ГОСУДАРСТВО И ПРАВО, 2008, № 10, с. 60–68

ПРАВО И ИНФОРМАТИКА

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА БАЗ ДАННЫХ

© 2008 г. О. И. Трофимов[1]

Потребности общественного развития побуждают государство не только развивать и совершенствовать правовое регулирование сложившихся сфер человеческой деятельности, но и устанавливать общеобязательные правила поведения в новых сферах жизнедеятельности общества. К одной из них относится информационная сфера, которая в настоящее время активно развивается. Информационное право регулирует информационные отношения: правовой режим получения, передачи, хранения и использования информации, юридические режимы информации разного содержания, пользования банками и базами данных, ответственность.

Информационные правоотношения в сфере телекоммуникаций в основном регулируются императивными методами, характерными для публично-правовой сферы и основанными большей частью на предписании и запрете. Прежде всего это относится к противоправным деяниям, предусмотренным гл. 28 УК РФ "Преступления в сфере компьютерной информации", деликтам в сфере телекоммуникаций и средств массовой информации, которым посвящены нормы УК РФ и Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ).

Однако проблема ответственности за совершаемые в сфере телекоммуникаций деяния непроста. Мнения исследователей, рассматривающих сферу информационных правоотношений, законодателей и правоприменителей, существенно различаются. Это обусловлено крайне непродолжительным периодом существования исследуемых правоотношений и неспособностью юридической практики к столь быстрому осмыслению и реагированию на технический прогресс, формирующий общество нового типа – информационное. "Юрисдикционные органы оказались в довольно сложном положении: возникла совершенно новая система общественных отношений, связанная с новейшими технологиями, и чтобы применить к ним нормы существующего законодательства, нужно, как минимум, понимать сущность и содержание этих отношений"[2].

Информационное право – комплексная отрасль, в том числе и по методам правового регулирования, имеющая сложную предметную структуру. Заимствуя у нескольких профилирующих отраслей часть их норм, она соответственно заимствует и методы правового регулирования. В информационном праве применяется вся совокупность способов регулятивного воздействия на информационные отношения: предписание, запрет и дозволение. Как отмечает В.А. Копылов, "поскольку информация сопровождает практически все области человеческой деятельности, то для регулирования информационных отношений применяются все возможные существующие методы права в зависимости от вида и назначения информации, характера поведения субъектов и возникающих при этом отношений"[3]. При регулировании общественных отношений в информационной сфере кроме императивных методов регулирования применяются и диспозитивные (характерные для гражданско-правовых отношений). Последние основаны на равенстве субъектов правоотношений, выражающемся прежде всего в их свободной волевой ориентации и независимости своей воли; самостоятельности участников правоотношений и свободном осуществлении ими своих прав; самостоятельности субъектов правоотношений в смысле ответственности по обязательствам[4]. Поэтому государство не должно вмешиваться в отношения частных лиц без их на то согласия (частный интерес) и допускать массовый характер подобных нарушений (общественный интерес)[5].

Таким образом, при рассмотрении информационных правоотношений следует учитывать соотношение интересов частного и публичного. Особую значимость рассматриваемое соотношение приобрело в последние годы, когда благодаря процессу компьютеризации архивы и картотеки были переведены на машинные носители. Ранее для того, чтобы собрать полные данные о человеке, необходимо было получить соответствующие

[1] Адвокат.

[2] *Смыслина Е.* Борьба с пиратской вольницей в мировой паутине // Росс. юстиция. 2001. № 6. С. 62.

[3] *Копылов В.А.* Информационное право. М., 2002. С. 100.

[4] См.: *Тихомиров Ю.А.* Публичное право. М., 1995. С. 47.

[5] См.: *Афонин А.И.* Правовое обеспечение противодействию спамингу в сервисе электронной почты. Автореф. дисс. … канд. юрид. наук. Воронеж, 2006. С. 17.

санкции для доступа ко многим разделенным ведомственными барьерами архивам, так как в каждой картотеке хранилась только часть этой информации. И лишь с появлением компьютерных сетей информация стала собираться в единое целое, и человек оказался менее защищенным и более открытым, чем это было прежде. Преобразование массивов информации в базы данных имело не только позитивные, но и негативные последствия, так что базы данных не только количественно, но и качественно меняют положение человека в обществе.

Особую настороженность вызывает отсутствие должной защиты баз данных со стороны операторов. В рамках исследования "Внутренние ИТ-угрозы в России" компания "InfoWatch" опросила около 400 российских организаций (из них около 60 – представители министерств и ведомств). Большая их часть (68%) не предпринимает мер для защиты своих чувствительных цифровых активов, а 32% принимают меры лишь для ограничения связи с внешними сетями[6]. Именно этим объясняются "утечки" баз данных, сообщения о которых так часто появляются в СМИ, а предложения о продаже самих баз – в Интернете. Еще более усугубляет положение ст. 1334 ГК РФ, определяющая исключительное право изготовителя базы данных извлекать из таковой материалы и осуществлять их последующее использование в любой форме и любым способом.

Прежде чем рассматривать некоторые аспекты правового регулирования возникающих информационных правоотношений, необходимо определить термин "оборот баз данных". По нашему мнению, *оборот (изготовление, создание, модификация, использование, копирование, распространение, владение, воспроизведение, приобретение, продажа, защита, хранение, регистрация, уничтожение, ввоз и вывоз из страны) баз данных представляет собой позитивно-негативное социально-правовое явление и системное единство их легального оборота (разрешенного и регламентированного законами и подзаконными актами), и нелегального(незаконного, нарушающего запреты административного и уголовного законодательства, нормы федеральных законов и подзаконных актов)*. Незаконный, или противоправный, оборот баз данных – это процесс нарушения норм действующего законодательства, совокупность дисциплинарных и административных проступков, преступлений, лиц, их совершивших.

Для пояснения проблемы рассмотрим легальный и нелегальный оборот баз данных операторов электросвязи и те информационные правоотношения, которые при этом возникают.

С середины 90-х годов XX в. на рынке мобильных коммуникаций наблюдается резкий рост числа преступлений, связанных с незаконным доступом и пользованием ресурсами (услугами) сотовой связи. Этот вид преступлений стал настолько распространен, что получил собственное название – *фрод*[7]. Отметим, что в отечественной юридической литературе применительно к криминальным действиям по неправомерному доступу и пользованию ресурсами сотовой связи используются термины "сотовое мошенничество" и "мошенничество в сетях сотовой связи". Следует согласиться с Г.В. Семеновым и П.Н. Бирюковым, которые обращают внимание на некорректность использования указанных терминов с позиции отечественного уголовного закона, поскольку "эти понятия заимствованы из зарубежного законодательства, а понятие "мошенничество" традиционно используется в нашей стране для обозначения несколько иного преступления"[8]. Поэтому будем употреблять термин "фрод", приводя примеры квалификации в соответствии с отечественными правовыми нормами.

Исходя из равенства субъектов правоотношений, каковыми являются абонент и оператор связи, можно выделить следующие виды правомерной и противоправной деятельности, при осуществлении которой возникают информационные правоотношения, регулируемые диспозитивными методами:

создание и функционирование баз данных об абонентах;

информирование абонентов о возможных негативных последствиях при предоставлении услуг;

ненадлежащая организация работы с данными о частной жизни абонентов;

ненадлежащая защита персональных данных клиентов;

создание и функционирование баз данных биллинговых систем[9];

несоблюдение конфиденциальности данных, приведшее к распространению информации.

Детальное рассмотрение всех указанных видов деятельности, регулируемых диспозитивными и

[6] 12 самых громких случаев ИТ-воровства в России // Cnews.ru. 2005. 2 дек.

[7] *Фрод* (от англ. *fraud* – мошенничество) – мошенничество с контрактами и счетами за услуги сотовой связи, например хищение и клонирование сотовых телефонов, а также всевозможные изощренные способы обмана сотовых компаний (см.: http://www.bb2.ru/lexicon/189.html).

[8] *Семенов Г.В., Бирюков П.Н.* Ответственность за "мошенничество" в сетях сотовой связи. Учебное пособие. Воронеж, 2002. С. 41.

[9] В соответствии со ст. 53 Закона о связи система расчета за оказанные услуги связи включает информацию о соединениях, трафике и платежах абонента.

императивными методами, в рамках одной статьи невыполнимо. Обозначим лишь основные, с нашей точки зрения, направления и принципы. Технические же проблемы нами рассматриваться не будут.

Создание и функционирование баз данных об абонентах. Согласно ст. 5 Закона о персональных данных их обработка должна осуществляться на основе принципа соответствия объема и характера обрабатываемых персональных данных, способов их обработки целям обработки персональных данных. К сведениям об абонентах (ст. 53 Закона о связи) относятся следующие: фамилия, имя, отчество или псевдоним абонента-гражданина, адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование. Однако операторы связи при заключении договора с абонентом предлагают ему указать и такие параметры, как дата рождения, пол, сфера деятельности и др. Нецелевое использование полученной операторами информации подтверждается проводимыми с их ведома социологическими исследованиями[10].

Особо следует выделить распространение баз данных телефонных номеров. Можно согласиться с мнением, что "в России очень сложно получить хоть какую-то достоверную информацию об утечке или даже подтвердить сам факт таковой. Даже в случае исчерпывающего раскрытия информации об утечке официальные лица пострадавшей организации вполне могут заявить, что все предлагаемые на черном рынке материалы сфабрикованы и никакой утечки не было"[11]. В государствах, процесс информатизации в которых имеет большую продолжительность, отношение к подобным происшествиям операторов значительно серьезнее[12].

В настоящее время в США рассматривается новый законопроект "Cyber-Security Enhancement and Consumer Data Protection Act", инициированный Юридическим комитетом Конгресса США. Он предусматривает ответственность частных компаний за сохранность персональных данных или информации секретного характера. Законопроект обязывает компанию в случае утечки закрытой информации в течение семи дней поставить в известность федеральное органы, такие как ФБР или другие спецслужбы США. Компании и федеральные власти могут в течение 30 дней не афишировать факт утечки. В том случае если информация имеет особо секретный характер, этот срок может быть продлен. Особо определена ответственность компаний. Если компания не сможет представить отчет о методах и конкретных действиях, принятых сразу после утечки, то за каждый день просрочки будет наложен штраф в размере 50 тыс. долл. (но не более 1 млн. долл.).

В России отношение к распространению баз данных с конфиденциальной информацией значительно лояльнее. Базы данных операторов телефонной связи начали продаваться в Москве и во многих городах России в 1992–1995 гг. В последующие годы периодически происходили утечки баз данных практически всех операторов сотовой связи – "*Билайна*", "*Мегафона*" и "*МТС*" в Москве и Санкт-Петербурге.

Информирование абонентов о возможных негативных последствиях при предоставлении услуг – обязанность оператора связи. Однако в большинстве случаев операторы пренебрегают своим долгом. При подключении аппаратов сотовой связи оператор не возлагает на себя ответственность за последствия непрофессионального обращения со сложным программно-техническим устройством, каким является сотовый телефон. Значительная часть абонентов не предполагает возможных негативных последствий своей неосведомленности: неправомерного доступа злоумышленника к незащищенным каналам *Bluetooth*, ненадежности технологии *Wi-Fi* и *ACL*[13], вероятного "заражения" вредоносными программами и др.

Пренебрежение обязанностью предоставлять полную информацию о защите конфиденциальности данных абонента прослеживается у провайдеров Интернета и операторов электронной почты. В настоящее время почти все провайдеры доступа к Интернету включают электронную почту в список стандартных услуг. Кроме того, в российской сети существуют сайты, предлагающие услуги *e-mail* бесплатно. Интересные данные были получены С. Смирновым и О. Кочевой, которые рассмотрели 12 бесплатных почтовых систем: *yandex.ru, mail.ru, hotbox.ru, zmail.ru, newmail.ru, km.ru, chat.ru, e-mail.ru, mail2000.ru, mail-*

[10] В письме Госкомитета РФ по телекоммуникациям "Об анализе внедрения системы повременного учета стоимости услуг местной телефонной связи (СПУС), проведенного Гостелекомом России" от 30 августа 1999 г. отмечено: "Как показало социологическое исследование, проведенное в г. Москве, более 15,0 % абонентов используют телефон для получения прибыли (частные нотариусы, рекламные агенты, диспетчеры и др.)" (см.: ИПС "Закон" // http://www.vcom.ru/cgi-bin/db/zakdoc?_reg_number=%C29904089).

[11] В подтверждение данного тезиса можно привести известные случаи распространения баз данных Госкомстата России в октябре 2002 г. и др. (см.: Утечки информации: российская действительность // www.securitylab.ru. 2005. 17 нояб.).

[12] См.: *Дмитриев М.* Тайвань: операторы ответят за утечку из своих баз данных личной информации об абонентах // http://www.onliner.by. 2004. 3 июня.

[13] См.: *Касперски К.* Защита беспроводных сетей // Mobi. 2005. № 8. С. 12.

gate.ru, rambler.ru, s-mail.com[14]. Гарантии приватности в каком-либо виде были обнаружены на восьми сайтах. Подробные, исчерпывающие гарантии конфиденциальности данных, включая использование *cookies*, предоставляют лишь *rambler.ru, yandex.r*u и *s-mail.com*. На этих сайтах политика приватности изложена в виде отдельного документа. Менее конкретно изложены условия использования данных на сайте *mail.ru*. На других почтовых сайтах гарантии сохранения конфиденциальности данных упоминаются кратко и включены в общие правила работы (иногда в варианте пользовательского соглашения). Только у *rambler.ru* и *s-mail.com* политика конфиденциальности персональных данных доступна по ссылке с главной страницы сайта. На остальных сайтах гарантии защиты данных неочевидны.

Основой гарантий является условие предварительного разрешения субъектом данных на их передачу третьим лицам. Изучение показывает, что на некоторых Интернет-сайтах сделана оговорка: "кроме случаев, предусмотренных законом". На трех сайтах упомянуто о праве администрации почтовой системы использовать данные в маркетинговых целях (без передачи третьим лицам); *s-mail.com* и *rambler.ru* собирают наибольшее количество данных, включая, например, дату рождения, пол, сферу деятельности; *mail.ru* и *km.ru* требуют немногим меньший объем персональных данных; остальные системы ограничиваются минимальным набором[15].

Из рассмотренных почтовых систем пять предоставляют защиту от несанкционированного доступа на основе шифрования. Пользователь может удалить свою учетную запись в системах *yandex.ru* и *rambler.ru*. В остальных системах электронный почтовый ящик удаляется через определенный период, в течение которого он не использовался (до четырех месяцев). Дальнейшее применение собранных данных после прекращения пользования сервисом, как правило, не оговаривается. Изложенное позволяет сделать вывод о ненадлежащей охране персональных данных абонентов электронной почты и тайны связи. Применительно к электронной почте сведениями, подлежащими охране наравне с самим сообщением, являются: адреса отправителя и получателя, время отправления или доставки, длина сообщения, т.е. те данные, которые обычно фиксируются в *лог-файле* почтового сервера.

Статья 24 Конституции РФ определяет недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Ненадлежащая организация работы с данными о частной жизни абонентов наглядно проявляется при рассмотрении отношений между провайдерами Интернета и клиентами. Обеспечение информационных прав клиента во многом зависит от добросовестности и оптимальности действий провайдеров. В качестве тестовых регионов были выбраны Москва (68 провайдеров), Екатеринбург (34 провайдера), Сибирь и Дальний Восток (22 города, 90 провайдеров). Тексты договоров были опубликованы на сайтах 33 московских, 13 екатеринбургских и 39 сибирских фирм. Еще две екатеринбургские и шесть сибирских фирм выслали тексты договоров по электронной почте по запросу. Таким образом, были проанализированы документы 93 Интернет-провайдеров. Только в 22% договоров четко указаны гарантии приватности, как правило, с оговоркой "кроме случаев, предусмотренных законодательством". Однако следует отметить, что в ряде случаев условие конфиденциальности распространяется в договоре только на данные, полученные при регистрации, в отношении иной информации условия не оговорены.

Сложным для оценки является вопрос отнесения веб-трафика к охраняемым сообщениям. Запрос пользователя к серверу и сообщение, передаваемое по Интернет-протоколу HTTP от веб-сервера пользователю, не являются аналогом письма от человека к человеку. Н.Н. Федотов определяет доступ пользователя к публичным веб-страницам как коммуникацию между человеком и "нечеловеком"[16]. Можно согласиться с автором, что "посещение человеком определённой веб-страницы, без сомнения, может считаться частью его личной жизни, хотя эта веб-страница и доступна неопределённому кругу лиц". Действительно, анализ искомых человеком сведений и посещаемых тематических сайтов позволяет получить информацию о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни и пр. Эта информация в соответствии со ст. 10 Закона о персональных данных относится к специальной категории персональных данных, обработка которых допускается в исключительных случаях, исчерпывающий перечень которых содержится в Законе. Из изло-

[14] См.: *Смирнов С., Кочева О.* Приватность в российском Интернете-2005 // http://www.internet-law.ru/info/private/index.htm.

[15] Подразумеваются данные, которые не являются необходимыми для доступа пользователя к его почтовому ящику (имя/логин, пароль) либо для восстановления забытого пароля. К такой факультативной информации можно отнести настоящие имя и фамилию, возраст, телефон, адрес, специальность, сферу занятости и интересов и т.д.

[16] См.: *Федотов Н.Н.* Тайна связи против технических средств защиты информации в Интернете // www.security-lab.ru. 2006. 21 мая.

женного следует, что факт запроса веб-страницы составляет тайну личной жизни пользователя.

Проведенный анализ договоров операторов электронной почты и Интернет-провайдеров позволяет сделать вывод о невыполнении ими требований Закона о персональных данных. Для решения данной проблемы необходимо стандартизировать договор операторов связи с абонентом. В соответствии с нормами Закона о персональных данных в договоре должны быть следующие обязательные положения: исчерпывающие гарантии конфиденциальности данных, изложенные в виде отдельного документа; описание механизма защиты от несанкционированного доступа; описание способа удаления учетной записи; основания для отказа в предоставлении доступа к Интернету и расторжения договора.

Использование *cookies*[17] как механизма негласного сбора информации об абоненте следует рассматривать особо. Cookies используются в работе почтовых серверов, для оформления заказов в онлайновых магазинах, при настройке индивидуального профиля зарегистрированного пользователя, для рекламы (определения целевой аудитории, например по географическому положению пользователей), отслеживания интересов клиентов, учета количества показов и проходов сквозь баннеры. Сбор и хранение информации о посетителях сайта с помощью cookies осуществляют не только частные, но и некоторые государственные серверы.

Системы статистики, например *SpyLog*, позволяют составлять точные "профили" посетителей сайта. Собранная информация хранится в базе данных и в любой момент может быть представлена для анализа. Статистические системы имеют возможности для сбора данных, позволяющих идентифицировать пользователей и составлять их досье. На российских серверах крайне редко встречается предупреждение об использовании cookies. Как правило, указание на это содержится в инструкции по изменению настройки браузера для разрешения приема cookies. В единичных случаях на серверах представлены информация о сохраняемых в cookies данных и гарантии в части конфиденциальности персональных данных.

В целях защиты прав абонентов на сохранение тайны частной жизни владельцы серверов российского сегмента Интернета должны на сайтах предоставлять сведения о содержащейся в cookies информации и указывать возможности дальнейшего использования полученных данных. Сбор данных посредством cookies без предупреждения является противозаконным.

Среди сервисов, предоставляемых операторами сотовых систем связи по запросу клиентов, особое место занимает многовариантная услуга местоопределения абонента. При реализации этих функций запрашиваемый абонент не извещается, а его согласие предполагается актом совместной регистрации. Необходимо отметить, что рассматриваемые виды сервиса могут нанести значительный ущерб сохранению тайны личной жизни абонентов.

Возможности географической локализации абонента изначально заложены в архитектуру мобильной сотовой связи, так как для организации соединения сеть в любой момент должна знать, в какой из ее ячеек (сот) находится каждый конкретный телефон. Данный потенциал может быть использован не только самим оператором связи, но любым, знающим протокол организации *SMS*. Подтверждение тому – программа, размещенная на сайте немецкой фирмы "Gate5", позволявшая всем желающим узнать без уведомления абонента о подключении в указанный момент времени произвольного сотового телефонного аппарата системы *GSM* в любой стране мира[18]. В настоящее время фирма "Gate5" предлагает два программных коммерческих продукта – *People Finder* и *Safety Walker*. Программы дают возможность определять текущее местоположение абонентов.

В целях охраны права абонентов на неприкосновенность информации о частной жизни операторы должны внести изменения в предлагаемые сервисы. В случае реализации сервиса дистанционного предоставления конфиденциальной информации об абоненте оператор связи должен дать абоненту возможность дистанционного получения сведений о касающихся его запросах и подключении сервисов.

Проведенный анализ проблем регулирования информационных отношений диспозитивными методами показывает, что во многих случаях действия операторов не соответствуют требованиям Закона о персональных данных. Вместе с тем череда "утечек" баз данных государственных и коммерческих структур показала неотработанность механизма реализации наказания за совершенные противоправные действия. Рассмотренные случаи нарушений интересов абонентов были проанализированы с позиций частных отношений абонентов с операторами связи, в которые государство не должно вмешиваться без их на то согласия. Однако при массовом характере подобных проявлений происходит нарушение обще-

[17] *Cookie* – файл небольшого размера, который записывается на компьютер пользователя извне во время работы в Интернете. В cookies могут быть сохранены данные, которые пользователь оставляет о себе в сети (логин и пароль, номер кредитной карточки, фамилия, адрес электронной почты, почтовый адрес, персональные настройки и т.п.).

[18] См.: *Perera R.* Ping service can test mobile phone availability // http://www.gate5.de/ english/news/coverages/view_ idg20011119. html. 2001. 21 нояб.

ственного интереса, и недопущение подобных деяний является прерогативой государства.

Ущерб, наносимый операторам связи со стороны недобросовестных клиентов, стремительно растет. Если в 2002 г. общемировые потери операторов составляли 20–25 млрд. долл.[19], то в 2005 г., согласно исследованиям CFCA, потери от мошенничества в отрасли электросвязи составили 54.4–60 млрд. долл.[20] Эксперты CFCA указывают, что убытки от фрода соответствовали 5% совокупного оборота всех операторов мира. В российских компаниях, по мнению аналитиков, потери достигают 10% выручки.

Эксперты CFCA насчитали более 200 видов фрода, основная часть которых направлена непосредственно против легальных абонентов и самих операторов связи. Наиболее распространенные виды фрода, выделяемые отечественными операторами связи и специалистами в сфере защиты информации, можно классифицировать по направлению использования: для проведения массовых (групповых) и индивидуальных целевых операций.

К первой категории относятся: распространение вредоносных программ для смартфонов и аппаратов сотовой связи, создание зомби-сетей, инициативная рассылка сообщений рекламного характера (*спам*), упущенный вызов и пр.

Ко второй категории следует отнести установление фактов частной жизни абонента, неправомерный доступ к информации пользователя, блокирование канала связи абонента, обман и вымогательство за несовершенное преступление, мошенничество с оплатой по перечислению, мошенничество в роуминге и пр. Следует отметить, что не все виды деяний, отнесенных к фроду отечественными и зарубежными специалистами, нормативно запрещены в России.

Критерием, с помощью которого законодатель дифференцирует деликты на преступления, административные и гражданско-правовые деликты, дисциплинарные проступки, является их общественная опасность[21]. При этом выделяют два типа неправомерных деяний: 1) объективно противоправные деяния, которые совершаются при отсутствии отрицательного отношения причинителя к интересам общества и связаны с незнанием закона или неправильным его пониманием; 2) собственно правонарушения и их наиболее опасные виды – преступления. Рассматривая классифицированные ранее виды фрода, отметим, что они не могут определяться как невиновные противоправные деяния. Более того, с высокой степенью уверенности можно утверждать, что совершить их может только человек, обладающий специальными познаниями, или под руководством специалиста. Вместе с тем следует согласиться с Г.В. Семеновым и П.Н. Бирюковым, которые отмечают, что обстоятельства, предполагающие наличие криминальной абонентской активности в сети сотовой связи, "могут быть вызваны не только преднамеренными криминальными действиями, но и сбоями средств компьютерной техники, обеспечивающих функционирование сети сотовой связи, ошибочными действиями персонала компании сотовой связи и т.д."[22]. Независимо от складывающихся ситуаций авторы предлагают на этапе проверки оснований для возбуждения уголовного дела выдвигать следующие версии: имело место преступление; имел место административно-правовой деликт; имело место гражданское правонарушение; факт, имевший место, не влечет юридической ответственности.

Наряду с этим практика раскрытия преступлений в сфере компьютерной информации показывает, что хорошо подготовленное и тщательно проведенное противоправное деяние часто даже не обнаруживается[23]. Нарушители, пользуясь низкой компьютерной грамотностью пользователей, стремятся к тому, чтобы их действия не были выявлены. Для определения общественной опасности противоправного деяния необходимо понимание происшедшего, установление причинно-следственной связи совершенных действий и наступивших последствий, правильная квалификация и точная оценка нанесенного ущерба. В целях получения ответов на поставленные вопросы необходимо рассмотрение каждого возможного противоправного деяния.

Распространение вредоносных программ для смартфонов и аппаратов сотовой связи. Хотя индустрия мобильных вирусов существует с 2002 г., первый российский случай заражения сотового телефона был зарегистрирован в лаборатории Касперского 12 января 2005 г. В дальнейшем возможно широкомасштабное заражение при их квалифицированном осуществлении. Вирус заражает телефонный аппарат при ответе на звонок или прочтении SMS-сообщения. Одни выводят телефон из строя, другие начинают рассылать дорогостоящие сообщения или пересылают злоумышленнику информацию абонента.

[19] См.: *Борейко А.* Многоликий фрод // Ведомости. 2002. 29 марта.

[20] *CFCA* – Всемирная ассоциация по контролю за фродом в телекоммуникациях (Communications Fraud Control Association) (см.: *Есауленко А.* В бесконечном противостоянии // Сети. 2006. № 12. С. 25).

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

[22] *Семенов Г.В., Бирюков П.Н.* Указ. соч. С. 42.

[23] См.: *Айков Д., Сейгер К.* Компьютерные преступления. М., 1999. С. 18.

Операторы связи обязаны противодействовать распространению зараженного контента, на что указывается в гл. 2.6. меморандума "О противодействии распространению вредоносных программ (вирусов) и несанкционированных рекламных рассылок (спам)"[24]: "Все операторы связи должны быть заинтересованы в обеспечении надежной и безопасной передачи информации как основы своей деятельности, поэтому должны располагать подготовленным штатом сотрудников и продуманными регламентами, в том числе по предотвращению распространения вредоносных программ и спама". Кроме того, операторы должны дополнительно выстраивать антивирусную защиту на почтовых и иных серверах и производить фильтрацию трафика с целью блокирования распространения вредоносных программ. Производители антивирусных программ отмечают значительную заинтересованность в своих продуктах со стороны операторов мобильной связи[25].

Распространение вредоносных программ можно квалифицировать по ст. 273 УК РФ "Создание, использование и распространение вредоносных программ для ЭВМ".

По нашему мнению, ответственность за распространение зараженного контента абонентом сотовой сети должна возлагаться на оператора связи.

Создание зомби-сетей[26] *для проведения последующих действий* – логическое продолжение рассмотренной ранее рассылки вредоносных программ. Вредоносная программа изменяет сетевые настройки зараженного компьютера, что приводит к возможности загрузки с серверов злоумышленников дополнительных кодов и превращению захваченных компьютеров в управляемые зомби для осуществления DoS-атак, рассылки спама, несанкционированного получения конфиденциальной информации или распространения новых версий вредоносного кода на другие компьютеры. По мнению Г. Клули, за атаками стоят организованные криминальные группы[27]. Движущая сила всех атак – стремление сделать деньги на ботнетах. С зомби-машин в настоящее время рассылаются 56–62% всех спамовых писем.

Инициативная рассылка сообщений рекламного характера на аппараты сотовой связи – один из наиболее результативных видов спама. Его эффективность обусловлена адресным распространением информации. SMS-сервисы популярны и удобны в случае недоступности голосовой связи. SMS передаются даже при отсутствии голосовой связи, что обусловлено небольшими объемами информации в сообщениях и наличием особого приоритетного канала передачи данных. Однако, по мнению Мак-Дэниела, при большом количестве сообщений SMS-канал не выдержит нагрузку и заблокирует передачу голосовых вызовов[28]. Максимально обезопасить мобильные системы от спама могло бы блокирование возможности передачи текстовых сообщений через Интернет, но операторы связи не согласятся это осуществить. Пользователи не в состоянии сами защитить себя, поэтому защита от спама возлагается вышеуказанным меморандумом на операторов связи, аналогично антивирусной защите.

В России отсутствуют нормы прямого действия, регулирующие отношения в сервисе электронной почты, на что неоднократно обращалось внимание. Можно согласиться с А.И. Афониным, отмечающим, что "в общем случае правоотношения, возникающие в результате причинения вреда адресатам при поступлении незапрошенных электронных сообщений, являются частными отношениями"[29]. Однако при распространении спама имеет значение соотношение интересов частного и публичного.

При поступлении незапрошенных электронных сообщений адресаты могут использовать следующие правовые механизмы: возбуждение гражданского дела по заявлению адресата (основанием могут служить причинение вреда, нарушение обычаев делового оборота и др.); возбуждение дела об административном правонарушении при наличии оснований, например по фактам распространения ненадлежащей рекламы, изготовления и распространения агитационных материалов с нарушением требований закона.

Упущенный вызов получил широкое распространение за рубежом, но в последнее время этот вид противоправных действий начал встречаться и в крупных городах России. Злоумышленник дозванивается до жертвы и прерывает связь, не дожидаясь ответа. Многие из любопытства перезванивают на определившийся незнакомый номер, который коммутируется на службу платных телефонных услуг. Деньги автоматически списываются со счета абонента или вписываются в счет

[24] Разработан общественно-государственным объединением "Ассоциация документальной электросвязи" в соответствии с поручением министра Российской Федерации по связи и информатизации в 2003 г.

[25] Финская компания "F-Secure" достигла соглашений об антивирусной защите сетей финского оператора Elisa и шведского оператора Swisscom. Японский оператор NTT DoCoMo заключает контракт с производителем антивирусов McAfee.

[26] *Зомби-сеть*, или *ботнет*, – сеть зараженных компьютеров и серверов, централизованно управляемых злоумышленниками, которые получают полный доступ к системе.

[27] *Г. Клули* (Graham Cluley) – старший консультант по вопросам технологий компании "Sophos" (см.: *Емельянова О.* Криминальное чтиво // http://www.spamtest.ru/document.html? context=15925. 2005. 24 авг.).

[28] См.: SMS-спам заглушит мобильники // http://bonanza.com.ua/news_detail.asp?num=1250. 2005. 13 окт.

[29] *Афонин А.И.* Указ. соч. С. 17.

на оплату услуг связи, отсылаемый по почте. К стандартному счету за услуги мобильной связи это отношения не имеет, но многие абоненты оплачивают все, не вникая в подробности. В Японии, где этот вид мошенничества получил широкое распространение, законодательство не предусматривает ответственности за данное деяние, и полиция лишь советует гражданам соблюдать осторожность и не разговаривать с незнакомцами по мобильному телефону. После введения в России оплаты только за исходящие разговоры следует ожидать увеличения в нашей стране такого рода мошенничества. Однако ввиду малого размера посягательства не следует ожидать увеличения обращений граждан, хотя действия злоумышленника в этом случае могут быть квалифицированы как правонарушение, предусмотренное ст. 7.27 КоАП РФ "Мелкое хищение".

Блокирование канала связи абонента как способ совершения воздействия на конкурента стал возможным с появлением автоматических систем и программируемых аппаратов связи. Поставив на автодозвон телефонные номера конкурентов, злоумышленник лишит его канала связи. В случае когда основой бизнеса являются информационные услуги, дискредитация коммутационного канала даже в течение непродолжительного срока может разорить конкурента. Аналогичная операция может быть применена в отношении его партнеров. В период, когда он должен получить или отправить срочное сообщение, его номер и номера его партнера блокируются. Результатом могут стать срыв контракта, дискредитация имиджа конкурента и его разорение. Сложность рассматриваемой ситуации в том, что определить описанное внешнее блокирование может только оператор связи, в биллинговой базе данных которого будут зафиксированы все попытки доступа к номеру абонента. Однако вряд ли оператор возьмет на себя ответственность за допущенное блокирование канала связи, которое привело к упущенной выгоде, моральным издержкам и др.

Обман и вымогательство за несовершенное преступление – один из новых способов мошеннических действий. Мошенник дозванивается до жертвы и, имитируя голос близкого родственника, говорит, что он попал в ДТП или другую неприятную ситуацию с участием представителей правоохранительных органов. Для неформального решения вопроса срочно нужны деньги. Различия в голосе объясняют волнением, плохой связью, лицевыми травмами при аварии, а звонок с чужого телефона – поломкой, потерей своего аппарата во время аварии или севшим аккумулятором. Затем телефон передается якобы представителю власти, который сообщает, что для освобождения родственника необходимо приобрести карты оплаты на крупную сумму (вплоть до нескольких тысяч) и продиктовать их коды по указанному номеру. В другом варианте предлагается привезти крупную сумму денег по указанному адресу и передать посреднику. На все операции жертве дают мало времени, постоянно перезванивая[30].

Мошенничество с оплатой путем перечисления имеет несколько вариантов исполнения. Первый вариант – звонок абоненту от имени оператора связи и сообщение о необходимости пополнить счет через карту оплаты. Абонент вводит платежные данные по указанному номеру, переведенному на подставную систему пополнения счета, и слушает рапорт автоответчика о поступлении средств. На самом деле деньги оказываются на счете мошенника. Несмотря на примитивность уловки, некоторые попытки достигают успеха.

Другой вариант – звонок или SMS-сообщение от имени известной радиостанции или торгового предприятия о выигрыше абонента в лотерее. Для получения награды необходимо приобрести карты оплаты на определенную сумму и продиктовать их скретч-коды. Когда денег собрано достаточно (все деньги переведены на нужные телефоны), а подозрения жертв еще не достигли критической отметки, мошенники выбрасывают отработанную SIM-карту и начинают все заново.

Во всех перечисленных случаях злоумышленники рассчитывают на доверчивость абонентов и их незнание особенностей работы биллинговой системы оператора сотовой связи. Рассмотренные противоправные деяния могут быть квалифицированы как правонарушения, предусмотренные ст. 7.27 КоАП РФ "Мелкое хищение". Однако следует учитывать, что SMS-рассылка производится во множественном количестве, что позволяет поставить вопрос о квалификации данных действий по ст. 159 УК РФ, поскольку налицо "хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием". База данных оператора связи незаконно используется злоумышленниками как справочник абонентов.

Мошенничество в роуминге осуществляется преступником при подключении из иностранной сети с использованием того факта, что оператор в его стране получит запись роуминг-звонка от оператора зарубежной сети через временной промежуток. Убытки составляют неоплаченные соединения[31]. Доказа-

[30] См.: *Воронин А.* Фрод или сотовые мошенники // http://www.3dnews.ru/phone/fraud. 2006. 20 июля.

[31] Примером является случай, когда злоумышленники зарегистрировали подставную компанию, арендовали платный номер во Франции и купили у российского оператора 50 телефонов, подключенных по кредитному тарифному плану. Затем они перевезли эти телефоны во Францию и поставили их на автодозвон до арендованного платного номера. Так они сгенерировали огромное количество очень дорогого трафика, приходящегося на этот номер. В конце месяца "France Telecom" выплатил арендаторам номера несколько сотен тысяч долларов. Единственным пострадавшим от мошенников оказался российский сотовый оператор, которому французская компания выставила роуминговые счета в размере около полумиллиона долларов (см.: http://www.phreaking.ru/showpage.php?s=&pageid=54239. 2006. 17 мая).

тельством вины мошенника могут служить записи соединений, представленных оператором или другой телефонной компанией, которая является членом соглашения о роуминг-сотрудничестве. Однако возникают проблемы в части применения правовых норм, оформления и передачи доказательств, выдачи преступников. Важным является вопрос об определении места совершения преступления, поскольку соединения происходят за пределами территории государства, на которой находится оператор. Записи переговоров позволяют установить страну, из которой был сделан звонок.

Подводя итог рассмотрению методов правового регулирования информационных правоотношений, возникающих при легальном и нелегальном обороте баз данных операторов связи, можно сделать вывод о наличии значительных недоработок в данной сфере. При этом существующие технологии противоправной деятельности разнообразны и постоянно совершенствуются. Следует отметить, что во всех рассмотренных случаях существенную роль играет неправомерный доступ к базам данных операторов электросвязи, которые используются злоумышленниками для получения информации об абонентах. Для защиты граждан от посягательств на тайну личной жизни необходима строгая правовая регламентация оборота баз данных. Только введение строгой ответственности операторов баз данных за нарушения сбора хранения и использования персональных данных об абонентах позволит гарантировать действенные меры правовой защиты интересов отдельных граждан и общества в целом.