интернете во многих странах приняты законы, определяющие правовое регулирование отношений, связанных с регистрацией и использованием доменных имен.

В России понятие «доменное имя» не закреплено законодательно. Некоторая правовая регламентация доменов установлена в ч. 4 Гражданского кодекса. Например, п. 9 ст. 1483 предусматривает: «Не могут быть зарегистрированы в качестве товарных знаков обозначения, тождественные … доменному имени, права на которые возникли ранее даты приоритета регистрируемого товарного знака». Ст. 1484 устанавливает, что «исключительное право на товарный знак может быть осуществлено для индивидуализации товаров, работ или услуг, в отношении которых товарный знак зарегистрирован, в частности, путем размещения товарного знака …в сети Интернет, в том числе в доменном имени и при других способах адресации». И наконец, ст. 1519 разрешает размещать в доменном имени наименования места происхождения товара.

---

[68] См.: http://www.icann.org/udrp-policy-24oct99.htm (дата последнего обращения: 28 апреля 2010).

Приведенные положения свидетельствуют о том, что законодатель связывает понятие доменного имени с товарным знаком.

В ст. 1477 ГК РФ товарный знак определяется как «обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей».

Главная функция товарного знака – отличительная, он помогает потребителям ориентироваться в однородных товарах различных производителей.

Товарный знак должен быть зарегистрирован в Государственном реестре товарных знаков. В этом случае выдается свидетельство на товарный знак, которое удостоверяет приоритет товарного знака и исключительное право на него в отношении товаров, указанных в свидетельстве.

Доменное имя как объект права имеет много общего с товарным знаком, но в то же время обладает рядом присущих только ему признаков:

– индивидуализирует не юридическое лицо или индивидуального предпринимателя, а информационный ресурс;

– может принадлежать человеку, не осуществляющему предпринимательскую деятельность, органу государственной власти;

– может быть только абсолютно новым, принцип «параллельного использования» товарного знака в разных сферах экономической деятельности (разных классах товаров) не должен применяться в киберпространстве;

– является уникальным не только для страны регистрации, но и всего мира.

Таким образом, домен является отличным от товарного знака средством индивидуализации. Разность этих объектов требует и разного правового регулирования.

В 2004 году один из ведущих специалистов в сфере правового регулирования Интернета А.Г. Серго писал о том, что «действующее российское законодательство сегодня объективно нуждается в регулировании доменного имени как самостоятельного средства индивидуализации, а не способа использования товарного знака, как сейчас это определено в действующем законодательстве. Правовое регулирование доменных имен должно быть разработано, опираясь не только на законодательство о товарных знаках (и других средствах индивидуализации), но и основываясь на законодательстве в информационной сфере»[69]. С принятием Четвертой части Гражданского кодекса вопросы правового регулирования доменного имени не нашли своего разрешения, и вывод А.Г. Серго по-прежнему актуален.

30 октября 2009 года Советом директоров ICANN была одобрена процедура Fast Track, регламентирующая создание ограниченного числа

[69] *Серго А.Г.* О некоторых подходах к правовому регулированию доменного имени. URL: http://www.lawmix.ru/comm/1900/ (дата последнего обращения: 29 апреля 2010).

доменов верхнего уровня, записанных символами национальных языков. Данное событие очень важно для той части интернет-сообщества, которая не использует символы латиницы в родном языке, оно будет способствовать активному вовлечению неанглоязычных пользователей в это сообщество.

Одной из первых была зарегистрирована российская заявка на кириллический домен .рф.

С 25 ноября 2009 по 25 марта 2010 года заявки на регистрацию доменов .рф в приоритетном порядке (т.е. до момента открытой регистрации для всех желающих) могли подаваться владельцами товарных знаков. С 20 апреля регистрация доменных имен в зоне .рф доступна всем заинтересованным лицам.

Отсутствие полноценного непротиворечивого правового регулирования регистрации доменных имен сказалось и в данном случае. Одна из российских компаний смогла, не нарушая правил, подать заявки на приоритетную регистрацию доменных имен, совпадающих с общеупотребительными словами русского языка: секс.рф, банк.рф, знакомства.рф, кино.рф. Для этого компания первоначально получила в Роспатенте свидетельства на соответствующие товарные знаки. Российское законодательство ограничивает регистрацию товарных знаков, совпадающих с общеупотребительными словами. Однако этот запрет действует только в том случае, если значение слова, регистрируемого в качестве товарного знака, напрямую указывает на ту сферу деятельности, в которой он будет использоваться. Используя данную норму, компания зарегистрировала слово «кредит» для категории товаров «кружева зубчатой формы, ленты, ленты орденские», а слово «секс» по классу «сумки женские, сумки пляжные, чемоданы». В результате приоритетная регистрация доменных имен в зоне .рф была приостановлена на несколько дней.

Специалисты считают, что нашей стране необходимо принятие самостоятельного нормативного правового акта, содержащего понятие, правовое регулирование доменных имен в Российской Федерации и порядок разрешения связанных с ними споров с учетом отечественной и зарубежной практики.

Модуль 4
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Тема 13. ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Понятие информационного оружия, информационной войны

Впервые термин «информационная война» появился в середине 80-х годов. Активно он начал использоваться во время американской операции в Ираке «Буря в пустыне».

Авторы дают разные определения информационной войны, каждый расставляет свои акценты:

1. **Информационная война** – это действия, предпринимаемые для достижения информационного превосходства, поддержки национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем[70].

2. **Информационная война** – целенаправленное, широкомасштабное оперирование смыслами: создание, уничтожение, модификация, навязывание и блокирование смыслов информационными методами для достижения поставленных целей[71].

3. **Информационная война** – борьба между государствами с использованием информационных технологий, базирующихся на промышленном производстве, распространении и навязывании информации.

Особенности информационной войны:

1)информация и информационные системы выступают и как оружие, и как объект защиты;

2)расширяется территориальное пространство ведения войны;

3)ведется как при объявлении войны, так и в кризисных ситуациях;

4)ведется специальными службами и гражданскими структурами (например, СМИ).

Концепция информационной войны и способы ее ведения:

1)подавление (в военное время) элементов инфраструктуры государства и военного управления противника;

---

70 См.: *Ковалева Н.Н.* Указ. соч. С. 145

71 *Расторгуев С.П.* Информационная война. Проблемы и модели. Экзистенциальная математика: Учеб. пособие для студентов вузов, обучающихся по спец. в области информационной безопасности. М., 2006. С. 8.

2)электромагнитное воздействие на элементы информационных и телекоммуникационных систем (создание помех);

3)получение разведывательной информации путем перехвата и дешифровки информационных потоков, передаваемых по каналам связи, за счет специального внедрения электронных устройств;

4)осуществление несанкционированного доступа к электронным системам – «хакерская война»;

5)формирование и массовое распространение по информационным каналам **противника** или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения, – «психологическая война»;

6)получение интересующей информации путем перехвата и обработки открытой информации (например, то, что составляет ценности или проблемы в данный момент).

Информационное оружие – средства, применяемые для активизации, уничтожения, блокирования или создания в информационной системе процессов, в которых заинтересован субъект, использующий оружие.

Отличие информационного оружия от обычного:

1)применение информационного оружия не предполагает «выделения энергии» (химической, ядерной, атомной) для уничтожения противника. Изначально считается, что противник обладает всеми необходимыми средствами для собственного уничтожения;

2)скрытность;

3)масштабность (не бомбежка одного города, а воздействие на всю страну или глобальные информационные сети);

4)универсальность.

Для широкого применения информационного оружия, как и любого другого, требуется, чтобы оно:

– максимально быстро могло быть применено;

– причинило объекту воздействия требуемый ущерб в заданный временной интервал;

– было достаточно простым и дешевым в изготовлении по сравнению с другим видом оружия того же класса воздействия (это особенно характерно для информационного воздействия – не надо мобилизовывать армию, ее одевать, кормить, вооружать, транспортировать, выплачивать компенсацию родным погибших и раненых, вместо солдат работают специалисты (программисты, журналисты, политологи, аналитики, рекламщики), многие из которых преследуют и собственные коммерческие интересы.

В последние десятилетия возникли условия, которые позволили говорить об информационном оружии как о наиболее значимом современной эпохи. К ним относятся:

– резкое удешевление производства данных благодаря появлению средств вычислительной техники. Производство информации ставится на конвейер;

– сокращение времени на доставку сообщений практически в любую точку планеты благодаря развитию телекоммуникационных средств;

– повышение эффективности информационного воздействия благодаря появлению теорий и практических разработок в области перепрограммирования ЭВМ и приемов информационно-психологического воздействия на людей (НЛП).

Информационное оружие может оказывать техническое, биологическое, социальное воздействие на процессы производства, обработки и передачи информации.

Техническое оружие – блокировка компьютеров, телекоммуникаций, вирусы, программные закладки, маскирующие помехи, излучения электромагнитного или ионизирующего воздействия через сети питания, средства генерации естественной речи конкретного человека.

Биологическое оружие – средства поражающего воздействия, направленные на мозг человека и воздействующие через слуховые и зрительные анализаторы. Необходимы защитные фильтры от такого рода воздействия, они могут устанавливаться на уровне общества или отдельного человека.

Социальное воздействие – манипулирование общественным сознанием, осмеяние, девальвация культурных ценностей и национальных традиций, внедрение в массовое сознание идеологических концептов противника; политическая переориентация социальных групп населения, дестабилизация политической системы, обострение межпартийной борьбы, подрыв авторитета органов власти, дискредитация органов управления и т.д. Воздействие оказывается как на подсознательном, так и на ментальном уровне.

Характеристика угроз, субъектов и объектов информационной безопасности

В основу определения информационной безопасности положено родовое понятие – это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз», закрепленное в Законе РФ «О безопасности» от 5 марта 1992 г. № 2446-1. **Понятие информационной безопасности России дается в Доктрине информационной безопасности Российской Федерации (утверждена Указом Президента РФ 09.09.2000) как «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»**.

Как замечает С.П. Расторгуев, ощущение защищенности может быть обманчивым, но объективных критериев, позволяющих измерить эту защищенность, не существует. Мерилом является человек, его мысли и чувства[72].

Одна из главных задач системы обеспечения информационной безопасности в социальной сфере заключается в создании и поддержании максимально адекватного событийному миру общественного сознания и собственного знания о мире. Тогда, несмотря на искажающее информационное воздействие, человек и общество смогут разобраться в происходящем, не позволить себя «перепрограммировать» или уничтожить.

Понятие **«информационная безопасность страны»** следует отличать от понятия **«безопасность информации».** «Безопасность информации» осуществляется комплексом мероприятий по защите, прежде всего, государственной тайны, а также другой конфиденциальной информации.

Чаще всего нарушение **безопасности информации (информационных ресурсов, информационных технологий, информационных систем)** определяют как **«несанкционированный доступ»** к объекту защиты. Кроме того, причиной нарушения безопасности информации может стать неудовлетворительная работа по организации охраны, защиты и использования соответствующего ресурса владельцем информации или субъектом, ответственным за обеспечение ее безопасности.

Таким образом, безопасность информации, информационных технологий, информационных систем является частью информационной безопасности страны.

При анализе информационного противостояния первостепенное значение имеют такие категории как:

– **национальные интересы;**
– **угрозы;**
– **объекты безопасности;**
– **субъекты безопасности.**

Как отмечалось выше, информационная безопасность Российской Федерации понимается как состояние защищенности ее национальных интересов. **Интерес** – осознанная потребность кого-либо в чем-либо. Интересы могут быть объективными и субъективными (связанными с осознанием данной потребности). Интересы различных социальных и экономических субъектов часто не совпадают или противоречат друг другу. Более того, в некоторых социальных системах, исповедующих индивидуализм, признается приоритет интересов личности по отношению к интересам государства. В других социальных системах, основными идеологемами которых являются соборность и коллективизм, главными считаются интересы государства, а не отдельного человека.

[72] См.: *Расторгуев С.П.* Указ. соч. С. 36.

Поэтому важными задачами внутренней политики государства являются, во-первых, определение национальных интересов и, наконец, поиск баланса (компромисса) между интересами личности, общества и государства.

Классификация угроз связана со сферами общественной деятельности (при этом они всегда носят информационный характер):

1. **Сфера экономики**. Сфера экономики считается одной из наиболее подверженных информационным угрозам, поскольку свобода рыночных отношений благоприятствует бесконтрольному созданию различных структур, занимающихся сбором, обработкой, хранением и передачей статистической, внешнеэкономической, финансовой, налоговой, таможенной, коммерческой, служебной информации, используемой в дальнейшем для инсайдерских целей, дезинформации и формирования тенденциозной информационной картины с последующим воздействием на оценки, намерения и политику хозяйствующих субъектов.

2. **Сфера внутренней политики.** Основные направления внутренней политики государства определяются Президентом РФ и Правительством РФ.

Наибольшую опасность в этой сфере представляют следующие угрозы информационной безопасности:

– нарушение 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 целей;

– распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране;

– деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности России, разжигание социальной, расовой, национальной и религиозной вражды, распространение этих идей в средствах массовой информации.

3. **Сфера внешней политики.** Можно выделить следующие угрозы: информационное воздействие иностранных военных и политических структур на разработку и реализацию внешней политики Российской Федерации; попытки несанкционированного доступа к информации; информационно-пропагандистская деятельность политических сил, общественных объединений, СМИ, искажающих стратегию и тактику внешнеполитической деятельности Российской Федерации.

4. **Сфера науки и техники.** Отношения в области науки и техники регламентируются Федеральным законом «О науке и государственной научно-технической политике» от 23 августа 1996 г. № 127-ФЗ. К числу основных угроз относятся:

– стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

– переориентация на западные страны наиболее перспективных ученых («утечка мозгов);

– активизация деятельности иностранных государственных и коммерческих организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

5. **Сфера духовной жизни** личности, и прежде всего массового сознания, более всего подвержена информационным манипуляциям и потому нуждается в особых мерах безопасности. Согласно Доктрине наибольшую угрозу представляют:

– деформация системы массового информирования за счет монополизации СМИ и неконтролируемого расширения сектора зарубежных СМИ в отечественном информационном пространстве;

– ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры;

– возможность нарушения общественной стабильности, нанесения вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм.

Можно назвать и другие сферы.

Объекты безопасности. Закон РФ «О безопасности» относит к основным объектам безопасности «личность – ее права и свободы; общество – его материальные и духовные ценности, государство – его конституционный строй, суверенитет и территориальную целостность». Кроме того, в число объектов безопасности следует включить информационные системы, сети связи, информационные технологии и информационные ресурсы.

Субъекты безопасности

В соответствии со ст. 2 Закона РФ «О безопасности» основным субъектом обеспечения безопасности является государство, кроме того, общественные и иные организации и объединения, граждане. Некоторые ученые считают, что субъекты в Законе определены неверно: «Обеспечение безопасности – исключительно прерогатива государства, поскольку граждане и общественные объединения не располагают соответствующими силами и средствами»[73].

Другие ученые исследователи утверждают, что раз национальная безопасность понимается как защищенность интересов личности, обще-

[73] *Шуберт Т.Э.* Нормативно-правовое регулирование вопросов безопасности // Журн. рос. права. 1999. № 11. С. 51.

ства и государства, то защита их интересов без участия их самих невозможна[74].

Государство должно создавать эффективные механизмы, при помощи которых достигается безопасность. Ряд носителей интересов – сообщества, выходящие за рамки национальных государств, а также человечество в целом. Ряд угроз носит транснациональный или общемировой характер, и для их решения необходимы усилия, согласованные на международном уровне. В информационной среде одной из таких глобальных проблем является компьютерная преступность.

Государственная политика в области информационной безопасности

Вопросам безопасности посвящен целый ряд нормативно-правовых актов и иных официальных документов, в числе которых важную роль играют документы политического характера. В первую очередь Концепция национальной безопасности РФ (утверждена Указом Президента РФ от 17.12.1997 № 1300 (в ред. от 10.01.2000г.)) и Доктрина информационной безопасности (утверждена Указом Президента РФ 09.09.2000).

Доктрина информационной безопасности Российской Федерации определяется как совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

В Доктрине предпринята попытка структурирования **национальных интересов** России в информационной сфере на **4 группы**:

1)соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей в обществе, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

2)информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике России, ее официальной позиции по социально значимым событиям российской и международной жизни;

3)развитие современных информационных технологий, отечественной индустрии информации, в том числе и средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка и выход этой продукции на мировой рынок. Обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

---

74 См.: *Антопольский А.А.* Информационная безопасность: на весах опасности информационных процессов // Информационное право: актуальные проблемы теории и практики. С. 442.

4)защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем на территории России.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, система лицензирования деятельности в области защиты государственной тайны и система сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально – экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупки импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно – телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения «информационного оружия» против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Общие **методы обеспечения информационной безопасности** Российской Федерации разделяются на **правовые, организационные, технические и экономические**.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности. Наиболее важными направлениями этой деятельности являются:

– внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация;

– разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

– определение статуса организаций, предоставляющих услуги глобальных информационно – телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций.

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

– соблюдении Конституции РФ, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

– открытости в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

– правовом равенстве всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

– приоритетном развитии отечественных современных информационных и телекоммуникационных технологий, производстве технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

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

Тема 14. ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА. ГОСУДАРСТВЕННАЯ ТАЙНА

Понятие тайны в праве

В процессе взаимодействия субъектов общественных отношений могут возникать ситуации, в которых разглашение информации, свободный доступ к ней становятся нежелательными. Нераспространение этих сведений может основываться на взаимной договоренности (служебная, профессиональная, коммерческая тайны), на элементарной порядочности (личная тайна), государство может принимать организационно-правовые меры для сохранения конфиденциальности определенной информации и устанавливать специальный режим ее правовой защиты (государственная тайна). С этим связано ограничение свободного доступа к информации, т.е. формирование правовых институтов тайны.

В российской правовой науке пока нет единого подхода к понятию тайны. Существует **два основных подхода**.

Сторонники **первого подхода** дают следующее определение: «Тайна – информация, доступ к которой ограничен». Другими словами, тайна – сведения, которые не являются общеизвестными и общедоступными, их разглашение может причинить вред чьим-либо интересам, их обладатель принимает меры по охране указанных сведений. Эта позиция получила закрепление в Законе РФ «О государственной тайне».

Термин «тайна» обычно используется с прилагательными коммерческая, служебная, банковская, аудиторская, врачебная, государственная, употребляется как синоним сведений, которые неизвестны либо должны быть неизвестны третьим лицам. Чаще всего применяется формула «сведения, составляющие» ту или иную разновидность тайны, например банковской (п. 2 ст. 857 ГК РФ), аудиторской (п. 3 ст. 8 Федерального закона «Об аудиторской деятельности»).

Можно сделать вывод, что законодатель рассматривает тайну как объективно существующие, но неизвестные третьим лицам сведения.

Второй подход можно сформулировать так: «Тайна – это особый правовой режим информации».

В последнее время все больше ученых говорят, что понятие «тайна» не сводимо к информации. Иными словами, **тайна** – не информация, а **особый правовой режим информации.** Поэтому информация не может составлять тайну, она может находиться в тайне. Эта позиция получила закрепление в Федерального закона «О коммерческой тайне».

Правовой режим – «комплекс правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создающих особую направленность регулирования»[75].

Правовой режим любого вида тайны включает три элемента:

1)ценность скрываемых сведений;

2)механизм защиты или ограничения доступа к конфиденциальным сведениям;

3)юридическую ответственность за несанкционированное получение и (или) распространение этих сведений.

Закон об информации не дает понятия тайны, он содержит определение «конфиденциальность информации» – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Виды тайн, предусмотренные российским законодательством

Ученые-юристы, по разным оценкам, насчитывают от 40 до 50 видов тайн в российском законодательстве.

Указом Президента РФ от 6 марта 1997 года утвержден перечень сведений конфиденциального характера, среди которых:

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

2)сведения, составляющие тайну следствия и судопроизводства;

3)служебная тайна;

4)профессиональная тайна;

5)коммерческая тайна;

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

Федеральный закон «Об информации» в ст. 9 дает более общую классификацию:

---

75 *Алексеев С.С.* Теория права. М., 1993. С. 170.

1)государственная тайна;
2)коммерческая тайна;
3)служебная тайна;
4)профессиональная тайна;
5)личная или семейная тайна.

Федеральными законами устанавливаются **условия отнесения** информации к сведениям, составляющим коммерческую, служебную и иную тайну, **обязательность соблюдения конфиденциальности** такой информации, а также **ответственность** за ее разглашение.

Термин «защита информации» закреплен в ст. 16 Федерального закона «Об информации», согласно которой **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.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Обладатель информации и 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 ней;

2)своевременное обнаружение фактов несанкционированного доступа к информации;

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

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

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

6)постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федераль-

ным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

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

Виды тайн определяются характером общественных отношений, возникающих по поводу интересов их охраны.

Рассмотрим эти тайны подробнее.

Правовое регулирование в области государственной тайны

Согласно Конституции РФ (ст. 29) перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Для государственной тайны устанавливается **особенный правовой режим**. Суть его заключается в жестком ограничении доступа к такой информации, надежной защите ее от несанкционированного доступа и четком определении круга лиц, которым предоставляется доступ к ней.

Режим государственной тайны устанавливает:

1)информацию, которая относится к государственной тайне, и информацию, которая не может быть к ней отнесена. Перечень сведений, отнесенных к государственной тайне, дается в ст. 5 Закона. В первоначальной редакции она называлась «Сведения, которые могут быть отнесены к государственной тайне». В 1997 году в статьи были внесены изменения и она стала называться «Перечень сведений, составляющих государственную тайну» (диспозитивная норма поменялась на императивную). Статья 7 Закона содержит «Перечень сведений, которые не могут относиться к государственной тайне». В первоначальной редакции была понятна логика: сведения, содержащиеся в ст. 7, засекречивать запрещается; если же они не относятся к ст. 7, то они проверяются на соответствие ст. 5 и при необходимости засекречиваются. Теперь Закон дает две императивные нормы. Вся информация как будто бы делится на два непересекающихся множества. Проблема в том, что иногда информацию сложно отнести к какому-то определенному виду. Например, если речь идет о заражении какой-либо местности в результате деятельности армии.

2)порядок отнесения информации к государственной тайне, т.е. порядок засекречивания сведений, составляющих такую тайну и порядок рассекречивания информации;

3)порядок передачи сведений, составляющих гостайну;

4)порядок обеспечения защиты гостайны;

5)ответственность за нарушение режима гостайны.

Отнесение сведений к государственной тайне и их засекречивание осуществляются в соответствии с **принципами законности, обоснованности и своевременности.**

Степень секретности сведений, составляющих гостайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения таких сведений. Устанавливаются **три степени секретности** сведений, составляющих государственную тайну, и для каждой из них существуют грифы секретности, устанавливаемые на их носителях: **«особой важности», «совершенно секретно» и «секретно».**

Порядок отнесения сведений к той или иной степени секретности устанавливается правительством.

Специальный «Перечень сведений, отнесенных к государственной тайне» утверждается Указом Президента.

На носители сведений, составляющих государственную тайну, ставятся реквизиты, включающие следующие данные:

– о степени секретности содержащихся в носителе сведениях;

– об органе государственной власти, который эти сведения засекретил;

– о регистрационном номере;

– о дате или условии рассекречивания сведений, либо о событии, после наступления которого сведения будут рассекречены.

Основаниями для **рассекречивания** сведений, т.е. снятия ограничения на распространение сведений, составляющих государственную тайну, и на доступ к их носителям, могут являться взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, отнесенными в Российской Федерации к государственной тайне, изменение объективных обстоятельств, вследствие чего дальнейшая защита сведений, составляющих государственную тайну, нецелесообразна.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению Межведомственной комиссии по защите государственной тайны.

6) особый порядок допуска должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск предусматривает для принимающих такое решение принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну.

1)согласие на частичные, временные ограничения их прав (права выезда за границу на срок, оговоренный в трудовом договоре, права на распространение сведений, составляющих государственную тайну, на использование открытий и изобретений, содержащих такие сведения, права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к гостайне);

2)письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

3)ознакомление с нормами законодательства Российской Федерации о гостайне, предусматривающими ответственность за его нарушение;

4)принятие решения руководителем органа государственной власти, предприятия учреждения или организации о допуске оформляемого лица к сведениям, составляющим гостайну.

Три формы допуска соответствуют трем степеням секретности: допуск к сведениям особой важности, совершенно секретным или секретным. Наличие допуска к сведениям более высокой степени секретности является основанием для допуска к сведениям более низкой степени секретности.

Тема 15. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ

Служебная и профессиональная тайны

В вопросе разграничения профессиональной и служебной тайны нет четкой правовой регламентации. В связи с этим понятие служебной и профессиональной тайн по-разному трактуется в научной литературе.

Служебная тайна – весьма специфичный правовой феномен, она часто упоминается, но является одной из наименее разработанных в отечественном праве.

До 1993 года служебная тайна входила в систему государственных секретов, после принятия в 1993 году Закона РФ «О государственной тайне» сформировалась категория государственной тайны, а институт служебной тайны законодательного оформления не получил.

Далее была принята часть первая ГК РФ, где действовала ст. 139 ГК РФ, которая регулировала отношения по поводу служебной и коммерческой тайн, которые определялись на основе общих признаков. С 1 января 2008 года эта статья утратила силу. Закон о коммерческой тайне был принят, а закона о служебной тайне нет до сих пор, хотя его проекты предлагались.

На сегодняшний день основным актом, регулирующим отношения в данной сфере, является Постановление Правительства РФ от 3 ноября

1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

К служебной информации **ограниченного распространения** согласно п. 1.2 указанного Положения «относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью».

В данном Положении устанавливается **перечень сведений, которые не могут быть отнесены к служебной тайне.**

Устанавливается также порядок работы с конфиденциальными документами.

Перечень сведений, относящихся к служебной тайне, отсутствует.

Служебная тайна – правовой режим защищаемой конфиденциальной информации, ставшей 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.

Виды служебной тайны:

1)военная тайна;

2)тайна следствия;

3)судебная тайна;

4)налоговая тайна;

5)охраноспособная конфиденциальная информация, составляющая коммерческую, профессиональную или личную тайну, ставшая известной в силу исполнения служебных обязанностей.

Субъекты служебной тайны:

1)военнослужащие;

2)работники прокуратуры, милиции, органов государственной безопасности и т.д., налоговых и таможенных органов;

3)судьи;

4)должностные лица;

5)государственные служащие.

Единого правового акта, устанавливающего правовой режим служебной тайны, нет. Отдельные виды информации, составляющие служебную тайну, регулируются соответствующим отраслевым законодательством.

Например, *тайна предварительного расследования* установлена Уголовно-процессуальным кодексом РФ. Согласно ч. 1 ст. 161 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.

На документах и изданиях, содержащих служебную информацию ограниченного распространения, в верхнем правом углу первой страницы ставится специальная пометка «Для служебного пользования». Такие документы подлежат специальному учету отдельно от несекретной информации, передаются работникам под роспись, размножаются (тиражируются только с письменного разрешения руководителя, учитывается каждый экземпляр размноженного документа), хранятся в надежно запираемых и опечатываемых шкафах. Исполненные документы с пометкой «Для служебного пользования» формируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется отметка «Для служебного пользования». Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования», проводится не реже одного раза в год комиссиями, назначаемыми приказами руководителя. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

Профессиональная тайна – правовой режим защищаемой законом информации, доверенной или ставшей известной лицу (конфиденту) исключительно в силу исполнения им профессиональных обязанностей, не связанной с государственной или муниципальной службой. Распространение этой информации может нанести доверителю материальный ущерб или причинить моральные страдания.

Виды профессиональной тайны:

1)врачебная тайна;
2)тайна связи;
3)нотариальная тайна;
4)адвокатская тайна;
5)тайна усыновления;
6)тайна страхования;
7)тайна исповеди.

К профессиональным тайнам относятся так называемые «тайны двоих», один из которых доверитель, а другой конфидент (его еще называют держателем информации), т.е. лицо, которое узнает данные сведения в силу исполнения своих профессиональных обязанностей: врач, нотариус, адвокат, работник детского дома и т.д. Для доверителя это будет личная тайна, а для конфидента – профессиональная. Обязанности по соблюдению профессиональной тайны возложены на конфидентов федеральными законами, регулирующими их профессиональную деятельность. Закон не устанавливает срока хранения профессиональной тайны. Напротив, говорится, что срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может

быть ограничен только **с согласия гражданина** (физического лица), предоставившего такую информацию о себе. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам (например, следователю) только в соответствии с федеральными законами и (или) по решению суда.

Субъекты профессиональной тайны:

1)доверитель (тот, чья тайна охраняется);

2)конфидент, или держатель тайны (врач, адвокат, работник ЗАГСа, нотариус, священник).

Например, режим *адвокатской тайны* установлен Федеральным законом от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации». 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 и после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех в случаях, когда они не входят в производство адвоката по делам его доверителей.

Режим *врачебной (медицинской) тайны* установлен в Основах законодательства РФ об охране здоровья граждан от 22 июля 1993 г. № 5487-1. К врачебной тайне относятся сведения о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении. Кроме того, Законом РФ «О психиатрической помощи и гарантиях прав граждан при ее создании» от 2 июля 1992 г. № 3185-1 предусмотрено отнесение к медицинской тайне сведений 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. Передача этих сведений третьим лицам допускается лишь с согласия гражданина или его законного представителя. На медицинский персонал и лица, которым в установленном порядке переданы эти сведения, возлагается обязанность обеспечить конфиденциальность этих сведений и предотвращать нарушение врачебной тайны со стороны третьих лиц.

Тайна завещания. Как установлено в ст. 1123 Гражданского кодекса РФ, до открытия наследства запрещено разглашать сведения, касающиеся факта совершения завещания, содержания завещания (т.е. сведений о самом наследодателе, наследстве, наследниках, наследственных долях, завещательном отказе и т.д.), изменения или отмены завещания.

Правовой режим коммерческой тайны

Согласно ст. 3 Федерального закона «О коммерческой тайне» от 29 июля 2004 года ***коммерческая тайна*** – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Таким образом, выделяются ***признаки информации***, защищаемой в режиме коммерческой тайны:

1)информация имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;

2)отсутствует свободный доступ к информации;

3)обладатель информации принимает меры к охране ее конфиденциальности.

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 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, каждого гражданина и населения в целом;

5)о численности, составе работников, системе оплаты труда, об условиях труда, в том числе и об охране труда, показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;

6)о задолженности работодателей по выплате заработной платы и иным социальным выплатам и др.;

Объекты коммерческой тайны:

1)сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе и о результатах интеллектуальной деятельности в научно-технической сфере;

2) секреты производства;

3)сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам.

Субъекты коммерческой тайны:

1)обладатель информации, составляющей коммерческую тайну, – лицо, которое владеет такой информацией на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

2)правопреемники – лица, которые на законном основании имеют доступ к информации, составляющей коммерческую тайну, например, сотрудники фирмы. Их ознакомление с такой информацией происходит с согласия ее обладателя или на ином законном основании при условии сохранения ее конфиденциальности, что определяется должностными инструкциями;

3)контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение ее перечня и состава ***принадлежит обладателю такой информации*** с учетом вышеизложенных положений Закона о коммерческой тайне.

Информация, составляющая коммерческую тайну, считается полученной незаконно, если доступ к ней осуществлялся с умышленным преодолением принятых обладателем информации, мер по охране ее конфиденциальности, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну и что осуществляющее передачу этой информации лицо не имеет на то законного основания.

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1)определение перечня информации, составляющей коммерческую тайну;

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

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

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

5)нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических

лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Только после принятия этих мер режим коммерческой тайны считается установленным.

Кроме того, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, а также другие не противоречащие законодательству Российской Федерации меры.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Охрана конфиденциальности информации осуществляется в рамках трудовых отношений. В целях охраны конфиденциальности информации работодатель обязан:

1)ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с ***перечнем информации***, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;

2)ознакомить под расписку работника с установленным работодателем ***режимом коммерческой тайны*** и с мерами ответственности за его нарушение;

3)создать работнику необходимые ***условия*** для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

Должностные лица органов государственной власти, органов местного самоуправления, государственные или муниципальные служащие не вправе разглашать или передавать другим лицам, органам государственной власти, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях. В случае нарушения конфиденциальности информации должностными лицами органов

государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

Правовое регулирование информационных отношений в области персональных данных

19 декабря 2005 года Россией была ратифицирована Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Вслед за этим 27 июля 2006 года был принят Федеральный закон «О персональных данных», который вступил в силу в январе 2007 года.

После вступления в силу Закона о персональных данных в России должна будет постепенно формироваться правовая культура защиты персональных данных, которая в некоторых европейских странах была сформирована более 30 лет назад. Необходимость в формировании системы правового обеспечения защиты персональных данных при их автоматизированной обработке в России возникла еще в середине 1990-х годов, когда стали продаваться телефонные и адресные базы данных граждан. Конфиденциальность персональных данных человека постоянно и повсеместно нарушалась, а должная правовая база практически отсутствовала. Отмечалось также, что статей 23 и 24 Конституции РФ о неприкосновенности частной жизни, личной и семейной тайн, о запрете сбора, хранения, использования и распространения информации о частной жизни лица недостаточно, поэтому необходима более развернутая нормативно-правовая база реализации этих конституционных правомочий граждан.

Правовые нормы, регулирующие работу с персональными данными, содержатся также в гл. 14 Трудового кодекса РФ «О защите персональных данных работника», в Законе об архивном деле в Российской Федерации от 22 октября 2004 года (ст. 25), в Законе об оперативно-розыскной деятельности (ст. 3, 5, 9, 10, 12, 21), в Законе РФ «О средствах массовой информации» (ст. 41, 43, 46, 51, 57), Законе об индивидуальном персонифицированном учете в системе государственного пенсионного страхования и др.

Под персональными данными понимается «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе и его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация». Несмотря на то что Закон о персональных данных содержит определенный перечень сведений, которые относятся к персональным данным человека, данный перечень является далеко не исчерпывающим, поскольку ис-

ходя из самой природы персональных данных полностью их перечислить довольно сложно, да и не нужно. Ключевой в определении персональных данных является оговорка «другая информация», подразумевающая любую информацию, позволяющую легко идентифицировать человека, которая и будет являться персональными данными, поэтому и нет необходимости приводить полный перечень персональных данных человека.

Закон содержит понятие «оператор», под которым понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных (п. 2 ст. 3 Закона о персональных данных).

Относительно деятельности СМИ и журналистов при работе с персональными данными Закон содержит норму, в соответствии с которой эти данные могут обрабатываться без предварительного получения согласия субъекта персональных данных в случае, когда такая «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» (п. 6 ч. 2 ст. 6).

В свою очередь, под понятием «обработка персональных данных» Закон понимает действия (операции) с такими данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе и передачу), обезличивание, блокирование, уничтожение персональных данных.

Обязательное требование – соблюдение конфиденциальности персональных данных, т.е. недопущение их распространения без согласия субъекта персональных данных, – касается не только оператора, но и любого иного лица, получившего доступ к указанным данным.

Закон оговаривает случаи, когда возможно распространение персональных данных без получения согласия субъекта, например, когда обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных и получение его согласия невозможно или когда осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе и персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, кандидатов на выборные государственные или муниципальные должности.

Статья 5 Закона о персональных данных устанавливает **шесть принципов обработки персональных данных,** защищающих персональную информацию человека. Во-первых, **персональные данные должны собираться и использоваться законно и добросовестно**. Эта норма говорит о том, что персональные данные должны быть собраны и использованы в соответствии с законодательством Российской Федерации и только с

согласия субъекта этих данных. Согласие на обработку своих персональных данных субъект персональных данных должен дать в письменной форме. При этом необходимо указать цель обработки персональных данных и их перечень, а также срок, в течение которого действуют согласие и порядок его отзыва.

Во-вторых, заранее **четко определенные цели использования персональных данных не должны изменяться**. Персональные данные не могут собираться и использоваться для иных целей, о которых субъект, давший письменное согласие на обработку своих данных, не был заранее информирован (п. 2 ч. 1 ст. 5).

В-третьих, **объем, характер и способы обрабатываемых персональных данных должны соответствовать целям** этой обработки. Данная норма направлена на исключение ситуаций, когда при сборе персональных данных пытаются получить иную персональную информацию, выходящую за рамки объявленных целей.

В-четвертых, персональные данные должны быть **достоверными**, а объем собираемой информации должен быть оправдан целями ее сбора. **Объем** собираемых персональных данных **не должен быть избыточным.** Если обнаружено, что были допущены ошибки и персональные данные неточны, субъекту указанных данных принадлежит право внести необходимые изменения (п. 3 ст. 20).

В-пятых, Закон **запрещает объединение персональных данных**, которые были собраны операторами персональных данных для разных целей, **в единую информационную систему**. Эта норма направлена на то, чтобы избежать ситуации, когда оператор связи содержит базу персональных данных человека, и в случае утечки такой базы человек будет уязвим перед несанкционированным и недобросовестным использованием этих сведений.

И наконец, в-шестых, хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. **Они подлежат уничтожению** по достижении целей обработки или в случае утраты необходимости в их достижении. Норма также направлена на защиту субъекта персональных данных от несанкционированного их использования.

Оператор и третьи лица, получившие доступ к персональным данным, должны обеспечивать их конфиденциальность (ст. 7), за исключением случая обезличивания персональных данных, когда невозможно по ним идентифицировать конкретного человека и относительно общедоступных персональных данных, которые в соответствии со ст. 8 Закона могут содержаться в адресных книгах, справочниках и иных общедоступных источниках персональных данных с согласия их субъекта.

Закон не допускает автоматизированную обработку так называемых специальных категорий персональных данных граждан, т.е. «чувствительной информации», к которой относится информация, касающаяся

расовой, национальной принадлежности человека, его политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Что касается сведений о судимости, они также относятся к специальной категории персональных данных человека и могут обрабатываться государственными и муниципальными органами только в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации.

Субъект персональных данных обладает следующими правами: правом на доступ к своим персональным данным; правом требовать от оператора уточнения своих персональных данных, а также их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; имеет право принимать предусмотренные Законом меры по защите вышеуказанных прав; а также запретительные права относительно использования персональных данных в целях продвижения товаров, работ, услуг на рынке, а также политической агитации.

Лица, виновные в нарушении требований Закона о персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Тема 16. ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Понятие ответственности в информационном праве

С точки зрения правовой доктрины юридическая ответственность – это «обязанность лица подвергнуться мерам государственного принуждения за совершенное правонарушение. Меры эти могут быть:

– личного характер (лишение свободы);
– имущественного характера (штраф);
– организационного характера (увольнение)»[76].

Юридическая ответственность является общеправовым институтом, который включен во все отрасли права и законодательства и реализуется с учетом специфики различных отраслей права, в которых возникают противоправные ситуации.

Можно сказать, что в сфере информационного законодательства институт ответственности действует как общеправовой институт права, характерный для любой отрасли права, и как специальный институт ин-

[76] *Малько А.В.* Теория государства и права: Учеб.-метод. пособие. М., 2005. С. 202.

формационного права, учитывающий особенности предметной области информационных правоотношений.

Таким образом, **институт ответственности в информационном праве представляет собой систему норм, реализуемых в целях пресечения правонарушений и установления вида и меры наказания за совершенные преступления или иные правонарушения в сфере информационных правоотношений.**

Особенности информационных правонарушений

Информационное правонарушение – это общественно опасное, противоправное виновное деяние деликтоспособного лица (лиц) в информационной сфере, т.е. области человеческой деятельности, непосредственно или опосредованно связанной с созданием, передачей, получением, обработкой, изменением, хранением, защитой и использованием информации, либо совершенное с применением информационных средств в иных сферах человеческой деятельности[77]. Следовательно, информационное правонарушение – разновидность правонарушений, которое обладает следующими признаками:

1)объектом является особый вид общественных отношений, складывающихся по поводу или в связи с удовлетворением информационных потребностей личности, общества государства;

2)предметом посягательств являются информация и производные от нее продукты;

3)используются определенные информационные средства и технологии.

Правонарушения в информационной сфере отличаются некоторыми характерными особенностями. Выделим некоторые из них.

1.**Субъектный состав**. К правонарушителям могут относиться физические, должностные и юридические лица, органы государственной власти или органы местного самоуправления. Особенность состоит также в том, что чаще всего это высокообразованные люди, обладающие специальными знаниями и навыками в области применения информационных технологий и работе с информацией, или ответственные исполнители установленных законодательством действий.

Причем они могут иметь легальный доступ к информационным ресурсам, программному обеспечению и технике, поскольку этого требует исполнение их непосредственных трудовых функций или служебных обязанностей (например, государственные служащие, в чьи обязанности входит размещение в электронной форме информации о госзаказах, ответы на обращения и запросы граждан).

---

77 См.: *Полушкин А.В.* Признаки информационных правонарушений // Конфликты в информационной сфере: Материалы теоретического семинара Сектора информационного права. Института государства и права РАН. 2008 г. М., 2009. С. 151.

Правовой проблемой являются неопределенность правового статуса некоторых субъектов правоотношений (особенно, если эти правоотношения протекают в Интернете) и как, следствие, трудности возложения ответственности.

2. **Большая общественная опасность**. Для информационной сферы, как ни для какой другой, характерно наличие ситуаций, когда может пострадать неопределенное (очень большое) число субъектов. В случае применения информационного оружия – общество в целом, государственные интересы. Если распространяется недостоверная реклама (когда биодобавки или косметические средства продаются в качестве лекарств от рака, артрита и т.д.), в массовом масштабе происходит умышленный обман людей, которые надеются на избавление от болезни, поэтому становятся особенно уязвимыми и внушаемыми. Известны случаи, когда распространение слухов приводило к возникновению паники в пределах целого города.

Оружием массового поражения в информационной среде являются компьютерные вирусы. Например, вирусом Mydoom было заражено 600 тыс. компьютеров в течение нескольких дней. В результате пострадали не только зараженные компьютеры, но и серверы провайдеров, которые обслуживают передачу электронной почты. Объектами нападения вируса Sasser стали около 300 млн компьютеров. Сообщения об атаках этого вируса поступали из России, Тайваня, Италии и Финляндии. На некоторое время вышли из строя электронные системы итальянских железных дорог и полиции. Звучат предупреждения о том, что «новые поколения вирусов способны привести к краху мировой финансовой системы и инфраструктуры, включая электросистемы, водопровод, транспортные коммуникации, остановить работу целых отраслей промышленности»[78].

3. **Сложность установления объективной стороны правонарушения:**

– трудности установления **места и времени правонарушения**, поскольку оно может быть зафиксировано не на территории определенного города или государства и сферы его юрисдикции, а в Интернете – информационном пространстве без границ, тогда не понятно, что считать «местом правонарушения» в классическом смысле слова, законодательство какой страны применять.

Выставленная в Интернете информация находится как бы вне времени, поскольку она может быть заархивирована и ее легко найти;

– сложность фиксации самого правонарушения с учетом совмещения процедур обмена документированной информацией и ее обращения в виртуальном пространстве информационных коммуникаций, необходимость проведения сложных процессуальных действий.

---

[78] *Акопов Г.Л.* Указ. соч. С. 238.

4. **Несовершенство действующего законодательства**, несоответствие форм и методов борьбы специфике правонарушений, наличие ряда правовых пробелов в информационном праве.

Информационно-правовое регулирование не носит системного характера, с этим связана определенная противоречивость правовых норм, регулирующих информационные правоотношения в различных сферах социальной и экономической жизни. Это осложняет противодействие и квалификацию правонарушений.

5. **Пренебрежение информационными правами и обязанностями**. Наблюдается недооценка информационных прав в публичной сфере в силу их неимущественного характера. Граждане не обращаются за защитой своих прав, когда их не информируют о чем-то, скрывают или выдают неполную информацию.

Виды ответственности в информационной сфере обычно классифицируются по степени опасности для общества и по методам реализации полномочий правоохранительных органов в этой области. С учетом степени опасности правонарушения делятся на преступления, административные правонарушения, служебные и дисциплинарные проступки, гражданско-правовые деликты.

Гражданско-правовая ответственность

Особенностью применения гражданско-правовой ответственности является **имущественный характер** принудительных мер воздействия на правонарушителя, например **возмещение убытков, взыскание неустойки, компенсация морального вреда**. Меры гражданско-правовой ответственности предусмотрены информационным законодательством и Гражданским кодексом РФ.

Например, ст. 152 ГК РФ предусмотрено право граждан требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Наряду с опровержением таких сведений гражданин вправе требовать возмещения убытков и морального вреда, причиненных их распространением.

Статья 152 ГК РФ предусматривает, что «по требованию заинтересованных лиц допускается защита чести и достоинства гражданина и после его смерти». В качестве заинтересованных лиц вправе выступать, например, родственники умершего. При этом следует иметь в виду, что по смыслу этой статьи с требованием о компенсации морального вреда вправе обращаться только «гражданин, в отношении которого распространены сведения, порочащие его честь, достоинство или деловую репутацию». Именно он несет нравственные или физические страдания, которые возмещаются (компенсируются) нарушителями. Как следствие, и взыскание компенсации морального вреда невозможно помимо воле-

изъявления пострадавшего. Данная позиция достаточно четко выражена в Обзоре судебной практики Верховного Суда РФ за I квартал 2000 года.

Согласно п. 7 ст. 152 ГК РФ «правила о защите деловой репутации гражданина соответственно применяются к защите деловой репутации юридического лица». При этом юридические лица вправе, во-первых, защищать только свою деловую репутацию, а не честь и достоинство, которыми они обладать не могут. Во-вторых, они имеют право только на опровержение или ответ, но не на компенсацию морального вреда. По своей природе они не могут испытывать нравственные или физические страдания и, следовательно, не вправе требовать компенсации морального вреда. На недопустимость взыскания морального вреда в пользу юридических лиц неоднократно обращалось внимание в решениях Высшего Арбитражного Суда РФ. В частности, Президиум ВАС в Постановлении от 5 августа 1997 года № 1509/973 указал, что «исходя из смысла статьи 151 Гражданского кодекса Российской Федерации моральный вред (физические и нравственные страдания) может быть причинен только гражданину, но не юридическому лицу». В то же время с требованиями о компенсации морального вреда вправе обратиться учредители юридического лица, его акционеры, работники и другие лица, чьи права оказались нарушенными в результате распространения порочащих сведений о самом юридическом лице. Однако в этом случае истцы должны доказать связь между ущемлением деловой репутации юридического лица и собственным моральным вредом.

Как следует из ст. 151 ГК РФ, моральным вредом являются испытываемые лицом нравственные или физические страдания. Более подробно понятие морального вреда раскрывается в Постановлении Пленума Верховного Суда РФ от 20 декабря 1994 года (№ 10) «Некоторые вопросы применения законодательства о компенсации морального вреда». Согласно данному постановлению «под моральным вредом понимаются нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага (жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п.) или нарушающими его личные неимущественные права (право на пользование своим именем, право авторства и другие неимущественные права в соответствии с законами об охране прав на результаты интеллектуальной деятельности), либо нарушающими имущественные права гражданина. Моральный вред, в частности, может заключаться в нравственных переживаниях в связи с утратой родственников, невозможностью продолжать активную общественную жизнь, потерей работы, раскрытием семейной, врачебной тайны, распространением не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина, временным ограничением или лишением каких-либо прав, физической болью, связанной с причи-

ненным увечьем, иным повреждением здоровья либо в связи с заболеванием, перенесенным в результате нравственных страданий и др.».

Обязанность доказывания факта причинения и степени морального вреда лежит на заявителе. Поэтому он должен предоставить суду убедительные доказательства причинения ему нравственных или физических страданий, а также наличия причинно-следственной связи между действиями ответчика и фактом страданий. Размер компенсации морального вреда определяется судом. Истцы предъявляют требования о компенсации, начиная с суммы в один рубль и заканчивая миллионами долларов. Суды, в свою очередь, взыскивают моральный вред в размере от одного рубля до нескольких сотен тысяч рублей.

Другим примером наступления гражданско-правовой ответственности является право потребителя потребовать от продавца уплаченной за товар суммы и возмещения других убытков, если ему не была предоставлена необходимая и достоверная информация о товаре (ст. 495 ГК РФ). Продавец, не предоставивший покупателю возможность получить соответствующую информацию о товаре, несет ответственность и за недостатки товара, возникшие после его передачи покупателю, в отношении которых покупатель докажет, что они возникли в связи с отсутствием у него такой информации.

Гражданско-правовая ответственность может наступить и в том случае, если права и законные интересы нарушаются путем разглашения информации ограниченного доступа или иным неправомерным использованием такой информации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования защиты информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица (ст. 17 Закона об информации).

Например, специальные меры гражданской защиты применяются в отношении секретов производства. Статья 1465 ГК РФ определяет, что секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе и о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. Обладатель секрета производства распоряжается исключительным правом на этот секрет.

Субъектом правонарушения в данном случае может быть одно из следующих лиц:

1)**неправомерно** получившее сведения и затем разгласившее или использовавшее их;

2)получившее доступ к этим сведениям **правомерно,** например по договору об отчуждении исключительного права (ст. 1468 ГК РФ) или по лицензионному договору (ст. 1469 ГК РФ), и разгласившее эти сведения;

3)получившее доступ к сведениям в связи с **выполнением своих трудовых обязанностей** либо заданием работодателя и не соблюдающее обязанности по сохранению конфиденциальности. Формой ответственности нарушителя является возмещение убытков обладателю ноу-хау.

Своеобразная природа секрета производства обусловливает вероятность освобождения от ответственности. Это возможно, если лицо, использовавшее секрет производства, не знало о незаконности своего действия. Кроме того, лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет.

Административная ответственность

Для административно-правовых норм характерно то, что их действие распространяется на неопределенный круг лиц, не ограничивается однократным исполнением, они действуют постоянно и многократно во всех случаях, когда есть условия, предусмотренные данной нормой[79].

Субъектами административного правонарушения согласно ст. 2.1 КоАП РФ являются **физические и юридические лица**. Большинство статей, регламентирующих ответственность в информационной сфере в гл. 13, предусматривают ответственность юридических лиц. Это так называемые специальные составы, поскольку объектом правонарушения являются отношения в области информации и связи.

Указанная глава предусматривает ответственность за такие правонарушения в информационной сфере, как нарушение установленного законом порядка сбора, хранения, использования и распространения информации о гражданах (персональных данных) (ст. 13.11), правил защиты информации (ст. 13.12), незаконная деятельность в области защиты информации (ст. 13.13), разглашение информации с ограниченным доступом (ст. 13.14), злоупотребление свободой массовой информации (ст. 13.15), воспрепятствование распространению продукции средства массовой информации (ст. 13.16), нарушение порядка представления статистической информации (ст. 13.19), правил хранения, комплектования, учета или использования архивных документов (ст. 13.20), порядка изготовления или распространения продукции средства массовой информации (ст. 13.21),

---

79 См.: *Козлов Ю.М.* Административное право. М., 2005. С. 87.

порядка представления обязательного экземпляра документов (ст. 13.23), требований законодательства о хранении документов (ст. 13.25).

Кроме того, Кодексом об административных правонарушениях предусмотрены составы, в которых основным объектом правонарушения являются другие (не информационные) права и свободы лиц, информационные правоотношения выступают дополнительным объектом. Например: нарушение права граждан на ознакомление со списком избирателей, участников референдума (ст. 5.1), изготовление, распространение и размещение агитационных материалов с нарушением требований законодательства о выборах и референдумах (ст. 5.12), непредоставление возможности обнародовать опровержение или иное разъяснение в защиту чести, достоинства или деловой репутации (ст. 5.13), сведений об итогах голосования или о результатах выборов (ст. 5.25), отказ в предоставлении гражданину информации (ст. 5.39), сокрытие или искажение экологической информации (ст. 8.5), нарушение законодательства о рекламе (ст. 14.3), представление ложных сведений для получения удостоверения личности гражданина (паспорта) либо других документов, удостоверяющих личность или гражданство (ст. 19.18).

Статья 5.39 вводит административную ответственность в виде штрафа до 1000 руб. за отказ в предоставлении гражданину информации. Данная статья содержит 5 составов правонарушения:

1)неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов;

2)несвоевременное предоставление таких документов и материалов;

3)непредоставление информации;

4)предоставление гражданину неполной информации;

5) предоставление гражданину заведомо недостоверной информации.

Важно отметить следующее: статья сформулирована так, что применение санкции не освобождает должностное лицо от исполнения обязанностей по предоставлению информации, т.е. после наложения штрафа чиновник обязан предоставить информацию, иначе возможно опять применение этой статьи.

В качестве санкций по данным составам применяются такие административные наказания, как предупреждение, административный штраф, конфискация технических средств и административное приостановление деятельности.

Предупреждение – мера административного наказания, выраженная в официальном порицании физического или юридического лица. Предупреждение выносится в письменной форме.

Административный штраф – денежное взыскание, выраженное в рублях и установленное для граждан в размере, не превышающем 5 тыс. руб., для должностных лиц – 50 тыс. руб., для юридических лиц – 1 млн руб.

Конфискация орудия совершения или предмета административного правонарушения – принудительная безвозмездная передача его в федеральную собственность или собственность субъекта Российской Федерации.

Административное приостановление деятельности – временное прекращение деятельности лиц, осуществляющих предпринимательскую деятельность, юридических лиц, их филиалов, представительств, структурных подразделений и т.д. Это относительно новый вид ответственности, который применяется в случае угрозы жизни или здоровью людей либо в случае совершения административного правонарушения в области общественного порядка и общественной безопасности. В соответствии с законодательством Российской Федерации за правонарушения в информационной сфере может быть приостановлена деятельность политической партии, общественного объединения, религиозной организации, средства массовой информации. Перечень общественных и религиозных объединений, деятельность которых приостановлена в связи со своей экстремистской направленностью, подлежит размещению в международной компьютерной сети Интернет на сайте федерального органа исполнительной власти, осуществляющего функции в сфере регистрации общественных и религиозных объединений. Указанный перечень также подлежит опубликованию в официальных периодических изданиях, определенных Правительством РФ.

Административное приостановление деятельности назначается судьей только в случаях, предусмотренных статьями Особенной части КоАП, если менее строгий вид административного наказания не сможет обеспечить достижение цели административного наказания.

Уголовная ответственность

Уголовная ответственность – самый строгий вид юридической ответственности. Она носит только личный характер, т.е. возлагается на виновное в совершении преступления физическое лицо. Основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного УК РФ.

Уголовное законодательство РФ содержит значительное количество норм, в соответствии с которыми деяния, совершенные в информационной сфере, признаются преступлениями.

Рассмотрим некоторые из них.

Согласно ст. 140 **неправомерный отказ должностного лица в предоставлении информации** либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, наказываются в размере до 200 тыс. руб. или в размере заработной платы до 18 месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет.

Для данного правонарушения характерен материальный состав – моментом окончания преступления будет считаться наступление вредных последствий (например, неполучение пенсии, пособия, тех или иных благ, льгот). Именно наступление вредных последствий отличает эту норму от подобной нормы Кодекса об административных правонарушениях.

Еще более серьезная ответственность предусматривается за **сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей** (ст. 237): сокрытие или искажение информации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией, наказываются штрафом в размере до 300 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 2 лет либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового. Если это преступление совершено лицом, занимающим государственную должность или главой органа местного самоуправления, а также в том случае, если причинен вред здоровью людей или наступили иные тяжкие последствия, наказание усиливается: штраф возрастает до 500 тыс. руб., срок лишения свободы – до 5 лет.

В рассматриваемой нами ст. 237 УК РФ состав преступления – формальный. Это значит, что преступление является оконченным с момента сокрытия либо искажения информации. Наступление вредных последствий не обязательно.

Уголовное законодательство устанавливает значительное количество норм, в соответствии с которыми нарушение **правовых режимов различных видов тайн**, признаются уголовными преступлениями.

Статьей 137 предусматривается, что незаконный сбор или распространение сведений о **частной жизни лица, составляющих его личную или семейную тайну**, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются штрафом в размере до 200 тыс. руб. либо обязательными работами на срок до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 4 месяцев.

Личную и семейную тайну могут составлять сведения, не подлежащие, по мнению заинтересованного в этом лица, оглашению. Это не обязательно должны быть факты, вызывающие неприязнь или осуждение, может быть, напротив, они вызывают жалость, сочувствие. Тем не менее лицо не хочет, чтобы об этом знали посторонние. Его желание является определяющим.

Личную, семейную тайну не могут составлять сведения, которые уже были ранее опубликованы либо оглашены каким-либо другим способом.

Незаконный сбор информации может осуществляться разными способами: с помощью прослушивания телефонных разговоров, разговоров, которые ведутся в частном порядке, проведения опросов граждан о частной жизни лица, в частности, под видом следователя или работника милиции.

Незаконность подобных действий, как правило, определяется следующими условиями:

1)отсутствием согласия со стороны потерпевшего;

2)тем, что лицо, собирающее такие сведения, не уполномочено законом на данную деятельность;

3)при сборе информации используются средства и методы, прямо запрещенные законом: обман, хищение документов, нарушение тайны переписки, телефонных переговоров и т.д.

Статья 138 защищает **тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений**. Наказание предусматривает в худшем случае ограничение свободы на срок до 3 лет.

В соответствии со ст. 183 сбор сведений, составляющих **коммерческую, налоговую или банковскую тайну**, путем похищения документов, подкупа или угроз, а равно иным незаконным способом наказывается штрафом в размере до 80 тыс. руб. либо лишением свободы на срок до 2 лет. Если же разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, было произведено лицом, которому она была доверена или стала известна по службе или работе, или если указанные действия привели к тяжким последствиям, наказание усиливается, и в худшем случае срок лишения свободы может быть увеличен до 10 лет.

Сразу несколько статей Уголовного кодекса РФ защищают **государственную тайну**. Это статьи 275 «Государственная измена», 276 «Шпионаж», 283 «Разглашение государственной тайны», 284 «Утрата документов, содержащих государственную тайну». Самые серьезные санкции предусматривают срок лишения свободы до 20 лет.

Кратко можно заметить, что разглашение государственной тайны включает в себя три основных компонента:

1)специальный субъект – лицо, которому были доверены сведения, составляющие такую тайну;

2)огласка им сведений, подлежащих соответствующей защите;

3)адресат этих сведений – лицо, не имеющее доступа к конкретной секретной информации.

Разглашение тайны может быть как результатом действия, так и бездействия, например, если оставить без присмотра документы, содержащие государственную тайну. Средства огласки различны: в разговоре,

переписке, публичном выступлении, публикации в средствах массовой информации, при демонстрации документов, изделий.

Разглашение государственной тайны является оконченным с момента, когда указанные сведения стали достоянием адресата – постороннего лица.

Если сведения передаются иностранному государству, иностранной организации или их представителям в целях проведения враждебной деятельности в ущерб безопасности Российской Федерации, эти действия будут считаться государственной изменой.

Статьями УК РФ устанавливаются санкции за распространение **вредной информации**. К таковой относятся: клевета (ст. 129), оскорбление (ст. 130); незаконное распространение порнографических материалов или предметов (ст. 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1), публичные призывы к осуществлению экстремистской деятельности (ст. 280), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282); публичные призывы к развязыванию агрессивной войны (ст. 354).

Клевета характеризуется заведомой ложностью распространяемых сведений, их надуманностью. В случае применения гражданско-правовой ответственности за распространение порочащих лицо сведений, не соответствующих действительности, не имеет значения вина распространившего указанные сведения лица. При применении уголовной ответственности за клевету лицо, распространяющее порочащие сведения, заранее (заведомо) знает о том, что они ложные, но, несмотря на это, сознательно использует все возможные способы для ее распространения, понимая, какой ущерб подобные сведения могут нанести потерпевшему, и желает умаления чести и достоинства потерпевшего.

Клевета, распространенная через средства массовой информации, обладает наибольшей общественной опасностью. Поэтому за клевету, распространенную в публичном выступлении, демонстрирующемся произведении или средствах массовой информации (ч. 2 ст. 130), предусмотрено более серьезное наказание.

Иногда сложно провести различие между клеветой и оскорблением. Можно выделить несколько отличительных моментов.

При клевете сознательно злоупотребляют содержанием, сущностью сведений, распространяются заведомо ложные измышления, преследующие цель опорочить гражданина в глазах семьи, друзей, знакомых, коллектива, где он работает или учится. Она всегда направлена на восстановление общественного мнения против данного гражданина.

Оскорбление же, как правило, вызывает личную обиду потерпевшего и может не сопровождаться изменением общественного мнения по отношению к нему.

Для клеветы не имеет значения форма выражения измышлений. Она может быть приличной, допустимой и неприличной. Оскорбление – это

унижение чести и достоинства другого лица, выраженное в неприличной форме. Таким образом, именно неприличная форма является определяющей при квалификации данного преступления. С точки зрения уголовного законодательства оскорбление может быть нанесено в устной форме и письменно, а также выражено в неприличных действиях. В связи с этим как оскорбляющие честь и достоинство можно рассматривать не только текстуальные выражения, но и изображения личности (шаржи, карикатуры), если они выполнены в неприличной форме.

Таким образом, в уголовных делах по статьям 129 и 130 решающее значение имеют вина лица, распространяющего порочащие сведения, и форма, в которой эти сведения выражены.

Другим преступлением в информационной сфере являются действия, направленные на **возбуждение ненависти, вражды, унижение достоинства человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе** (ст. 282), совершенные публично или с использованием средств массовой информации. Такие действия наказываются штрафом в размере до 300 тыс. руб., а в худшем случае – лишением свободы на срок до 2 лет. Распространение взглядов, идей, мнений, которые подрывают уважение к конкретной расе или национальности, религиозной конфессии или социальной группе, вызывают неприязнь к образу жизни, культуре, религиозным обрядам людей той или иной расы и национальности, незаконно. Главным при распространении негативных оценок является желание унизить, оскорбить, показать ущербность людей, принадлежащих к той или иной национальной, социальной и религиозной группе. Обязательным условием привлечения к уголовной ответственности по данной статье УК РФ является публичность таких действий или использование СМИ.

Важно отметить, что содержание указанных норм УК РФ переносятся правоприменителем на отношения по распространению информации в Интернете, несмотря на неопределенность правового статуса источников информации.

Например, в феврале 2008 года было возбуждено первое уголовное дело, поводом к которому послужил комментарий в живом журнале. Это дело Саввы Терентьева, который в одной из записей в блоге известного журналиста грубо отозвался о работниках правоохранительных органов.

Последовавшая за этим социогуманитарная экспертиза установила, что текст, написанный Терентьевым, направлен на возбуждение ненависти и вражды, а также на унижение достоинства группы лиц по принадлежности к социальной группе, совершенных публично. Блогеру было предъявлено обвинение по ст. 282 УК РФ: «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства». Терентьев был осужден, ему назначили штраф и 1 год лишения свободы условно с испытательным сроком в 1 год.

Одной из важных проблем является **незаконное распространение порнографических материалов, а также детской порнографии** (ст. 242, 242.1). Интернет-технологии являются идеальным инструментом для распространения такого рода материалов, поэтому с его развитием такие преступления получили «второе дыхание».

Согласно данным Фонда интернет-наблюдений – организации по борьбе с противозаконной деятельностью в Интернете, 28,2% всех сайтов с детской порнографией размещались на хостинговых площадках России. Трудности законодательной борьбы с детской порнографией заключаются в том, что это преступление носит двойственный характер. С одной стороны, детская порнография (если она не является компьютерной графикой) изначально предполагает насилие над ребенком – незаконное вовлечение его в действия сексуального характера, их съемку и распространение. С другой стороны, просмотр порнографических материалов является соучастием в насилии над ребенком[80]. Поэтому в ряде стран (Канада, США, Великобритания) преступлением считаются не только производство, передача, публикация, продажа, экспорт и импорт детской порнографии, но и ее просмотр, а также запрос в Интернете. В России с 2003 года действует норма, согласно которой запрещены изготовление, хранение, распространение, публичная демонстрация или рекламирование, перемещение через государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования материалов с порнографическими изображениями заведомо несовершеннолетних, а также их привлечение в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера. Это преступление наказывается лишением свободы сроком до 6 лет, а в случаях с отягчающими обстоятельствами – до 8 лет.

Однако просмотр детской порнографии в домашних условиях не является преступлением, что является существенным недостатком данной нормы.

В связи с распространением противозаконной информации различных видов в Интернете возникает вопрос о возложении ответственности за ее размещение на провайдеров, поскольку зачастую возникают проблемы с установлением подлинного автора этой информации. В то же время именно провайдер имеет больше всего организационных и технических возможностей для пресечения подобных правонарушений. Для того чтобы провайдеры могли контролировать содержание контента, предлагается законодательно закрепить их право на проведение проверок и блокирование информации, распространение которой запрещено. Если же провайдер не может самостоятельно решить вопрос о законности/незаконности информации, он обращается в компетентные органы.

---

80 См.: *Кобзева С.* Законодательные меры по борьбе с детской порнографией в Интернете: мировой опыт и российские реалии // Информационное право. 2009. № 2. С. 23.

На сегодняшний день, согласно рекомендациям представителя ОБСЕ, международная практика и российское законодательство исходят из того, что «провайдер не должен привлекаться к ответственности просто за передачу или размещение контента»[81]. Федеральный закон «Об информации» устанавливает, что в случае распространения ограниченной или запрещенной федеральными законами информации «гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1)либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2)либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации» (п. 3 ст. 17).

Провайдер должен нести ответственность за качество информации, размещаемой на его сервере, только в следующих случаях:

– если данная информация размещалась по его инициативе или за его счет;

– провайдер был осведомлен или имел возможность быть осведомленным о содержании этой информации;

– преднамеренные или непрофессиональные действия провайдера повлекли размещение незаконной информации на его сервере.

Характеристика компьютерных преступлений

Первое преступление, совершенное с использованием компьютера в Советском Союзе, официально зарегистрировано в 1979 году в Вильнюсе. Тогда, по оценке правоохранительных органов, нанесенный ущерб государству составил 78,5 тыс. руб. (90 тыс. долл.). Данное происшествие было зафиксировано в международном реестре правонарушений в области компьютерной преступности и явилось своеобразной точкой отсчета зарождения и дальнейшего развития этого вида преступлений в нашей стране[82].

Борьба с киберпреступностью является, пожалуй, самой обсуждаемой в информационном праве. Предлагаются различные классификации компьютерных преступников. Классической является следующая классификация:

1)нарушители правил пользования ЭВМ – совершают преступления из-за недостаточного знания техники, желания ознакомиться с интересующей их информацией, похитить какую-либо программу или бесплатно пользоваться услугами ЭВМ;

---

[81] Рекомендации представителя ОБСЕ по вопросам свободы СМИ: Справочник по свободе массовой информации в Интернете. Вена, 2004. С. 15.

[82] См.: *Конявский В.А., Лопаткин С.В.* Компьютерная преступность: В 2 т. М., 2006. Т. 1. С. 100–101.

2)«белые воротнички» – бухгалтеры, казначеи, управляющие финансами различных фирм. Для них характерно использование ЭВМ в целях получения материальной выгоды или сокрытия других преступлений. Наиболее часто совершаемые преступления – компьютерный шантаж конкурентов, фальсификация информации;

3)компьютерные шпионы – хорошо подготовленные в техническом отношении специалисты, целью деятельности которых является получение стратегически важной информации в различных областях;

4)хакеры – наиболее технически и профессионально подготовленные лица, отлично разбирающиеся в вычислительной технике и программировании. Их деятельность направлена на несанкционированное проникновение в компьютерные системы, кражу, модификацию или уничтожение имеющейся в них информации. Зачастую они совершают преступления, не преследуя при этом прямых материальных выгод[83].

Более современной является классификация преступников, предлагаемая профессором В.Н. Черкасовым[84]:

– хакер – запускает программы, автоматически проникающие в сотни включенных в сеть компьютеров, копирует и изменяет данные на чужих компьютерах, блокирует работу сети, программного обеспечения, операционных систем, распространяет вредоносные программы для взлома компьютерной системы и последующего уничтожения информации. При этом проникновение в компьютер чаще всего превращается в источник доходов (хищение средств из банков, дорогостоящего программного обеспечения, промышленный и коммерческий шпионаж);

– кракер – взламывает различные программные продукты, имеющие зашиту от несанкционированного копирования;

– вирмэйкер – создает вредоносные программы – вирусы;

– фрикер – «обманывает» электронные устройства в телефонах, счетчиках, банкоматах, турникетах;

– кардер – занимается изготовлением поддельных электронных карт (кредитных, телефонных и др.).

А.А. Тедеев, рассматривая проблему безопасности информационных ресурсов государственного и муниципального управления, разделяет всех нарушителей на внешних и внутренних по признаку несанкционированного доступа к ресурсам информационной системы[85].

Под внутренними нарушителями понимаются субъекты, имеющие доступ к работе со штатными средствами системы и ее компонентами. К ним могут быть отнесены пользователи (потребители информационных сервисов системы), обслуживающий персонал (администраторы и

---

[83] См.: Компьютерные технологии в юридической деятельности: Учеб.-практ. пособие / Под ред. Н. Полевого, В. Крылова. М., 1994. С. 234.

[84] См.: *Черкасов В.Н.* Дело «балаковских хакеров». Факты и размышления // Информационная безопасность регионов. 2009. № 2. С. 111.

[85] См.: *Тедеев А.А.* Информационное право.. С. 158.

инженеры, отвечающие за эксплуатацию и сопровождение технических средств системы), программисты, отвечающие за разработку и сопровождение общесистемного и прикладного программного обеспечения, другие сотрудники, которым предоставлен доступ к помещению, где расположено оборудование. Таким образом, к внутренним нарушителям относятся высококвалифицированные специалисты в области разработки и эксплуатации программного обеспечения и технических средств, которые знают специфику задач, решаемых обслуживающими подразделениями, являются системными программистами, способными модифицировать работу операционных систем, правильно представляют функциональные особенности работы системы и процессы, связанные с предоставлением сервисов системой, могут использовать только штатное оборудование и программное обеспечение, имеющееся в составе системы. Существуют угрозы, связанные с их деятельностью. Путем несанкционированного доступа такое лицо может запустить задачи (программы) по обработке информации, создать и запустить собственные программы с новыми функциями, воздействовать на базовое программное обеспечение, включить в состав средств вычислительной техники собственные технические средства с новыми функциями по обработке информации.

К внешним нарушителям относятся лица, которым не предоставляется санкционированный логический доступ к ресурсам системы и пребывание которых в помещениях с оборудованием без контроля со стороны администраторов системы невозможно.

Внешний нарушитель осуществляет перехват, анализ и модификацию информации, передаваемой по линиям связи, проходящим вне контролируемой территории системы. Он проводит анализ топологии и структуры системы, используя корпоративные или общедоступные сети передачи данных и размещенную в Интернете информацию, реализует попытки несанкционированного доступа к ресурсам системы, используя специальные технические средства, и модификацию служебной или пользовательской системы, что приводит к нарушению работоспособности системы.

В России, как и во всем мире, нарастает криминальная активность в информационной сфере. При этом объектами преступных посягательств являются и информация, и информационно – телекоммуникационные ресурсы, и непосредственно финансовые средства, доступ к которым возможен через глобальные компьютерные сети. Анализ криминальной обстановки показывает, что ежегодно количество выявленных органами внутренних дел преступлений в сфере информационных технологий увеличивается в 1,8–2 раза. Из общего числа уголовных дел, возбужденных по признакам данных составов преступлений, 55% составляет неправомерное использование сетевых реквизитов при авторизации в сети Интернет, 10,6% – компьютерное пиратство (распространение контрафактной программной продукции, в частности, с использованием сети

Интернет), 8% – распространение порнографии, включая детскую, 4,1% – распространение вредоносных программ как в сети, так и на машинных носителях, включая контроллеры ЭВМ.

Анализ личности выявленных преступников дает следующие результаты: 16,3% – лица до 18-летнего возраста, 58,9% – от 18 до 25 лет. Таким образом, свыше 75% выявленных преступников составляет молодежь. Следует отметить, что 67% от общего числа преступников имеют высшее или неоконченное высшее образование, что говорит о высоком интеллектуальном уровне противодействующей стороны.

Подобные преступления носят скоротечный, многоэпизодный, а зачастую и трансграничный характер.

Структурный анализ преступности в сфере высоких технологий показывает, что наиболее распространенными деяниями являются: неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ и нелицензионного программного обеспечения, посягательства на электронно-платежные системы, распространение порнографических материалов с участием несовершеннолетних.

Сложность раскрытия этих преступлений связана с анонимностью интернет-пользователей, техническими особенностями (скоротечность, отсутствие материальных следов), трансграничным характером киберпреступлений и зачастую нежеланием огласки со стороны пострадавших.

В последние годы прослеживается тенденция объединения злоумышленников в транснациональные организованные группы для занятия вымогательством, «кардингом», «фишингом» и др. Для сокрытия своей причастности к совершению преступлений они используют похищенные реквизиты доступа в Интернет, анонимные прокси-серверы, вредоносные программы и другие способы электронной конспирации[86].

Показательным примером деятельности организованной киберпреступной группировки может служить так называемое дело «балаковских хакеров». В октябре 2006 года Балаковским горсудом Саратовской области трое участников были приговорены к восьми годам лишения свободы каждый и штрафу в 100 тыс. руб. Они обвинялись в вымогательстве, создании, использовании и распространении вредоносных программ. Как установило следствие, с октября 2003 по март 2004 года, используя компьютеры, зараженные специальными вирусами, они осуществляли DDoS-атаки на серверы девяти букмекерских контор Велибритании. Электронные взломщики парализовали работу сайтов, заблокировав их, сделав недоступными для клиентов, как раз во время проведения наиболее значимых спортивных соревнований. За прекращение атак они требовали

---

[86] См.: *Сухаренко А.Н.* Транснациональные аспекты российской организованной киберпреступности // Информационное право. 2009. № 3. С. 29.

от 10 до 40 тыс. долл. Одновременно вымогатели придумали и сложную систему легализации средств, поступавших от электронного шантажа. В результате своей деятельности они получили более 4 млн долл. Общая сумма потерь пострадавших компаний составила 73 млн долл. Помимо обвинения в вымогательстве (по УК за такое преступление, совершенное в составе организованной группы, предусмотрено наказание от 7 до 15 лет лишения свободы), подсудимые также были признаны виновными в «создании и распространении вредоносных программ для ЭВМ». Впервые в мире расследование проводилось совместно британской службой SOCA и ФСБ России.

Главную трудность в обвинении хакеров составляло получение необходимых доказательств, что именно они создавали вредоносные программы и участвовали в DDoS-атаках. С участием ученых Саратовского государственного университета был проведен ряд дополнительных экспертиз, в ходе которых на жестких дисках компьютеров, изъятых у обвиняемых, были обнаружены следы создания и распространения вредоносных компьютерных программ, а также следы переписки, указывающей на угрозы в адрес жертв шантажа.

В целях обеспечения эффективного предупреждения и пресечения транснациональных киберпреступлений в 2001 году было принято Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации. С 2004 года Россия является участницей Конвенции ООН против транснациональной организованной преступности. К сожалению, на сегодняшний день наша страна не присоединилась к Конвенции Совета Европы о киберпреступности от 21 ноября 2001 года.

Ответственность за компьютерные преступления

Ответственность за компьютерные преступления предусматривается гл. 28 УК РФ «Преступления в сфере компьютерной информации». Данная глава содержит 3 состава (ст. 272–274).

Статья 272 указывает, что **неправомерный доступ** к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до 200 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2 лет.

То же деяние, совершенное группой лиц по предварительному сговору либо лицом с использованием своего служебного положения, наказывается штрафом в размере 300 тыс. руб. или в размере заработной платы

или иного дохода осужденного за период до 2 лет либо исправительными работами на срок до 2 лет, либо лишением свободы на срок до 5 лет.

Исходя из определения, данного законодателем, можно выделить обязательные признаки неправомерного доступа к охраняемой законом компьютерной информаци

1)общественно опасное **деяние,** к которому законодатель относит **неправомерный доступ** к охраняемой законом информации;

2)общественно опасные **последствия;**

3)наличие **причинной связи** между совершенным деянием и наступившими последствиями.

Отсутствие хотя бы одного из перечисленных признаков исключает уголовную ответственность по ст. 272 УК[87].

Под доступом понимается действие лица с устройствами ЭВМ с целью проникновения к компьютерной информации, в результате чего это лицо получает возможность воздействовать на данную информацию (копировать, блокировать, уничтожать или модифицировать ее).

Исходя из понятия неправомерный «доступ» нельзя считать таковым хищение компьютера или носителя информации. Физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не образует состава этой статьи (речь будет идти об умышленном или неумышленном повреждении имущества).

Неправомерность доступа к информации – обязательный признак, характеризующий рассматриваемое преступление с объективной стороны. УК РФ не дает определения неправомерного доступа к охраняемой информации, он раскрывает лишь последствия: уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

В диспозиции рассматриваемой статьи указывается на неправомерный доступ именно к компьютерной информации, а не к носителям, на которых она содержится. На практике же именно неправомерный доступ к носителям квалифицируется по этой статье.

Возможно двоякое толкование термина «неправомерный доступ» – техническое и юридическое. В техническом плане неправомерный доступ означает доступ к информации, произведенный вследствие несанкционированного преодоления программной, аппаратной или комплексной защиты. Такой защитой может быть пароль на файле документа или вход администратора на сервер с помощью магнитной карты-ключа и ввода усложненного 16-символьного пароля. Преодоление защиты и в первом, и во втором случае с технической точки зрения будет несанкционированным доступом к защищенной информации. Но если для доступа не предусмотрена защита, такой доступ несанкционированным

---

87 См.: Комментарий к Уголовному кодексу Российской Федерации / Под ред. Ю.И. Скуратова, В.М. Лебедева. М., 2001. С. 698.

назвать нельзя. Например, если информация конфиденциального характера расположена на жестком диске компьютера, подключенного к локальной компьютерной сети, и доступ к этим данным открыт с любого компьютера, подключенного к данной сети, можно сказать, что данные общедоступны.

С юридической точки зрения дело обстоит несколько иначе. Ряд авторов обращают внимание на то, что неправомерным признается доступ «**не обладающего правами** на это лица к компьютерной информации, в отношении которой принимаются **специальные меры защиты**, ограничивающие круг лиц, имеющих доступ»[88]. А.В. Сизов указывает еще на две важные характеристики неправомерного доступа: правомерный доступ представляет собой санкционированное владельцем информации ознакомление конкретного лица с информацией; при неправомерном доступе такая **санкция владельца отсутствует**. Кроме того, неправомерность доступа характеризуется нарушением **установленного порядка** доступа к этой информации[89].

А.А. Тедеев обращает внимание на то, что «неправомерным (несанкционированным) считается доступ к информации, нарушающий установленные **правила разграничения доступа**. Неправомерный доступ к информации бывает **непосредственным**, при помощи штатных средств системы либо с использованием специализированных программно-технических средств, и **опосредованным путем внедрения в систему вредоносных программных кодов** (вирусов, компьютерных червей, троянских программ)»[90].

Важно сказать и о необходимости защиты информации ее владельцем. Федеральный закон «Об информации» возлагает на обладателя информации и оператора информационной системы ряд обязанностей. Они должны обеспечить:

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

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;

---

88 *Андреев Б.В., Пак П.Н., Хорст В.П.* Расследование преступлений в сфере компьютерной информации. М., 2001. С. 37.

89 См.: *Сизов А.В.* Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2009. № 1. С. 33.

90 См.: *Тедеев А.А.* Информационное право. С. 172.

6)постоянный контроль за сохранением уровня защищенности информации.

Опасность несанкционированного доступа состоит в том, что он, являясь сам по себе компьютерным правонарушением, создает предпосылки для совершения более тяжких правонарушений.

Систематизированный перечень путей несанкционированного доступа к компьютерной информации выглядит так: считывание данных в массивах других пользователей, чтение остаточной информации после выполнения санкционированных запросов; маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа; маскировка несанкционированных запросов под запросы операционной системы (мистификация); использование программных ловушек; умышленный вывод из строя механизмов защиты[91].

Говоря об общественно опасных последствиях, следует отметить, что в данной статье альтернативно определены уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

В том случае когда неправомерный доступ к компьютерной информации приводит к серьезным повреждениям компьютерной техники и тем самым причиняет значительный ущерб собственнику или владельцу, прибавится дополнительная квалификация за умышленное уничтожение или повреждение имущества.

Данное преступление считается оконченным с момента наступления общественно опасных последствий, перечисленных в диспозиции. В случае если последствия не наступают (даже по независящим от этого лица обстоятельствам), преступление не считается полным. Это будет покушение на преступление.

Но согласно ч. 2 ст. 30 УК РФ уголовная ответственность наступает за приготовление к тяжкому и особо тяжкому преступлению. Данные преступления законодатель относит к преступлениям небольшой и средней тяжести, и поэтому покушения на них не являются уголовно наказуемыми.

Более серьезным преступлением согласно УК РФ будет **создание, использование и распространение вредоносных программ для ЭВМ** (ст. 273).

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до 3 лет

---

[91] См.: *Попов Л.Л., Мигачев Ю.И., Тихомиров С.В.* Информационное право: Учебник. М., 2010. С. 448.

и штрафом в размере до 200 тыс. руб. В случае наступления тяжких последствий срок лишения свободы увеличивается до 7 лет.

Объективная сторона преступления может включать

1)**создание** вредоносных программ;

2)**использование** вредоносных программ;

3)**распространение** таких программ или машинных носителей с такими программами;

4)**внесение изменений** в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ либо их сети.

Иными словами, **каждое** из этих действий уже **является преступлением**.

Вредоносность программы не может определяться способностью уничтожать, блокировать, модифицировать или копировать информацию, так как это рабочие функции очень большого количества программ. Основной **особенностью вредоносных программ** является то, что они выполняют эти функции **без предварительного уведомления и без всякого согласия владельца информации.**

Согласно сложившейся юридической точке зрения в этой области:

– использование вредоносной программы – это **запуск** программы для осуществления ее функций;

– распространение вредоносных программ – **предоставление доступа** к программе для ЭВМ в **машиночитаемом** виде различными способами;

– распространение машинных носителей с вредоносными программами – **передача машинных носителей** либо предоставление возможности пользоваться ими третьим лицам.

Преступление считается оконченным **с момента создания**, использования или распространения вредоносной программы. **Наступления последствий не требуется**. Наступление тяжких последствий – это уже ч. 2 анализируемой статьи. К тяжким последствиям можно отнести:

– гибель людей или причинение вреда их здоровью;

– крупный имущественный ущерб;

– безвозвратную утрату особо ценной информации;

– выход из строя уникальных технических средств;

– длительную приостановку работы предприятия.

Для систем компьютерной информации особую опасность представляют те разновидности вредоносных программ, которые способны к самовоспроизводству и самораспространению. Некоторые из них могут бездействовать длительное время, ожидая для своей активизации наступления заранее определенных условий или внешней команды, или самопроизвольно и скрытно присоединяться к иным файлам, программам или базам данных.

И наконец, третий вид преступлений, выделяемый УК РФ – **нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети** лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет либо обязательными работами на срок до 240 часов, либо ограничением свободы на срок до 2 лет. Если такие действия повлекли по неосторожности тяжкие последствия, наказанием может стать лишение свободы на срок до 4 лет.

Необходимым условием для законного и обоснованного привлечения лица к уголовной ответственности являются наличие и правильность установления правил пользования ЭВМ. Иными словами, **правила эксплуатации должны быть утверждены письменным приказом руководителя**. С этими правилами должны **ознакомиться сотрудники** (под роспись). В ряде случаев им должен быть выдан **специальный допуск**.

Объективная сторона состоит в действии или бездействии и выражается в следующем:

1)**нарушении правил** эксплуатации;

2)уничтожении, блокировании, модификации охраняемой законом информации, **причинивших существенный вред**;

3)**причинной связи** между нарушением правил и наступившими вредными последствиями.

Непосредственно противоправное деяние по рассматриваемой нами статье состоит в несоблюдении или прямом игнорировании определенных правил, обеспечивающих безопасность компьютерной информации.

К существенному вреду можно отнести перебои в производственной деятельности, остановку работы предприятия или организации, необходимость дорогостоящего ремонта вычислительной техники.

Ни одна из статей УК РФ не предусматривает ответственности за DDoS-атаку. На практике правоприменительные органы квалифицируют данные действия именно по ст. 274, исходя из того, что если один компьютер заходил на сайт 1000 раз в секунду, значит, его неправильно использовали, а также нарушались правила использования сети. В то же время ученые-теоретики информационного права говорят о том, что «под сетью понимается только внутренняя сеть ведомства или организации, на которую могут распространяться требования правил и инструкций. Нормы комментируемой статьи относятся только к преступлениям, совершаемым в локальных сетях. По отношению к глобальным сетям, например Интернету, она не применяется»[92].

Это еще одно свидетельство необходимости модернизации института ответственности в сфере информационных отношений.

---

92 *Попов Л.Л., Мигачев Ю.И., Тихомиров С.В.* Информационное право. С. 484.

Для сравнения, Конвенция о киберпреступности включает 7 видов преступлений: противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств (включая компьютерные программы, пароли, коды доступа), подлог и мошенничество с использованием компьютерных технологий.

Одной из наиболее распространенных и применяемых на практике является классификация компьютерных преступлений Генерального секретариата Интерпола. Выделяются следующие основные виды:

– несанкционированный доступ и перехват;

– изменение компьютерных данных (включая такие методы, как применение логической бомбы, троянского коня, компьютерного вируса, компьютерного червя и пр.);

– компьютерное мошенничество (например, с банкоматами, игровыми автоматами, платежными средствами, программами ввода-вывода, телефонное мошенничество);

– незаконное копирование;

– компьютерный саботаж (с аппаратным и программным обеспечением);

– прочие компьютерные преступления (использование досок объявлений, хищение информации, составляющей коммерческую тайну и т.д.).

На основе данной классификации была создана и функционирует специализированная информационно-поисковая система. В настоящее время ее услугами пользуются более чем в 100 странах мира.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Бачило И.Л. Информационное право: Учебник для вузов. М., 2009.
Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. акад. РАН Б.Н. Топорнина. 2-е изд., доп. СПб., 2005.
Городов О.А. Информационное право: Учебник. М., 2007.
Ковалева Н.Н. Информационное право России: Учеб. пособие. М., 2009.
Копылов В.А. Информационное право: Учебник. М., 2004.
Попов Л.Л., Мигачев Ю.И., Тихомиров С.В. Информационное право. М., 2010.
Рассолов И.М. Интернет-право: Учеб. пособие для вузов. М., 2004.
Тедеев А.А. Информационное право: Учебник. М., 2005.
Чаннов С.Е. Информационное право: Пособие для сдачи экзаменов. М., 2006.

Учебное издание

Куликова Светлана Анатольевна

ИНФОРМАЦИОННОЕ ПРАВО РОССИИ

Учебное пособие для студентов,
обучающихся по специальностям (направлениям)
«Юриспруденция» и «Прикладная информатика в юриспруденции»

Редактор *Е.А. Малютина.* Технический редактор *Л.В. Агальцова*
Корректор *Е.Б. Крылова.* Оригинал-макет подготовила *Н.И. Степанова*

Подписано в печать 15.09.2010. Формат 60x84 $^1/_{16}$.
Бумага офсетная. Гарнитура Таймс. Печать офсетная.
Усл. печ. л. 11,39 (12,25). Уч.-изд. л. 11,8.
Тираж 150 экз. Заказ 82.

Издательство Саратовского университета. 410012, Саратов, Астраханская, 83.
Типография Издательства Саратовского университета.
410012, Саратов, Астраханская, 83.