ГОСУДАРСТВО И ПРАВО, 2008, № 6, с. 79–87

ПРАВО И ИНФОРМАТИКА

О ПРАВОВОЙ ОХРАНЕ БАЗ ДАННЫХ

© 2008 г. О. И. Трофимов[1], А. И. Горев[2]

Современное общество определяется как общество информационное. В нем информация стала определяющим ресурсом, порой более значимым, чем природные, трудовые и иные ресурсы. Информация накапливается и собирается, продается и покупается, обменивается и распространяется. Однако следует отметить частичную нерегламентированность процессов информационного обмена, что в отдельных случаях объясняется отсутствием правового регулирования информационных отношений или неверным толкованием юридических норм в новой для общества сфере. Развитие технологического прогресса, наблюдаемого в информационной сфере, существенно опережает развитие информационного права как отрасли юридической науки. Информация (как определяющий ресурс общества и объект правоотношений) требует соответствующего нормативного определения и четкой классификации.

Попытки дать определения информации предпринимаются учеными в течение более чем 100 лет, однако, как отмечает В.А. Копылов, ни философское, ни кибернетическое, ни семантическое, ни иные определения информации, данные в рамках естественных наук, для права неприемлемы, как и неприемлемо, например, регулирование отношений по поводу материи вообще. "Информация как объект правоотношений должна быть конкретизирована, организована должным образом, "привязана" к ситуации и конкретному виду отношений, классифицирована по видам и иным образом "подготовлена" для осуществления по ее поводу действий, регулируемых нормами права"[3].

В Федеральном законе "Об информации, информационных технологиях и защите информации" от 27 июля 2006 г. (далее – Закон об информации) информация определена как "сведения (сообщения, данные) независимо от формы их представления". В литературе приводится множество признаков и свойств информации, находящихся за пределами указанного определения. Так, Ю.И. Черняк, анализируя экономическую информацию, приходит к выводу о существовании пяти ее важнейших свойств: полезности, наличия в ней смысла, знаковой воплощенности, перерабатываемости в определенной алфавитной системе по соответствующим грамматическим правилам, способности воплощаться в различные сигналы и восстанавливаться из них[4]. В.Н. Лопатин, выделяя основные свойства информации, принципиальные для целей правового опосредования отношений по ее поводу, называет в их числе идеальность, количественную определенность, неисчерпаемость, нелинейность, системность, обособленность[5]. В.А. Копылов выделяет свойства физической неотчуждаемости, обособляемости, тиражируемости, организационной формы, информационной вещи и экземплярности[6]. Однако следует отметить, что часть указанных свойств характеризует не саму информацию, а ее носитель. Причем, определяя информационный объект, В.А. Копылов утверждает, что "информация передается и распространяется ***только*** (выделено нами) на материальном носителе или с помощью материального носителя".

Представляется, что перечень указанных особенностей и свойств, несомненно юридически значимых для регулирования информационных правоотношений, не является исчерпывающим. Информация характеризуется свойствами, делающими ее уникальным объектом, в отношении которого в обществе возникают и существуют уникальные правоотношения. Одним из таких свойств является свойство ***критического объема***, заключающееся в хорошо известном переходе количества в качество. Для информации это обязательное свойство заключается в возможном получении новых знаний из анализа большого количества обрывочной, разрозненной, неполной информации. Вся история развития естественных наук строится на переходе от частного к общему: наблюдении, обобщении результатов и фактов с последующим построением теории. В правоприменительной деятельности следователь, собирая разрозненные факты и показания свидетелей, воссоздает полную картину происшедшего.

Возникает правомерный вопрос о применимости и значимости свойства критического объема

[1] Адвокат.
[2] Кандидат юридических наук.
[3] *Копылов В.А.* Информационное право. М., 2002. С. 39.
[4] См.: *Черняк Ю.И.* Информация и управление. М., 1974. С. 62–64.
[5] См.: *Бачило И.Н., Лопатин В.И., Федотов М.А.* Информационное право / Под ред. Б.Н. Топорнина. СПб., 2001. С. 143–145.
[6] См.: *Копылов В.А.* Указ. соч. С. 49–50.

для целей регулирования информационных правоотношений. Это не риторический вопрос: в течение всего периода становления и развития информационного права известное с древних времен свойство не отмечалось исследователями. Ответ заключается в том, что его значимость стала проявляться только в последние годы, когда использование современных алгоритмов обработки информации в совокупности с высокоскоростными вычислительными системами позволило быстро, иногда в режиме "реального времени"[7], производить сложнейший многофакторный анализ информации.

Процессы компьютеризации и информатизации, проходившие последнее десятилетие, затронули все сферы жизни общества. Внедряемые компьютерные технологии позволили существенно ускорить процессы обработки информации, уменьшить трудоемкость операций по сбору, хранению и передаче больших массивов данных. Ранее узкоспециальный термин "база данных" стал широко использоваться в правовой сфере – в текстах более 300 действующих нормативных правовых актов упоминаются базы данных различного назначения. Однако, как правильно отмечает С.И. Семилетов, "ни действующее законодательство, ни имеющиеся проекты законов не рассматривают электронный документ как сложный объект и не учитывают структурные особенности его формирования, разные формы его реального представления, оборота и употребления"[8].

В ст. 1260 ГК РФ база данных определяется как "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 (ЭВМ)". База данных отнесена к составным произведениям, авторские права на которые осуществляются при условии соблюдения прав авторов произведений, использованных для создания составного произведения.

Легальное определение базы данных существенно отличается от традиционного понимания базы данных в информатике как об одной из прикладных задач: совокупность сведений о конкретных объектах реального мира в какой-либо предметной области, представленная в виде набора данных и объектов, связанных общей задачей[9]. Сам термин "данные" в информатике определяется как "информация, с которой имеет дело ЭВМ"; данные различаются как входные, промежуточные и выходные[10]. Существуют элементы данных различных типов в зависимости от значений, которые они могут принимать: числовые (целые и вещественные), текстовые, логические (истина или ложь), календарные даты и т.д. Файл, являющийся совокупностью элементов данных, в зависимости от создавшей его программы может быть любого типа: текстовый, электронной таблицы, графический, мультимедийный, архивный и т.д. Но независимо от типа файла он сохраняется на компьютере в структурированном массиве каталогов и, естественно, может быть найден и обработан с помощью ЭВМ.

Таким образом, можно сделать вывод о том, что законодатель, определяя объективную форму представления и организации совокупности данных (например: статей, расчетов и т.д.) для обработки с помощью ЭВМ должен был определить дефиницию "информационное обеспечение". В состав информационного обеспечения входят базы знаний систем искусственного интеллекта, автоматизированные банки данных – локальные и распределенные, общего и индивидуального назначения[11].

Обращаясь к базам данных, необходимо выделить их основную особенность, отличающую от иного информационного обеспечения. Этим свойством является запись информации в файле базы данных в соответствии со структурой этого файла. Подобно тому, как в карточку из картотеки информация заносится в соответствии с полями, порядок занесения информации в файл базы данных определяется структурой файла. Именно структурированность информации отличает файл базы данных от текстового файла или файла графического изображения. Таким образом, определяя базу данных как объект правового регулирования, следует указать на ее основную особенность: база данных – объективная форма представления и организации совокупности ***структурированных*** данных (например: статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

---

[7] Режим "реального времени" означает способность системы обрабатывать поступающую информацию, не дожидаясь окончания события.

[8] Под основной и первичной формой представления электронного документа С.И. Семилетов понимает в том числе записи в базе данных, которые являются "источником для формирования различных вторичных форм отображения или передачи содержательной информации" (см.: *Семилетов С.И.* Правовые проблемы организации электронного оборота документов в государственном управлении // В кн.: Теоретические проблемы информационного права. М., 2006. С. 163).

[9] См.: *Шафрин Ю.А.* Информационные технологии. М., 2000. С. 302.

[10] Правовая информатика и кибернетика / Под ред. Н.С. Полевого. М., 1993. С. 80.

[11] Вычислительные машины, системы и сети / Под ред. А.П. Пятибратова. М., 1991. С. 22.

По мнению И.Л. Бачило, информационный объект является предметом "комплексного правового регулирования", в том числе посредством права интеллектуальной собственности и вещного права[12]. Сходных взглядов придерживается В.А. Копылов, считая, что база данных как объект информационных правоотношений должна охраняться двумя институтами права – вещной собственности и интеллектуальной собственности. Исходя из двуединства информации и материального носителя, он ввел понятие "информационной вещи", под которой подразумевал информацию как сложную вещь, состоящую из носителя информации и самой информации, отображенной на носителе[13].

Однако мы считаем, что выбор правовых мер охраны базы данных существенно зависит от ее содержания (контента). Для подтверждения выдвигаемого тезиса необходимо детально рассмотреть классификацию баз данных по типу данных и формату хранения информации – документальные, мультимедийные и фактографические. Следует отметить, что базы данных всех типов для удобства пользователя часто распространяются со специальной управляющей программой – программной оболочкой, предназначенной для выполнения операций по поиску и воспроизведению данных.

Документальные базы данных используются для хранения текстовых документов и их библиографических описаний. В настоящее время в связи с широким распространением безбумажных технологий документооборота этот вид информационного обеспечения приобретает все большее распространение. Современный порядок ведения дел на предприятиях и в организациях требует большого объема работы с документами. Процедуры поиска, утверждения и согласования становятся сложными и обременительными. Эффективным подходом в подобной ситуации является использование современных технологий и максимальная автоматизация всех этапов работы с документами. В системах документооборота единицей хранения информации является документ. Системы хранят документы, ведут их историю, обеспечивают их движение по организации, позволяют отслеживать выполнение того, для чего документ готовился. Любой документ в системе документооборота снабжается "карточкой", конкретный набор полей которой определяется типом документа. База данных системы электронного документооборота хранит содержимое полей карточек и сами документы.

В зависимости от комплекса решаемых задач существующие системы документооборота можно классифицировать на электронные архивы, системы маршрутизации и хранения документов, системы делопроизводства. Примером самых простых из них (электронных архивов) являются справочно-правовые системы для хранения нормативной правовой информации. Следует отметить, что в соответствии со ст. 1259 ГК РФ не являются объектами авторских прав официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы. Однако ст. 1260 ГК РФ определяет, что права автора составного произведения охраняются как права на самостоятельные объекты авторских прав независимо от охраны прав авторов произведений, на которых основано произведение.

Более того, справочно-правовые системы распространяются со специальными программами, позволяющими производить обработку данных по сложным алгоритмам. Современные системы документооборота позволяют производить поиск с использованием ключевого слова или метода полного текста. В некоторых системах поисковый механизм, обладающий интеллектом, обеспечивает поиск близких грамматических конструкций.

Системы маршрутизации и хранения документов, системы делопроизводства предназначены для обеспечения процесса документооборота организации. Программа, обеспечивающая работу системы, охраняется авторским правом. Однако обрабатываемые в системе делопроизводства документы могут содержать информацию служебного пользования, что естественным образом меняет статус правовой охраны самой системы. Документальные базы данных, содержащие текстовые документы, в полной мере соответствуют определению ст. 1260 ГК РФ как составные произведения. Эта категория баз данных распространяется и функционирует со специальными программами, предоставляющими сервисные функции по поиску и сопровождению данных. Управляющие программы также охраняются авторским правом. Содержащийся в системах документооборота контент дополнительно может быть объектом охраны институтом служебной, коммерческой или иной тайны.

Мультимедийные базы данных позволяют хранить и обрабатывать в композиции текст, статическую и динамическую графику, звук. Специфическим видом современного информационного обеспечения становятся результаты цифровой

[12] См.: *Бачило И.Л.* О праве собственности на информацию // Труды Института законодательства и сравнительного правоведения. 1992. № 52. С. 71–74.
[13] *Копылов В.А.* Указ. соч. С. 272.

обработки видео- и аудиоинформации с использованием в качестве носителей для их записи и хранения устройств хранения компьютерной информации: CD- и DVD-диски[14] различных модификаций, флэш-карточки[15] памяти. Записанная после операции аналого-цифрового преобразования, видео- и аудиоинформация в форматах хранения компьютерных данных соответствует определению базы данных. Современные устройства обработки компьютерных форматов информации – CD- и DVD-проигрыватели, MP3-плейеры, цифровые диктофоны, фото- и видеокамеры – записывают контент на традиционные для индустрии высоких технологий носители информации. Процессор, обрабатывая информацию, осуществляет аналого-цифровое преобразование сигнала при записи и цифро-аналоговое – при воспроизведении контента.

Мультимедийные базы данных содержат контент, традиционно охраняемый авторским правом: аудио, видео, графические произведения. Независимо от формата записи и вида носителя, мультимедиа-информация распространяется без программ воспроизведения произведений. В настоящее время программы-проигрыватели стали неотъемлемым атрибутом любой операционной системы. Наиболее частым видом правонарушений в данной сфере является нарушение авторских и смежных прав. Однако с развитием и совершенствованием информационных технологий возможно появление новых видов деликтов. Уже сейчас существуют и активно применяются технологии распознавания потокового аудио- и видеосигнала и фиксации его на компьютерный носитель в случае совпадения заданных критериев, в качестве которых могут выступать ключевые фразы в телефонном разговоре[16], марка, цвет и государственный номер проезжающего автомобиля[17] и пр. Поиск и выборка информации по интересующим параметрам проводится автоматически или по запросу оператора. Доступность и относительная дешевизна компьютерных технологий позволяют сделать прогноз о возможном применении в противоправной деятельности в ближайшем будущем мультимедийных баз данных, созданных с использованием технологий распознавания потокового сигнала.

Фактографические базы данных обеспечивают хранение и обработку информации о конкретных фактах или явлениях в структурируемом виде подобно таблицам. Они являются наиболее часто используемым способом хранения и обработки информации конечных пользователей. Базы данных этого типа создаются и часто функционируют под управлением специальных программ – систем управления базами данных. Наиболее близким аналогом простейшей однофайловой фактографической базы данных является картотека, все карточки которой имеют одинаковую структуру и поля заполнения.

Ценность фактографических баз данных определяется спецификой и объемом накопленной информации. Исходя из этого, при рассмотрении вопроса правовой охраны баз данных следует в первую очередь обращать внимание на составляющий их контент. База данных подобно картотеке содержит систематизированную и структурированную информацию о субъектах и объектах. В этом случае следует признать, что приравнивание фактографической базы данных к сборнику произведений в ст. 1260 ГК РФ нельзя считать правомерным. Независимо от тематики картотеки данные, систематизированные в ней, представляют интерес как сведения о субъектах и объектах: лицах, событиях, предметах. Эти сведения могут составлять конфиденциальную информацию. И правовая охрана в этом случае должна предоставляться не базе данных как авторскому произведению, а информации, содержащейся в этой базе. Отграничением от объектов, охраняемых авторским правом, Л.А. Букалерова предлагает считать отсутствие "творческого труда по подбору и организации данных"[18].

Однако данный критерий нельзя считать приемлемым из-за его неопределенности. В соответствии со ст. 1260 ГК РФ автору составного произведения (антологии, энциклопедии, базы данных, атласа или другого подобного произведения) принадлежат авторские права на осуществленные ими подбор или расположение материалов (составительство), определяя составительство как творческий труд. Однако, по нашему мнению, выбор правовых мер охраны базы данных должен

[14] *Digital video disk* – диск для записи видеоинформации в цифровом формате. В настоящее время существует пять различных форматов DVD.

[15] *Флэш-память* – энергонезависимое устройство для записи и длительного хранения информации в цифровом формате. В настоящее время широко применяется в микрокомпьютерах, цифровых фотоаппаратах и диктофонах, аппаратах сотовой телефонии, MP3-плейерах и др.

[16] Наиболее известным представителем этого класса является американская система "Эшелон", контролирующая радио-, телефонные, факсимильные каналы на территории Европы. Отчет, подготовленный в конце 1997 г. Европарламентом, подтверждает существование проекта "Эшелон" (Project Echelon), который обеспечивает Агентство национальной безопасности (США) контролем по "ключевым словам" практически за всеми коммуникациями в Европе (см.: *Смирнов С.* Частная жизнь и права человека // http:// hro.org. 2006. 10 июня).

[17] Примером является система распознавания движущихся автомобилей, применяемая ГИБДД с 1998 г.

[18] *Букалерова Л.А.* Базы данных, содержащие официальную информацию, как объекты авторских, имущественных и иных охраняемых уголовным правом отношений // В кн.: Контрафакт как угроза экономической безопасности России. Сборник статей. Н.Новгород, 2006. С. 422.

определяться мерами охраны содержащейся в ней информации. Ограничения в доступе, накладываемые даже на часть информации в базе данных, должны экстраполироваться на весь информационный массив. Особое значение приобретает правовая охрана баз данных с информацией ограниченного доступа. В ст. 5 Закона об информации данная категория определена как информация, доступ к которой ограничен федеральными законами.

Ранее в Федеральном законе "Об информации, информатизации и защите информации" для определения ограничения в доступе использовалась дефиниция "конфиденциальная информация" – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации[19]. Документированную информацию закон определял как зафиксированную на материальном носителе с реквизитами, позволяющими ее идентифицировать. Данное определение было некорректно, и А.В. Минбалеев правильно замечает, что не только документированная информация может быть конфиденциальной – сведения, составляющие личную и семейную тайны, охраняются независимо от фиксации их на материальном носителе[20]. В указанном Законе были и другие недостатки, требовавшие изменений. Однако вместо внесения изменений законодатель принял новый Закон об информации.

К сожалению, во вновь принятом Законе отсутствует определение "конфиденциальной информации". Вместо него законодатель в ст. 2 определил "конфиденциальность информации" как "обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя". Указанную замену нельзя считать равнозначной. В отечественном законодательстве не было и нет общей нормы о защите конфиденциальной информации и мерах ответственности за неправомерный ввод ее в оборот. Отнести группу сведений к конфиденциальной информации можно было только тогда, когда существовал законодательно определенный механизм ограничения доступа к указанной информации. В принятом новом Законе об информации введено определение конфиденциальности как режима доступа, который может быть установлен обладателем информации произвольно, независимо от нормативного ограничения. Указанное положение противоречит норме самого Закона, изложенного в п. 2 ст. 3 "Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации", в которой определено установление ограничений доступа к информации только федеральными законами. Указанная коллизия существенным образом осложняет правоприменительную деятельность в данной сфере. Еще более усугубляет положение ст. 1334 ГК РФ, в которой определено, что изготовителю базы данных, создание которой (включая обработку или представление соответствующих материалов) требует существенных финансовых, материальных, организационных или иных затрат, принадлежит исключительное право извлекать из базы данных материалы и осуществлять их последующее использование в любой форме и любым способом (исключительное право изготовителя базы данных). Изготовитель базы данных может распоряжаться указанным исключительным правом. При отсутствии доказательств иного базой данных, создание которой требует существенных затрат, признается база данных, содержащая не менее 10 тыс. самостоятельных информационных элементов (материалов), составляющих содержание базы данных.

Для пояснения проблемы рассмотрим формирование и функционирование баз данных оператора сотовой связи. В соответствии со ст. 53 ФЗ "О связи" "сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются конфиденциальной информацией"[21].

При оказании услуги связи программа фиксирует в базе данных параметры, необходимые для расчета взимаемой платы: время звонка, номера вызывающего и вызываемого абонентов, длительность телефонного разговора, места нахождения абонентов и ряд других параметров. В соответствии с ч. 5 ст. 55 ФЗ "О связи" претензии к работам в области электросвязи предъявляются в течение 6 месяцев со дня оказания услуги связи, отказа в ее оказании или дня выставления счета за оказанную услугу связи. Следовательно, ука-

[19] См.: Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 г. // Собрание законодательства РФ. 1995. № 8. Ст. 609.

[20] См.: *Минбалеев А.В.* Система информации: теоретико-правовой анализ. Дисс. … канд. юрид. наук. Челябинск, 2006. С. 184.

[21] Там же определено, что "к сведениям об абонентах относятся фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента-юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента".

занные данные хранятся не менее 6 месяцев для разрешения конфликтных ситуаций[22].

Указанное ранее свойство "критического объема" наглядно проявляется в возможности получения расширенной информации об абоненте, исходя из анализа предоставленных ему услуг. Детальный анализ зафиксированной в базе данных системы информации о соединениях и предоставленных дополнительных услугах (SMS, MMS, почтового ящика, переадресации вызова и др.) позволяет однозначно определить владельца SIM-карты, т.е. идентифицировать его личность. В качестве исходных данных анализа может быть использовано время и телефонные номера известных абонентов. Дополнительным анализируемым параметром выступает место нахождения абонента во время фиксируемого события – звонка или иной услуги. В специальной литературе и средствах массовой информации описаны случаи раскрытия преступлений и установления личностей преступников по анализу телефонных звонков[23].

При достижении "момента критического объема" анализ накопленной информации позволит получить критически значимую информацию о субъекте персональных данных и даже спрогнозировать его последующие действия. Однако в каждом конкретном случае количество записей, которое позволит получить качественное изменение данных о субъекте, будет различным. Определение данного момента и связанного с ним временем накопления информации о субъекте персональных данных, – является сложной задачей, существенно зависящей от множества параметров:

вида информации, собираемой в базе данных (услуги телефонной связи, кредитная история, налоговые отчисления и прочее);

интенсивности пользования услугой, информация о предоставлении которой фиксируется в базе данных;

случайности или периодичности процесса (периодичность налоговых отчислений, телефонных звонков и других услуг связи);

индивидуальных особенностей субъекта персональных данных и др.

Но даже не проводя вычислений, можно утверждать, что данные о предоставленных услугах, накопленные за один месяц в базе оператора связи, позволяют достаточно полно охарактеризовать абонента. Продолжительность хранения указанной информации является фактором, определяющим возможность получения расширенных данных об абоненте, установлении его окружения: сотрудников по работе, друзей, круга личного общения, характере профессиональной деятельности. Наличие в базе данных информации о тысячах абонентов за длительный промежуток времени делает возможным проведение анализа на предмет получения сведений об опосредованных связях абонентов.

Норма ст. 53 ФЗ "О связи" относит сведения об абонентах и оказываемых им услугах связи к разряду конфиденциальной информации, не включая ее в тайну связи (ст. 63 ФЗ "О связи"). Рассматривая данное частное противоречие, следует обратить внимание на Определение Конституционного Суда РФ "Об отказе в принятии к рассмотрению запроса Советского районного суда г. Липецка о проверке конституционности ч. 4 ст. 32 Федерального закона от 16 февраля 1995 года "О связи" от 2 октября 2003 г.[24]. Но в общем случае подобное деление сведений создает правовую коллизию – владелец конфиденциальной информации, не отнесенной законом к охраняемой тайне, не несет ответственность за ее санкционированное или несанкционированное распространение.

Во многих случаях операторы баз данных не защищают свою информацию должным образом. В рамках исследования "Внутренние ИТ-угрозы в России" компания InfoWatch опросила около 400 российских организаций (из них около 60 являлись представителями министерств и ведомств). Большая часть (68% организаций) вообще не предпринимают никаких мер для защиты своих чувствительных цифровых активов, а оставшиеся 32% в большинстве своем принимают меры лишь для ограничения связи с внешними сетями[25]. Именно этим объясняются периодиче-

[22] Срок хранения данных об абонентах и оказанных им услугах увеличен до трех лет. Постановление правительства Российской Федерации "Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность" от 27 августа 2005 г. обязывает оператора связи "своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи".

[23] Эти данные настолько широко известны, что преступники после хищения сотового телефона обязательно удаляют SIM-карту.

[24] В Определении однозначно указано, что "право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи".

[25] 12 самых громких случаев ИТ-воровства в России // Cnews.ru. 2005. 2 дек.

ские "утечки" баз данных государственных органов и коммерческих структур, сообщения о которых появляются в СМИ, а предложения о продаже самих баз – в Интернете. Анализ происшедших за последние годы инцидентов позволяет сделать вывод о возможности неправомерного доступа к информации в автоматизированных системах.

Особую обеспокоенность вызывает отсутствие заинтересованности в пресечении "утечек" и поиске источников со стороны некоторых операторов баз данных. Так, в октябре 2002 г. Госкомстат предпочел игнорировать факт утечки, заявив, что федеральная организация не виновата. С аналогичным заявлением выступило в ноябре 2004 г. Министерство по налогам и сборам. А заместитель начальника Управления безопасности и защиты информации Московского главного территориального управления Банка России В. Бабкин на пресс-конференции в рамках Всероссийского форума "Банковская безопасность: состояние и перспективы развития" 25 октября 2005 г. в сообщении о перекрытии канала утечки информации по банковским проводкам заявил, что "выявление конкретных источников утечки информации является прерогативой правоохранительных органов"[26].

Создание, использование и распространение баз данных, содержащих персональные данные различных субъектов, должно регулироваться в соответствии с Федеральным законом "О персональных данных" от 27 июля 2006 г. Естественно, что в случае, когда действия с информационным обеспечением приводят к нарушению установленных законом норм, возникает необходимость их квалификации. Понятие правонарушения в юридической науке безальтернативно. Это "общественно вредное виновное действие или бездействие участника общественных отношений, запрещенное правом". Определение административного правонарушения, данное законодателем в ст. 2.1 КоАП РФ, отличается от приведенного видом деятельности и субъектом правонарушения, что является существенным моментом: КоАП РСФСР называл в качестве субъекта только физическое лицо. Данной точки зрения придерживался Д.Н. Бахрах, который считал, что "при анализе нормативной основы административной ответственности организаций следует обратить внимание на то, что КоАП РСФСР на действия коллективных субъектов не распространяется"[27]. Это следовало из отсутствия в КоАП РСФСР дефиниции "юридическое лицо". КоАП РФ в ч. 1 ст. 2.1 "Административное правонарушение" однозначно определяет субъектов административной ответственности – это физические и юридические лица.

Наиболее опасным видом правонарушения являются преступления, влекущие уголовную ответственность. Именно общественная опасность является критерием, с помощью которого законодатель дифференцирует деликты на преступления, административные и гражданско-правовые нарушения, дисциплинарные проступки[28]. Общественную опасность распространения информации персонального характера, содержащейся в базах данных, трудно переоценить, поскольку оно наносит ущерб личности (становятся известными персональные данные, относящиеся к информации ограниченного распространения) и государству (которое, декларируя защиту информации и ответственность за ее нарушение, на деле не может защитить своих граждан от преступных посягательств). Но выразить ущерб, нанесенный отдельному гражданину несанкционированным распространением данных частной жизни, в стоимостном выражении весьма проблематично. Оператору распространенной базы данных грозит только гражданская ответственность, устанавливаемая судом индивидуально в интересах каждого субъекта персональных данных. В странах, где накоплен значительный опыт обращения с персональными сведениями, отношение к утечкам из баз данных значительно серьезнее[29].

Следует обратить внимание на то, что возбуждение уголовного дела по ст. 137 УК РФ "Нарушение неприкосновенности частной жизни" не приводит к положительному результату. Статья 19 УК РФ определяет субъектов уголовной ответственности как "только вменяемое физическое лицо, достигшее возраста, установленного настоящим Кодексом". Персонифицирование уголовной ответственности существенно затрудняет осуществление наказания за утечку данных. Особенно это проявляется в том случае, когда оператор не предпринимает должных мер защиты информации и контроля доступа к ней: по данным опроса компании InfoWatch лишь 1% респондентов использует технические продукты для борьбы с утечками, хотя 87% считают их самым эффективным средством решения проблемы. При таком уровне защиты данных поиск источника утечки информации становится неразрешимой задачей.

[26] Там же.

[27] *Бахрах Д.Н.* Административное право России. М., 2001. С. 566.

[28] См.: Комментарий к Уголовному кодексу Российской Федерации / Под ред. Ю.И. Скуратова и В.М. Лебедева. М., 2001. С. 19.

[29] Генеральный директорат Тайваня по телекоммуникациям оштрафовал трех операторов за халатность в обращении с данными абонентов на $10 тыс. каждого (см.: *Дмитриев М.* Тайвань: операторы ответят за утечку из своих баз данных личной информации об абонентах // http://www.onliner.by. 2004. 3 июня).

Усложняет применение уголовного наказания также то, что в соответствии с ч. 3 ст. 20 УПК РФ уголовные дела о преступлениях, предусмотренных ч. 1 ст. 137 УК РФ считаются уголовными делами частно-публичного обвинения и возбуждаются не иначе как по заявлению потерпевшего. В соответствии с ч. 5 ст. 20 УПК РФ уголовные дела о преступлениях, предусмотренных ч. 2 ст. 137 УК РФ считаются уголовными делами публичного обвинения. Парадоксальность ситуации заключается в том, что установить служебную принадлежность источника утечки к организации-оператору можно только в ходе следствия по возбужденному уголовному делу. Низкая правовая грамотность граждан России объясняет крайне редкие случаи возбуждения уголовных дел частно-публичного обвинения по ч. 1 ст. 137 УК РФ.

По нашему мнению, при рассмотрении вопроса об ответственности операторов баз данных за утечку информации персонального характера следует ориентироваться на квалификацию данного деяния по ст. 13.11 КоАП РФ "Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)". В соответствии со ст. 23 Закона "О персональных данных" уполномоченным органом по защите прав субъектов персональных данных является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В случае неправомерных действий с базами данных, содержащих информацию персонального характера, для защиты конституционных прав граждан уполномоченный орган имеет право привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона (п. 9 ч. 3 ст. 23).

В пользу административного наказания свидетельствует простота его осуществления и отсутствие трудоемких оперативно-розыскных и следственных действий при расследовании правонарушения. Программно-техническая экспертиза в первом случае также будет значительно проще, поскольку сведется к идентификации базы данных и установлению примерной даты ее утечки.

В соответствии со ст. 13.11 КоАП РФ нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет наложение административного штрафа на юридических лиц в размере от 50 до 100 минимальных размеров оплаты труда. Если принять во внимание, что базы данных без обновления быстро теряют актуальность, можно сделать вывод о том, что доступные в Интернете и торговых точках базы данных обновляются постоянно. При наличии экспертного заключения об обновлении продаваемой базы данных федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, имеет право привлечь к административной ответственности оператора за повторное нарушение. Воздействие штрафными санкциями, совпадающими по периодичности с совершаемыми утечками, заставит оператора баз данных ужесточить контроль и принять меры к выявлению и ликвидации каналов утечки информации.

Рассматривая возможные меры защиты информации персонального характера, содержащейся в автоматизированных системах обработки информации, следует руководствоваться нормой ст. 5 Закона о персональных данных, в которой среди важнейших принципов определены "соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных" и указано на "недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных".

В целом, оценивая свойства баз данных, содержащих конфиденциальную информацию и отличая их от традиционных бумажных архивов и картотек, можно констатировать качественное изменение в соотношения интересов человека и общества. Человек оказался открыт в значительно большей степени, чем это было прежде. И эта тенденция продолжает усиливаться.

Подводя итог сказанному, можно сделать следующие выводы.

1. Базы данных выступают специфическими объектами правовой охраны ввиду того, что они являются особыми формами представления информации. Правовая охрана фактографической базы данных, содержащей конфиденциальную информацию, должна осуществляться не авторским правом, а тем институтом, которому соответствует содержащаяся в этой базе информация.

2. Доступность, простота использования и относительная дешевизна компьютерных технологий, с одной стороны, и низкий уровень защиты информационных систем – с другой, способствуют количественному росту правонарушений и увеличению причиняемого материального и морального ущерба правообладателям и субъектам данных.

3. Для ликвидации существующих пробелов в правовом регулировании как конфиденциальной информации в общем, так и персональных данных в частности, необходимо ввести в Закон об информации определение "конфиденциальная информация – информация, доступ к которой

ограничивается в соответствии с законодательством Российской Федерации".

4. Для гарантии конституционных прав граждан следовало бы дополнить ст. 63 ФЗ "О связи", изложив ч. 1 в следующей редакции: "На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и почтовой связи. Гарантируется тайна сведений обо всех видах сообщений, передаваемых по сетям электросвязи и почтовой связи".

5. Для защиты сведений персонального характера, содержащихся в автоматизированных системах обработки информации, необходимо ввести дополнение в ст. 5 Закона о персональных данных, изложив требование к структуре баз данных, используемых операторами: "Базы данных, используемые операторами и обрабатывающие в автоматическом режиме информацию о предоставляемых услугах конкретным субъектам, не должны содержать персональные данные, т.е. данные, позволяющие идентифицировать субъекта".