МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ЮРИДИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ И КРИМИНАЛИСТИКИ

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-РЕСУРСОВ И ПРАВОВОГО РАЗРЕШЕНИЯ КОНФЛИКТОВ С УЧАСТИЕМ СУБЪЕКТОВ ИНТЕРНЕТ-СООБЩЕСТВА

Материалы международной научно-практической конференции, посвященной 20-летию Юридического института НИУ «БелГУ» в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апреля 2013 г.

Белгород 2013

Министерство образования и науки Российской Федерации
Белгородский государственный национальный исследовательский университет
ЮРИДИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА СУДЕБНОЙ ЭКСПЕРТИЗЫ И КРИМИНАЛИСТИКИ

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-РЕСУРСОВ И ПРАВОВОГО РАЗРЕШЕНИЯ КОНФЛИКТОВ С УЧАСТИЕМ СУБЪЕКТОВ ИНТЕРНЕТ-СООБЩЕСТВА

Материалы международной научно-практической конференции, посвященной 20-летию Юридического института НИУ «БелГУ» в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апреля 2013 г.

Белгород 2013

УДК 343.98:340.6
ББК 67.52+67.711-91
П 78

Печатается по решению
редакционно-издательского совета
НИУ «БелГУ»

Организационный комитет конференции:

председатель – и.о. ректора НИУ «БелГУ», доктор политических наук, профессор ***О.Н. Полухин***

заместитель председателя – директор Юридического института НИУ «БелГУ», доктор юридических наук, профессор ***Е.Е. Тонков***

заместитель председателя, ответственный редактор – заведующий кафедрой судебной экспертизы и криминалистики, доктор юридических наук, профессор ***И.М. Комаров***

П 78 **Проблемы законодательного регулирования Интернет-ресурсов и правового разрешения конфликтов с участием субъектов Интернет-сообщества :** материалы междунар. науч.-практ. конф. в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апр. 2013 г.: / отв. ред. И.М. Комаров. – Белгород : ИД «Белгород» НИУ «БелГУ», 2013. – 276 с.

ISBN 978-5-9571-0683-8

В сборнике представлены материалы конференции «Проблемы законодательного регулирования Интернет-ресурсов и правового разрешения конфликтов с участием субъектов Интернет-сообщества», посвященной 20-летию Юридического института НИУ «БелГУ», которая состоялась 19 апреля 2013 года в Белгородском государственном национальном исследовательском университете.

Для студентов, аспирантов, преподавателей вузов, научных работников и практикующих юристов, а также читателей, проявляющих интерес к криминалистике и судебной экспертизе.

УДК 343.98:340.6
ББК 67.52+67.711-91

ISBN 978-5-9571-0683-8

СОДЕРЖАНИЕ

Авдеева Г.К.

ИННОВАЦИОННЫЕ ПРИЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Проанализированы следы преступлений в сфере использования информационных технологий, а также инновационные средства и методы борьбы с ними.

Ключевые слова: инновационный прием, информационная технология, компьютерная преступность.

Abstract. Analyzed traces of crimes in the sphere of information technologies, as well as innovative means and methods of struggle with them.

Key Words: innovative technique, information technology, computer crime.

Развитие современных информационных технологий[1] и телекоммуникационных систем, компьютеризация общества в целом приводят к появлению новых средств и методов преступной деятельности. Это, в свою очередь, требует использования инновационных приемов для своевременного выявления, квалифицированного расследования и профилактики преступлений в сфере использования информационных технологий.

Инновационными являются не любые нововведения, а лишь такие средства и методы, которые существенно повышают эффективность определенной деятельности.

Преступления в сфере использования электронно-вычислительных машин, систем и компьютерных сетей (раздел 16 – ст. ст. 361-363 УК Украины) подразделяются на такие виды:

– несанкционированный доступ в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей;

– создание с целью использования, распространения или сбыта вредоносных программных продуктов или технических средств, а также их распространение или сбыт;

– несанкционированные сбыт или распространение информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации;

– преступления, совершенные путем использования компьютерной системы, как средства достижения преступной цели и другие.

---

1 В Законе Украины «О Национальной программе информатизации» указано, что «информационной технологией (IT) является целенаправленная организованная совокупность информационных процессов с использованием средств вычислительной техники, обеспечивающих высокую скорость обработки данных, быстрый поиск информации, доступ к информации независимо от места ее расположения». – См.: Про Національну програму інформатизації. Закон України // ВВР, 1998, N 27-28, ст.181 с изменениями, внесенными в соответствии с Законом N 2684-III от 13.09.2001, ВВР, 2002, N 1, ст.3.

Одним из средств совершения преступления в сфере использования компьютерных технологий являются вредоносные программные продукты.

Сегодня в сети Интернет размещены предложения хакеров по осуществлению DDoS-атак[1] за деньги. 12 января 2013 в Киеве задержан хакер, который совершал такие атаки на сайты украинских и зарубежных коммерческих структур по заказу конкурентов. В целях конспирации хакер общался с заказчиками через анонимные интернет-пейджеры, а средства получал с помощью виртуальных платежных систем, зарегистрированных на подставных лиц.

Термин «преступления, совершаемые с использованием компьютерных технологий» охватывают все действия, предполагающие использование достижений этих технологий и те, которые посягают на компьютерную информацию.

В криминалистическом аспекте такое определение позволило разработать инновационные типовые приемы, средства и методы обнаружения, фиксации и исследования компьютерной информации.

Одним из важнейших определяющих факторов в борьбе с данными преступлениями является область их совершения – киберпространство. Киберпространством называют сферу существования компьютерной информации, которая образована совокупностью средств компьютерной техники[2].

Компьютерная информация[3] в зависимости от характера преступных деяний выступает как предмет посягательства и как область возможного сохранения следов преступной деятельности.

Компьютерная информация имеет ряд специфических свойств:

– отсутствие неразрывной связи с материальным носителем;

– динамичность, возможность мгновенного переноса в пространстве (в том числе из одной части земного шара в другую);

– возможность изменения и уничтожения информации любого объема за короткие промежутки времени (в т.ч. – при помощи удаленного доступа)[4].

Кроме того, все копии компьютерной информации (не зависимо от вида носителя) идентичны оригиналу.

Компьютерная информация является новым объектом криминалистического исследования, а компьютерная техника – как технико-

---

[1] DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) – атака при помощи вредоносного программного обеспечения на компьютерную систему с целью ее блокировки, создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам). Атаку, осуществляемую одновременно с большого числа компьютеров, называют DDoS-атакой. – См.: Дремлюга Р.И. Интернет-преступность: моногр. / Р.И. Дремлюга. – Владивосток: Изд-во Дальневост. ун-та, 2008. – С. 23.

[2] См: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж: Издательство Воронежского государственного университета, 2002. – С. 41.

[3] Компьютерной информацией является информация в электронном (цифровом) виде, которая может быть зафиксирована на определенном носителе, в электронно-вычислительной машине (ЭВМ), в телекоммуникационной системе или сети ЭВМ.

[4] Криминалистика: Учебник / Под ред. Т.А. Седовой, А.А. Эксархопуло. – СПб.: Издательство «Лань», 2001. – С. 370.

криминалистический средство для работы с компьютерной информацией, придает этой информации значение источника доказательства.

В частности, сегодня разработано и используется значительное количество эффективных средств восстановления уничтоженной электронной информации.

В зависимости от ситуации и решаемых задач к осмотру средств компьютерной техники и поиску необходимой цифровой информации привлекают специалиста в области компьютерной техники, программных продуктов, телекоммуникационных сетей и средств.

При осмотре и исследовании операционной системы компьютера можно получить данные об информации, хранящейся в памяти компьютера. Например, можно установить последовательность действий, выполнявшихся ранее пользователем, а также информацию о преступнике и его определенной деятельности.

Следы совершения преступления в сфере компьютерной информации редко остаются в виде изменений внешней среды. Они носят информационный характер, т.е. представляют собой внесение изменений в компьютерную информацию.

Информационные следы образуются в результате воздействия на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Такими изменениями могут быть следы уничтожения, модификации, копирования, блокирования информационной системы. Следы изменений остаются на машинных носителях информации и отражают изменения в информации, которая в них хранится, (по сравнению с исходным состоянием). Часто преступниками осуществляются модификации баз данных, программ, текстовых файлов, находящихся на жестких дисках ЭВМ, дискетах, магнитных мини-дисках, флешкартах, оптических дисках, предназначенных для многократной перезаписи информации.

Кроме того, электронная информация может нести следы ее частичного уничтожения или модификации (удаление из каталогов имен файлов, удаления или добавления отдельных записей, физического разрушения или размагничивания носителей). Информационными следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть обнаружены при экспертном исследовании компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, программного обеспечения.

Наиболее часто встречаются такие информационные следы в сети Интернет, позволяющие установить лицо, совершившее неправомерный доступ к компьютерной информации:

Данные о фирме-провайдере, при помощи которого пользователь подключен к сети Интернет. В сети Интернет существует специальная служба Whois, предназначенная для установления наименования и адреса провайдера, через которого произошел неправомерный доступ. В общедоступном сервисе по адресу www.ripe.net необходимо указать электронный адрес (IP) атакующего

компьютера. Время работы абонента в сети можно установить у провайдера по специальному лог-файлу (журналу).

Протокол выхода в Интернет с определенного компьютера автоматически ведется на каждом компьютере, с которого возможен выход во всемирную сеть. Совпадение данных этого протокола с лог-файлом провайдера может служить неоспоримым доказательством несанкционированного доступа в определенную компьютерную систему.

Данные о пользователе электронной почты (фамилия, имя, отчество, дата и место рождения, место жительства, работы и проч.).

Данные о пользователе социальных сетей (фотоснимки, родственники, друзья, интересы, контакты и др.), устанавливаемые посредством поиска по электронному адресу, фамилии и др.

Большую информационную ценность имеют смс-сообщения, которые автоматически фиксируются и накапливаются на сервере мобильного оператора. Можно получить у оператора мобильной связи распечатку перечня телефонных звонков и текстов смс-сообщений.

В 2002 году изучение и анализ смс-сообщений позволили обезвредить организованную преступную группу, которая в Харькове, Киеве, Запорожье и др. городах Украины при помощи различных мошеннических действий и «театральных» представлений шантажировала состоятельных людей и в течение нескольких лет получала огромные суммы денежных средств.

Многие программы фирмы Microsoft создают резервные копии файлов, файлы-отчеты, хранят информацию о последних проведенных операциях и выполненных программах, а также содержат иную информацию, имеющую значение для расследования. В частности, почтовая программа Microsoft Outlook Express сохраняет в своей базе данных все письма, которые были отправлены, получены или удалены. Браузер Microsoft Internet Explorer сохраняет информацию о местах в сети Интернет, которые посетил пользователь.

Следами, указывающими на посторонний доступ к информации, могут быть такие: переименование каталогов и файлов, изменение размеров и содержимого файлов, изменение стандартных реквизитов файлов, даты и времени их создания; появление новых каталогов, файлов и другие следы.

Наиболее распространенный вид мошенничества в системах интернет-банкинга состоит из трех основных этапов: получение информации для осуществления неправомерного доступа в систему «Клиент-банк», проведение мошеннической операции и перевод денежных средств в наличные.

Для хищения персональных (авторизационных) данных пользователя системы ДБО – дистанционного банковского обслуживания – (логина, пароля и ключей подписи) злоумышленники используют специальное вредоносное программное обеспечение. Чаще всего это – модификации хорошо известных банковских троянов с дополнительными функциями[1].

---

[1] Комплексное расследование мошенничества в системах интернет-банкинга. [Электронный ресурс]. – Режим доступа: http://www.group-ib.ru/images/media/Group-IB_AntiFraud.pdf.

Новейшие методы и методики судебной экспертизы телекоммуникационных сетей и средств позволяют установить факт несанкционированного доступа к банковской системе, время такого доступа и IP-адрес компьютера, с которого он осуществлялся.

В компьютере преступника часто хранятся экземпляры скопированной с компьютера «жертвы» информации, а также так называемые «скриншоты» (графические изображения экраны монитора компьютера-»жертвы»). Там могут быть обнаружены присланные с компьютера-жертвы значения паролей и «логинов» для входа в определенную информационную сеть, копии украденной электронной корреспонденции и другая информация.

Сегодня для решения проблем борьбы с компьютерными преступлениями криминалистами исследуется технический характер их осуществления. Особое внимание уделено разработке новейших технических средств и приемов обнаружения, изъятия, фиксации и исследования следов преступлений с использованием компьютерных технологий.

Борьба с компьютерной преступностью не ограничивается установлением уголовной ответственности за конкретное совершенное преступление. Сегодня активно осуществляется построение международной системы борьбы с данными видами преступлений, объединяются необходимые кадры, разрабатываются методики, уточняются процедуры взаимодействия с международными структурами и правоохранительными органами других стран (в т.ч. – при помощи телекоммуникационных средств и систем).

Авершин С.О.
Степанюк А.В.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ, РАСПРОСТРАНЯЕМОЙ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Аннотация. Доклад посвящен рассмотрению вопросов правового регулирования защиты детей от информации, причиняющей вред их здоровью и развитию, распространяемой посредством информационно-телекоммуникационных сетей, выделению проблемных вопросов противодействия распространению вредоносной информации.

Ключевые слова: информационно-телекоммуникационные сети; защита детей от информации, причиняющей вред их здоровью и развитию; вредоносная информация.

Abstract. The report deals with examination of the issues related to legal regulation of protection of children against information impairing their health and development which is distributed through information and telecommunication networks, identification of problematic issues related to countermeasures against harmful information distribution.

Key words: information and telecommunication networks, the protection of children from information harmful to their health or development; malicious information.

Развитие технологий в последние десятилетия привело к тому, что возможности доступа граждан к информации различного рода принципиально расширились. Необходимую информацию заинтересованные лица получают не только из традиционных источников – печатных изданий, радио и телевидения, но и из информационно-телекоммуникационных сетей, прежде всего, сети «Интернет». И если еще несколько лет назад для работы с данной сетью требовался персональный компьютер, то сегодня все ресурсы сети «Интернет» доступны через средства подвижной связи, т.е. через телефоны, смартфоны и т.п. С одной стороны это сделало процесс получения необходимой информации более оперативным, но с другой – доступ к информационным ресурсам практически стал неконтролируемым. Взрослый человек в силу своего развития и жизненного опыта сам способен защитить себя от негативного воздействия информации, критически отнестись к ее содержанию, чего нельзя сказать о несовершеннолетних. При этом, ни для кого не является секретом, что в сети «Интернет» широчайшим образом распространены информационные ресурсы, которые способны нанести непоправимый вред здоровью, нормальному развитию ребенка и даже его жизни. Это информационные ресурсы поощряющие и делающие привлекательным употребление наркотических средств и психотропных препаратов, ресурсы развивающие суицидальные наклонности и др.

Долгое время законодатель не уделял данному вопросу должного внимания, отсутствовал комплексный подход к решению проблемы защиты детей от вредоносной информации. Ситуация изменилась с принятием Федерального за-

кон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1] (далее – Закон о защите детей).

Прежде всего, Закон о защите детей ввел ряд понятий, которые свидетельствуют о распространении его действия на отношения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Так, п.5 ст.2 указанного закона предусматривает понятие «информационная продукция», под которой понимается предназначенная для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, ***посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет»***, и сетей подвижной радиотелефонной связи. В свою очередь, в п.12 ст.2 содержится понятие «оборот информационной продукции», т.е. предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, ***информационно-телекоммуникационных сетей, в том числе сети «Интернет»***, и сетей подвижной радиотелефонной связи.

Закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред здоровью и (или) развитию детей, т.е. информации (в том числе содержащейся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в установленном порядке. При этом, изучение закона показывает, что законодатель рассматривает в качестве одного из наиболее вредоносных видов информации – информацию порнографического характера. В соответствии с п.8 ст.2 Закона о защите детей информация порнографического характера – это информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного. При этом под натуралистическим изображением или описанием понимается изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах. Следует отметить, что в Законе о защите детей впервые в современном российском законодательстве предпринята попытка формулировки определения понятия «информация порнографического характера», что имеет важное значение не только для достижения целей указанного закона, но и для применения положений уголовного законодательства при осуществлении борьбы с оборотом материалов порнографического характера.

---

[1] См.: Собрание законодательства РФ. 2011. № 1. Ст.48; 2012. № 31. Ст.4328.

В ст.5 Закона о защите детей детализируются виды информации, причиняющей вред здоровью и (или) развитию детей. Данная информация подразделяется на информацию, запрещенную к распространению среди детей, и информацию, распространение которой среди детей определенных возрастных категорий ограничено.

Так, согласно ч.2 ст.5 Закона о защите детей **информация, запрещенная для распространения среди детей** – это информация: 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных законом; 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; 5) оправдывающая противоправное поведение; 6) содержащая нецензурную брань; 7) содержащая информацию порнографического характера.

В соответствии с ч.3 ст.5 Закона о защите детей **информация, распространение которой среди детей определенных возрастных категорий ограничено**, – это информация: 1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия; 2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий; 3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной; 4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Важным положением Закона о защите детей является выделение категории информационной продукции в зависимости от возраста детей (ч.3 ст.6). При этом выделяются следующие категории информации: 1) информационная продукция для детей, не достигших возраста шести лет; 2) информационная продукция для детей, достигших возраста шести лет; 3) информационная продукция для детей, достигших возраста двенадцати лет; 4) информационная продукция для детей, достигших возраста шестнадцати лет; 5) информационная продукция, запрещенная для детей.

В ст.ст.7-10 Закона о защите детей раскрывается содержание понятия «информационная продукция», применительно к каждой из указанных категорий. Согласно ч.1 ст.6 Закона о защите детей производитель или распространитель должен, руководствуясь критериями, установленными в ст.ст.7-10 Закона о защите детей, самостоятельно осуществить классификацию своей продукции. Классификация продукции является основанием для размещения на ней знака информационной продукции с целью оборота на территории РФ. При этом, в соответствии с Законом классификацию можно осуществить при помощи экс-

перта, экспертов или экспертной организации. Порядок проведения экспертизы регламентируется Приказом Министерства связи и массовых коммуникаций Российской Федерации от 29 августа 2012 года № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей»[1]. Обращение в данном случае к экспертному сообществу представляется целесообразным, поскольку самостоятельная классификация может оказаться неправильной, а ведь от этого зависит решение о привлечении виновного (виновных) к ответственности (административной, уголовной или гражданской).

Отдельно законодатель регламентировал особенности распространения информации посредством информационно-телекоммуникационных сетей (ст.14 Закона о защите детей). Так, доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», в местах, доступных для детей, предоставляется лицом, организующим доступ к сети «Интернет» в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию. Сайт в информационно-телекоммуникационной сети «Интернет», не зарегистрированный как средство массовой информации, может содержать знак информационной продукции (в том числе в машиночитаемом виде) и (или) текстовое предупреждение об ограничении ее распространения среди детей, соответствующие одной из категорий информационной продукции, установленных ч.3 ст.6 Закона о защите детей. Классификация сайтов осуществляется их владельцами самостоятельно согласно требованиям закона.

Принятие Закона о защите детей, безусловно, имеет положительный характер. Но, представляется необходимым обратить внимание на некоторые обстоятельства, которые, по нашему мнению, способны снизить эффективность противодействия распространению вредоносной информации через информационно-телекоммуникационные сети, в том числе и сеть «Интернет».

Во-первых, перечень распространителей и источников вредоносной информации достаточно широк. Он включает в себя и средства массовой информации, и печатную продукцию, и аудиовизуальную продукцию на любых видах носителей, и программы для электронных вычислительных машин (программы для ЭВМ), базы данных, зрелищные мероприятия, а также информационно-телекоммуникационные сети, в том числе сеть «Интернет», и сети подвижной радиотелефонной связи. Однако, такие источники как, например, печатная продукция, зрелищные мероприятия относительно легко поддаются контролю. Нарушение Закона о защите детей невыгодно, прежде всего, самим распространителям и организаторам. Но, если говорить о сети «Интернет», которая исключительно глобализирована, то осуществление контроля практически невозможно. Любая попытка взять под контроль поток информации, распространяемой через «Интернет» рассматривается в определенных кругах как посягательство на достижения демократии и свободу слова, т.е. цензура. Однако, цинизм подобного

[1] http://www.rsoc.ru/mass-communications/p679/ – официальный сайт Роскомнадзора.

подхода выражается в том, что в жертву приносятся личные ценности, права интересы одной из самых уязвимых категорий российских граждан – детей.

Во-вторых, недостаточно эффективным представляется механизм формирования специального реестра доменных имен, указателей страниц сайтов, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный вопрос регламентируется постановлением Правительства РФ от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». В настоящее время организация ведения реестра распределена между Роскомнадзором (информация порнографического характера), ФСКН (информация, побуждающая употреблять наркотические средства, психотропные и одурманивающие препараты) и Роспотребнадзором (информация, побуждающая к суициду). Однако, обращают на себя внимание следующие обстоятельства: 1) реестр является закрытым; 2) реагирование на выявляемые ресурсы нельзя признать оперативным; 3) ресурс, содержащий вредоносную информацию, может достаточно быстро поменять место своего размещения. Наличие проблемы в этой области признается и самими уполномоченными ведомствам, о чем свидетельствует пресс-релиз Роспотребнадзора о взаимодействии с интернет-сообществом по профилактике суицида[1].

Подводя итог сказанному, нам бы хотелось отметить, что вопрос о защите детей от вредоносной информации, распространяемой через информационно-телекоммуникационные системы, нуждается не только в надлежащем правовом регулировании, но и в создании эффективных организационно-технических механизмов пресечения проникновения данной информации в российское информационное пространство и создания вредоносных ресурсов на территории России. Ужесточение мер контроля, противодействия и ответственности в данной сфере не может рассматриваться как ограничение мнимых «демократических» достижений, а является закономерным и неизбежным средством защиты прав и законных интересов российских граждан, интересов национальной безопасности и конституционных основ российской государственности. Следует отметить, что борьба с распространением вредоносной информации через «Интернет» является не только обязанностью государства, но и конституционным долгом каждого гражданина (например, сообщить об опасном контенте можно через сайт Лиги безопасного интернета – http://www.ligainternet.ru/hotline.php).

[1] http://rospotrebnadzor.ru/press_center/-/asset_publisher/0L3h/content – официальный сайт Роспотребнадзора.

Андреев Ю.Н.

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

Аннотация. Статья посвящена выявлению некоторых особенностей исключительных прав на результаты интеллектуальной деятельности и средства индивидуализации. Ссылаясь на эти особенности, автор пытается обосновать существование такой подотрасли гражданского права как исключительное право

Ключевые слова: исключительные права, результаты интеллектуальной деятельности, средства индивидуализации, способы защиты исключительных прав.

Abstract. Article is devoted to some of the features of the exclusive rights to results of intellectual activity and means of individualization. Referring to these features, the author tries to prove the existence of a sub-branch of civil law as the exclusive right

Key words: exclusive rights of intellectual property, means of identification, how to protect the exclusive rights.

Исключительные права являются видовым понятием интеллектуальных прав, регулирующих общественные отношения в особой сфере человеческой деятельности – интеллектуальной. Для результатов интеллектуальной деятельности характерны творческое начало, новизна, оригинальность. В переводе с латинского языка интеллект (intellectus) – это ум, рассудок, разум, мыслительная способность человека[1].

Современные исключительные права на результаты интеллектуальные деятельности и средства индивидуализации в объективном смысле – это совокупность правовых норм, позволяющих их правообладателям (авторам, исполнителям, изготовителям, вещательным организациям, патентообладателям, обладателям товарных знаков, фирменных наименований и коммерческих обозначений) удовлетворять свои имущественные интересы, монопольно использовать принадлежащие им результаты интеллектуальной деятельности, средства индивидуализации и распоряжаться этими правами исключительно самим по собственному усмотрению на предусмотренных законом условиях с запрещением другим лицам пользоваться этими правами и результатами интеллектуальной деятельности, средствами индивидуализации без согласия правообладателя, за исключением случаев, предусмотренных законом.

Под субъективными исключительными правами понимаются права конкретного субъекта интеллектуальных правоотношений (управомоченного лица) по беспрепятственному осуществлению известных действий и полномочий в отношении результатов своей интеллектуальной деятельности и средств индивидуализации, а также возможность требовать от обязанного лица исполнения возложенных на него обязанностей, обращаться к уполномоченным законом органам власти и должностным лицам за защитой своих нарушенных или оспариваемых прав.

---

[1] См.: Словарь иностранных слов / Отв. редакторы В.В. Бурцева, Н.М. Семенова. – М.: Русь. яз. – Медиа, 2003. – С. 264.

Конституция нашей страны гарантирует свободу литературного, художественного, научного, технического и других видов творчества. Интеллектуальная собственность охраняется законом (ч. 1 ст. 44). Исключительные права на результаты интеллектуальной деятельности признаны нормами международного права, многими зарубежными государствами. Российская Федерация является участницей ряда соответствующих международных договоров, конвенций и соглашений[1].

В части четвертой ГК РФ создана стройная система исключительных прав на: 1) авторские произведения; 2) объекты смежных прав (исполнения артистов-исполнителей, дирижеров, постановки режиссеров; фонограммы; сообщения передач организаций эфирного и кабельного вещания; базы данных; произведения науки, литературы и искусства, обнародованные после перехода в общественное достояние); 3) объекты патентных прав (изобретения, полезные модели, промышленные образцы); на нетрадиционные объекты «промышленной собственности» (секреты производства, топологии интегральных микросхем, селекционные достижения); 4) средства индивидуализации (фирменное наименование, товарный знак (знак обслуживания), наименование места происхождения товара, коммерческое обозначение).

Своим названием исключительные права обязаны субъектному составу, содержанию, назначению, социальной функции и иным существенным признакам исключительности.

Обладателем исключительных прав на результат интеллектуальной деятельности, средство индивидуализации российский закон признает определенный круг лиц. Только исключительно законный обладатель этих субъективных прав, за исключением случаев, предусмотренных законом, может использовать результат своей интеллектуальной деятельности или средство своей индивидуализации по своему усмотрению любым не противоречащим закону способом, распоряжаться принадлежащим ему правом на тот или иной результат своей интеллектуальной деятельности или средство индивидуализации.

Гражданским кодексом предъявлены повышенные требования к установлению и соблюдению процедуры признания государством исключительного права конкретного заявителя на конкретный объект – результат интеллектуальной деятельности (см., например, ст. 1374 – 1400 ГК РФ).

---

[1] См., например: Конвенция, учреждающая Всемирную организацию интеллектуальной собственности (Стокгольм, 14 июля 1967 г.; вступила в силу для СССР 26 апреля 1970 г.); Бернская конвенция по охране литературных и художественных произведений (Берн, 9 сентября 1886 г.; вступила в силу для Российской Федерации 13 марта 1995 г.); Всемирная конвенция об авторском праве (Женева, 6 сентября 1952 г.; вступила в силу для СССР 27 мая 1973 г.); Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Рим, 26 октября 1961 г.; вступила в силу для Российской Федерации 26 мая 2003 г.); Конвенции об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм (Женева, 29 октября 1971 г.; вступила в силу для Российской Федерации 13 марта 1995 г.).

В содержание исключительных прав входят право использования и право распоряжения этими правами. Гражданин или юридическое лицо, обладающее исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации, вправе использовать такой результат или средство по своему усмотрению любым не противоречащим закону способом. Другие лица не могут использовать результат интеллектуальной деятельности или средство индивидуализации без согласия законного правообладателя, за исключением случаев, предусмотренных законом. Несогласованное использование чужого интеллектуального продукта или приравненного к нему средства индивидуализации за исключением случаев, предусмотренных законом, является правонарушением, влекущим за собой гражданско-правовую, административную или уголовную ответственность (ст. 1229 ГК РФ).

Еще в конце XIX начале XX в.в. талантливый исследователь проблем интеллектуального права Г.Ф. Шершеневич писал, что так же как вещное право является юридической возможностью пользования материальными вещами с устранением всех прочих от пользования теми же объектами, исключительное право представляет юридическую возможность совершения известного рода действий с устранением всех прочих от подражания. Именно в связи с предоставлением известным лицам исключительной возможности совершения известных действий с запрещением всем остальным возможности подражания Габриэль Феликсович предлагал называть права субъектов интеллектуальной деятельности (авторские, промышленные) исключительными правами[1].

Совместный Пленум Верховного Суда РФ и Пленум Высшего Арбитражного Суда РФ подчеркнул, что, согласно п. 1 ст. 1233 ГК РФ правообладатель может распорядиться принадлежащим ему исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации любым не противоречащим закону и существу такого исключительного права способом[2].

Исключительное право на результат интеллектуальной деятельности и средства индивидуализации может быть передано автором другому лицу по договору, а также перейти к другим лицам по иным основаниям, установленным законом (ст. 1228 ГК РФ). В законе указывается на такие внедоговорные формы правопреемства, как наследование, реорганизация юридического лица и обращение взыскания на имущество правообладателя.

К числу качественных характеристик объектов исключительных прав ряд ученых относит нематериальный характер, коммерческую ценность, эстетическое, информационное содержание, возможность обособления от других объек-

---

[1] См.: Шершеневич Г. С. Авторское право на литературные произведения. – Казань, 1891. – С. 73; Он же: Учебник русского гражданского права (по изд. 1907 г.). – М.: Спарк, 1995. – С. 254 – 255.

[2] См.: Постановление Пленума Верховного Суда РФ и Пленума Высшего Арбитражного Суда РФ от 26 марта 2009 г. № 5/29 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» (п. 11 и 12) // Бюллетень Верховного Суда РФ. – 2009. – № 6.

тов[1]. Другие исследователи выделяют такие признаки, как нематериальная природа, объективная форма, передаваемость посредством воспроизведения, правовая определенность, коммерческая ценность[2]. Третья группа исследователей называют такие черты объектов исключительных прав, как стоимостная оценка, наличие авторов, непотребляемость, возможность использования неопределенным кругом лиц,[3] легитимность, новизна, объективная форма[4].

Несмотря на то, что результаты интеллектуальной деятельности содержатся в материальном носителе, имеют объективированную форму, в юридической науке и законодательстве вполне обоснованно признают их нематериальность. Сохраняя свой идеальный характер, результаты интеллектуальной деятельности выражаются в объективной форме, доступной для восприятия индивидом посредством фиксации нематериальных пространственных, изобразительных или звуковых образов на материальных носителях с помощью различных технических средств. Будучи разновидностью интеллектуальных прав, исключительные права не зависят от права собственности на материальный носитель (вещь), в котором выражены соответствующие результат интеллектуальной деятельности или средство индивидуализации. Переход права собственности на вещь не влечет переход или предоставление исключительных прав на результат интеллектуальной деятельности или на средство индивидуализации, выраженные в этой вещи, за исключением случая, предусмотренного пунктом 2 ст. 1291 ГК РФ (ст. 1227 ГК РФ).

Обладая нематериальным характером, исключительное право имеет в то же время имущественный характер. Наделением таким свойством исключительное право обязано прежде всего юридической возможности использовать произведение для удовлетворения авторских личных имущественных интересов, участию в имущественном обороте на возмездной основе, способности выполнять функции товара. Не являясь вещью в ее классическом (римском) понимании, исключительные права имеют все-таки имущественно – меновое значение для правообладателя. В ст. 1226 ГК РФ исключительное право прямо называется имущественным правом.

Исключительность «исключительного права» подчеркивается и набором специфических способов его защиты с учетом существа нарушенного права и последствий правонарушения. В целях защиты законных интересов обладателя исключительного права или средства индивидуализации законодатель предоставляет потерпевшему адекватные способы правовой защиты: пресечение про-

---

[1] См., например: Дозорцев В.А. Указ. соч. – С. 38 – 39.

[2] См.: Бабкин С.А. Интеллектуальная собственность в сети Интернет. – М.: АО «Центр ЮрИнфоР», 2005. – С. 10.

[3] См.: Гальперин Л.Б., Михайлова Л.А. Интеллектуальная собственность: сущность и правовая природа // Право интеллектуальной собственности. – Новосибирск, 1992. – С. 11.

[4] См.: Астахова М.А. Результаты интеллектуальной деятельности как объект гражданских прав: понятие и квалифицирующие признаки // Юридический мир. – 2006. – № 4 // СПС «КонсультантПлюс».

тивоправных действий, возмещение убытков, взыскание компенсации, публикацию судебного решения, изъятие и уничтожение контрафактного материального носителя, оборудования, прочих устройств и материалов, использованных и предназначенных главным образом для совершения нарушений исключительного права (ст. 1250, 1252 ГК РФ)[1].

Таким образом, можно сделать вывод о существовании (наряду с подотраслями вещного, обязательственного, корпоративного, наследственного, семейного права) такой подотрасли гражданского права, как исключительное право.

[1] См. подробнее: Андреев Ю.Н. Судебная защита исключительных прав: цивилистические аспекты. – М.: Норма : ИНФРА-М, 2011. – С. 17 – 61.

Архипцев Н.И.

К ВОПРОСУ ОБ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЕ ОТ ПОСЯГАТЕЛЬСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Статья посвящена влиянию современных информационных технологий на развитие и совершенствование уголовного законодательства.

Ключевые слова: преступление, информационные сети, сохранность и обеспечение электронных форм, контрафактная продукция, уголовная ответственность.

Abstract. Article assesses the impact of modern information technology on the development and improvement of the criminal law.

Key Words: crime, information networks, and to ensure the safety of electronic forms, counterfeit products, criminal liability.

Следует иметь в виду, что в 2012 году в Российской Федерации достаточно громкую и далеко неоднозначную реакцию вызвал законопроект, подготовленный в Государственной Думе, который предусматривал применение суровых мер административной и уголовной ответственности за широкий перечень преступлений и правонарушений, совершаемых с использованием Интернет, таким образом, была предпринята попытка «наложить» нормы этих отраслей права на сферу Глобальной информационной сети[1].

В частности, в законопроекте предлагалось установить действенную правовую защиту всех видов предусмотренных УК РФ преступлений, если они совершены с применением современных технологий: угрозу жизни и здоровью человека, клевету, мошенничество[2], доведение до самоубийства и ряд иных посягательств. Речь, разумеется, шла о тех посягательствах, которые совершаются под прикрытием анонимности, когда некое аморфное лицо либо иной субъект выдает себя за другого и, может, в частности, третировать иное физическое лицо, распространяя о нем клеветнические сведения. Как представляется, подобного рода действия не могли способствовать ни развитию российского общества, ни развитию цивилизованных отношений в обществе, ни развитию самих информационных сетей. Ведь любая технология могла быть использована как для конструктивных, так и для неконструктивных технологий. И когда эти цели деструктивны, уголовное законодательство, на наш взгляд, должно иметь эффективный инструментарий для борьбы с такими нарушениями. Полагаем, мало вычислить, обнаружить, установить, надо еще и иметь возможность привлечь виновного к уголовной ответственности. В этой связи самое главное, сделать так, чтобы анонимность не только создавала иллюзию безнаказанности, но и само следствие и обвинение получили достаточную емкую правовую основу для того, чтобы изобличить преступника.

---

[1] См., подробно: Богданов В. Анонимки напросвет // Российская газета. 2011.11 сентября.

[2] Федеральным законом № 207 от 29 ноября 2012 года была введена уголовная ответственность за мошенничество в сфере компьютерной информации // Российская газета. 2012. 3 декабря.

Не касаясь довольно широкого и многогранного круга вопросов, связанных с обеспечением уголовно-правовой защиты от деяний с использованием современных информационных технологий, считаем целесообразным в данной публикации, остановиться лишь на адекватном реагировании на вмешательство в области сохранности электронных форм, созданных правоохранительными и судебными органами, а также на особенностях противодействия обороту контрафактных произведений с использованием системы Интернет.

Как известно, Судебный департамент при Верховном суде России в настоящее время разрабатывает масштабный проект по созданию единого информационного пространства судов общей юрисдикции. Так, планируется ввести сквозной автоматизированный единый судебный документооборот, начиная от судебных участков мировых судей вплоть до Верховного суда Российской Федерации. Это создается для того, чтобы граждане, зайдя на портал, могли открыть любое дело и увидеть дистанционно все стадии его рассмотрения и вынесенные по нему решения независимо от места рассмотрения. Также планируется в перспективе обеспечить возможность обращения граждан в суд в электронной форме[1].

Как представляется, нуждается в правовом регулировании не только сам порядок использования, но и соответствующее правовое обеспечение и защита сохранности электронных форм при обращении граждан в судебные органы.

Здесь уголовно-правовое противодействие противоправным действиям по сохранности электронных форм, созданных правоохранительными и судебными органами, может заключаться в применении к правонарушителям статьи 274 УК РФ, устанавливающей ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Ни для кого сегодня не секрет, что для российского рынка контрафакт остается одной из наиболее актуальных проблем. По данным МВД РФ в среднем он составляет 20 процентов, а в текстильной и легкой промышленности доля контрафактной продукции доходит до 30 процентов. Контрафакт присутствует в парфюмерии, бытовой химии и даже в продуктах питания. В 2012 году таможенные органы выявили более 19 миллионов единиц контрафактных товаров и ими предотвращен ущерб, который мог быть нанесен правообладателям, на сумму 2,3 миллиарда рублей[2].

Считаем, что наиболее радикальный способ защиты торговых марок – их включение в таможенный реестр объектов интеллектуальной собственности, который формируется на основании заявлений как отечественных, так и зарубежных правообладателей. Возможно создание специализированного ведомства по борьбе с контрафактом, может быть следует пересмотреть международные конвенции по охране интеллектуальной собственности и расширить в системе арбитражных судов суды по интеллектуальным правам.

---

[1] См., подробно: Куликов В. VIP-звонок защитят // Российская газета. 2013. 12 февраля.
[2] См., подробно: Кузьмин В. Чистые мотивы // Российская газета. 2012. 23 октября.

Мы согласны с планируемыми Правительством РФ поправками в Уголовно-процессуальный кодекс и Кодекс об административных правонарушениях о безусловном уничтожении контрафактной продукции легкой промышленности. Уже сейчас Минторг России согласовывает с ведомствами избранный ассортиментный перечень таких товаров[1].

Вместе с тем, проблема, которую многие пока недооценивают, – это интернет-торговля. Это уже не отдельные граждане по каталогам через Интернет заказывающие себе имущество, которое отсутствует в российских магазинах или там оно гораздо дороже, уже сейчас посредством этой сети в страну доставляются значительные товарные партии, оформляемые в основном через подставных физических лиц, действующих в обход таможенных правил и пошлин. Причем, за 2012 год неуправляемая и нерегулируемая интернет-торговля возросла в несколько раз, а на 2013 год прогноз еще более настораживающий[2].

В плане борьбы с данным негативным социальным явлением следует не только использовать в таможенной сфере электронный информационный обмен и готовить технологические карты взаимодействия с федеральными органами власти, но и совершенствовать действующее уголовное законодательство с учетом развития интернет-технологий.

Изучение международного опыта и опыта отдельных зарубежных стран противодействия обороту контрафактных произведений позволяет нам сделать вывод о необходимости не только реконструкции действующих редакций статей 146 и 147 УК РФ, но и дополнения уголовного законодательства статьей об ответственности за оборот технических приспособлений, способствующих нарушению авторских, смежных, изобретательских или патентных прав. Известно, что нарушитель, желая начать тиражирование контрафактной продукции, обычно первоначально должен предпринять меры по нейтрализации защиты и получению доступа к лицензионной копии произведения или фонограммы.

Нами предлагается:

– дополнить ст.ст. 146 и 147 УК РФ квалифицирующим признаком – «с использованием сети Интернет»;

– дополнить УК РФ статьей 180.1 «Оборот защитных приспособлений, способствующих посягательствам на результаты интеллектуальной деятельности», где в части 1 указать: «Приобретение, хранение, передача, перевозка защитных приспособлений, предназначенных для удаления инструментов защиты от незаконного воспроизведения или приема результатов интеллектуальной деятельности», а в части 2 сформулировать повышенную ответственность за изготовление или сбыт защитных приспособлений[3]. Данную норму, мы полагаем, мо-

---

[1] См., подробно: Зыкова Т. Приказано уничтожить // Российская газета. 2013. 14 февраля.

[2] См.: Зыкова Т. Цвет коридора // Российская газета. 2013. 25 января.

[3] Аналогичные позиции предложены и другими исследователями. См., например: Иванченко Р.Б., Толмачев Ю.Н. Организационные и уголовно-правовые меры противодействия обороту контрафактных аудиовизуальных произведений и фонограмм. Белгород: ООНИ и РИД БелЮИ МВД России. 2009. С. 132-147; Маркарьян Р.В. Предложения по совершенствованию информационно-правового регулирования распространения информации через Интернет в Российской Федерации: критический анализ // Российский следователь. 2011. № 14. С. 36.

жно применять для уголовно-правовой защиты любых результатов интеллектуальной деятельности.

В свете многочисленных преобразований преступлений, связанных с использованием Интернета, которые могут существенно затронуть нормы уголовного законодательства, на память приходят слова профессора М. Шаргородского. Напомню, что он, рассуждая о значении юриспруденции в системе права, подчеркнул важную мысль о том, что «юридическая наука начинается там, где она говорит законодателю нет». Но поскольку динамика развития и совершенствования уголовного законодательства интенсивно продолжается, то требуется скорое и детальное обоснование потребности создания новой уголовно-правовой структуры с учетом резерва возможностей ее последующего дополнения и изменения, а также необходимости учета реальных регулятивных и охранительных возможностей уголовного права.

Бакирова Е.Ю.
Свинарь А.Л.

ЗАЩИТА АВТОРСКИХ ПРАВ В СЕТИ ИНТЕРНЕТ НА ПРИМЕРЕ ФАЙЛООБМЕНЫХ СЕТЕЙ

Аннотация. В статье рассматривается вопрос ответственности владельцев пиринговых сетей и их пользователей за нарушение авторских прав, а так же практика европейских государств по данной проблеме.

Ключевые слова: Авторские права. Пиринговые сети. Торрент-трекер. Торрент-файл. BitTorrent. Peer-to-peer. Сеть Интернет.

Abstract. We consider the question of liability of owners peering networks and their users for copyright infringement, as well as the practice of European countries on the issue.

Key Words: Copyright. Peer network. Torrent tracker. Torrent file. BitTorrent. Peer-to-peer. Internet.

В настоящее время все чаще поднимается проблемный вопрос защиты авторских прав в сети Интернет. Ни для кого не секрет, что сеть Интернет это особое явление, развитие и деятельность которого достаточно трудно регулировать с точки зрения закона, в силу его глобального характера.

Используя сеть Интернет можно найти книги, аудио– и видеозаписи и другие объекты авторских или смежных прав. Среди них большое число составляют объекты, размещенные без согласия правообладателя, в нарушение его законных интересов.

Наиболее остро стоит вопрос о так называемых файлообменных сетях на базе сетевого протокола BitTorrent или peer-to-peer (p2p) – торрент-трекерах.

Данный протокол был разработан еще в 2001 году американским программистом Брэмом Коэном. Суть функционирования данного протокола заключается в том, что пользователь ПК с помощью сети Интернет присоединяется к торрент-трекеру (то есть к серверу, на котором хранится информация об имеющихся файлах на жестких дисках ПК других пользователей) и сообщает им свой адрес, а получает уже адреса других пользователей ПК, которые раздают или скачивают этот же файл. Таким образом, данные пользователи по частям скачивают друг у друга недостающие фрагменты определенного файла, получая на выходе совокупность всех частей этого файла, т.е. файл целиком. В данном случае речь идет о том, что пользователи соединяются в сети Интернет друг с другом напрямую в случайном порядке, а сам трекер не принимает непосредственного участия в файлообменном процессе. Он просто регулярно обновляет информацию о подключившихся к скачиванию файла пользователях.

Таким образом, встает вопрос о поиске нарушителей авторских и смежных прав, закрепленных в Части четвертой Гражданского Кодекса Российской

Федерации[1]. На торрент-трекере хранится не сам объект авторских или смежных прав, а только лишь торрент-файл, который содержит в себе информацию о местонахождении ресурса Сети Интернет (URL), информацию о закачиваемом файле (размер, длительность и т.д.), а так же контрольную сумму файла (чтобы в итоге собрать все его части и получить единое целое). Отсюда можно сделать вывод, что администрация данного интернет ресурса не может нести ответственность за нарушение авторских и смежных прав, так как ни в одном нормативно – правовом акте не закреплен прямой запрет на размещение и распространение файлов, носящих информационный характер (файлы метаданных).

Объект авторского права появляется на конкретном ПК пользователя сети Интернет, в результате обмена с другими пользователями по указанным адресам в файле метаданных частями. До того, как данная система обмена информацией получила такую популярность среди пользователей ПК, правообладатели напрямую обращались к владельцам пиринговых сетей с требованием закрыть доступ к объектам авторских и смежных прав, размещенных на принадлежащих им серверах. В настоящее время такая возможность отсутствует, и теперь правообладатели могут только лишь требовать заблокировать доступ на трекере к какому-либо торрент – файлу, содержащему информацию об объекте авторских прав.

Возникает вопрос: несут ли ответственность за нарушение авторских прав владельцы пиринговых сетей? Дать однозначный ответ на данный вопрос не представляется возможным, ведь законом данная ситуация прямо не урегулирована, а судебная практика по таким делам отсутствует.

Мнения по данному вопросу разделились:

- Владельцы пиринговых сетей не распространяют объекты авторских прав, они лишь создают условия, предоставляют технические средства для обмена файлами в Интернете, которые отнюдь не должны быть нелегальными (пользователи могут обмениваться личными файлами, файлами, не содержащими охраняемые авторским правом объекты, и т.п.). Т.е. они не совершают правонарушающее действие (не передают файл и не контролируют передачу конкретного файла).
- Учитывая природу пиринговых сетей и особенно то, в связи с чем, например, стали популярны торрент-сети, и то, как они используются, а также учитывая техническую возможность их создателей фильтровать авторский материал, действия владельцев пиринговых сетей являются нарушением авторских прав[2].

---

[1] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ// «Российская газета», N 289, 22.12.2006.

[2] Пиринговые сети (P2P), в т.ч. торрент. Правовая ответственность за их создание // Kolosov.Info URL: http://www.kolosov.info/kommentarii/avtorskoe-pravo-i-piringovye-seti (дата обращения: 12.03.2013).

Ввиду отсутствия четкой позиции законодательства РФ по данной проблеме представляется возможным обратиться к практике европейских государств. Борьба с пиринговыми сетями ведется во многих странах Европы. Одним из главных законодательных актов в этой области является Директива Европарламента от 22.05.2001 № 2001/29/ЕС «О гармонизации некоторых аспектов авторского права и смежных прав в информационном обществе»[1]. Многие страны приняли отдельные национальные законы в развитие положений Директивы. Но некоторые страны решили проблему ужесточив положения данного нормативно – правового акта. Например, Швеция. Так, в соответствии с общеевропейской Директивой сама по себе загрузка контента не является правонарушением. Нельзя лишь предлагать его для загрузки, то есть выкладывать для обмена. Между тем законодательные нормы Швеции с недавнего времени устанавливают ответственность за загрузку из Интернета защищенных копирайтом материалов. Необходимо отметить, что около 10% шведов обмениваются мультимедийными файлами в p2p сетях. Ярким примером судебного противостояния правообладателей, с одной стороны, и владельцев p2p сетей, а также пользователей — с другой, является дело «Пиратской бухты» (www.thepiratebay.org), одного из крупнейших торрент-трекеров в Западной Европе, количество активных пользователей которого более 25 млн. Шведская полиция 31.05.2006 провела рейд, в результате которого было арестовано все руководство ресурса и изъяты серверы, а деятельность «Пиратской бухты» прекращена. Но, как и обещало руководство сайта, уже через пару дней он заработал вновь, так как трекер арендовал еще пару серверов в Нидерландах[2].

Как видно, проблема охраны авторских прав в сети Интернет приобрела транснациональный характер. Несмотря на классический подход к абсолютной защите имущественных прав авторов и правообладателей, весьма тяжело относить миллионы пользователей, пользующихся p2p сетями, к категории «пиратов» и осуществлять их преследование. В связи с этим, представляется, что в российском законодательстве необходимо закрепить правовое положение торрент-трекеров, а так же разработать специальные меры ответственности как для владельцев пиринговых сетей, так и для пользователей ПК, которые нарушают своими действиями авторские права. Кроме того, необходимо учесть, что не все файлы в пиринговых сетях являются охраняемыми объектами авторского права.

---

[1]Директива N 2001/29/ЕС Европейского парламента и Совета Европейского Союза «О гармонизации некоторых аспектов авторских и смежных прав в информационном обществе» (Принята в г. Брюсселе 22.05.2001)// Директива на английском языке опубликована не была.

[2] Копирайт против торрентов //gazeta-yurist.ru URL:http://www.gazetayurist.ru/article.php?i=740 (дата обращения: 12.03.2013).

Батова О.В.
Левченко В.Е.

СУДЕБНЫЙ ПОРЯДОК ЗАЩИТЫ ПРАВ АВТОРА ИЗОБРЕТЕНИЯ

Аннотация. Судебный порядок – это наиболее приспособленный для установления истины порядок защиты нарушенного субъективного права автора или патентообладателя. Формой обращения в суд за защитой нарушенного или оспариваемого права является исковое заявление, которое в соответствии с нормами гражданского процессуального законодательства предъявляется по месту нахождения ответчика.

Ключевые слова: судебный порядок, территориальная подсудность, интеллектуальная деятельность, соавторство, авторское право.

Abstract. The judicial order is the most adapted for truth establishment an order of protection of the violated subjective right of the author or the patent holder. Appeal to the court form behind protection of the violated or challenged right is the statement of claim which according to standards of the civil procedural legislation is shown in the location of the respondent.

Key words: judicial order, territorial jurisdiction, intellectual activity, co-authorship, copyright.

Основная масса споров рассматривается районными, городскими, областными и иными судами общей юрисдикции. Если обоими участниками спорного правоотношения являются юридические лица, возникший между ними спор относится к подведомственности арбитражного суда. По соглашению участников авторского правоотношения спор между ними может быть передан на разрешение третейского суда. В качестве средства судебной защиты прав и охраняемых законом интересов выступает иск, т. е. обращенное к суду требование об отправлении правосудия, с одной стороны, и обращенное к ответчику материально-правовое требование о выполнении лежащей на нем обязанности или о признании наличия или отсутствия права, с другой стороны. Судебный, или, как его еще называют, исковой порядок защиты применяется во всех случаях, кроме тех, которые прямо указаны в законе[1].

По общему правилу, иск заявляется по месту нахождения ответчика (ст. 28 Гражданско-процессуального кодекса РФ), однако по соглашению сторон территориальная подсудность дела может быть изменена (ст. 32 Гражданско-процессуального кодекса РФ)[2]. На требования, вытекающие из нарушения личных неимущественных прав авторов, не распространяется действие исковой давности. Иски, связанные с нарушением имущественных прав и интересов, могут быть заявлены в течение трех лет со дня, когда истец узнал или должен был узнать о нарушении своего права.

Истец, может по своему усмотрению обратиться за защитой своих нарушенных прав и охраняемых законом интересов в вышестоящий орган ответчика или в антимонопольный орган. Средством защиты в данном случае является не

---

[1] Близнец И. А., Лукницкий С. П. История и задачи правоохранительной и судебной системы по защите прав творческих личностей. М.: ИНИЦ Роспатента, 2003. – С. 112.

[2] «Гражданский процессуальный кодекс Российской Федерации» от 14.11.2002 N 138-ФЗ (ред. от 14.06.2012)

иск, а заявление, порядок подачи и рассмотрения, которой регламентированы административным законодательством[1].

Согласно ст. 1225 Гражданского кодекса РФ охраняемыми в судебном порядке результатами интеллектуальной деятельности рассматриваются следующие объекты: произведения науки, литературы и искусства; программы для электронных вычислительных машин (программы для ЭВМ); базы данных; исполнения; фонограммы; сообщение в эфир или по кабелю радио– или телепередач (вещание организаций эфирного или кабельного вещания); изобретения; полезные модели; промышленные образцы; селекционные достижения; топологии интегральных микросхем; секреты производства (ноу-хау); фирменные наименования; товарные знаки и знаки обслуживания; наименования мест происхождения товаров; коммерческие обозначения [2].

Материалы судебной практики свидетельствуют о том, что имеют место случаи, когда в соавторы изобретения, полезной модели включаются без законных оснований руководители и другие должностные лица организаций и предприятий. Делается это либо в силу сложившихся в коллективе «обычаев», либо из-за чувства благодарности автора за оказываемые ему услуги в оформлении заявки, а чаще всего за содействие в их внедрении. Подобное лжеавторство наносит существенный ущерб автору и несовместимо с общественными интересами.

В целях устранения отмеченных недостатков необходимо более подробно определять объем творческого участия каждого из соавторов в создании изобретения, полезной модели.

При рассмотрении споров о соавторстве суд устанавливает характер участия каждого из лиц, претендующих на соавторство, в создании технического решения, совокупность признаков которого получила отражение в формуле изобретения, учитывая при этом, что соавторство возникает только по поводу одного общего для нескольких лиц творческого решения[3].

Если технические решения, совпадающие по содержанию, сделаны каждым из авторов самостоятельно, независимо друг от друга, то соавторство отсутствует. Но в том случае, когда даты приоритета заявок на выдачу патента совпадают, все авторы, упомянутые в заявках, в административном порядке признаются соавторами.

Автор ранее заявленного основного изобретения не может считаться соавтором созданного впоследствии дополнительного изобретения, если он не принимал творческого участия в работе над дополнительным изобретением.

При наличии нескольких самостоятельных разработок творческое участие в создании одной из них не может служить основанием для признания соавтор-

---

[1] Постановление Пленума Высшего Арбитражного Суда Российской Федерации от 15 февраля 1998 г. «О некоторых вопросах практики применения споров, связанных с защитой права собственности и других вещных прав» // Вестник Высшего Арбитражного Суда Российской Федерации, 1998. №10.

[2] «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 N 230-ФЗ (ред. от 08.12.2011)

[3] Обзор арбитражной практики от 28 апреля 1997г. // Вестник Высшего Арбитражного Суда Российской Федерации. 1997. №7.

ства в другой, в том числе и в случаях, когда речь идет о сложных технических решениях, реализуемых в одном объекте.

При рассмотрении спора об авторстве (соавторстве) суд нередко выясняет, что патент выдан одному лицу, а в творческой работе, приведшей к созданию изобретения, полезной модели или промышленного образца, участвовали другие лица или авторство на обозначенные объекты принадлежит не тем, кто указан в патенте.

При удовлетворении иска об авторстве (соавторстве) на изобретение, полезную модель или промышленный образец и признании недействительным патента суд направляет копию, вступившего в законную силу решения в Роспатент, с целью исправления записи о регистрации изобретения, полезной модели или промышленного образца и выдачи автору (соавтору) документов в соответствии с решением суда.

Определенный ряд особенностей рассмотрения имеют споры об установлении факта использования изобретения или полезной модели. Как показывает судебная практика, иски подобного рода – самые сложные и требуют для своего разрешения, кроме вопросов правового характера, особых познаний, как в технических областях, так и в области патентоведения [1].

Наиболее простым случаем такого спора может быть отрицание предприятием факта использования им изобретения по различным причинам, самой распространенной из которых является несвоевременная осведомленность предприятия о том, что оно изготавливает продукцию с использованием какого-либо изобретения.

При разрешении этих споров суд устанавливает наличие или отсутствие факта применения изобретения путем сравнения формулы изобретения с техническим решением, используемым ответчиком. Правовая защита нарушенного права авторства заключается в том, что предъявляется иск о признании права авторства либо об исключении того или иного лица (лиц) из числа соавторов.

Спор об авторстве может быть решен только после того, как будет выяснено, является ли заявленное решение изобретением, соответствующим условиям патентоспособности, поскольку без решения этого вопроса спор об авторстве в рамках действующего законодательства невозможен.

Данная категория споров является наиболее сложной из всех споров, связанных с охраной прав, удостоверяемых патентом, так как авторство на изобретение, полезную модель и промышленный образец предопределяет имущественные и неимущественные права авторов, предусмотренные действующим законодательством.

Спор об авторстве – это выяснение вопроса о том, кто является действительным создателем изобретения, полезной модели, промышленного образца, с целью защиты имущественных и личных неимущественных прав. Однако это не лишает автора технического новшества возможности отстаивать право ав-

[1] Письмо Верховного Суда Российской Федерации «Некоторые вопросы судебной практики по гражданским делам» //Бюллетень Верховного Суда Российской Федерации. 1997. №10.

торства в рамках такого института интеллектуальной собственности, как ноу-хау (секреты производства).

Разновидностью споров об авторстве являются споры о соавторстве, которые означают, что заявитель не ставит под сомнение авторство лица, указанного в качестве такового в патенте. Однако он утверждает, что в достигнутом решении технической задачи имеется и его творческий вклад. В свою очередь лицо, оформившее изобретение на свое имя, либо полностью отрицает причастность заявителя к разработке изобретения, либо утверждает, что его участие не носило творческого характера, а сводилось лишь к оказанию технической, материальной или организационной помощи[1].

Изобретение считается использованным, если при изготовлении продукта (устройства, вещества, штамма микроорганизма, культуры клеток растений или животных) или осуществлении способа применены все признаки, перечисленные в каждом независимом пункте формулы изобретения. Часто возникают споры о факте использования изобретения или полезной модели, которые реализованы либо в опытных образцах, либо прошли экспериментальную проверку.

При рассмотрении данного вида споров тяжело избежать неточностей и ошибок. Суды иногда не принимали во внимание факт использования признаков изобретения или при изготовлении устройства, а исходили из факта применения этих признаков при его эксплуатации. Также суды необоснованно отказывали в рассмотрении споров об установлении факта применения изобретения или полезной модели отдельно от исков о вознаграждении, считая первые разновидностью споров о вознаграждении.

В судебной практике встречаются случаи, когда предприятие при изготовлении продукции использовало не все признаки изобретения в явном виде, а заменило один или несколько признаков, изложенных в независимом пункте формулы изобретения, другим или другими взаимозаменяемыми элементами (эквивалентами) и добросовестно считает, что изобретение им не использовано[2].

Если судом будет установлено, что имеет место эквивалентная замена одного или нескольких признаков изобретения, отраженных в каждом независимом пункте формулы, то изобретение считается использованным.

Предприятие, изготовившее устройство, признается использующим изобретение. Если же данное устройство изготавливается по частям несколькими предприятиями, организациями, учреждениями (для последующей сборки), то предприятие, осуществляющее сборку устройства, признается использующим изобретение. Спор об установлении патентообладателя предполагает, что, по мнению истца, в патенте неправильно указан патентообладатель.

---

[1] Гришаев С.П. Интеллектуальная собственность. М.: Юристь, 2004. – С.17

[2] Обзор арбитражной практики от 28 апреля 1997 г. // Вестник Высшего Арбитражного Суда Российской Федерации. 1997. №7

Нарушение исключительных прав на изобретение означает, что были нарушены исключительные права на использование указанного объекта способами, предусмотренными в ст. 1229 Гражданского кодекса РФ [1].

Споры о праве автора на вознаграждение включают споры о вознаграждении за использование изобретений, созданных в порядке выполнения служебного задания, при выполнении работ по государственному контракту для федеральных государственных нужд и так далее. Споры о порядке исчисления и нарушения сроков выплаты вознаграждения, как свидетельствует судебная практика, встречаются довольно редко и возникают обычно в составе каких-либо других споров.

Чаще в судах рассматриваются споры между соавторами о распределении авторского вознаграждения за использованное изобретение. Поскольку причитающаяся каждому соавтору доля вознаграждения определяется в соответствии со степенью его участия в разработке изобретения, суд назначает техническую экспертизу, в задачу которой может входить определение доли творческого участия каждого из соавторов.

Если между соавторами не достигнуто соглашение о распределении вознаграждения, суду необходимо привлечь к участию в деле всех соавторов и определить долю каждого из них в вознаграждении [2].

Вознаграждение за изобретение распределяется между соавторами в процентном отношении по их письменному соглашению. Если наследник не подписывает соглашение, например, в связи с отказом от наследственных право или по каким-либо иным причинам, то возникает спор о распределении вознаграждения. С иском с суд имеет право обратиться и один из заинтересованных соавторов.

Таким образом, при рассмотрении подобных споров в задачу суда входит правомерное отделение творческого вклада соавтора в создание изобретения от других видов работ [3]. В случаях, когда невозможно определить степень участия каждого из соавторов, их доли признаются равными.

---

[1] «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 N 230-ФЗ (ред. от 08.12.2011)

[2] Казаков Ю. В. Защита интеллектуальной собственности.– М.: Мастерство: Академия, 2002. – С. 116.

[3] Чигир В.Ф. Интеллектуальная собственность. – Минск: ООО «Амалфея», 1997. – С. 415

Белецкая А.А.

ИНТЕРНЕТ-РЕСУРСЫ КАК ЭЛЕМЕНТ ИНФРАСТРУКТУРНОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья посвящена определению взаимосвязи сферы интернет и инноваций. Интернет – ресурсы рассмотрены как один из элементов инфраструктурного обеспечения инновационной деятельности, так как реализация инновационных проектов, осуществляемая организациями, образующими инновационную инфраструктуру, включает информационные услуги.

Ключевые слова: инновации, инновационная деятельность, правовое регулирование, интернет-ресурсы, инновационная инфраструктура.

Abstract. Article is devoted to the relationship online and innovation. Internet-resources considered as part of the infrastructural support of innovation, as the implementation of innovative projects by the organizations that make up the innovation infrastructure, including information services.

Key Words: innovations, innovative activities, legal regulation, Internet-resources, innovation infrastructure.

На сегодняшний день, инновационная деятельность является одним из ключевых механизмов модернизации национальной экономики в условиях рыночных отношений. Создаваемые в рамках государственной поддержки условия, способствующие расширению масштабов инновационной деятельности, касаются, в том числе, развития ее инфраструктурного обеспечения. Дополнительные возможности развития информационной базы инфраструктурного обеспечения инновационной деятельности формируются в результате активного использования Интернет-ресурсов.

Обратимся к рассмотрению основных понятий инновационной сферы.

Рассмотрим понятие «инновация», которое является одним из ключевых в анализируемой сфере.

Интересным, на мой взгляд, является анализ самого термина «innovatio». Он представляет собой синтез двух слов: investio – «вложение» и novatio – «обновление», сочетая в себе не только новизну, но и процесс её достижения. Поэтому, в настоящее время понятие «инновация» следует рассматривать с учетом этих двух значений:

– во-первых, это новшество, т.е. новый или усовершенствованный продукт (работа, услуга), технология, разработанные и предназначенные для внедрения в производственно-хозяйственную деятельность, потребление, общественную жизнь;

– во-вторых, это процесс осуществления изменений или создания (достижения) новшеств.

Нельзя согласиться с мнением Н.И. Михайлова и А.Г. Лисицына – Светланова[1] о том, что понятия инноваций и инновационной деятельности не нашли

[1] Михайлов Н.И. Правовые средства активизации деятельности корпоративных субъектов в инновационной сфере // Российский юридический журнал. 2011. № 5. С. 143-147; Лисицын-

достаточного отражения в законодательных актах, так как не принят специальный закон об инновациях. При отсутствии специального законодательного акта, тем не менее, на сегодняшний день федеральным законом от 20 июля 2011 г. № 249-ФЗ в статью 2 ФЗ «О науке и государственной научно-технической политике» внесены изменения, закрепляющие дефиниции указанных понятий.

Так, инновации, согласно указанным актам, представляют собой введенный в употребление новый или значительно улучшенный продукт (товар, услуга) или процесс, новый метод продаж или новый организационный метод в деловой практике, организации рабочих мест или во внешних связях[1].

Согласно научно-практическому комментарию к Федеральному закону от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике» под редакцией В.Е. Усанова, в тексте комментируемого Закона впервые законодательно закрепляется необходимость государственной поддержки инновационной деятельности. Определение этого нового для законодателя и правоприменителя понятия дается в статье 2 комментируемого Закона, согласно которой научная, технологическая, организационная, финансовая и коммерческая деятельность является инновационной при условии ее направленности (т.е. постановки соответствующих целей и задач, получения результатов) на создание инновационной инфраструктуры и обеспечение ее деятельности.

При этом, важная роль интернет – ресурсов во взаимодействии с инновационной деятельностью так же закреплена законодательно.

Так, в п.3 статьи 16.1. «Основные цели и принципы государственной поддержки инновационной деятельности» среди принципов государственной поддержки инновационной деятельности закреплена публичность оказания государственной поддержки инновационной деятельности посредством размещения информации об оказываемых мерах государственной поддержки инновационной деятельности в информационно-телекоммуникационной сети «Интернет».

Как отмечает В. Э. Полетаев, в развитых странах поддержка инновационного предпринимательства выступает приоритетным направлением государственной политики[2]. В рамках государственной политики формируется система инфраструктурного обеспечения инновационного предпринимательства, включающая в себя совокупность взаимосвязанных и взаимодополняющих организаций, обеспечивающих поддержку деятельности предпринимателя, направленной на создание, коммерциализацию и (или) использование инноваций[3].

Светланов А.Г. Интеллектуальная собственность и инновационные процессы в современной России // Вестник Российской академии наук. 2010. № 1. Т. 80. С. 4.

[1] Федеральный закон от 20 июля 2011 г. № 249-ФЗ «О внесении изменений в Федеральный закон «О науке и государственной научно-технической политике» и статью 251 части второй Налогового кодекса Российской Федерации в части уточнения правового статуса фондов поддержки научной, научно-технической и инновационной деятельности» // Российская газета. № 161. 2011.

[2] Полетаев В.Э. Государственная поддержка частного бизнеса в России в контексте инновационной политики // Дискуссия. 2011. № 9. С. 49–56.

[3] Ермакова Н.С. Развитие информационной составляющей инфраструктурного обеспечения инновационного предпринимательства // Проблемы современной экономики. 2012. № 1 (41).

В России инновационная инфраструктура представляет собой совокупность организаций, способствующих реализации инновационных проектов, включая предоставление управленческих, материально-технических, финансовых, информационных, кадровых, консультационных и организационных услуг[1].

Как отмечают Т.Г. Философова, Л.С. Банникова, развитие инновационной экономики невозможно без развития ее инфраструктуры. Инфраструктура инновационной экономики – это совокупность взаимосвязанных, взаимодополняющих производственно-технических систем, организаций, фирм и соответствующих организационно-управляющих систем, обеспечивающих осуществление инновационной деятельности. Развитая инфраструктура определяет темпы инновационного развития экономики страны и, в конечном итоге, возможности для роста благосостояния ее населения.

Инфраструктура, обеспечивающая осуществление инновационного процесса, включает различные институты поддержки инновационной деятельности, в частности законодательство, регулирующие отношения в сфере разработки и коммерциализации инноваций, форсайт-центры, форсайт-проекты, независимая экспертиза научно-исследовательских проектов и перспективности направлений научно-исследовательских работ, мероприятия для снижения рисков внедрения новых продуктов и координации усилий коллективов-разработчиков, фонды, центры коммерциализации технологий и разработок и т.д.[2]

Сюда же можно отнести и механизмы финансирования инновационной деятельности, выделенные О. Безруковой и В. Елизаровой:

– организация и финансирование инновационной деятельности частным капиталом;

– венчурные инновационные компании;

– совместные предприятия;

– консорциумы компаний;

– научно-технические альянсы;

– бизнес-инкубаторы и технопарки[3].

Однако, по мнению Н. С. Ермаковой, в рамках политики по формированию инфраструктурного обеспечения важно не только создавать организации поддержки бизнеса, но и информировать предпринимателей о предоставляемых такими организациями услугах. Данная задача может решаться с помощью развития информационной составляющей инфраструктурного обеспечения инновационного предпринимательства. С целью создания информационного про-

---

[1] Федеральный закон от 20 июля 2011 г. № 249-ФЗ «О внесении изменений в Федеральный закон «О науке и государственной научно-технической политике» и статью 251 части второй Налогового кодекса Российской Федерации в части уточнения правового статуса фондов поддержки научной, научно-технической и инновационной деятельности» // Российская газета. № 161. 2011.

[2] Философова Т.Г., Банникова Л.С., Инновационная экономика: опыт развития технопарков // Лизинг № 8. 2011 г. С.4.

[3] Безрукова О., Елизарова В. Механизмы финансирования инновационной деятельности: возможности использования в России // Корпоративный юрист. 2009. № 5. С. 13.

странства все более активно используются ресурсы сети Интернет. Начало использования Интернет-ресурсов обусловило появление дополнительных возможностей поддержки инновационного предпринимательства, а у информационной составляющей в целом возникла новая функция, в рамках которой она по отношению к другим организациям инфраструктурного обеспечения стала выступать средством информирования предпринимателей о самом существовании таких организаций и оказываемой ими поддержке[1].

Таким образом, интернет-ресурсы, на мой взгляд, представляют собой один из элементов инфраструктурного обеспечения инновационной деятельности, так как реализация инновационных проектов, осуществляемая организациями, образующими инновационную инфраструктуру, включает информационные услуги.

[1] Ермакова Н.С. Развитие информационной составляющей инфраструктурного обеспечения инновационного предпринимательства // Проблемы современной экономики. 2012. № 1 (41).

Белоус В.В.

ИСПОЛЬЗОВАНИЕ БИОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ИДЕНТИФИКАЦИОННЫХ ЗАДАЧ В КРИМИНАЛИСТИКЕ

Аннотация. Путем интеграции в криминалистику достижений биологии и генетики предложено решение проблем идентификации личности на основе современных информационных технологий.

Ключевые слова: Идентификация, ДНК, информационные технологии.

Abstract. By integration of the achievements of the biology and genetics into criminalistics the problem solution of the personal identification on the basis of modern information technologies was suggested.

Key words: Identification, DNA, information technologies.

Криминалистическая идентификация – один из основных методов установления истины в уголовном судопроизводстве, когда возникает необходимость в выявлении связи подозреваемого, принадлежащих ему предметов и других объектов с расследуемым преступным событием по оставленным следам и иным материальным отображениям[1]. Актуальность поиска идеального идентифицирующего признака – «каиновой печати», способствующей отождествлению лица, причастного к совершенному преступлению, а также приемов, способов и средств безошибочного установления его конкретного тождества с ростом численности населения планеты только усиливается.

За более чем сто лет своего существования и развития криминалистика обогатилась многими современными теориями и в настоящий момент является универсальной прикладной юридической наукой, своеобразными адаптационными «воротами» для применения в уголовном судопроизводстве последних достижений научной и технической мысли[2]. «Криминалистическое мышление» позволяет создать наиболее эффективные информационные технологии по поиску, собиранию, анализу и выверенному использованию доказательственной и иной криминалистически значимой и любой иной фактической юридической информации[3]. Процесс создания таких технологий, направленный на достижение синергетического эффекта, требует одновременного синтеза знаний разных отраслей науки. Примером может служить открытие органического носителя информации в биологии, методов и средств его обращения в накопитель цифровых данных – в информатике, способов использования для решения идентификационных задач – в криминалистике.

---

[1] Ищенко Е. П. Криминалистика. Стандарт третьего поколения : учеб. пособие / Е. П. Ищенко. – СПб.: Питер, 2013. – С. 42.

[2] Волчецкая Т. С. Перспективы и пути развития современной криминалистики / Современное состояние и развитие криминалистики: сб. науч. тр. / под ред. Н. П. Яблокова и В. Ю. Шепитько. – Х.: Апостиль, 2012. – С. 6.

[3] Яблоков Н. П. Основные тенденции развития криминалистики как науки и учебной дисциплины в современной России / Современное состояние и развитие криминалистики: сб. науч. тр. / под ред. Н. П. Яблокова и В. Ю. Шепитько. – Х.: Апостиль, 2012. – С. 65.

Как альтернатива традиционным неорганическим накопителям информации в последнее время всё больший интерес вызывает дезоксирибонуклеиновая кислота (ДНК) – молекула живых организмов, содержащая всю генетическую информацию о них и передающая ее от поколения к поколению всем потомкам («молекула жизни», «природный банк данных», «основной носитель генетической информации»).

Авторство открытия ДНК в 1869 г. принадлежит швейцарскому врачу Ф. Мишеру. Способы практического использования уникальности ДНК для идентификации человека в рамках генотипоскопической экспертизы предложил английский генетик А. Джеффрис в середине 80-х XX ст. Благодаря тому, что молекулярно-генетический, генотипоскопический или ДНК-анализ относится к одним из наиболее доказательных и достоверных методов исследования, а методика генноидентификационного исследования высокочувствительна (установление с ее помощью конкретного тождества возможно при наличии малого количества биологического материала (одной капли крови или стержня одного волоса), возможности генотипоскопической экспертизы сегодня широко применяются в деятельности зарубежных и отечественных правоохранительных и судебных органов.

Вместе с тем, предлагается обратить внимание и на тот факт, что как энергонезависимый носитель информации, молекула ДНК является идеальной формой для хранения не только генетически предопределенных, но и искусственно созданных данных. Успешные эксперименты по кодированию цифровой информации в молекулах на основе ДНК позволяют вести речь о создании технологии, которая уже через несколько десятилетий позволит хранить в подобных биомолекулах не только персональные данные человека, но и любые электронные файлы, включая аудиозаписи в формате MP3, текстовые документы, цифровые фотоснимки и видеозаписи. Главным препятствием на пути повсеместного внедрения этой технологии пока остается неготовность общества объективно оценить все ее преимущества и недостатки, высокая себестоимость и потребность в разработке нового оборудования для работы с ДНК-накопителями, которое не ограничивалось бы только секвенсорами и синтезаторами. Технологическая сторона разрешима в обозримом будущем с помощью создания полностью избавленной от промежуточной электроники системы прямого кодирования в ДНК-код аналоговых сигналов, включая аудио- и видеопоток.

В 2012 г. профессор генетики Д. Чарч (Гарвардский университет, США) с помощью последовательностей из ДНК-групп закодировал в молекуле ДНК целую книгу[1]. В след за этим, коллектив ученых Европейского института биоинформатики (EMBL-EBI, Великобритания) во главе с молекулярным биологом Н. Голдманом разработал более совершенную масштабируемую и надежную систему архивирования информации в ДНК[2] и продемонстрировал ее работо-

---

[1] *George M. Church, Yuan Gao, Sriram Kosuri* Next-Generation Digital Information Storage in DNA. – Режим доступа: http://www.sciencemag.org/content/337/6102/1628.

[2] *Nick Goldman, Paul Bertone, Siyuan Chen, Christophe Dessimoz, Emily M. LeProust, Botond Sipos & Ewan Birney* Towards practical, high-capacity, low-maintenance

способность, закодировав в одной молекуле ДНК 26-секундный отрывок из аудиозаписи знаменитой речи Мартина Лютера Кинга «У меня есть мечта», фундаментальную работу о природе ДНК в формате PDF, текстовый файл со всеми сонетами Шекспира в формате ASCII, цветную фотографию лаборатории, где проходила работа над проектом, в формате JPEG, и описание использованного метода конвертации информации в ДНК. Общий объем закодированной информации составил 739 килобайт. Удельный вес записанной информации на молекуле ДНК составил при этом около 2,2 петабайт (ПБ) на 1 г вещества. Применив к кодированию подход, который практически исключает появление и накопление ошибок в исходной информации, британским ученым в сотрудничество с компанией «Agilent Technologies» (США) удалось синтезировать фрагменты ДНК и продемонстрировать успешное секвенирование и последующее восстановление исходных файлов со 100% точностью. До этого информацию с цифровых носителей точно отобразить в органике не удавалось.

Изложенное позволяет выделить такие преимущества ДНК перед традиционными носителями информации: 1) энергонезависимость; 2) практически безграничное количество воспроизводимых носителей информации. Все клетки организма (кроме красных кровяных клеток) содержат копию ДНК. Развернутая цепь всех клеток ДНК человека имеет протяженность около 16 млрд. км (расстояние от Земли до Плутона и обратно); 3) предельно малый размер. Флэш-память и другие способы энергонезависимой памяти практически исчерпали пределы миниатюризации, в то время как молекулы ДНК оптимальны для длительного хранения больших массивов данных на носителях микроскопических размеров; 4) колоссальная емкость. Для ДНК характерна высочайшая плотность информации – 2,2 ПБ на 1 г ДНК. Например, Европейская организация по ядерным исследованиям, оперирующая Большим адронным коллайдером, ежегодно производит 15 ПБ информации. Для хранения такого объема информации необходимы миллионы CD или километров магнитной ленты. Однако для удовлетворения этих потребностей будет достаточно всего около 7 г ДНК, так как 1 г вещества может хранить столько же информации, сколько вмещается на более чем миллионе CD. Одна цепь ДНК способна хранить до 100 млн. часов высококачественного видео в формате HD; 5) повышенная надежность, связанная с тем, что кодирование файлов в ДНК предусматривает некоторый уровень избыточности. Каждая часть файла представлена четырьмя разными фрагментами, что позволяет восстановить данные даже в случае повреждения отдельных фрагментов; 6) длительность хранения информации, исчисляемая тысячелетиями (ДНК мамонта сохранилась в течение 60 тыс. лет практически без информационных потерь).

В свете разрешения задач криминалистики наиболее важным является тот факт, что электрофореграммы ДНК в некоторых случаях выступают единственным средством, позволяющим идентифицировать личность, благодаря тому, что: 1) клетки любых микрочастиц, оставленных человеком на месте преступ-

---

information storage in synthesized DNA. – Режим доступа: http://www.nature.com/nature/journal/vaop/ncurrent/full/nature11875.html#/affil-auth.

ления (кровь, сперма, волосы, фрагменты кожи и т.п.), содержат его уникальный ДНК-код; 2) вероятность абсолютного совпадения количества минисателлитов (мутаций ДНК), распределения их длины и последовательности у двух разных людей (за исключением однояйцевых близнецов) практически равна нулю; 3) устойчивость ДНК-кода как идентифицирующего признака – абсолютна (наследственную информацию в клетках организма ни стереть, ни изменить невозможно). А технология кодирования в ДНК персональных данных способна ускорить и упростить идентификационный процесс, повысить надежность его результатов.

Решение проблем установления личности жертв техногенных катастроф, стихийных бедствий, военных конфликтов и преступлений, розыска и идентификации пропавших без вести и подозреваемых в совершении преступных деяний, удовлетворение ряда иных, не менее актуальных потребностей судебно-следственной практики обуславливают: 1) разработку международного стандарта, законодательное урегулирование и осуществление всеобщей генетической регистрации населения Земли с кодированием в ДНК персональных данных, традиционно фиксируемых в документах, удостоверяющих личность (паспортах, в т.ч. оснащенных электронными чипами, ID-картах); 2) создание национальных банков данных ДНК и международный обмен этими данными с использованием сетевых ресурсов Интернет в рамках предоставления международной правовой помощи при расследовании преступлений; 3) разработку и внедрение в деятельность правоохранительных органов средств компьютерной техники и программного обеспечения («считывающих устройств»), способствующих идентификации личности по персональным данным, закодированным в ДНК обнаруженных на месте события микрочастиц биологического происхождения, в «полевых» условиях с использованием «облачных» технологий Интернет.

Белоус О.П.

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-РЕСУРСОВ В ЦЕЛЯХ ВЫЯВЛЕНИЯ И ПРЕКРАЩЕНИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ «КОНВЕРТАЦИОННЫХ ЦЕНТРОВ»

Аннотация. Рассмотрены направления противодействия функционированию «конвертационных центров» с использованием Интернет-ресурсов.

Ключевые слова: Интернет-ресурс, «конвертационный центр».

Abstract. The trends of opposition to the operation of the «conversion centers» with the use of Internet resources were examined.

Key words: Internet resource, «conversion center».

В условиях глобализации мировой экономики и построения всемирного информационного общества эффективность предпринимательской деятельности напрямую корреспондирует способности ее участников использовать не только современные инструменты рыночной экономики, но и достижения научно-технического прогресса, способствующие экономии ключевых ресурсов (финансовых, материальных, трудовых, временных), а также обеспечению надежной коммуникации участников бизнес-процессов. Одним из наиболее востребованных средств является глобальная сеть Интернет с широким спектром сервисов, позволяющих увеличить скорость обработки данных, подготовки документов и осуществления финансово-хозяйственных операций, расширить клиентурную сеть, повысить мобильность участников процесса во времени и пространстве. Миграция в виртуальное пространство как отдельных операций и рабочих мест, так и бизнес-процессов в целом обусловила возникновение целого ряда новых направлений предпринимательской деятельности (Интернет-банкинг, Интернет-трейдинг, электронные биржи и торговые площадки, Интернет-аукционы и т.п.).

Вместе с тем, всё возрастающие возможности Всемирной сети используется не только для достижения социально полезных целей. В злонамеренных руках отдельных граждан и преступных сообществ Интернет-пространство оказалось благодатной почвой как для модернизации способов классических видов преступлений (например, построение «виртуальных» финансовых пирамид), так и для возникновения новых, ранее неизвестных видов преступных деяний («киберпреступность»). Эти процессы не обошли стороной и сферу налогообложения. Например, стремительно развивающаяся система денежных расчетов посредством Интернет и «электронные кошельки» предоставляют возможность получать в виртуальном пространстве реальные неконтролируемые доходы[1]. А с учетом того, что только в Украине оборот «электронных», «Интернет-денег» за три квартала 2012 г. (1164 млн грн.) увеличился почти в десять раз по сравнению с показателем за весь 2011 г. (116 млн грн.)[2], то устранение условий

[1] Медиа-центр ГНС в г. Киеве. – Режим доступа: http://kyiv.sts.gov.ua.

[2] Пресс-служба НБУ.

для возможных злоупотреблений и в этой сфере становится первостепенной задачей контролирующих и правоохранительных органов.

Современные средства и методы осуществления информационных процессов, в особенности Интернет, создают своего рода особую виртуальную реальность, представляя специфическую картину реальной действительности путем передачи сообщений, изображений, текстов и т.п. Насыщение современной жизни компьютерными системами, телекоммуникациями, виртуальной реальностью не только существенно видоизменяет преступность, но и открывает новые возможности борьбы с ней. Эти возможности необходимо как можно быстрее и полнее интегрировать в отечественную криминалистику[1]. С учетом актуальности обеспечения защиты от преступных посягательств экономического базиса государства считаем, что неотложной интеграции возможностей Интернет требует обеспечение деятельности органов уголовной юстиции в направлении выявления и изучения закономерностей использования Всемирной сети в целях подготовки, совершения и сокрытия налоговых преступлений, а также их выявления и расследования.

Обескровливающие государственный бюджет классические теневые операции банков включают в себя операции по «отмыванию» «грязных» денег, перевод безналичных денег в наличную форму для обслуживания разных видов теневой экономики, финансирования терроризма, коррупции, увод прибыли в оффшоры и другие подобные операции. По данным ЦРУ, объем таких «классических» операций банков в мировом масштабе составляет 3-4 трлн долл.[2] С учетом этого, операция «Конверт», направленная на выявление и уничтожение «центров конвертации средств» справедливо определена в качестве одного из наиболее важных направлений деятельности Государственной налоговой службы Украины[3], а эффективная работа по ликвидации последствий деятельности «конвертационных центров» является одним из семи приоритетов деятельности налоговой милиции[4]. За предшествующий 2013-му год прекращена незаконная деятельность 82 преступных сообществ – «конвертационных центров», преступный оборот которых составил около 12,7 млрд грн. с вероятными потерями бюджета только по НДС в размере 2,1 млрд грн. Выявлено 546 субъектов хозяйствования с признаками фиктивности, установлено 9102 контрагентов, воспользовавшихся услугами «конвертационных центров», и 1530 контрагентов, сотрудничавших с последними[5].

В целях своевременного выявления и прекращения преступной деятельности «конвертационных центров» сетевые ресурсы Интернет целесообразно использовать в таких направлениях, как:

---

[1] Ищенко Е. П. Криминалистика. Стандарт третьего поколения: учеб. пособ. – СПб.: Питер, 2013. – С. 56.

[2] Шокуючі дані про світовий банківський бізнес. – Режим доступа: http://www.epravda.com.ua.

[3] Налоговая определилась с направлениями работы. – Режим доступа: http://news.liga.net.

[4] Медиа-центр ГНС Украины. – Режим доступа: http://sts.gov.ua.

[5] Звіти ДПС України за 2012 рік. – Режим доступа: http://sts.gov.ua.

1. Завершение полного перехода на электронную форму подачи налоговой отчетности (в 2011 г. электронная отчетность по НДС составляла 38%, к началу 2013 г. – 98%[1]) и дальнейшее развитие функционирующих в налоговых органах электронных сервисов (в частности, «электронный (виртуальный) кабинет налогоплательщика», с помощью которого за счет объединения всех необходимых баз данных налоговая отчетность конкретного субъекта хозяйствования формируется автоматически), а также аналитических инструментов (например, рискоориентированная система мониторинга, позволяющая отслеживать налоговые риски и применение схем минимизации).

2. Мониторинг Интернет-ресурсов в целях выявления источников предложения противоправных услуг «конвертационных центров». В этом направлении уже накоплен определенный позитивный опыт. Например, анализ объявлений в печатных СМИ и в Интернете позволил органам ГНС выявить в 2012 г. 1073 жителя столицы Украины, нелегально сдававших в аренду принадлежащие им помещения. Это повлекло за собой доначисление 5,438 млн грн. налога на доходы физических лиц, что на 36% превысило показатель 2011 г. В последние несколько лет эти источники все активнее используются для выявления признаков уклонения от уплаты налогов и в действиях работодателей, размещающих объявления о приеме на работу с указанием заработных плат, существенно отличающихся от декларируемых в отчетности, и даже звезд шоубизнеса, утаивающих сведения о реальных суммах полученных гонораров[2]. Использование поисковых систем Интернет по таким ключевым словам, как «конвертация», «обнал», «однодневки» способствует установлению «операторов и потребителей рынка», а изучение размещенных на профессиональных Интернет-форумах тематических материалов – актуальных технологий их преступной деятельности.

3. Мониторинг Интернет-ресурсов в целях выявления лиц, причастных к противоправной деятельности, путем установления несоответствия реальных расходов официальным доходам. Так, Министерство доходов и сборов Украины изучает возможность оценивать реальные доходы граждан посредством социальных Интернет-сетей. Такой подход уже нашел свое применение в Великобритании, где фискальное ведомство анализирует доходы и расходы граждан путем сопоставления сведений из более чем 25 различных баз данных, включительно с записями в Facebook[3]. К наиболее востребованным направлениям использования соцсетей в криминалистике применительно к цели данного исследования следует отнести: установление круга лиц, причастных к совершению преступления, розыск лица, скрывающегося от уголовного преследования, установление психологического профиля разыскиваемого лица или участника уголовного процесса, иных обстоятельств расследуемого события. Известен опыт создания в США «системы высокотехнологического слежения национального масштаба» для быстрого извлечения информации о подозреваемых

---

[1] Налоговый ремонт: интервью с А. Клименко // Эксперт. – 2012. – № 49-50. – С. 12-14.

[2] Медиа-Центр ГНС в г. Киеве. – Режим доступа: http://kyiv.sts.gov.ua.

[3] Налоговый ремонт: интервью с А. Клименко // Эксперт. – 2012. – № 49-50. – С. 14.

гражданах из социальных сетей – RIOT (Rapid Information Overlay Technology), позволяющей получать сведения об активности подозреваемого (его социальных контактах, карте перемещений и др.). Информация извлекается в том числе из EXIF-заголовков фотографий, опубликованных в личных фотоальбомах на разных сайтах.

4. Создание псевдопредложения услуг «конвертационного центра» (уголовно-релевантное инсценирование) в целях изучения спроса, выявления круга пользователей и сбора сведений о них, выявления конкретных признаков преступной деятельности путем внедрения легендированных сайтов[1], применение которых с учетом новелл УПК Украины целесообразно распространить на производство негласных следственных (розыскных) действий, направленных на достижение целей досудебного расследования.

5. Снятие информации с транспортных телекоммуникационных сетей и электронных информационных систем в целях выявления преступной сети коррумпированных должностных лиц ГНС Украины, курирующих функционирование know how отечественной организованной преступности – «госпрограммы» и «сертифицированных площадок».

[1] Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ: моногр. за ред. О. О. Подобного. – О.: Юрид. літ., 2011. – С. 99.

Davidova Y.A.
Stepanyuk A.V.

SOME PROBLEMS OF LEGAL STATUS REGULATION OF AN INTERNET PROVIDER

Аннотация. Доклад посвящен проблематике формулировки определения понятия «интернет-провайдер» в российском законодательстве. Рассматривается вопрос о правах интернет-провайдеров и их ответственности за качество информации, размещаемой в Интернет-сети.

Ключевые слова: Интернет, понятие «интернет-провайдер», права и обязанности интернет-провайдер, ответственность интернет-провайдера, правовое регулирование интерент-отношений с иностранным элементом.

Abstract. The report is focused on the problems of an «internet provider» language definition in Russian legislation. A question of ISPs rights and their responsibility for the quality of information available on the Internet network is considered.

Key words: the Internet, the concept of an «Internet Service Provider», the rights and obligations of an internet provider, internet-provider liability, legal regulation of internet-relationship with a foreign element.

A major issue in a system formation of a legal regulation in the sphere of the «Internet» is the regulation of the status of, perhaps, a central participant of this relationship – ISP.

Currently, the meaning of an «Internet Service Provider» in professional environment is defined as follows. An Internet Service Provider (sometimes ISP, from English, abbr. ISP – Internet service provider) – is an organization that provides services to access the Internet and other Internet-related services. In accordance with the provided services they can be classified into categories:

- access providers,
- hosting providers,
- backbone providers,
- channel providers,
- last mile providers[1].

It should be noted that the definition of an «Internet Service Provider» in Russian legislation is not given, as well as an answer to the question – who can act in this capacity – an individual and (or) a legal entity. These circumstances already determine the relevance of the issue.

For example, there is the definition of the hosting provider in Article 2, claim 18 of the Federal Law from July 27, 2006 № 149-FL «On Information, Information Technologies and Protection of Information»[2]. Thus, a hosting provider is a person rendering services in providing computing power for placing information to the information system which is constantly connected with the «Internet». First, as it was

[1] See the article «Internet service provider» // site «Wikipedia: The Free Encyclopedia.» Access mode: http://ru.wikipedia.org/wiki. Accessed on the 15th of February, 2013.

[2] See: Code of Laws of the Russian Federation. 2006. № 31 (Part 1). St.3448.

noted above, a hosting provider – is one of the types of an Internet service provider. Secondly, this definition appeared in a relevant law only in 2012[1].

Meanwhile, approaches to the formulation of ISP definition are proposed in draft laws. Thus, the Federal draft Law № 47538-6 «On amendment to the first, the second, the third and the fourth parts of the Civil Code of the Russian Federation and also to the Certain Legislative Acts of the Russian Federation» (which was passed by the State Duma of the Federal Assembly of the Russian Federation in the first reading on the 27th of April, 2012) proposes to insert it to the Civil Code article 1253.1. «Features of information intermediary liability.» In addition to the paragraph 1 of the article an information intermediary (ISP) – is a person who carries out the transmission of material on the Internet or provides a possibility of placing the material in this network[2]. In Article 3 of the Federal draft Law «On electronic commerce» the term «information broker» is also used; it refers to a person who sends, receives or stores electronic documents or provides other services in relation to these documents on behalf of another person[3].

But, based on the logic of the legislator one can consider sellers of printed literature, audio and video recordings as information intermediaries. To the point, a social and practical function of all the subjects under consideration is the same. The only difference is in the tools: paper, ribbons, plates, cables, hard drives, servers. Thus, one can talk about an artificial substitution of a general concept of the term, a special relevance in law is put there; this relevance is based on the technological process specificities.

One can become a user of the Internet network after making a contract with an Internet service provider for the provision on access services to the Internet. On the basis of these things, essential services provided by Internet service providers are: providing access to the Internet; a hosting service which belongs to the third person.

In our view, a contract for hosting services should be considered as a public category. That's why, the inclusion to the Federal draft law «On communication» of a compulsory contract ISP regulation is not a sufficient guarantee for a client. Foreign jurisprudence draws attention here. Thus, the Federal Court of Germany decided that access to the World Wide Web is just as important as a simple telephone service. That's why, a provider who won't be able to provide their customers with normal and stable access to the network, will be obliged to pay a compensation[4].

Russian legislation currently lacks adequate accountability mechanisms of ISP, including those for placing an inaccurate information on the sites they serve. Also, a mechanism of making demands for the quality of the posted information is not regulated.

In our opinion, the amendments to Russian legislation should be made on the principle according to which one should do preparatory linguistic work on formulating the terms based on a network internet specificity, and make efforts to establish relationships and compliances with juridical and civil law concepts.

---

[1] See: Federal Law of July 28, 2012 № 139-FZ «On Amendments to the Federal Law» On Protection of children from information harmful to their health and development, «and some legislative acts of the Russian Federation» / / Assembly legislator -RF properties. 2012. Number 31. St.4328.

[2] See Supplemental legal system «Consultant: Bills.»

[3] See Supplemental legal system «Consultant: Bills.»

[4] http://www.novoteka.ru/sevent/6028731

In our opinion, the responsibility of an Internet service provider for the quality of information provided on server occurs if:

1) information was placed on its initiative (contractual obligations);

2) intentional or unprofessional actions of a provider entailed placement of harmful (illegal) information on its server.

In the case of offense, proof of confession of a provider should be assigned to the very provider, who should be involved in a judicial process as a respondent with the authors of illegal information. Such an accountability mechanism will be fully justified, taking into account, that information is actually on a server owned by the provider (i.e., a provider acts in the capacity of an information replication agent). In this case, providers will be interested in a more careful and independent verification of information.

A list of information categories requires a legislative recognition and liable check and the rights of an internet service provider according to the results of the verification. In particular, the right to delete information, identify the illegality, which content does not require special knowledge or inform the relevant bodies of the competent authorities about any suspicious information for a more thorough and legal review.

By bringing to book of a provider his interest in finding a proper defendant – an author of harmful information, is stimulated, besides a provider has enough opportunities, allowing him to search for the best advantage.

Participation regulation of Internet service providers in information relationships on the Internet network, depends on the further development of the Internet.

The analysis shows that significant complications cause Internet relations which occur in the virtual space, weighted by a foreign element. In practice, quite often there is a situation when a consumer of information, an owner of a resource provider and a host provider are of different nationalities. Between the parties of proceedings occur issues:

1) to which state and which country legal relationship is subordinated;

2) the right of which state is applicable and what role plays a binding «the server's location.»

Legal regulation in this area is in the process of formation. The result may follow in the way, that the decision of the court on relations dispute connected with the Internet, as well as the choice of applicable law and its content will depend on understanding degree of the Internet by a judiciary system, specificity of online relationships and ability to provide all the features of law adequate interpretation by the court and the applicable law.

In terms of positive law and judicial practice there is a possibility of judicial proceedings in relation to the parties, who are not citizens of the European countries, and not in their territories.

A possible solution is to determine disputes jurisdiction through interstate coordination measures applied, through the unification of the rules governing relations on the Internet, through the formation of a special international legal regime specifically for the Internet network. The problem, of course, is not simple. But there are already special legal regimes of oceans, Antarctica and outer space.

Introduction to the special legal rules and procedures may not be rational, because illegal acts committed on the Internet, not only involve the imposition of legal liability for professionals, but also relate to each user and the Internet, a network system of a global and planetary scale.

Демко О.С.
Родионова М.Ю.

К ВОПРОСУ О МЕРАХ ПО БОРЬБЕ С ПРОПАГАНДОЙ НАРКОТИЧЕСКИХ СРЕДСТВ В СОЦИАЛЬНЫХ СЕТЯХ И ИНЫХ РЕСУРСАХ СЕТИ ИНТЕРНЕТ

Аннотация. В представленной статье рассматриваются отдельные спорные вопросы, касающиеся мер по борьбе с пропагандой наркотических средств в сети Интернет. Авторы оценивают влияние социальных сетей на подростков, причины, условия и особенности пропаганды наркотиков среди молодежи в социальных сетях, а также предлагают к рассмотрению различные способы и пути решения данной проблемы.

Ключевые слова: Проблема наркотизации молодежи, отклоняющееся поведение, влияние социальных сетей на подростков, пропаганда наркотиков посредством сети Интернет, борьба с наркотизацией молодежи.

Abstract. In the present article deals with some controversial issues relating to measures against the propaganda of drugs on the Internet. The authors consider the impact of social media on teenagers, the causes, conditions, and especially promoting drug use among young people in social networks, as well as the offer to consider the various ways and means of solving this problem.

Key words: the problem of drug addiction youth deviant behavior, the impact of social networks on adolescent drug propaganda through the Internet, fighting anesthesia youth.

На сегодняшний день наркомания в России уже стала важнейшим фактором социальной дезорганизации, представляющим большую угрозу нормальному функционированию современного общества и государства. Осознание этого факта как национальной проблемы, которая требует личного участия каждого гражданина Российской Федерации, является важнейшей задачей профилактической работы государственных органов и общественных учреждений. В настоящее время Россия стала очевидным лидером в сфере антинаркотической дипломатии. Это наглядно следует не только из высокой активности МИД, ГАК и ФСКН России, но, прежде всего, прослеживается в инициативах Президента России по созданию широкой антинаркотической коалиции.

«Употребление детьми и молодежью психоактивных веществ представляет собой серьезную проблему современного общества. Косвенно или напрямую она затрагивает практически каждого пятого жителя страны»[1].

По мнению председателя Государственного антинаркотического комитета, директора ФСКН России Виктора Иванова, «наркозависимость – это заболевание мозга, поэтому лечить надо и психологически, а не только наркологическими методами». Неслучайно, Федеральная служба по контролю за незаконным оборотом наркотиков в 2011 году закрыла 1,5 тысячи интернет-сайтов, где пропагандировалось употребление запрещенных веществ или предлагалась возможность купить их. За минувший год ликвидировано 1,5 тысячи сайтов, которые были вовлечены в преступную деятельность. Ведомство вырабатывает

[1] Проблема молодежной наркомании (казахстанский и международный опыт). Информационно-публицистический ресурс «НЕТ НАРКОТИКАМ» [Электронный ресурс] // Режим доступа: http://www.narkotiki.ru/research_6455.html

серьезный противовес использованию этого человеческого ресурса (интернета – ИФ) античеловеческими методами.[1]

Однако, проблема пропаганды наркотиков среди молодежи в сети Интернет в настоящее время по-прежнему актуальна. Особенно явно она проявляется в социальных сетях, которые охватывают все киберпространство и где каждый если не первый, то второй подросток имеет свой профиль. Пользователи социальных сетей не только активно занимаются пропагандой, но и создают группы, где рассказывают о способах приобретения наркотических средств, указывают цены на них и контакты дилеров. Нельзя не отметить, что современная музыка, фильмы и иные ресурсы, содержащиеся в социальных сетях, так же оказывают пагубное влияние на психику подростков, так как пропагандируют асоциальный образ жизни, употребление запрещенных препаратов, нередко основываясь на примерах из жизни наркозависимых людей, якобы добившихся успеха, но продолжающих употреблять наркотики.

Для того чтобы понять, насколько серьезной является проблема пропаганды наркотиков в социальных сетях, необходимо уяснить, какую роль социальные сети играют в жизни современных подростков, какое влияние они могут оказать на психику подрастающего поколения.

Итак, социальная сеть (от англ. social networking service) — платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений, визуализацией которых являются социальные графы[2]. С одной стороны, социальные сети расширяют возможности современного человека, позволяют ему общаться с друзьями, коллегами, родственниками независимо от их места нахождения. С другой стороны, социальные сети ограничивают человека, заменяя ему встречи с друзьями в реальной жизни общением в виртуальном мире. Что касается подростков, то нельзя не согласиться с мнением о том, что компьютер для большинства их них – это отдельная жизнь: там есть и друзья, и враги, и хобби, и любовь и вообще почти вся жизнь[3]. Зачастую в социальных сетях подросток пытается решить свои проблемы, среди которых нередко встречается непонимание со стороны родителей и сверстников, чувство одиночества, желание обрести свою индивидуальность. Находясь в пубертатном возрасте, человек не всегда может дать объективную оценку окружающей действительности и поэтому для многих социальная сеть – это единственный пусть самоутвердиться и получить одобрение со стороны «друзей». Безусловно, общение в социальных сетях имеет как позитивные, так и негативные моменты. К позитивным моментам можно отнести получение подростками социально полезной информации и навыков, негативным момен-

---

[1] См.: Информация от 24.05.2012 // Официальный сайт ФСКН России / Режим доступа: www.fskn.gov.ru.

[2] Википедия. Социальная сеть. [Электронный ресурс] // Режим доступа: http://ru.wikipedia.org/wiki/Социальная_сеть

[3] Социальные сети и подросток: плюсы, минусы и альтернативы. «Дети. Психологический навигатор» [Электронный ресурс] // Режим доступа: http://deti.psynavigator.ru/articles.php?code=135

том, по мнению Е.Р. Баткаевой, является влияние социальных сетей на процесс социализации, становления и развития личности молодых людей[1]. Являясь основным средством проведения досуга, социальные сети оказывают огромное влияние на подрастающее поколение. В настоящее время информация, которая доступна в социальных сетях, может иметь различный характер. В некоторых случаях она бывает полезной, мотивирует подростков, формирует их взгляды в установленных обществом, правом и моралью пределах. В других случаях – способствует проявлению антиобщественного, аморального поведения молодежи. Разумеется, пропаганда употребления наркотических средств оказывает пагубное влияние на подростков, нередко способствует тому, что у подрастающего поколения формируется своя система ценностей, среди которых – уподобление известным личностям (музыкантам, актерам и др.), употребляющим наркотики.

Почему именно подростки наиболее восприимчивы к пропаганде наркотиков в сети Интернет и в частности – в социальных сетях? Как справедливо отмечает Л.А. Журавлева, у преобладающего большинства детей и подростков отсутствует превентивная психологическая защита, ценностный барьер, препятствующий приобщению к психоактивным веществам. Несовершеннолетний, начинающий принимать наркотики, оказывается в сложной социально-психологической ситуации – с одной стороны, мощный прессинг рекламных предложений нового стиля жизни, связанного с наркотизацией, новых ощущений в сочетании с доминирующими у подростка мотивами любопытства и подражания, с другой – безучастность или некомпетентность сверстников, педагогов, родителей.[2]

Не секрет, что наркомания, алкоголизм и проституция являются наиболее часто встречающимися формами отклоняющегося поведения среди учащейся молодежи. Безусловно, эти формы деформации создают своего рода «базис» для будущей преступной деятельности молодого человека. Социальная дезорганизация, резкое ухудшение криминогенной обстановки и рост явлений девиантного поведения приводит к формированию в рамках молодежной субкультуры определенного образа жизни, неразрывно связанного с потреблением наркотиков[3].

Мы считаем, что подходить к решению проблемы наркотизации подростков посредством пропаганды в социальных сетях необходимо комплексно, так как проблема эта многоплановая, и для ее решения следует применять различные методы и средства.

В первую очередь, необходимо ограничивать доступ подростков к социальным сетям и ресурсам сети Интернет. И задача эта должна решаться в пер-

---

[1] Баткаева, Е. Р. Роль социальных сете в социализации молодежи. [Электронный ресурс] // Режим доступа: http://www.pareto-center.ru/smi-59.html

[2] Журавлева Л. А. Факторы и условия наркотизации молодежи / Л. А. Журавлева // Социс. – 2000. – № 6. – С. 43-48.

[3] См.: Ишкильдина Г. Р. Правосознание молодежи: проблемы становления и эволюции в современных условиях: дис. ... канд. юрид. наук. – Уфа, 2002. – С. 81.

вую очередь на уровне семьи, школы, университета. В настоящее время Интернет-провайдеры оказывают такую услугу, как «Родительский контроль», позволяющий ограничить возможности посещения различных ресурсов сети Интернет, в том числе и социальных сетей.

Кроме того, следует разработать комплекс мер оперативного реагирования на появление в социальных сетях любой информации, призывающей к употреблению наркотиков. В данном случае наиболее эффективным будет создание отдела в системе ФСКН, который занимался бы вопросами борьбы с пропагандой наркотиков в сети Интернет. Необходимо так же определить условия взаимодействия между модераторами социальных сетей (в первую очередь, русскоязычных) и сотрудниками правоохранительных органов. К сожалению, в настоящее время далеко не всегда администрация сайтов «ВКонтакте», «Одноклассники» и др. оперативно реагирует на появление подобного рода информации. Как средство борьбы с пропагандой наркотиков в социальных сетях можно предложить и создание групп, пропагандирующих здоровый образ жизни, разумеется, под контролем или при непосредственном участии сотрудников правоохранительных органов.

Нельзя забывать и о том, что подросток, обладающий достаточно высоким уровнем правосознания, не станет употреблять наркотические средства, даже если заметит призывы в социальных сетях к их употреблению.

Таким образом, эффективность мер по противодействию наркотизации населения во многом зависит от уровня правосознания.

Высокий уровень правовой культуры молодежи, нетерпимость к правонарушениям – есть важное средство профилактики молодежной преступности и наркомании. Считаем, что конкретной мерой профилактики на общем, групповом, индивидуальном уровнях выступает правовое образование и воспитание учащейся молодежи.

На наш взгляд, для преодоления различных форм девиантного поведения (проявляющихся, в том числе, в сети Интернет) и наркомании среди учащейся молодежи особое значение следует уделять правовому обучению и воспитанию указанной социальной группы. Считаем, что повышать уровень правовой культуры, в частности, студентов необходимо через разработку и реализацию соответствующих приемов и способов правового обучения и правового воспитания, которые бы сопровождали самовоспитание молодого человека и определяли в совокупности целостную систему правового образования в современном российском обществе. Кроме того, государство, посредством законодательных и исполнительно-распорядительных органов и их должностных лиц, призвано, на наш взгляд, разработать, внедрить и обеспечить реализацию соответствующих технологий, направленных на развитие активной гражданской позиции и правовой культуры молодежи с учетом ее возрастных, позиционных и статусных различий. Именно такая инновационная деятельность правового и организационного характера наряду с оптимальной внутривузовской моделью правового образования, позволит, на наш взгляд, не только сформировать, но и в дальнейшем эффективно осуществлять мотивационную деятельность по развитию

активной гражданской позиции, поддержанию на высоком уровне правовой культуры учащейся и студенческой молодежи.

В настоящее время мы считаем, что основное назначение правового обучения состоит не только в повышении качественного уровня правовых знаний, но и в формировании мировоззренческих, познавательных и поведенческих аспектов правовой культуры личности студента посредством внедрения в учебный процесс специальной учебной дисциплины, применяя в процессе ее преподавания соответствующие методы правового обучения.

Определяя приемы и способы механизма борьбы с наркотизацией молодежи в связи с пропагандой в социальных сетях наркотических средств, мы предлагаем:

1. Разработать новые и усовершенствовать имеющиеся программы, позволяющие ограничить доступ подростков к ресурсам сети Интернет.

2. Разработать комплекс мер оперативного реагирования на появление в социальных сетях любой информации, призывающей к употреблению наркотиков.

3. Создать отдел в системе ФСКН по вопросам борьбы с пропагандой наркотиков в сети Интернет.

4. Разработать, внедрить и обеспечить реализацию технологий, направленных на развитие активной гражданской позиции и правовой культуры молодежи.

Долженко Н.И.
Шапошник Е.И.
Винокуров Э.А.

К ВОПРОСУ О ПРОБЛЕМАХ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В статье рассматриваются проблемы расследования кибератак на финансовый сектор, а также предлагаются меры борьбы с киберпреступлениями посредством привлечения ИТ-компаний.

Ключевые слова: расследование киберпреступности, кибератака, ИТ-подразделения.

Abstract. The article deals with statistics on cyber attacks, the notion of cyber crime, and the problems of cybercrime investigations. Proposes measures to combat cybercrime by attracting IT companies.

Key words: cyber crime, cyber attack, IT companies.

Интенсивное развитие компьютерных технологий, а также их внедрение во все сферы жизни современного человека является реалиями сегодняшнего времени. Уровень информатизации позволяет непросто обмениваться определенными сведениями, но и использовать ее, в том числе, в финансовой сфере. Компьютеризация данной области сопровождается совершенствованием технологии финансовых операций и повышением уровня их управляемости.

Однако в настоящее время в мире наблюдается активный рост преступлений в финансовой сфере посредством использования информационных технологий.

По результатам ежегодного исследования Norton Cybercrime Report 2012, – одного из крупнейших в мире исследований в сфере киберпреступлений в отношении пользователей, ущерб от киберпреступности за 2012 год оценивается в $2 миллиарда в год в России и в $110 миллиардов в мире[1].

Активный рост преступлений в сфере информационных технологий приходится именно на Россию. По данным годового отчета производителя антивирусного программного обеспечения ESET, российский рынок киберпреступности так же растет очень быстро. Основная масса кибератак приходится на финансовые стратегически важные для развития экономики компании[2], что ведет к значительному обогащению преступников. Так, объем заработанных киберпреступниками денежных средств в 2010 году составил 2-2,5 млрд. евро.

В октябре 2012 года МВД опубликовало статистику по преступлениям в сфере высоких технологий за первое полугодие 2012 года. По данным Министерства, в России было зафиксировано 5696 киберпреступлений, что почти на 11% больше, чем в аналогичном периоде 2011 года. Среди них преобладают преступления, связанные с созданием, распространением и использованием вредоносных программ, а также с мошенничеством в сети Интернет[3].

---

[1] Итоги исследования: Киберпреступность в России и мире. http://startupafisha.ru/.

[2] *Киберпреступники в России заработали 2,5 млрд евро.* http://www.tadviser.ru/index.php/.

[3] Киберпреступность. http://www.tadviser.ru/index.php/.

Одной из причин стремительной эволюции и развития преступности в области высоких технологий является слабая юридическая база в сфере квалификации действий и преследования хакеров в правовом поле. Это приводит к ощущению безнаказанности для «виртуальных» мошенников. Из-за неразвитой правоприменительной практики в области расследования этой категории преступлений такие инциденты зачастую предпочитают скрывать, что является дополнительным стимулом активности киберпреступников.

Всесторонне правовое рассмотрение вопросов борьбы с киберпреступностью имеет еще один важный аспект: киберпреступность подрывает государственный строй страны в целом.

Следовательно, необходимо принимать меры для сдерживания действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными, путем обеспечения уголовной наказуемости таких деяний, и предоставления полномочий, достаточных для эффективной борьбы с такими уголовными преступлениями, путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества.

В целях обеспечения определенной стабильности был принят Указ Президента Российской Федерации от 15 января 2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Данный указ возлагает на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом[1]. Однако нельзя возлагать надежды только на одно специальное подразделение и для успешного противодействия данному виду преступлений необходимо разрабатывать рекомендации направленные на противодействию этому явлению.

В целом, киберпреступность достаточно широкое понятие, так как к нему относят большую группу правонарушений, связанных с использованием инфокоммуникационных технологий. Нам не удалось обнаружить какое-либо четкое определение данного термина в нормативных актах Российской Федерации.

По определению ООН, киберпреступность подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Следовательно, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. Преступление, совершен-

[1] «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»: Указ Президента Российской Федерации от 15 января 2013 г. №31с // СЗ РФ. 2013. №3. Ст. 178.

ное в киберпространстве – это виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ[1]. При этом каждое из перечисленных деяний образует самостоятельный состав преступления, требующего индивидуального подхода к его расследованию.

Однако из-за неразвитой правоприменительной практики в области расследования преступлений в сфере информационной безопасности потенциальные потерпевшие, как владельцы крупных финансовых компаний, так и более мелких, такие инциденты зачастую предпочитают скрывать, что, создает дополнительные трудности в рамках их раскрытия.

Кроме того, отсутствие достаточной практики расследования данного вида преступлений, нехватка человеческих и технических ресурсов порождает достаточно пассивную позицию правоохранительных органов в отношении возбуждения и ведения уголовных дел в борьбе с киберпреступностью.

На сегодняшний день разрабатываются многочисленные программные продукты и технические средства защиты информации для обеспечения информационной безопасности, но, как правило, их оказывается недостаточно для решения специфических задач расследования. Помощь в предотвращении данных преступлений возможна путем создания высокотехнологичного оборудования для борьбы с киберпреступлениями, а также подготовки специалистов в данной области, которые помогут правильно настроить оборудование и квалифицированно применить. Причем такой специалист должен в полном объеме владеть методиками и процедурами сбора и представления доказательств, знанием нормативно-правовых актов в данной области и тонкостями, позволяющими оказывать следствию помощь в формировании доказательной базы.

В настоящее время сложилась такая практика, при которой первоначальный сбор информации, носящей признаки преступления, доверяют сотрудникам ИТ-подразделения организации, на которую была совершена кибератака. В результате важная доказательственная информация может быть утрачена в силу того, что эти специалисты не обладают достаточной квалификацией, необходимой для нужд расследования.

Одним из обоснованных решений, данной проблемы, представляется налаживание более тесных взаимодействий структурных подразделений органов федеральной службы безопасности с ИТ-компаниями, которые находятся как в самой России, так и за рубежом, сферой деятельности которых является защита информации и оказание профессиональных услуг, в том числе в сфере безопасности государства от кибепреступности в целом.

[1] Киберпреступность. http://it-sektor.ru.

Евтушенко И.В.

ПРОБЛЕМЫ АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ НА РЫНКЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И УСЛУГ ПО ПРЕДОСТАВЛЕНИЮ ДОСТУПА К СЕТИ ИНТЕРНЕТ

Аннотация. В статье был проведен анализ функций и задач ФАС России который позволил выявить основные цели службы направленные на защиту конкуренции в сфере информационно коммуникационных-технологий и телекоммуникаций, явившиеся неотъемлемой частью эффективной реализации конституционного права на информацию.

Ключевые слова: информационно коммуникационные-технологий, интернет, антимонопольное регулирование, оператор связи, интернет-провайдер.

Abstract. In article the analysis of functions and tasks of FAS Russia which allowed to reveal those main objectives of service directed on protection of the competition in the sphere was carried out is information the communication – technologies and the telecommunications, been compound part effective realization of a constitutional law on information.

Key words: it is information communication – technologies, internet, antimonopoly regulation, communications operator, the Internet-provider.

Право на получение информации получило свое закрепление в Конституции Российской Федерации, из буквального толкования части 4 статьи 29 следует, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения данного правам существуют только для информации конфиденциальной; для сведений, составляющих государственную тайну, перечень которых определяется федеральным законом[1].

Новая эра свободного доступа и получения информации в России была обусловлена распространением информационных технологий и взлетом интереса к глобальной сети интернет, с дальнейшим проникновением ее в различные сферы деятельности общества и государства. Появление глобальной сети способствовало заполнению информационного вакуума в обществе, а сам интернет стал наиболее полным воплощением конституционной свободы на получение информации.

В начале 2000-х годов в России данным сегментом рынка был дан импульс развития и совершенствования для правового регулирования отношений в области информационных технологий и телекоммуникаций. Приняты базовые законодательные акты, такие как Федеральный закон Российской Федерации от 27.06.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон Российской Федерации от 07.07.2003 N 126-ФЗ «О связи», Закон Российской Федерации Российской Федерации от 21.07.1993 N 5485-1 «О государственной тайне», Федеральный закон Российской Федерации от 27.06.2006 N 152-ФЗ «О персональных данных», Федеральный закон Российской Федерации от 10.11.2002 N 1-ФЗ «Об электронно-

[1] Бархатова Е.Ю. Комментарий к Конституции Российской Федерации (постатейный). М.: Проспект, 2010. – 256 с.

цифровой подписи», а также четвертая часть Гражданского кодекса Российской Федерации (N 230-ФЗ от 18.12.2006).

Вместе с тем процесс совершенствования государственного регулирования отношений в области информационных технологий не завершен и находится лишь в начальной стадии.

На сегодняшний день одной из главных задач государства остается обеспечение равного доступа к информации и устранение цифрового неравенства. В силу этого доработки требуют многие подзаконные акты, регулирующие отношения в сфере телекоммуникаций, IT-технологий и доступа к сети Интернет. Это все в определенной мере осложняет упорядочение гражданско-правовых отношений в связи с использования информационных технологий и телекоммуникаций, препятствует рассмотрению споров о нарушении антимонопольного законодательства, осложняет защиту объектов авторских прав.

Развитие конкуренции на рынках информационных технологий и равного доступа к рынкам данного сегмента предусматривает весомое участие государства в части реализации соответствующих законодательных инициатив, определения процедур, связанных с регламентированием и стандартизацией, создания выгодных условий деятельности для предпринимателей в сфере предоставления доступа к услугам сети интернет.

Для достижения вышеуказанной цели, а также решения иных задач связанных с предупреждением и пресечением монополистической деятельности и недобросовестной конкуренции существует Федеральная антимонопольная служба Российской Федерации (далее – ФАС России).

Концепция деятельности службы в сфере регулирования услуг телекоммуникаций и услуг по предоставлению доступа к сети Интернет в настоящее время заключается в двух аспектах – с одной стороны, это применение мер антимонопольного контроля и регулирования за рынком данных услуг, а с другой – осуществление мер по содействию развитию рынков и обеспечения недискриминационного доступа к сети интернет.

Все, что касается антимонопольного контроля и регулирования, определено нормами Федерального закона Российской Федерации от 26.07.2006 N 135-ФЗ «О защите конкуренции» (далее по тексту – Закон «О защите конкуренции»). Указанный закон распространяется на отношения, связанные с защитой конкуренции, в том числе с предупреждением и пресечением монополистической деятельности, в которых участвуют российские и иностранные юридические лица, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления. В соответствии со статьей 22 и 23 Федерального закона Российской Федерации «О защите конкуренции» определены функции и полномочия, возложенные на антимонопольный органа для достижения целей настоящего Закона.

При попытке проанализировать практику пресечения нарушений антимонопольного законодательства на данном рынке, становится понятно, что в сфере информационно-коммуникационных технологий, а также на рынке услуг по предоставлению доступа к сети Интернет не все благополучно. Территориаль-

ные органы ФАС России зачастую сталкиваются с нарушения, которые касаются как операторов связи, в частности операторов, действующих в сфере предоставления доступа к сети Интернет, так и тех организаций, которые владеют объектами инфраструктуры.

Зачастую граждане не могут воспользоваться услугами интернет – провайдера, которого они хотели бы получить. Из-за различных препятствия со стороны застройщиков домов и управляющих компаний (далее – УК). Препятствия со стороны УК для интернет-провайдеров выражены в создание дискриминационных условий при доступе последних к общедомовой инфраструктуре многоквартирных жилых домов, а также пользование ей.

Нарушение же антимонопольного законодательства в сфере коммуникационных технологий, а также на рынке предоставления доступа к сети интернет со стороны операторов занимающих доминирующее положение на рынке по предоставлению данных видов услуг выражены в злоупотреблениях касающихся навязывания невыгодных условий договора, либо услуг, в которых не нуждается абонент. Реже в практике применения мер антимонопольного реагирования встречаются нарушения связанные с экономически, технологически и иным образом не обоснованное установление различных цен (тарифов) на один и тот же товар. Примером неправомерных действий нарушающих антимонопольное законодательство в данном сфере является дело № 197-10-АЗ, в соответствии с которым ОАО «ЦентрТелеком» в нарушение требований статьи 426 ГК РФ, пункта 38 Правил оказание телематических услуг связи установило экономически и технологически необоснованную различную абонентскую плату в рамках тарифного плана в зависимости от места жительства абонента, в связи с чем и было признано Белгородским УФАС России нарушившим часть 1 статьи 10 Закона «О Защите конкуренции»[1].

Стоит остановить свое внимание еще на нескольких нарушениях посягающем на порядок обращения товара на рынке информационно коммуникационных-технологий и услуг по предоставления доступа к сети Интернет.

Первое связано с проблемой появления в России принципа «сетевого нейтралитета». Обобщенно под сетевым нейтралитетом подразумевают обеспечение получения пользователями доступа к любым услугам, которые могут быть предоставлены с помощью сети Интернет, без дифференциации по видам, объемам и происхождению трафика, без дискриминации.[2]

В Российской Федерации основополагающие принципы сетевого нейтралитета (прозрачность оказания услуг, информирования пользователей и оказания публичных услуг всем пользователям на равных условиях) получили должное законодательное закрепления. Вместе с тем, нормативными правовыми актами в отрасли связь закреплённые принципы, противоречат основам сетевого

---

[1] Постановление ФАС Центрального округа от 30.05.2011 по делу N А08-4142/2010-27//СПС Консультант Плюс.

[2] В ФАС России состоялось заседание Экспертного совета по вопросам связи // URL: http://www.fas.gov.ru/fas-news/fas-news_31856.html.

нейтралитета: при определении порядка пропуска трафика, при установлении различных подходов к регулированию услуг связи по передаче данных в зависимости типа передаваемых данных (голосовой и иной информации). В связи с этим, для реализации принципов сетевого нейтралитета необходимо обеспечить технологическую нейтральность отраслевого регулирования.

При этом практика ФАС России по рассмотрению дел о нарушениях антимонопольного законодательства показывает, что зачастую управление трафиком операторами связи осуществляется не в технологических целях, не для обеспечения безопасности или единства сетей связи, а в целях получения необоснованных конкурентных преимуществ. Это дела касающиеся взаимодействия операторов сотовой и фиксированной связи, дела, связанные с ограничением конкуренции на рынке услуг доступа в Интернет.

Возможность по-разному тарифицировать или ограничивать потребление интернет-трафика имеет преимущественное значение, в первую очередь, для операторов беспроводной связи: ресурс беспроводных сетей для передачи данных ограничен, и его способна целиком израсходовать относительно небольшая часть абонентов, увлекающаяся просмотром потокового видео или загрузкой файлов больших объёмов. Для фиксированных операторов, абоненты которых являются пользователями безлимитных тарифных планов, выгодно, чтобы абоненты меньше «качали», для мобильных операторов нежелательными являются такие сервисы, как «Skype», которые угрожают основному бизнесу – передаче голоса, так как попросту подменяют его.

Федеральной комиссией по коммуникациям США (FCC) в декабре 2010 г. в целях развития онлайн-сервисов были утверждены правила «сетевого нейтралитета», которые запрещали интернет-провайдерам блокировать или ухудшать связь при доступе к определенным интернет-ресурсам. Например, при доступе к Torrent – трекерам, размещенным в Интернете файлообменным системам, с которых абоненты загружают большие объемы информации. Однако в апреле 2011 г федеральный суд США вынес постановление о невозможности обязать операторов связи, предоставляющих доступ к Интернету, держать свои сети открытыми для всех видов контента, и предоставил операторам связи возможность самостоятельно снижать скорость передачи трафика при доступе к популярным файлообменным системам.

Не однозначна и практика в России, так определением ВАС РФ отказано в передаче дела Президиум ВАС РФ для пересмотре в порядке надзора судебных актов по делу о нарушении антимонопольного законодательства, с формулировкой что ограничение пропуска трафика, не предусмотренного договором, осуществлено обществом в допустимых пределах осуществления гражданских прав и не является злоупотреблением доминирующим положением[1].

ФАС России в настоящее время вплотную занимается данными вопросом правомерности ситуации «сетевого нейтралитета», пытаясь выработать основ-

1 Определение ВАС РФ от 19.11.2012 N 14517/12 по делу N А09-3830/2011//СПС Консультант Плюс;

ные критерии квалификации и готовности разных участников данного сегмента рынка.

Второе связано с взаимоотношениями между хозяйствующими субъектами данного сегмента рынка. Оператор связи владеет объектом кабельной канализации, а другие операторы услуг связи, которые хотят оказывать услуги пользователям, те же интернет-провайдеры, иные компании не могут попасть в эту кабельную канализацию, в связи с неправомерным отказом владельца объектов инфраструктуры, вывод данные действия могут быть расценены как отказ от заключения договора или создание препятствий доступу на товарный рынок, что будет нарушать формальные требования Закона «О защите Конкуренции».

Основным же нарушениям со стороны хозяйствующих субъектов, которое посягает на основы свободы и добросовестности конкуренции является соглашения или согласование действия между хозяйствующих субъектов, не допустимые в соответствии с антимонопольным законодательством.

Из системного толкования статьи 11 Закона Федерального закона Российской Федерации «О Защите конкуренции» следует что, согласованные действия являются особой моделью группового поведения хозяйствующих субъектов, замещающей конкурентные отношения между ними сознательной кооперацией, наносящей ущерб интересам потребителей и ограничивающей конкуренцию[1].

К сожалению, нарушают антимонопольное законодательство и органы власти. Специфика нарушений с их стороны за частую связана с установлением административных барьеров для входа на рынок и создание препятствия для деятельности на нем, уже действующим хозяйствующим субъектам. Зачастую нарушения связаны ущемлением права и законные интересов участников рынка при выделении частот, лицензий и разрешений. Но основным же нарушением выражаются в различных ограничениях доступа к проводившимся торгам, а также при издании нормативно-правовых актов, регламентирующих требования к формату представляемых данных.

При этом во всех вышеописанных случаях антимонопольный орган компетентен пресекать и осуществлять действия по обеспечению конкуренции, защищая своими действиями не только законные права и интересы Интернет-провайдера (или другого оператора связи), а также и интересы пользователей услуг.

В целях содействие развитию конкуренции в области телекоммуникаций и доступа к сети Интернет, а также рассмотрения вопросов, связанных с соблюдением хозяйствующими субъектами, федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, иными осуществляющими функции указанных органов на территории Российской Федерации в области информационных технологий, при ФАС России создан экспертные совет для введения конструктивного диалога бизнеса и власти.

---

[1] Постановление Восемнадцатого арбитражного апелляционного суда от 22.02.2012 N 18АП-161/2012 по делу N А07-13938/2011,// СПС Консультант Плюс.

Разработка правил недискриминационного доступа к услугам общедоступной связи и объектам инфраструктуры широкополосного доступа к сети Интернет, проблемы сетевого нейтралитета, вопросы технологической нейтральности, доступа на рынок новых сервисных услуг. Также вопросы административной реформы в области телекоммуникаций являются неотъемлемой частью экспертных советов созданных при ФАС России.

На сегодняшний день антимонопольный контроль за данным сегментом рынка со стороны ФАС России является не только эффективной реализацией конституционного права на информацию, но и эффективным механизмом реализацией государственных гарантий единства экономического пространства, свободы перемещение товаров, поддержки конкуренции и свободы экономической деятельности в сфере информационно коммуникационных-технологий и услуг по предоставлению доступа к сети Интернет.

Жилина Н.Ю.

ОСНОВНЫЕ ДЕТЕРМИНАНТЫ НАРКОПРЕСТУПНОСТИ В РОССИИ

Аннотация: Данная статья посвящена анализу общих вопросов преступной детерминированности, а также в частности проблеме выявления причин и условий наркопреступности в России на современном этапе развития общества. Автор делает вывод о том, что наркотизации населения и наркопреступности способствует целый комплекс причин и условий различного уровня.

Ключевые слова: причинность, факторы преступности, детерминация, наркопреступность, наркотизация населения

Abstract. This article analyzes the general questions of crime determinacy, as well as in particular a problem of revealing the drug crime's reasons and conditions in Russia at the present stage of society's progress. The author draws a conclusion that the population's narcotization and the drug crime the whole complex of the reasons and conditions of a various level assists.

Key words: causality, factors of crime, determination, drug crime, population's narcotization

Отметим, что по нашему мнению, изучение причин наркопреступности имеет большое значение не только для непосредственного анализа объективных истоков конкретного правонарушения, но и для выработки эффективных профилактических мер.

Причины преступности – это социально-психологические факторы, от которых непосредственно зависит совершение преступлений, которые воспроизводят преступность и преступления как свое закономерное следствие[1]. Именно причины преступности оказывают решающее воздействие на факт принятие решения о совершении преступления, формирование мотива и цели, выбор конкретных преступных способов достижения этой цели.

Разумеется, нельзя выделить какую-то единственную, «главную» причину, которая бы являлась единственной предпосылкой для совершения преступлений во всем их разнообразии.

Под условиями преступности понимаются такие общественные явления, которые хоть непосредственно и не вызывают совершение преступления, тем не менее являются вспомогательными. То есть это то, что само по себе не порождает преступность или преступление, но, тем не менее, влияет на процессы порождения преступного поведения, участвует в детерминации преступности[2]. Именно от условий, сопутствующих совершению конкретного деяния зависит выбор способа реализации преступного намерения, объекта преступного посягательства. Условиями определяются размеры и характер причинённого вреда, место и время совершения преступления.

Кроме того, одно и то же обстоятельство, в зависимости от конкретной ситуации может выступать, и в качестве причины преступления, и в качестве

[1] Криминология: Учебник для вузов / Под общ. ред. А. И. Долговой. М., 2001. – С. 230.

[2] Кудрявцев В. Н. Причинность в криминологии. О структуре индивидуального преступного поведения. М., 2007. – 246 с.

условия. Отметим также, что причины и условия преступности действуют совместно: причина порождает следствие лишь при наличии определённых условий[1].

Преступность связана со множеством явлений, состояний, процессов. Из них *причинами* являются лишь те, которые воздействуют генетически, т. е. порождают, воспроизводят преступность как свое следствие. *Условия* как разновидность детерминации лишь способствуют этому, обеспечивая возможность действия причин. Вместе с тем надо иметь в виду, что при изучении процессов детерминации преступности должна учитываться относительность деления явлений и процессов на причины и условия. То, что в одном отношении явилось причиной, в другом выступает как следствие и наоборот.

По мнению А. И. Гурова, причины наркомании и наркопреступности следует рассматривать в тесной связи с причинами собственно преступности[2]. Криминальная ситуация в современной России, ее устойчивость и высокий уровень обусловили выделение двух групп факторов по отношению к преступности:

- внешние криминогенные факторы – экономические, социально-политические, правовые, организационные, социально-психологические, технические, медико-социальные, экологические и др.;
- внутренние факторы преступности – криминальный рецидив, профессионализм, криминальная организованность, традиционные и вновь нарождающиеся криминальные обычаи.

Среди внешних криминогенных факторов ученые особо выделяют экономический кризис, детерминирующий следующие факторы:

- всеобщее снижение уровня жизни населения;
- увеличение экономического расслоения людей по признаку обеспеченности, появление «сверхбогатых» на фоне обнищания масс;
- изменение структуры внутригосударственной экономики;
- неравномерность развития социально-экономических показателей в регионах;
- деиндустриализация страны, заключающаяся в разрушении промышленного потенциала и смещении инвестиций в сырьевой сектор экономики;
- коррумпирование органов власти и управленческого аппарата, криминализированность хозяйственной и финансовой деятельности;
- массовый социально-психологический и нравственный сдвиг, вызванный снижением уровня жизни и вовлекший значительное количество населения в противоправные отношения.

По нашему мнению, для выявления детерминанта наркопреступности и объективной оценки наркоситуации в стране недостаточно изучить лишь

---

[1] Криминология: Учебник / Под ред. Н. Ф. Кузнецовой, В. В. Лунеева. М., 2004. – С. 166.

[2] Предупреждение, пресечение и раскрытие преступлений в сфере оборота наркотических средств и психотропных веществ. Методическое пособие для сотрудников правоохранительных органов государств – участников СНГ. Под общ. ред. А. И. Гурова. Н. Новгород, 2003. – 345 с.

статистические показатели наркопреступности, ведь уголовная статистика не дает полного представления о степени распространенности этого явления потому, что значительная часть наркопреступлений не выявляется правоохранительными органами, т.е. является латентной. В связи с этим, их фактическое количество, а также размер ущерба причиненного обществу и государству остается невыясненным.

Все детерминанты наркопреступности, наркотизма и наркомании можно классифицировать по следующим основаниям[1]:

1. По источникам:

Объективные (внешние) – экономические, социально-политические, правовые, организационные, социально-психологические, технические, медико-социальные, экологические и ряд других детерминант;

Субъективные (внутренние) – криминальный рецидивизм, профессионализм, криминальная организованность, сложившиеся и вновь нарождающиеся криминальные традиции, а также ресоциализация лиц, отбывших наказание.

2. По уровню функционирования:

Способствующие росту наркопреступности, наркотизма и наркомании на *общесоциальном уровне*. Причины распространения наркотиков имеют по большей части социально обусловленный характер и непосредственно связаны с внутренними и внешними противоречиями развития нашей социальной системы. Следовательно, на данном уровне существуют общие причины, одинаково присущие всем преступлениям, в том числе и связанным с наркотиками;

Способствующие росту наркопреступности, наркотизма и наркомании на *специально-криминологическом уровне*. Одна из особенностей нынешней наркоситуации в России выражается в том, что негативная динамика наркопреступности придает наркотизму статус социально-культурного явления с формированием особой субкультуры. Ломка старой социальной системы ценностей приобрела специфический характер в современном обществе: наркотики становятся неотъемлемым атрибутом времяпрепровождения многих людей, принадлежащих к самым различным социальным слоям и группам. А доступность наркотиков приводит к вовлечению несовершеннолетних и молодежь в криминальные структуры;

Способствующие росту наркотизации населения на *индивидуальном уровне*. Причины злоупотребления наркотиками коренятся в конфликте между подростком (личностью) с окружающими его людьми и обществом. Эти конфликты могут проявляться через конкретные жизненные обстоятельства. Накладываясь на индивидуальные психофизиологические особенности подростка, они способны влиять на мотивационную сферу и облегчить возникновение тяги к приему наркотиков, а в дальнейшем и совершению преступлений

---

[1] Клименко Т. М. Совершенствование уголовного законодательства как важнейшая предпосылка повышения эффективности борьбы с наркоманией и наркотизмом / Т. М. Клименко // Человек: преступление и наказание. 2008. № 2 (61). – С. 79-82.

либо связанных с наркотизмом, либо совершенных под воздействием наркотиков.

3. По содержанию:

К социально-психологическим детерминантам наркопреступности, наркотизма и наркомании можно отнести утрату населением веры в справедливость и искренность высоких слов, идеалов, лозунгов, произносимых с трибун и пропагандируемых средствами массовой информации. Безверие породило целую гамму негативных явлений, связанных с философией потребительства, бездуховностью, равнодушием, отчужденностью, погоней за «сладкой жизнью», ростом преступности, проституции и других негативных явлений;

Организационно-управленческие детерминанты наркопреступности, наркотизма и наркомании подразумевают отсутствие надлежащих мер по охране мест выращивания мака и конопли, должного контроля над реализацией наркотических средств в аптеках, больницах, при их переработке на предприятиях, при хранении на складах; разобщенность действий правоохранительных органов при выявлении фактов транспортировки наркотиков на территорию нашего государства контрабандным путем; ненадлежащую координацию и взаимодействие с органами здравоохранения; слабую работу по профилактике наркотизма;

Культурно-воспитательные детерминанты наркопреступности, наркотизма и наркомании связывают с существовавшей долгое время практически легальной пропагандой наркотиков. Стремительное формирование возможностей СМИ, глобальной компьютерной сети Интернет, через которые развивается субкультура наркомании и идет активная пропаганда потребления наркотиков; а также неорганизованность досуга и утрата общепризнанных ценностей значительной частью молодежи затрудняют проводимые мероприятия по формированию здорового образа жизни.

Росту наркопреступности способствует также высокий уровень общей преступности, в особенности организованной и профессиональной ее части.

Неблагоприятная эволюция наркоситуации в России объясняется и воздействием ряда способствующих резкой интенсификации незаконного оборота наркотиков объективных и субъективных условий:

– отсутствие эффективной системы выявления потребителей наркотиков на ранних стадиях заболевания наркоманией;

– наличие высокого спроса на наркотики со стороны молодежных, богемных и даже маргинальных групп населения, потерявших в переходный период социальную ориентацию или перспективу либо ставших жертвой целенаправленной пропаганды, примера кумиров или моды;

– быстрый рост потребительской среды, прежде всего в промышленных городах. Социологические опросы в 20 городах России показали, что к регулярному потреблению наркотиков приобщаются не только традиционные потребители, но и предприниматели, рабочие, безработные, студенты, учащиеся, домохозяйки;

– разветвленная транспортная сеть, наличие собственного наркосырья и наркопроизводства, соответствующего оборудования, лабораторий, широкие

возможности для привлечения к производству наркотиков нуждающихся студентов, фармацевтов, квалифицированных химиков с использованием оборудования по месту их работы, а к распространению наркотиков – безработных из разных социальных слоев, используемых в качестве курьеров, сбытчиков, боевиков[1];

– пограничные этнические конфликты, дестабилизирующие ситуацию в регионах с интенсивным наркобизнесом;

– поиск международным наркобизнесом новых путей межгосударственной транспортировки наркотиков взамен ставшего для него более опасным так называемого «балканского» пути.

Следует также указать и на следующие специфические процессы, негативно влияющие на ситуацию в сфере незаконного оборота наркотиков:

– распространение средствами массовой информации так называемой наркотической идеологии, включая пропаганду употребления возбуждающих и одурманивающих средств как якобы неотъемлемого атрибута современной молодежной субкультуры;

– демонстрация соответствующих сцен в кинофильмах, видеофильмах, телевизионных передачах, нейтрализующих отрицательное отношение к наркотикам у массовой аудитории и, наоборот, искусственно разжигающих интерес к ним;

– подражание определенной части молодежи западным движениям анархического протеста (хиппи, рокеры и т.п.), в среде которых потребление наркотиков является составной частью повседневного образа жизни;

– активизация усилий преступной среды по вовлечению в нее подростков и лиц молодого возраста, в том числе за счет приобщения к традиционному для нее потреблению наркотиков;

– скачкообразный рост криминального наркобизнеса и формирование в России национального наркорынка в силу его особой прибыльности (до 10 млрд. долларов ежегодно) для производителей и распространителей наркотиков и увеличения этой прибыльности из-за ослабления системы контроля над незаконным оборотом наркотиков на территории постсоветского пространства, появления «прозрачных границ» и т.д.;

– растущая заинтересованность международных преступных сообществ, специализирующихся на незаконных операциях с наркотиками, в транзите их через территорию России (с учетом ослабления контроля на границе и транспортных магистралях, из-за их протяженности и неупорядоченности пограничного режима), а равно в закупках наркотического сырья в Средней Азии, на Дальнем Востоке, в приобретении разного рода синтетических наркотических средств, производимых в подпольных лабораториях или на нелегальных химфармпредприятиях, а также вывозе прекурсоров в регионы мира, где сконцентрировано крупное нелегальное производство наркотиков.

---

[1] Калачев Б.Ф. Проблемы борьбы с преступностью в системе обеспечения внутренней безопасности Российской Федерации: учеб. пособие / Б.Ф. Калачев, П.Н. Кобец. М.: ВНИИ МВД России, 2008. -141 с.

Наряду с причинами наркопреступности, считаем необходимым также выделить причины употребления наркотиков, так как эти два элемента тесно связанны и взаимозависимы при рассмотрении преступности в сфере незаконного оборота наркотиков. В соответствии со статистическими данными, предоставленными ФСКН по Белгородской области, наиболее часто встречающимися причинами способствующими употреблению наркотиков в немедицинских целях являются:

- отсутствие возможности самореализации;
- отсутствие жизненной перспективы;
- проблемы взаимоотношений со сверстниками;
- жизненная неустроенность;
- неумение противостоять давлению окружающих[1].

Таким образом, наркопреступности способствует целый ряд детерминантов. И неверно было бы выделять какую-то одну причину, как более значимую, недооценивая роль остальных. Наркотизации населения способствуют в тех или иных ситуациях разные наборы криминогенных обстоятельств.

[1] См.: Федеральная служба Российской Федерации по контролю за оборотом наркотиков. – М., 2012. – http://www.fskn.gov.ru/pages/main/info/legal_foundation/4114/9723/index.shtml

Звертаева Ю.Ю.

ИНТЕРНЕТ-РЕСУРСЫ В ОБЕСПЕЧЕНИИ СВОБОДЫ ДЕЯТЕЛЬНОСТИ ОБЩЕСТВЕННЫХ ОБЪЕДИНЕНИЙ

Аннотация: В данной статье рассмотрены аспекты обеспечения свободы деятельности общественных объединений посредством Интернет-ресурсов. Проанализированы формы взаимодействия институтов гражданского общества и публичных структур. Выявлена и обоснована необходимость расширения использования Интернет-пространства в обеспечении рассматриваемого принципа свободы деятельности общественных объединений.

Ключевые слова: свобода деятельности общественных объединений, Интернет-пространство, Интернет-ресурсы, Конституция Российской Федерации, органы власти, взаимодействие, гражданское общество.

Abstract: This article examines aspects of the freedom of public associations through Internet resources. The forms of interaction of civil society and public institutions. Identified and justified the need for increased use of the Internet to provide the space of the principle of freedom of activity of public associations.

Key words: freedom of public associations, the Internet space, Internet resources, the Constitution of the Russian Federation government, cooperation, civil society.

Исследования принципа свободы деятельности общественных объединений целесообразно осуществлять, помимо прочего, и в контексте Интернет-ресурсов, что сопряжено с ч. 4 ст. 29 Конституции Российской Федерации о свободе поиска, получения, передачи, производства и распространения информации любым законным способом[1].

Конституционный принцип информационной открытости власти является основополагающим для демократического правового государства, поскольку реализация данного права обеспечивает фактическое, а не формальное участие в управлении делами государства. В то же время, непосредственное отношение к участию граждан в управлении делами государства, является закреплённое в ст. 30 Конституции России за каждым право на объединение, в том числе и на создание общественных объединений.

Истинная демократия «должна иметь механизмы постоянного и прямого действия, эффективные каналы диалога, общественного контроля, коммуникаций и обратной связи»[2]. Именно такими инструментами, позволяющими реализовать закреплённые конституционные права, свободы и законные интересы, способны выступить Интернет-ресурсы. Полагаем, их роль в обеспечении свободы деятельности общественных объединений и в дальнейшем будет возрастать.

Федеральным законом «Об информации, информационных технологиях и о защите информации»[3] установлены принципы правового регулирования данного рода отношений. Среди них открытость информации о деятельности государственных органов и местного самоуправления и свободный доступ к

[1] См. Конституция Российской Федерации / Российская газета. № 7. 2009.

[2] См. Путин В.В. Демократия и качество государства // Коммерсант. 2012. 6 февраля.

[3] См. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3448.

такой информации, достоверность информации и своевременность её предоставления[1].

Данные принципы адресуются и общественным объединениям. Гражданское общество, выступая в качестве независимого и влиятельного участника общественно-политических процессов в стране[2], взаимодействует с публичными институтами. Цель данного общения в рамках Интернет-пространства заключается в получении необходимой и в достаточном объёме информации о структуре, задачах и иных существенных условиях деятельности органов власти. Одновременно – это возможность представить широкой общественности сведения и о самих общественных объединениях, о целях и задачах их деятельности[3].

Возможны разнообразные формы взаимодействия институтов гражданского общества и публичными структурами, в которых раскрывается свобода деятельности общественных объединений с использованием Интернет-ресурсов. В частности, одним из примеров могут служить обращения (предложения, заявления, жалобы) общественных объединений, направляемые в форме электронного документа в государственные органы и органы местного самоуправления[4]. Направление запросов в органы государственной власти общественными объединениями о предоставлении им информации, которая в последующем может быть положена в основу законодательной инициативы, также может рассматриваться как форма реализации объединениями своих конституционных прав и свобод с использованием Интернет-пространства.

Несмотря на то, что народная законотворческая инициатива не закреплена на конституционном уровне, она по праву относится к формам реализации демократических начал общества, и в ряде регионов напрямую закреплена в их Уставах. Примером может служить Устав Белгородской области, в ст. 30 которого право законодательной инициативы в Белгородской областной Думе закреплено, в том числе, и за общероссийскими, межрегиональными и региональными общественными объединениями[5]. Аналогичные положения закреплены и в Конституциях (Уставах) иных субъектов Российской Федерации, среди которых Республика Карелия[6], Приморский край[7], Тульская область[8] и другие. Данные аспекты представлены и в ряде исследований[9].

---

[1] См. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. № 165. 2006. 29 июля.

[2] См. Доклад о состоянии гражданского общества в Российской Федерации за 2012 год. – М.: Общественная палата Российской Федерации. 2012. – С. 44.

[3] См. Едина Россия Официальный сайт партии. // http://er.ru/public_associations/. *Российский союз молодежи*, Общероссийская общественная организация. // www.ruy.ru. *Общество "Знание" России*, Общероссийская общественная организация // www.znanie.org.

[4] См. Федеральный закон от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // Собрание законодательства Российской Федерации. 2006. № 19. ст. 2060.

[5] См. Устав Белгородской области // Сборник нормативных правовых актов Белгородской области. Сентябрь-декабрь 2004. № 56 (ч. 1).

[6] См. Конституция Республики Карелия // http://www.gov.karelia.ru/Constitution/.

[7] См. Устав Приморского края. // http://www.zspk.gov.ru/about/ustav.html.

[8] См. Устав (Основной закон) Тульской области. // http://constitution.garant.ru/region/ustav_tulsk/.

[9] См. Д.В. Афиногенов. Законодательная инициатива граждан и их объединений в Российской Федерации. // Электронная библиотека «Гражданское общество». URL: http://www.civisbook.ru/.

Отметим и такую форму реализации принципа свободы деятельности общественных объединений посредством Интернет-ресурсов как участие в различных форумах органов власти. Обратная связь для органов государственной власти – это «часть процесса политической коммуникации»[1]. Так, участвуя в обсуждении наиболее актуальных вопросов регионального и государственного значения, общественным объединениям предоставляется возможность аккумулировать и доводить до органов власти общественные интересы, представлять их в публичном пространстве, а также осуществлять защиту и реализацию данных интересов. Примером может служить создание на официальном сайте Белгородской областной Думы форумов «Обсуждение законопроектов», «Гражданская инициатива» и «Обсуждение реализации законов Белгородской области»[2], в которых активнейшее участие принимают, в том числе, и общественные объединения. Таким образом, посредством Интернет-ресурсов общественным объединениям предоставлена возможность в проведении открытой экспертизы социально-значимых проектов Белгородской области, внесения предложений и инициатив по формированию законодательной базы, а также участия в оценке эффективности реализации законов на уровне рассматриваемого субъекта Российской Федерации.

Использование Интернет-ресурсов позволяет в оптимально короткие сроки мобилизовать и спланировать действия участников общественных объединений для реализации своих конституционных прав и свобод, в том числе, и нашедших своё закрепление в ст. 31 Конституции Российской Федерации[3]. Данное обстоятельство позволяет представителям общественных объединений оперативно реагировать на социально-значимые события в обществе. Примером могут служить митинги, проведённые в субъектах Российской Федерации с 5 февраля по 3 марта 2012 г. с агитацией в поддержку кандидатов в Президенты Российской Федерации, организованные и скоординированные в максимально сжатые сроки с вовлечением большого количества участников с использованием, в том числе, и Интернет-ресурсов.

Данные аспекты показывают лишь часть многогранности использования Интернет-пространства в обеспечении свободы деятельности общественных объединений, которое на нынешнем этапе развития России представляется территорией, способствующей реализации структурирования общества. «Интернет и другие информационно-коммуникационные технологии (ИТК) стали для российских граждан одновременно полем и инструментом самоорганизации»[4], что в действительности соответствует нынешнему этапу развития общества.

---

[1] См. Князев Р. М. Муниципальный интернет-ресурс как форма эффективного взаимодействия муниципальной власти и населения [Текст] / Р. М. Князев // Проблемы современной экономики: материалы междунар. заоч. науч. конф. (г. Челябинск, декабрь 2011 г.). – Челябинск: Два комсомольца, 2011. – С. 36-42.

[2] См. Сайт Белгородской областной Думы. // http://belduma.ru/.

[3] См. Конституция Российской Федерации / Российская газета. № 7. 2009.

[4] См. О.Н. Яницкий. Мобилизационный потенциал гражданского общества // Мир России. 2011. № 2. – С. 116.

Зюлин М.А.

ИНТЕРНЕТ: ТРАНСФОРМАЦИЯ ИНТЕРПРЕТАЦИЙ КОНСТИТУЦИОННОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Статья посвящена анализу позиций Конституционного Суда Российской Федерации в отношении роли интернет-ресурсов в реализации гражданами права на информацию.

Ключевые слова: Конституция Российской Федерации, Конституционный Суд, Интернет, право на информацию.

Abstract. The paper studies the position of the Constitutional Court of the Russian Federation regarding the role of the Internet-resources in the implementation of the right of citizens to information.

Key words: Constitution of the Russian Federation, Constitutional Court, Internet, right to information.

Согласно последним исследованиям, динамика проникновения интернета в жизнь общества в процентном соотношении к числу населения Российской Федерации составила с 35% в 2005 г. до 75% в 2012 г. При этом к 2014 г. ожидается, что 80 % россиян будут интернет-пользователями. Возрастающая популярность интернета как средства массовой информации, не могла обойти стороной судебную систему.

В 2008 г. был принят Федеральный закон № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», которым установлен порядок размещения в сети Интернет информации о деятельности суда, судебных документов.

Обеспечению реализации права граждан на информацию, повышению открытости органов власти для общества послужило принятие в 2009 г. Федерального закона № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Конституция России закрепила обязанность государства признавать, соблюдать и защищать права и свободы человека и гражданина. Главная роль в выполнении задач защиты прав граждан от неправомерных посягательств и ограничений возложена на органы правосудия.

Тот факт, что Интернет является одним из важнейших факторов современного уровня жизни, не подвергается сомнению никем, в том числе и Конституционным Судом Российской Федерации.

Председатель Конституционного Суда В. Зорькин, встречаясь 18 февраля 2011 г. с Верховным комиссаром ООН по правам человека Навантехм Пиллай, отметил в качестве одного из показателей открытости конституционного производства соответствующий мировым стандартам уровень информатизации Конституционного Суда. В частности, отметил он, с 2008 г. возможен просмотр публичных заседаний Конституционного Суда в сети Интернет. Вместе с тем было упомянуто об имеющихся технических проблемах, мешающих сделать он-лайн трансляцию заседаний общедоступной.

При незыблемости Конституции России, Конституционный Суд осуществляет свою работу в соответствии с изменяющимися реалиями жизни, реагируя на изменение структуры информационного пространства в современных условиях.

Конституционный Суд России, признавая важную роль интернет-технологий в жизни общества, указывал, что «современные информационные технологии не могут не заслуживать поддержки и одобрения с точки зрения исполнения предусмотренной статьей 24 (часть 2) Конституции Российской Федерации обязанности обеспечения каждому возможности ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы»[1].

Сам термин «Интернет» в решениях Конституционного Суда РФ прошел некую эволюцию. Так, если в 2005 г. в Определении Конституционного Суда он упоминается как «размещение информации в «Интернете»[2], то позднее Конституционный Суд использует понятие «информация, распространенная в сети «Интернет»[3].

В размещении информации в сети Интернет, наряду с опубликованием в средстве массовой информации, Конституционный Суд видит прозрачность деятельности государственных органов в демократическом обществе, отмечая, что это «направлено на создание условий (гарантий) обеспечивающих максимальную информационную открытость государственных органов и органов местного самоуправления для граждан и иных субъектов гражданского общества, и согласуется с принятой Советом Европы 27 ноября 2008 года Конвенцией о доступе к официальным документам»[4].

«Интернет дает реальную возможность ознакомления с нормативными правовыми актами, не создавая неоправданных усилий по их поиску»[5].

---

[1] Постановление Конституционного Суда РФ от 27.03.2012 года № 8-П «По делу о проверке конституционности пункта 1 статьи 23 Федерального закона «О международных договорах Российской Федерации» в связи с жалобой гражданина И.Д. Ушакова» // СЗ РФ. 2012. № 15. Ст. 1810.

[2] Определение Конституционного Суда РФ от 12.07.2005 года № 333-О «Об отказе в принятии к рассмотрению жалобы гражданина Волкова Андрея Григорьевича на нарушение его конституционных прав положениями статьи 71 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», а также ряда законов Томской области»

[3] Определение Конституционного Суда РФ от 20 марта 2007 года № 195-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Шмонина Андрея Владимировича на нарушение его конституционных прав пунктом 1 статьи 152 Гражданского кодекса Российской Федерации»

[4] Определение Конституционного суда РФ от 08.12.2011 года № 1624-О-О «По жалобе граждан Андреевой Татьяны Алексеевны, Морозова Филиппа Владиславовича и других на нарушение их конституционных прав пунктом 1 статьи 1 Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

[5] Определение Конституционного суда РФ от 3.04.2007 года № 171-О-П «По жалобе гражданина О.Б. Гуртуева и коллективной жалобе граждан – жителей Кабардино-Балкарской Рес-

Вместе с тем, Конституционный Суд РФ не рассматривает использование Интернета как источник традиционного официального опубликования, относя его к «иным» возможностям современного информационного пространства.[1]

Позиция Конституционного суда РФ по определению роли Интернета в политической жизни общества ярко проявилась в Определении от 14 ноября 2005 года № 10-П «По делу о проверке конституционности положений пункта 5 статьи 48 и статьи 58 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», пункта 7 статьи 63 и статьи 66 Федерального закона «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» в связи с жалобой Уполномоченного по правам человека в Российской Федерации»[2].

Здесь интересны обстоятельства, послужившие основанием для обращения Уполномоченного по правам человека с жалобой в Конституционный Суд России: гражданин В.Б. Бочков постановлением мирового судьи признан виновным в том, что в период избирательной компании по выборам депутатов Государственной Думы составил, подготовил для печати, а затем распространил листовку с призывом к избирателям голосовать против всех кандидатов, оплатив изготовление агитационного материала из собственных денежных средств, нарушив тем самым статью 63 Федерального закона «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации».

Рассматривая жалобу Уполномоченного по правам человека в Российской Федерации, Конституционный Суд подтвердил право граждан Российской Федерации осуществлять предвыборную агитацию против всех кандидатов (против всех списков кандидатов) посредством проведения массовых мероприятий, если это не сопровождается денежными расходами на производство агитационных материалов, и – при соблюдении того же условия – посредством иных не запрещенных законом методов (в частности, через сети общего пользования, включая Интернет).

Из приведенных решений Конституционного Суда следует, что Интернет признан данным органом как пусть и не традиционное средство массовой информации, но как важнейший фактор общественной жизни, позволяющий гражданам выражать свою позицию по любым социально значимым вопро-

---

публики на нарушение их конституционных прав положениями Законов Кабардино-Балкарской Республики «Об административно-территориальном устройстве Кабардино-Балкарской Республики», «О статусе и границах муниципальных образований в Кабардино-Балкарской Республике» и Федерального закона «Об общих принципах организации местного самоуправления в Российской Федерации» // СЗ РФ. 2007. № 21. Ст. 2561.

[1] Постановление КС РФ от 27.03.2012 № 8-П.

[2] Определение КС РФ от 14 ноября 2005 года № 10-П // СЗ РФ. 2005. № 47. Ст. 4868.

сам, оказывающий помощь в понимании современных политических процессов и, безусловно, заслуживающий признания.

Так, Конституционный Суд признал недопустимым использование сети «Интернет» в качестве средства надлежащего извещения сторон по делу о времени и месте судебного заседания, предполагая лишь возможность доступа заинтересованных лиц к сети Интернет, не обязательно имеющуюся у всех субъектов процесса по конкретному делу[1].

Таким образом, «Интернет» признается Конституционным Судом Российской Федерации как инструмент, позволяющий гражданам получить информацию «из первых рук», помогающий им реализовывать их конституционные права, принимать участие в политической жизни общества, и в этом смысле, безусловно заслуживающий одобрения, однако пока он еще не завоевал в полной мере доверие этого органа конституционного контроля (правосудия) как полноценное средство доведения информации до граждан (несмотря на включение в 2011 году Интернет-сайта в перечень средств массовой информации.

[1] Постановление Конституционного Суда РФ от 30.11.2012 № 29-П «По делу о проверке конституционности положений части пятой статьи 244.6 и части второй статьи 333 Гражданского процессуального кодекса Российской Федерации в связи с жалобами граждан А.Г. Круглова, А.В. Маргина, В.А. Мартынова и Ю.С. Шардыко»// СЗ РФ. 2012. № 51. Ст. 7323.

Ищенко Е.П.

К ВОПРОСУ О КИБЕРПРЕСТУПНОСТИ

Аннотация. В статье рассматривается такое сложное криминальное явление, как киберпреступность, дается ее понятие, раскрываются содержание и некоторые криминалистические особенности.

Ключевые слова: киберпреступность, информационные технологии, Интернет.

Abstract. The article deals with a complex criminal phenomenon as cybercrime, given its concept, reveals the content and some forensic features.

Key words: cybercrime, information technology, the Internet.

Быстрое развитие новых информационных технологий, их активное внедрение во все сферы жизнедеятельности привело к тому, что цивилизованное человечество стало очень зависимым от бесперебойной работы компьютерных сетей и устройств, в особенности тех, которые включены в глобальные системы жизнеобеспечения. В параллельном режиме, как это ни прискорбно, развивалась и киберпреступность.

В соответствии с рекомендациями экспертов ООН, понятие «киберпреступность» включает в себя любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках такой системы или сети, против компьютерной системы или сети. Иначе говоря, к киберпреступлениям относятся такие уголовно-наказуемые деяния, которые совершаются в киберпространстве против компьютерных данных с помощью или посредством компьютерных систем или сетей, а также иных средств доступа к киберпространству.

В более конкретном контексте киберпреступность — это преступления в сфере высоких информационных технологий, совершаемые злоумышленниками, использующими эти технологии для достижения противоправных целей. По УК РФ такие преступления включают в себя неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных компьютерных программ (ст. 273), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Весьма распространенными посягательствами стали взломы паролей, кражи номеров кредитных карт и других банковских реквизитов, распространение через Интернет противоправной информации (порнографических материалов, клеветнических сведений, материалов, возбуждающих межнациональную и межрелигиозную рознь, вражду и т.п.).

Кроме того, одним из наиболее опасных и распространенных киберпреступлений, совершаемых с использованием Интернета, стало мошенничество. Яркий пример такого мошенничества – интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленных на аукцион товаров. В зарубежных государствах, в частности, в США, получили распространение мошенничества, связанные с продажей доменных имен. Для этого производится массовая рассылка электронных писем, в которых, например, сообщается

о попытках неизвестных лиц зарегистрировать доменные имена, похожие на те, которые принадлежат адресатам. Владельцам сайтов предлагается вновь зарегистрировать доменное имя, чтобы опередить злоумышленников.

В УК ФРГ к преступлениям в сфере оборота компьютерной информации (киберпреступлениям) отнесены:

- действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a);
- нарушение тайны телекоммуникационной связи (§ 206);
- действия лиц, учиняющих подделку или использующих поддельные технические записи, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268);
- аналогичная подделка данных, имеющих доказательственное значение (§ 269);
- действия лиц, уничтожающих, изменяющих или утаивающих технические записи (§ 274);
- действия лиц, противоправно аннулирующих, уничтожающих, приводящих в негодность или изменяющих данные (§ 303a);
- действия лиц, нарушающих обработку данных путем разрушения, повреждения, приведения в негодность установки для обработки данных или носителей информации (§ 303b).
- незаконное вмешательство в деятельность телекоммуникационных установок (§ 317).

Кроме того, уголовное законодательство Федеративной Республики Германии устанавливает уголовную ответственность за компьютерное мошенничество, под которым понимаются умышленные деяния с намерением получить для себя или третьих лиц имущественную выгоду, заключающиеся в причинении вреда чужому имуществу путем воздействия на результат обработки информации путем неправильного создания программ, использования искаженных данных, неправомочного их использования или иного воздействия на результат обработки данных (§ 263a).

Общественная опасность противоправных деяний в области компьютерной техники и высоких информационных технологий выражается в том, что они могут повлечь за собой грубое нарушение деятельности автоматизированных систем управления и контроля различных важных объектов, а также работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом большим группам людей.

Бурное развитие цифровых технологий привело к тому, что следователи в последнее время постоянно сталкиваются с новой средой отражения преступлений – цифровым киберпространством, образованным носителями информации, представленной в дискретном виде. По мнению Верховного Суда США «киберпространство» – это «уникальная среда, не расположенная в географиче-

ском пространстве, но доступная каждому человеку в любой точке мира посредством доступа в Интернет»[1].

В последние годы привычная реальность все более смешивается с виртуальной реальностью (киберпространством), так что впору говорить о совмещенной реальности, включающей в себя обе эти ипостаси. Не случайно авторы «модельного закона о киберпреступности» из Международного Союза Электросвязи (2009 г.) определяют киберпространство как «физическое и не физическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движения данных, и пользователи».

Поэтому представляется совершенно необходимым безотлагательное закрепление на российском законодательном уровне понятий не только киберпреступлений, но и киберпространства, как это было сделано в США. Такой подход позволил бы решить проблемы, связанные с пониманием правоприменителями этих дефиниций, в особенности той среды, в которой совершаются киберпреступления. Последних, кстати сказать, в зарубежных странах совершается все больше, растет и причиняемый этими деликтами материальный ущерб. По последним оценкам Европола, потери от киберпреступлений составляют в глобальном масштабе 750 млрд евро в год.

В этой связи весьма важно выработать процессуальный порядок и тактические приемы обнаружения, закрепления, изъятия, сохранения и экспертного исследования компьютерной информации как судебного доказательства[2]. Вместе с тем, механизм формирования компьютерной информации как процессуального доказательства разработан явно недостаточно[3], что создает трудности в уголовном судопроизводстве по их собиранию, проверке и оценке. Здесь для криминалистов, можно сказать, непочатый край работы, хотя ряд шагов в нужном направлении уже предпринят[4].

---

[1] Цит. по: Дашян Н. Обзор Конвенции Совета Европы о киберпреступности //Современное право. 2002. №11. С. 20.

[2] См. подробнее: Протасевич А.А., Зверянская Л.П. Проблемы теории и практики выявления и расследования киберпреступлений // Криминалистика и судебная экспертиза: наука, обучение, практика. СПб, 2012. С. 573-578; Старичков М.В. Тактика осмотра и выемки машинных носителей информации // Криминалистические чтения на Байкале-2012: материалы Всероссийской науч.-практ. конф. Иркутск, 2012. С. 126-133.

[3] См. об этом: Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 4.

[4] Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дис. … канд. юрид. наук. Волгоград, 1995; Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Волгоград, 1997; Остроушко А.В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Волгоград, 2000; Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук. М., 2000; Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. Воронеж, 2001; Соловьев Л.Н. Расследование преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ: автореф. дис. … канд. юрид. наук. М., 2003;

Характерная особенность киберпространства состоит в том, что взаимодействующие в нем объекты (файлы данных и программ), которые участвуют в процессе следообразования, не имеют внешнего строения. Весь арсенал средств и методов работы со следами, накопленный трасологией, здесь оказывается бесполезным. Приемы обращения с виртуальными следами не нашли пока надлежащего отражения в УПК РФ, фигурируя лишь в виде отдельных криминалистических рекомендаций.

Под виртуальными следами В.А. Мещеряков предлагает понимать «следы, сохраняющиеся в памяти технических устройств, в электромагнитном поле, на носителях машиночитаемой информации, занимающие промежуточное положение между материальными и идеальными».[1]

Новые информационные технологии усложнили не только следовую картину преступлений и такие понятия, как место и время совершения киберпреступлений[2], но и круг предметов и документов – вещественных доказательств. Появилась группа таких доказательств – носителей цифровой информации – особая в силу свойственной им электронной специфики. Получение и анализ таких доказательств по уголовным делам о киберпреступлениях настоятельно требует наличия у следователей, оперативных работников, а также судей специальных знаний в области компьютерной техники и программного обеспечения.

В России борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД РФ. В 2008 году их сотрудники расследовали 14 тыс. киберпреступлений, в 2009 году их число превысило 17,5 тыс., из которых оказалось 9489 случаев несанкционированного доступа к компьютерной информации, 2097 фактов распространения вредоносных программ, 1010 кибермошенничеств и 320 преступлений, связанных с распространением детской порнографии. В первом полугодии 2011 г. число киберпреступлений выросло на 95% к аналогичному периоду 2010 г.[3]. Криминалистическому обеспечению эффективности работы по выявлению и расследованию таких преступлений необходимо уделить самое

Егорышев А.С. Расследование и предупреждение неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук. Самара, 2004; Белевский Р.А. Методика расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ : дис. ... канд. юрид. наук. СПб., 2006; Иванова, И.Г. Выявление и расследование неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук. Барнаул, 2007; Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. ... канд. юрид. наук. Омск, 2009; Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. Саратов, 2012.

[1] Мещеряков В.А. Преступления в сфере компьютерной информации. Воронеж, 2002. С. 102.

[2] См. подробнее: Кушниренко С.П. Пространственно-временная категория в структуре преступлений в сфере высоких информационных технологий // Криминалистика и судебная экспертиза: наука, обучение, практика. СПб, 2012. С. 541-546.

[3] См.: Топузис Д. Криминалистика и киберпреступность //К 90-летию со дня рождения Р.С. Белкина. М., 2012. С. 120-121.

пристальное внимание. Во всех профессиональных тонкостях их работы криминалисты – ученые и практики – должны хорошо разбираться[1].

Это тем более необходимо, что преступления в сфере высоких информационных технологий очень часто являются международными, когда преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Конвенция Совета Европы о преступности в сфере компьютерной информации ETS N 185 была подписана 23 ноября 2001 г. в Будапеште. Ее, в частности, подписали Россия, США и Япония. Эта Конвенция подразделяет преступления в киберпространстве на четыре группы. В первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст. 2), незаконный перехват (ст. 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) (ст. 4) или системы (ст. 5). В эту же группу преступлений входит противозаконное использование специальных технических устройств (ст. 6) – компьютерных программ, разработанных или адаптированных для совершения преступлений, предусмотренных в ст. 2-5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой ее части). Нормы ст. 6 применимы только в том случае, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.

Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст. 7-8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.

Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение детской порнографии, а также владении детской порнографией, находящейся в памяти компьютера (ст. 9).

Четвертую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

Согласно Конвенции Совета Европы, каждое государство-участник обязано создать необходимые правовые условия для предоставления следующих вохзможностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целости и сохранности хранимых компьютерных данных, относящихся к уголовному делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Кроме того, Конвенция требует создать необходимые правовые условия, обязывающие интернет-провайдеров проводить сбор и фиксацию либо перех-

---

[1] См. об этом: Иванов Н.А. Экспертиза электронных документов и машинограмм. М.: Издательство «Юрлитинформ», 2009. С. 8-135.

ват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать интернет-провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

Осмысление сущности Интернета позволяет заключить, что необходимо рассматривать его как некий глобальный феномен, оказывающий все возрастающее влияние на характер и структуру современной преступности. В качестве такового он обладает рядом специфических свойств, анализ которых позволяет глубже понять криминалистические проблемы раскрытия и расследования сетевых и связанных с использованием IT-технологий деликтов (киберпреступлений). Наиболее значимы среди них, на наш взгляд, следующие:

1. Надгосударственный и децентрализованный характер Интернета, отсутствие единой организации, полностью координирующей и контролирующей его функционирование. В большинстве стран, в том числе и в России, система регулирования и контроля Интернета находится в фазе становления.

2. Технологическая незащищенность Глобальной сети, которая изначально создавалась как открытая среда коммуникации исследовательских и военных компьютерных центров (сейчас в нее входит более 10500 телекоммуникационных сетей разных типов).

3. Возможность анонимной деятельности в Интернете, упрощенные процедуры регистрации пользователей, практически полное отсутствие достоверных идентификаторов личности посетителей Интернета существенно затрудняют выявление лиц, совершающих киберпреступления.

Указанные факторы, перечень которых может быть существенно расширен, усугубляются неразвитостью научных и правовых основ противодействия преступным посягательствам в Интернете и механизмов их реализации.

В то же время ресурсная база Интернета может быть использована: а) как источник оперативной информации; б) как информационный канал для оперативной связи с населением; в) как средство влияния на население в интересах раскрытия и расследования преступлений; г) как средство влияния на лиц, совершивших преступление, с целью побудить их к явке с повинной или к совершению ошибочных действий, способствующих их задержанию компетентными органами[1].

В этой связи традиционные сыскные технологии в оперативно-розыскной деятельности в последние годы заметно уступили место оперативно-техническим мероприятиям, таким как снятие информации с технических каналов связи, прослушивание телефонных переговоров, использование средств пеленгации, анализ телефонного трафика, в том числе предусматривающий привязку к базовым станциям, обращение к оцифрованным информресурсам и др.[2].

---

[1] См. об этом: Ишин А.М. Некоторые аспекты использования информационных технологий в ходе раскрытия и расследования преступлений //Современные проблемы информационно-криминалистического обеспечения расследования и его оптимизация. – Краснодар: Краснодарский университет МВД России, 2011. С. 16-22.

[2] См. подробнее: Ищенко Е.П. О некоторых подходах к выявлению и расследованию преступлений, совершаемых в виртуальном пространстве // Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы информационной безопасности: Сб. материалов науч.-практ. конф. Выпуск 7. – Калининград, 2006. С. 214-226; Ишин А.М. Некоторые особенности использования глобальной сети

Здесь мог бы пригодиться и опыт, накопленный в полицейской практике ФРГ, по организации розыскных мероприятий, связанных с целенаправленной компьютерной обработкой различных баз данных в целях поиска сведений о лицах и предметах, представляющих криминалистический интерес. В их число входят: розыск в полицейских информационных системах, а также в иных базах данных, формируемых в интересах уголовного преследования; «сетевой» розыск, связанный с обработкой персонифицированных данных; и растровый розыск.

Сущность последнего заключается в том, что он представляет собой автоматизированный поиск неизвестных преступников путем компьютерной обработки различных информационных массивов персональных данных, собираемых для иных целей, нежели уголовное преследование. В ходе растрового розыска компьютерная обработка широкого круга персональных информационных массивов осуществляется с учетом так называемого «профиля» (криминалистической информационной модели предполагаемого преступника), представляющего собой упорядоченный набор поисковых признаков лиц, совершающих данный вид преступлений.

В результате обработки баз персональных данных с помощью специальной программы из огромного информационного массива выбираются те субъекты, которые соответствуют составленному растру (профилю). По результатам применения растрового метода формируется список людей, которые соответствуют поисковым признакам потенциального подозреваемого. Их дальнейшая проверка на причастность к содеянному, осуществляется с помощью традиционных оперативно-розыскных и следственных действий (электронное наблюдение, задержание, допросы, обыски и др.)[1].

Обобщая вышеизложенное, можно заключить, что одним из весьма перспективных направлений приложения усилий криминалистов представляется изучение и использование в сфере борьбы с киберпреступностью компьютерной информации, нередко фигурирующей в виде цифровых следов. Такие следы оставляют в различных информационных системах средства мобильной связи, кредитные, дисконтные, банковские карты, проездные документы, снабженные магнитным кодом, сетевые ПК и др.

Выявление, фиксация, расшифровка таких следов, в массовом порядке остающихся и циркулирующих в киберпространстве, будет способствовать успешному раскрытию и расследованию самых различных кибрепреступлений, становящихся в последнее время все более распространенными и опасными.

Интернет в оперативно-розыскной деятельности //Криминалистика и судебная экспертиза: наука, обучение, практика. СПб, 2012. С. 519-526.

[10] См. подробнее: Сокол В.Ю. Растровый розыск преступников в Германии: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2009. С. 6-37.

Карачевцева О.С.

СОЦИАЛЬНО-ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Аннотация. Статья посвящена проблеме защиты прав и интересов несовершеннолетних при использовании ими сети Интернет и разработке рекомендаций в данной сфере.

Ключевые слова: дети, интернет, защита от негативной информации.

Abstract. The article is devoted to protecting the rights and interests of minors in their use of the Internet and the development of recommendations in this area.

Key words: children, internet, protection from negative information.

Уже достаточно долгое время Интернет стал жизненно необходимой вещью, без которой человек уже не может. Было бы достаточно банально перечислять все блага, которые нам может предоставить интернет, тем не менее, важно то, что мы глубоко «погрязли» в паутине и отказаться от этого изобретения человечества многим просто не под силу, особенно если эти многие – дети. Специфика человеческой психики такова, что мы быстро привыкаем к новой среде в которой комфортно себя чувствуем, изоляция же нас из этой среды равносильна насилию.

Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Согласно последней статистике около 50% детей выходят в Сеть без контроля взрослых: 28% из вышедших в Интернет детей «серфят» в поисках «клубнички». По данным вышеупомянутого исследования, 19% детей иногда посещают порносайты, еще 9% делают это регулярно. 38% детей, просматривают страницы о насилии, 16% детей просматривают страницы с расистским содержимым, 26% детей участвуют в чатах о сексе.[1]

Ситуация обстоит так, что распространяется не только беспроводной, но и мобильный интернет, которым активно пользуются дети, здесь они могут подвергаться тем же рискам, что и сидя за компьютером. В связи с этим важно проанализировать данную ситуацию с позиции прав и интересов детской аудитории. Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу.

С одной стороны, многие дети могут найти для себя в интернете много полезной информации, необходимой для развития личности, образования. С другой стороны, огромное количество негативной информации, подрастающее поколение ежедневно просматривает на сайтах в интернете. В последнее время мировое сообщество изучает и разрабатывает подходы и законы, касающиеся защиты прав и интересов ребенка в сети интернет. Так, в 2010 году был принят Федеральный закон Российской Федерации от 29 декабря 2010 г. №463-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [2].

---

[1] http://www.nestor.minsk.by/kg/2006/33/kg63308.html

[2] ФЗ РФ от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющих вред их здоровью и развитию» // Собрание законодательства. 2011. №1. Ст.48.

Важным является то, что здесь определены многие понятия, использующиеся в данной сфере, например такие как «дети, здоровье детей, развитие детей», «доступная для детей форма распространения информационной продукции»; «информация, информационная продукция»; «возрастная категория классификации информационной продукции»; «оборот информации»; «пропаганда, пропаганда насилия и жестокости, натуралистические изображение или описание, демонстрация насилия, демонстрация жестокости»; «информация устрашающего характера, провоцирующая детей к потенциально опасным поступкам, к антиобщественному поведению, содержащая ненормативную лексику, информация эротического характера, детская порнография» и другое.

«Информация» – это продукция любых СМИ, печатные издания, кино и видеофильмы, компьютерные игры, а также «иная аудиовизуальная продукция на любых видах носителей», распространяемая через Интернет, по каналам мобильной связи и даже «посредством публичных зрелищных мероприятий». В законе предлагается разделить всю предназначенную для детей информацию на категории в зависимости от её воздействия на здоровье и психику ребёнка. В предназначенной для детей печатной продукции, в аудио, видео и кинопродукции, предназначенной для детей или семейного просмотра, а также в компьютерных информационных сетях открытого доступа, не допускается размещение: объявлений физических и юридических лиц о знакомствах и встречах с детьми, а также объявлений о знакомствах с сексуальной целью, вопросников и тестов, требующих предоставления конфиденциальной информации, касающейся детей».

Защиту детей от информации, наносящей вред их здоровью и развитию, обязаны осуществлять органы государственного контроля (надзора), прокуроры, Уполномоченный по правам человека в Российской Федерации, Уполномоченные по правам человека и Уполномоченные по правам ребёнка в субъектах Российской Федерации, а также лица, осуществляющие мероприятия по образованию, воспитанию, развитию, охране здоровья, социальной защите и социальному обслуживанию ребёнка, содействию его социальной адаптации, социальной реабилитации иные мероприятия с его участием. Однако, на наш взгляд, в законопроекте недостаточное внимание уделяется вопросу распространения информации посредством Интернета.

По нашему мнению, России, в вопросе защиты детей от негативной информации в сети, следует брать пример с зарубежных стран. «Модель законодательной защиты прав несовершеннолетних в сети Интернет наиболее полно реализована в США – стране, являющейся мировым лидером по числу законодательных актов в этой сфере. Среди действующих законов следует отметить «Акт о защите частной жизни несовершеннолетних» 1998 год, закрепляющий обязательную классификацию web-ресурсов для детей моложе 13 лет с целью обеспечения более эффективного контроля со стороны родителей за работой детей в Интернет. Во-вторых, законопроект – «Акт о защите частной жизни несовершеннолетних», устанавливает правило, по которому распространение информации частного характера о детях моложе 16 лет возможно лишь после соответствующего согласия на это их родителей. Несовершеннолетние не могут иметь своего Интернет-адреса, персонального канала и прочее. Федеральной

комиссии по связи данный Акт предписывает в течение 1 года разработать специальные правила по регулированию деятельности несовершеннолетних в сфере Интернет. "Акт о защите детей в Интернет" огранивает доступ к ряду Интернет-ресурсов, содержащих информацию непристойного характера в общественных местах, таких как школы и публичные библиотеки»[1].

Известно, что полностью защитить наших детей от информации негативного содержания мы не в силах, но государство должно на законодательном уровне контролировать эти процессы. Во-первых, должны быть законы, которые смогли бы оградить детей от вредной информации в интернете. Так, в школах в классах информатики необходимо установить программы контентной фильтрации, чтобы учащиеся не имели доступа на запрещенные сайты. Во-вторых, обязать (на законодательном уровне) операторов связи, предоставляющих доступ к сети Интернет, устанавливать по просьбе пользователя программные фильтры и иные средства, пресекающие доступ к информации, запрещенной к распространению законодательством Российской Федерации.

Необходимо обязать государственные органы, органы местного самоуправления в соответствии со своими полномочиями реализовывать функции по защите детей от незаконной информации, распространяемой в сети Интернет. Одним из важных моментов, на наш взгляд, является расширение сотрудничества и обмена опытом по деятельности, связанной с развитием безопасного интернета, между различными отечественными и международными организациями.

[1] Кобзева С. «Модели защиты прав несовершеннолетних в сети Интернет: мировой опыт и рекомендации для России // http://www.ifap.ru/pi/10/

Каторгина Н.П.

О ВОЗМОЖНОСТИ ПРОИЗВОДСТВА ПРАВОВЫХ ЭКСПЕРТИЗ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация: в статье проанализированы мнения ученых о возможности проведения правовых экспертиз, а также высказано мнение автора по данному вопросу. Обращено внимание на то, что в судебной практике подобные экспертизы проводятся достаточно давно в связи с принятием большого объема нормативно-правовых актов, которые зачастую противоречат друг другу.

Ключевые слова: специальные знания, правовая (юридическая) экспертиза, уголовное судопроизводство.

Abstract: This paper analyzes the opinions of scientists about the possibility of legal expertise, but also felt the author on the subject. Attention is drawn to the fact that in the jurisprudence of such examinations are held for a long time in connection with the adoption of a large amount of regulations that often contradict each other.

Key words: special expertise, legal (legal) examination, criminal justice.

На протяжении нескольких последних лет среди ученых ведутся дискуссии о том, являются ли юридические знания специальными. Следует заметить, что ни в одном из законов прямого указания на запрет привлечения эксперта или специалиста для решения правовых вопросов нет, и нигде прямо не указывается, что правовые (юридические) знания не могут быть специальными. Тем не менее, дискуссия по данному вопросу не ослабевает, напротив разгорается все с большей силой.

Так, В.В. Клевцов, Ю.Г. Корухов, В.В. Степанов, Л.Г. Шапиро[1] и другие безоговорочно исключают правовые вопросы из понятия специальных знаний в уголовном судопроизводстве. Авторы утверждают, что судья, следователь обязаны знать право в силу получения высшего профессионального образования по специальности (направлению) «Юриспруденция» и соответственно юридические знания для них специальными не являются.

В утратившем юридическую силу Постановлении Пленума Верховного Суда СССР от 16 марта 1971 г. № 1 «О судебной экспертизе по уголовным делам» указывалось, что «суды не должны допускать постановку перед экспертом правовых вопросов, как не входящих в его компетенцию (например, имело ли место хищение либо недостача, убийство или самоубийство и т.п.)»[2]. П. 4 Постановления Пленума Верховного суда РФ от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» поясняет, что «постановка перед экспертом правовых вопросов, связанных с оценкой деяния, разрешение которых относится к исключительной компетенции органа, осуществляющего расследо-

[1] Корухов Ю.Г. Допустимы ли правовые и юридические экспертизы в уголовном процессе // Законность. – 2000, № 1 / ИПС Консультант плюс; Степанов В.В., Шапиро Л.Г. О судебной правовой экспертизе // Вестник криминалистики. – 2007, Вып. 4 (24) / ИПС Консультант плюс; Клевцов В.В. Понятие специальных знаний в уголовном судопроизводстве // Судебная экспертиза. – 2009, № 3. С. 113.

[2] Постановление Пленума Верховного Суда СССР от 16 марта 1971 г № 1 «О судебной экспертизе по уголовным делам» / ИПС Консультант плюс.

вание, прокурора, суда (например, что имело место – убийство или самоубийство), как не входящих в его компетенцию, не допускается»[1]. То есть в постановлении речь идет лишь о квалификации преступления, но не о юридических знаниях вообще.

Первым признанием юридических знаний в качестве специальных стал Федеральный Конституционный закон от 21 июля 1994 г. № 1-ФКЗ «О Конституционном Суде Российской Федерации». В ст. 63 указанного закона сказано, что в заседание Конституционного Суда РФ может быть вызвано в качестве эксперта лицо, обладающее специальными знаниями, по вопросам, касающимся рассматриваемого дела. По сути противоречий не усматривается с приведенным выше подходом большинства ученых, если бы не одно «но». В Конституционный Суд РФ, в основном, в качестве экспертов приглашаются высококвалифицированные юристы (доктора и кандидаты юридических наук) и на их разрешение ставятся вопросы исключительно правового характера.

В.В. Степанов утверждает, что привлечение юристов к оказанию помощи Конституционному суду ошибочно именуется правовой экспертизой, такая деятельность имеет организационный, технический, подготовительный характер и заключается в анализе норм права, отыскании пробелов и противоречий в нормативных актах и т.д. Данные лица привлекаются в качестве технических помощников, консультантов в связи с большой загруженностью судей Конституционного суда[2].

По мнению А.В. Кудрявцевой, Ю.Д. Лившиц, Ю.К. Орлова правовые знания не относятся к специальным, однако на практике достаточно сложно запретить обращаться за консультациями и следователям, и судьям к специалистам в иных отраслях права (финансовом, валютном, предпринимательском, гражданском, банковском и др.)[3]. Данные консультации доказательственное значение не имеют, но могут повлиять на формирование субъективного мнения.

Н.П. Яблоков не исключает возможность обращения к специалистам, но все чисто юридические вопросы должны решаться следователем, прокурором, судьей самостоятельно на основе своих собственных знаний[4].

---

[1] Постановление Пленума Верховного Суда РФ от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам» / ИПС Консультант плюс.

[2] Степанов В.В. О правовой экспертизе в уголовном судопроизводстве // Современные тенденции развития криминалистики и судебной экспертизы в России и Украине: материалы междун.науч.-практ.конф. в рамках пректа «Российско-украинские криминалистические чтения на Слобожанщине», 25-26 марта 2011 г.: в 2 т. / отв.ред. И.М. Комаров. – Белгород: Изд-во БелГУ, 2011. Т. 2. С. 133-134.

[3] Кудрявцева А., Лившиц Ю. Доказательственное значение «правовых» экспертиз в уголовном процессе // Российская юстиция. – 2003, № 1. С. 36-38; Орлов Ю.К. Судебная экспертиза как средство доказывания в уголовном судопроизводстве: научное издание. – М, 2005. С. 15-20.

[4] Яблоков Н.П. Возможности использования в уголовном судопроизводстве письменных заключений специалистов-правоведов // Современные тенденции развития криминалистики и судебной экспертизы в России и Украине: материалы междун.науч.-практ.конф. в рамках

А.А. Эксархопуло и Е.Р. Россинская[1] высказываются за принципиальную возможность производства правовых экспертиз по уголовным делам. Свою позицию ученые аргументируют возникновением широкого круга правоотношений и наличием особенностей их правового регулирования. А.А. Эксархопуло, утверждал, что «обязывание работников правоохранительных органов быть компетентными по всем вопросам всех существующих сегодня отраслей права, знание которых может потребоваться при расследовании преступления, ставит их в безвыходное положение, в котором есть обязательство знать, но нет реальной возможности освоить эти знания в полном объеме»[2].

В связи с этим нельзя согласиться с Т.В. Аверьяновой, утверждающей, что незнание следователями, судьями, дознавателями в необходимых пределах определенных отраслей права – это проблема правоприменителя, а попытки решить ее означают переложить на эксперта бремя доказывания[3].

Очевидно, что вследствие развития юридической науки невозможно лицу, в чьем производстве находится уголовное дело, следователю, прокурору, судье быть специалистом во всех отраслях права, соответственно существует реальная необходимость в проведении правовых исследований, но не в абсурдных ситуациях. Так, А.А. Эксархопуло считает, что «экспертизы качества проведенного расследования, проводимые по его результатам, либо экспертные исследования материалов незавершенных уголовных дел, имеющие цель определить перспективы их расследования могут оказаться особенно полезными для начинающих следователей, прокуроров, судей». Автор отмечает, что эксперт не принимает «правового решения» подобно следователю, а лишь высказывает свое мнение о том, как с точки зрения правовой науки тот или иной вопрос следует решать при известных ему исходных данных. Решение юридического вопроса экспертом не будет при таком понимании «решения» подменой полномочий следователя[4].

Безусловно, необходимость назначения и производства правовых экспертиз в уголовном судопроизводстве вовсе не говорит об обязательности их назначения повсеместно и об отсутствии правовых знаний у следователя, судьи. Для того чтобы правовые экспертизы не назначались с целью переложить на судебных экспертов решение задач, относящиеся к компетенции следователя и суда, необходимо чтобы данная экспертиза, как и другие ее виды, имела свой

пректа «Российско-украинские криминалистические чтения на Слобожанщине», 25-26 марта 2011 г.: в 2 т. / отв.ред. И.М. Комаров. – Белгород: Изд-во БелГУ, 2011. Т. 1. С. 117.

[1] Эксархопуло А.А. Специальные познания и их применение в исследовании материалов уголовного дела. – СПб.: Издательский Дом С.-Петерб.гос.ун-та, Издательство юридического факультета С.-Петерб.гос.ун-та, 2005; Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е.Р. Россинская. – 3-е изд., доп. – М.: Норма: ИНФРА-М, 2011. С. 14-24.

[2] Эксархопуло А.А.Специальные познания в уголовном процессе и их нетрадиционные формы // Вестник криминалистики. – 2001, Вып.2. С.27.

[3] Аверьянова Т.В. Судебная экспертиза: Курс общей теории. – М., 2006. С. 187.

[4] Эксархопуло А.А. Специальные познания и их применение в исследовании материалов уголовного дела. – СПб.: Издательский Дом С.-Петерб.гос.ун-та, Издательство юридического факультета С.-Петерб.гос.ун-та, 2005. С. 67, 99.

объект, задачи, методы и методики, а также предмет, что является весьма дискуссионным.

Так, Е.Р. Россинская предлагает назвать данную экспертизу судебно-нормативной, а предметом будут выступать фактические данные, устанавливаемые в гражданском, административном, уголовном и конституционном судопроизводстве путем исследования с использованием специальных знаний нормативных и нормативно-технических актов[1].

Ю.К. Орлов говорит, что предметом правовой экспертизы может быть только вопрос о том, какой закон и подзаконные акты подлежат применению в данном деле, а его толкование не является предметом экспертизы[2]. Не разделяя точку зрения автора, мы полагаем, что перед экспертом могут быть вопросы, касающиеся оценки содержания и толкования правовых норм.

Заметим, что некоторые авторы (Т.В. Сахнова, А.А. Эйсман и др.) предлагают считать данные исследования не экспертизой, а консультацией. Считаем данный подход неоправданным. Ученые пытаются свести производство экспертизы к справочно-консультативной деятельности, тем самым полученная информация будет иметь только консультативное, а не процессуальное значение.

В последнее время правовые исследования имеют место при решении вопросов о соблюдении правил дорожного движения, пожарной безопасности, неправомерных действиях при банкротстве и т.д.

Так, например, на кафедре гражданского права и процесса НИУ «БелГУ» была проведена правовая экспертиза по факту о неправомерных действиях при банкротстве (ч. 1 ст. 195 УК РФ). Перед экспертом были поставлены вопросы о разъяснении порядка ведения конкурсных мероприятий по реализации дебиторской задолженности, о наличии в действиях конкурсного управляющего при проведении процедуры конкурсного производства нарушения Федерального закона от 26.10.2002 г. № 127-ФЗ «О несостоятельности (банкротстве)».

Экспертом была дана оценка всех обстоятельств дела, определен круг правовых актов, на основе которых проводилось исследование. По результатам исследования дано экспертное заключение[3], которое в совокупности с иными доказательствами легло в основу обвинительного заключения.

Таким образом, можно утверждать, что в настоящее время существует реальная необходимость в производстве правовых экспертиз. Данное обстоятельство связано с большим объемом правовых актов, принятых за последние годы, а также неоднозначностью их применения при расследовании преступлений.

---

[1] Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе / Е.Р. Россинская. – 3-е изд., доп. – М.: Норма: ИНФРА-М, 2011. С.22-23.

[2] Орлов Ю.К. Судебная экспертиза как средство доказывания в уголовном судопроизводстве: научное издание. – М, 2005. С. 20.

[3] Заключение эксперта по уголовному делу № 20062360735.

Кислицина И.Н.

О ПРОБЛЕМАХ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ

Аннотация: В статье рассматриваются проблемы использования автоматизированных информационно-поисковых систем в деятельности криминалистической регистрации и автоматизированных систем для решения экспертных криминалистических задач.

Ключевые слова: криминалистическая регистрация, компьютеризация, криминалистически значимая информация, автоматизация, автоматизированные системы, информационно-поисковые системы.

Abstract. In article questions the problems of the use of automated information retrieval systems in the work of forensic registration and automated solutions to problems of forensic expert

Key Words: forensic registration, computerization, forensic material information, automation, automated systems, information retrieval systems.

Повышение эффективности работы правоохранительных органов невозможно без применения современных компьютерных технологий. Задача повышения уровня компьютеризации следственных, оперативных и экспертно-криминалистических подразделений продиктована необходимостью более эффективного противодействия преступности, в том числе наиболее опасным её формам, отличающимся высоким уровнем организации, специализацией участников преступной деятельности, их высокой технической оснащённостью. Современные достижения науки и техники беспрепятственно используются преступностью, которая в этом отношении не ограничена ни финансовыми средствами, ни правовыми рамками.

В последние годы в органах внутренних дел произошло много положительных изменений, в том числе и в обеспечении следственных, оперативных и экспертно-криминалистических подразделений компьютерной техникой, программным обеспечением. Это должно было улучшить деятельность по раскрытию и расследованию преступлений[1]. С другой стороны, развитие систем накопления и анализа информации, собранной по уголовным делам, не отвечает требованиям времени. Криминалистические учёты регистрируют лишь небольшую долю получаемой криминалистически значимой информации. Имеющиеся информационные потоки не урегулированы, существующие базы и банки данных разобщены и несовместимы. В свою очередь, следователи недостаточно часто обращаются к данным криминалистических, оперативно-справочных учётов ввиду невозможности получения ответа в короткие сроки и невысокого качества предоставляемой информации.

Таким образом, повышение уровня компьютеризации повысит эффективность накопления, хранения и использования данных криминалистической ре-

[1] Из выступления министра внутренних дел генерал-лейтенанта полиции В. Колокольцева на расширенном заседании коллегии МВД [Электронный ресурс]. – 08.02.2013.URL: http://www.kremlin.ru/news/17461(дата обращения: 18.02.2013).

гистрации и качество проводимых экспертных исследований в экспертно-криминалистических подразделениях.

Под компьютеризацией принято понимать технику, математические методы и специальное программное обеспечение, применяемые для сбора, хранения и переработки информации, используемые в различных процессах управления, а также для получения различного рода информационных и вычислительных услуг[1]. Это собирательное понятие. Оно объединяет в единое целые процессы использования логики, математического аппарата, теории информации и информационных систем и компьютеров как технических средств автоматизации информационных процессов.

Тенденции компьютеризации активно затрагивают деятельность в сфере криминалистической регистрации и производства экспертных исследований.

Несмотря на множество определений криминалистической регистрации, данных такими авторами, как Р.Е. Дёминой[2], Р.А. Усмановым[3], П.П. Ищенко[4], можно определить криминалистическую регистрацию как регистрационно-информационную систему получения, сосредоточения, обработки и выдачи криминалистически значимой информации в целях информационного обеспечения процесса раскрытия, расследования и предотвращения преступлений. Данная деятельность основана на нормах права, а при их отсутствии – на инициативе правоохранительных органов.

Систему криминалистической регистрации составляют различные виды учётов определённых объектов – носителей криминалистически значимой информации. В настоящее время все учёты, составляющие систему криминалистической регистрации принято разделять на оперативно-справочные, криминалистические и справочно-вспомогательные.

Учёты могут вестись в форме картотек, фотоальбомов, натуральных коллекций, компьютерных банков данных, автоматизированных информационно-поисковых систем (АИПС) и др. В современных условиях всё большее количество учётов ведётся в форме автоматизированных баз данных.

Автоматизация криминалистической регистрации ведётся по следующим основным направлениям:

1. Автоматизация дактилоскопических учётов.

Дактилоскопические учёты в настоящее время формируются в виде автоматических дактилоскопических информационных систем – АДИС. Их внедрение – одно из необходимых условий организации высокоэффективной работы правоохранительных органов. Как правило, такие системы позволяют вводить и хранить дактилокарты и следы с мест происшествий, автоматически проверять

---

[1] Терминологический словарь по автоматике и вычислительной технике. М., 2012.

[2] Дёмина Р.Е. Криминалистическая регистрация и её использование в расследовании преступлений: Учебное пособие. – Саратов: СЮИ МВД России, 2009. – с.11.

[3] Беляков А.А.,Усманов Р.А. Криминалистическая регистрация – Ростов н/Д.: Феникс, 2006. – с. 47.

[4] Ищенко П.П. Информационное обеспечение следственной деятельности. – М.: Юрлитинформ, 2011. – с.34.

следы и дактилокарты по базе данных и обмениваться информацией с другими подобными системами по международным стандартам, а в итоге получать информацию о причастности лица к совершённому преступлению.

Одним из лидирующих мировых программно-технических комплексов для дактилоскопии является система Sherlock, эксплуатирующаяся во многих странах, в том числе и в России, например в УВД Тульской, Липецкой областей и ГУВД Красноярского края.

Среди российских автоматизированных дактилоскопических систем заслуженной популярностью пользуется АДИС «Папилон», полностью удовлетворяющая техническим требованиям МВД, поддерживающая стандарты ФБР и ANSI-NIST и созданная при активном участии Академии МВД России. Система позволяет вводить в компьютер как дактилокарты, так и отдельные следы, производить проверку не только по дактилокартам, но и по следам, причем качество следов может быть улучшено путем обработки изображений.

2. Автоматизация габитоскопических учётов.

Здесь можно выделить два направления: биометрическая идентификация человека по признакам внешнего облика и составление композиционного портрета преступника – фоторобота.

Биометрическая идентификация по признакам внешнего облика осуществляется на основе трёх групп признаков. Первая группа – размерные характеристики изображения лица. Вторая группа – описывает форму лица в целом. Третья определяет форму области глаз, носа, рта и других анатомических признаков. Характеристики всех трёх трупп рассчитываются автоматически.

К системам второго типа относятся специализированные компьютерные программы, существенно ускоряющие процесс создания фотороботов, что крайне важно для получения наиболее полного описания подозреваемого в максимально короткие сроки. Кроме того, компьютерная система по составлению фотороботов позволяет не только создавать субъективный портрет подозреваемого в совершении преступления, но и прогнозировать возможные изменения внешности преступника, например его старение. Необходимо отметить, что фрагменты лица не просто берутся из базы, а могут тут же модифицироваться для максимального приближения к реальности (масштабироваться, наклоняться, поворачиваться и пр.). По окончании работы с программой автоматически формируется готовое изображение[1]

3. Автоматизация баллистических учётов.

Не менее востребованы и коллекции пуль, гильз и патронов со следами оружия, изъятых с мест преступлений, и утраченного (похищенного) оружия (пулегильзотеки), которые ведутся на двух уровнях: федеральном (Федеральная пулегильзотека – ФПГТ) и региональном (региональная пулегильзотека – РПГТ).

Учитывая необходимость применения микроскопического оборудования при считывании информации с тех же следов полей нарезов на пулях, или с ре-

---

[1] Гаврилин Ю.В. Расследование преступлений против личности и собственности: Учебное пособие. – М.: «Ось-89», 2006. – с. 105.

льефа дна следа бойка на гильзах, ручная обработка все увеличивающихся массивов пулегильзотек крайне затруднена и неэффективна. Кроме того, поверхность на пулях и гильзах, на которых образованы следы огнестрельного оружия, после длительного хранения окисляется, происходит оплывание (сглаживание) неровностей микрорельефа поверхности следов. В результате чего пули и гильзы после трех лет пребывания в массиве теряют часть индивидуальных признаков и становятся непригодными для идентификации конкретного экземпляра оружия, из которого они были стреляны. Поэтому предпринимаются попытки фиксации поверхностей пуль и гильз и помещения их в электронном виде в базу данных автоматизированных пулегильзотек.

Наиболее легким оказалось проведение автоматизации информационно-вспомогательной части массива ФПГТ. В настоящее время в ЭКЦ МВД РФ функционируют следующие автоматизированные системы:

– «Клеймо» – маркировочные изображения и клейма охотничьего нарезного оружия и припасов к нему;

– «Пламя» – тактико-технические характеристики, разборка и сборка деталей, маркировочные обозначения, внешний вид автоматических пистолетов отечественного и импортного производства;

– «Боеприпасы» – изображение, характеристики и маркировочные обозначения;

– «Оружие» – описание (без изображения) и характеристики автоматических пистолетов, автоматов и карабинов;

– «Ружье» – изображение, тактико-технические характеристики, маркировочные обозначения отечественного охотничьего и спортивного оружия;

– «Патрон» – изображение, тактико-технические характеристики, маркировочные обозначения, особенности заряда патронов к охотничьим ружьям отечественного производства.

Для работы с массивом пуль и гильз, изъятых с мест происшествий, в ФПГТ ЭКЦ МВД РФ установлена и внедрена в практику автоматизированная идентификационная поисковая система «Bullet proof», сочетающая две идентификационные подсистемы: по стрелянным гильзам и выстрелянным пулям. Однако, в силу различных причин (в первую очередь, из-за дороговизны проекта) эта система не смогла воплотиться в проекты регионального уровня. Вследствие чего, на уровне региональных пулегильзотек стали разрабатываться и внедряться отечественные автоматизированные идентификационные баллистические системы.

Среди российских автоматизированных баллистических идентификационных систем (АБИС) в практику экспертно-криминалистических подразделений были внедрены система «Арсенал», система «ТАИС».

Помимо перечисленного в МВД России и информационных центрах ведутся автоматизированные информационно-поисковые системы (АИПС) «Антиквариат», «Вещь», «Автопоиск», «Розыск» др.

К числу основных проблем, связанных с функционированием данных систем, относится то, что в разных регионах взяты на вооружение разные комплексы. В результате этого, проверка, например, обнаруженных следов пальцев по

следотекам соседних регионов осуществляется путём пересылки фотографий. Кроме того, отмечают низкую скорость исполнения запросов и низкое качество предоставляемой информации. Также, установленный порядок и технологии обращения следователя к учётам не соответствует скорости изменения следственной ситуации. «Общение» следователя с компьютеризированной частью учётов должно быть интерактивным и обеспечивать получение ответа на запрос в реальном масштабе времени. Технически это осуществляется обеспечением прямого доступа пользователя к информационным ресурсам.

Тенденция компьютеризации также активно затрагивает и судебную экспертизу. Одним из основных направлений внедрения компьютерных технологий в экспертную деятельность является создание информационных автоматизированных систем, действующих по специальной технологии поиска и выдачи запрашиваемых данных.

Одним из направлений в информационной технологии экспертной деятельности является разработка *автоматизированных программных комплексов (АПК) для решения экспертных задач.*

Для идентификации по голосу и речи, то есть по фонограммам, используются специальные программно-аппаратные комплексы со специальным программным обеспечением.

Основная задача фоноскопической экспертизы — идентифицировать человека по голосу и установить аутентичность (подлинность) приобщенной к уголовному делу фонограммы.

Вариантов программного обеспечения для фоноскопии как на мировом, так и на российском компьютерном рынке сегодня немало. Стоит обратить внимание, например, на рабочее место эксперта-фоноскописта «ОТ-КОНТАКТ» – удобную систему автоматической оперативной идентификации голоса, получившую положительные отзывы на II международной биометрической конференции разработчиков Biometrics 2003. OTExpert позволяет осуществлять все исследования голоса и речи, необходимые для проведения криминалистических экспертиз по голосу.

Специально для работы в экспертных лабораториях МВД, ФСБ и Минюста России создавался инструментальный комплекс анализа и шумоочистки звуковых сигналов «ИКАР» компании «Центр речевых технологий (ЦРТ)», который можно рассматривать как универсальный инструмент, предназначенный для идентификации дикторов по фонограммам речи, шумоочистки и текстовой расшифровки низкокачественных фонограмм речи, диагностики личности говорящего и установления подлинности фонограмм речи и выявления следов аналогового и цифрового монтажа.

Полностью удовлетворяет требованиям, предъявляемым экспертными учреждениями МВД и ФСБ, автоматизированное рабочее место эксперта-фоноскописта МСР-ФОНО, ориентированное на полное техническое исследование фонограмм с возможностью обработки зашумленных фонограмм. С помощью подобных комплексов не сложно осуществить исследование двух фонограмм или отдельных участков одной фонограммы, например, сравнив их по определенным параметрам.

Идентификация огнестрельного оружия проводится с помощью автоматизированных баллистических систем и информационно-вспомогательных систем.

Наибольшее распространение получили идентификационные баллистические системы (АБИК) на базе криминалистического микроскопа и компьютера со специальным программным обеспечением. Они предназначены для проведения баллистических экспертных исследований пуль и гильз с целью определения огнестрельного оружия по представленным пулям и гильзам; для идентификации пуль и гильз, поступивших на исследование, с пулями и гильзами из библиотеки изображений; для идентификации огнестрельного оружия по представленным на экспертизу пулям и гильзам, а также по пулям и гильзам из постоянно пополняемой библиотеки изображений. Системы для баллистической экспертизы позволяют провести сравнительный анализ следов на стреляных пулях и гильзах в трех измерениях, а также компьютерную обработку большого объема данных в автоматическом режиме и сделать вывод относительно их идентификации.

Среди российских автоматизированных систем наиболее популярны АБИК «КОНДОР» и «КОНДОР–М», «ТАИС» и «Арсенал».

Принимая во внимание необходимость проведения огромного количества баллистических экспертиз вследствие роста правонарушений с применением огнестрельного оружия, появления новых видов боеприпасов и оружия, распространения оружия, становится очевидно, что подобные комплексы незаменимы.

В рамках федеральной пулегильзотеки МВД РФ функционирует целая группа информационно-поисковых автоматизированных систем: «Клеймо» — маркировочные изображения и клейма охотничьего нарезного оружия и припасов к нему; «Пламя» — тактико-технические и прочие характеристики автоматических пистолетов отечественного и импортного производства; «Боеприпасы» — изображение, характеристики и маркировочные изображения существующих боеприпасов и др. По заявке ГУВД была разработана программа-генератор экспертных заключений «Клинок», предназначенная для генерирования экспертных заключений по холодному оружию. Действуют системы «Учет оружия» — для автоматизации учета оружия, поступившего на проверку по пулегильзотеке; «Учет объектов» — для автоматизации учета поступивших объектов (патронов, пуль и гильз);

Кроме перечисленных, в настоящее время в экспертную практику активно внедряются следующие аппаратно-програмные комплексы (АПК):

– «Контакт» для обнаружения контактов волокнистых материалов (например, волокон на одежде);

– «Внешняя баллистика» для установления возможности поражения пулей или дробью из огнестрельного оружия;

– «ГАЗХРОМ» для криминалистической экспертизы материалов, веществ и изделий из них с использованием газовой хроматографии;

– комплексы для судебной экспертизы почерков, в том числе умышленно измененных;

– для анализа подписей и обнаружения поддельных подписей и др.

Для производства и иллюстрации экспертных заключений разработана автоматизированная программа «Растр», предназначена для получения цифровых изображений, необходимых при производстве дактилоскопических, трасологических, баллистических, почерковедческих экспертиз, обработки и сравнительных исследований изображений, подготовки иллюстраций к проведенным экспертизам, подготовки и печати приложений к заключениям экспертов.

Однако, автоматизацию проведения криминалистических экспертных исследований сдерживают как объективные так и субъективные факторы: необходимость выделения на разработку и установку программ значительных ресурсов (финансовых, технических, кадровых); имеющиеся автоматизированные программы автономны и не связаны с аналогичными; низкая компьютерная культура экспертов экспертно-криминалистических подразделений.

Таким образом, в статье были выделены проблемы использования компьютерных технологий в криминалистических подразделениях, а именно: отсутствие высокоскоростных каналов между экспертно-криминалистическими подразделениями, отсутствие и недостаточная разработка имеющихся информационно-поисковых систем и автоматизированных программных комплексов.

Ковылов А.В.

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В СЕТИ ИНТЕРНЕТ

Аннотация. В данной статье рассматриваются отдельные аспекты защиты права на неприкосновенность частной жизни, нарушение которого произошло в сети Интернет.

Ключевые слова: частная жизнь, защита права, Интернет.

Abstract. This article discusses some aspects of protection of the right to privacy, violation of which occurred in the Internet.

Key words: privacy, protection of rights, the Internet.

Среди различных прав человека и гражданина, предусмотренных Конституцией Российской Федерации, право на неприкосновенность частной жизни занимает особое положение. В российском законодательстве данное право провозглашается высшей ценностью человека и гражданина, но нередко носит декларативный характер.

Право на неприкосновенность частной жизни предоставляет человеку возможность контролировать информацию о самом себе, препятствовать разглашению сведений частного характера, которые сам человек хочет сохранить в тайне. Однако развитие информационных технологий, расширение возможностей информационного обмена создают угрозу нарушения права личности на неприкосновенность частной жизни.

С приходом компьютерной эры неизмеримо возросло значение защиты права на неприкосновенность частной жизни в информационной сфере. С одной стороны, в условиях современного развития цивилизации и повсеместного внедрения информационных технологий расширяется доступ людей к информации, что способствует осуществлению права индивида на свободу информации. С другой стороны, доступ физических лиц к базам персональных данных усиливает риск вторжения в сферу частной жизни и нарушения права на ее неприкосновенность. Неприкосновенность коммуникаций и приватность присутствия человека в Интернете становится не менее важной, чем, например, неприкосновенность жилища. Таким образом, информационные и телекоммуникационные технологии предельно обострили правовые проблемы, связанные с дилеммой «раскрытие информации – защита частной жизни». Кроме того, неразвита сама законодательная база в области защиты персональных данных, как сведений о частной жизни, в Интернете.

Действительно, в настоящее время информация о частной жизни человека содержится в сети Интернет в огромных количествах. Различные базы данных государственных органов, социальные сети, электронная почта – все это может стать неисчерпаемым источником информации о частной жизни человека, завладеть которой может любое иное лицо, так как случаи продажи баз данных, скажем ГИБДД или налоговой инспекции, наши дни, к сожалению не редкость, а информация, размещенная в социальных сетях зачастую подвергается хищению и последующему распространению.

Что же делать человеку, если в сети Интернет незаконно размещена информация о его частной жизни? Вопросы приватности пользователей Интернета в российском законодательстве регулируются общими нормами о необходимости защиты частной жизни и персональных данных. Часть 2 ст. 150 ГК РФ относит неприкосновенность частной жизни к охраняемым законом нематериальным благам. Федеральным законом от 07.07.2003 № 126 «О связи» гарантируется также тайна связи. В ст. 63 этого Закона операторам связи вменяется в обязанность обеспечение тайны связи: «Вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами». К конфиденциальной информации отнесены «сведения об абонентах и оказываемых им услугах связи» (ст. 53 Закона № 126). Сведения об абонентах запрещается использовать для оказания справочных услуг без их письменного согласия.

Гарантии прав граждан при проведении оперативно-розыскных мероприятий определяются в Федеральном законе от 12.08.1995 № 144 «Об оперативно-розыскной деятельности». Сотрудники органов, осуществляющих такую деятельность, обязаны обеспечить приватность граждан.

Кроме того, в ст. 152.2 проекта ГК РФ предусмотрено, что если информация о частной жизни физического лица, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, указанное лицо вправе обратиться в суд с требованием об изъятии таких носителей из оборота и их уничтожении без какой бы то ни было компенсации.

Итак, вопросы охраны частной жизни в сети Интернет регулируются различными отраслями права и, казалось бы, обеспечивают надлежащую защиту права на неприкосновенность частной жизни гражданина. Вместе с тем, Ю. Донцова считает, что «несмотря на большое разнообразие законодательных актов, они все же не могут урегулировать вопросы защиты частной жизни в сети Интернет. Законотворческий процесс идет медленно и бессистемно. Специальные органы или структуры по защите частной жизни отсутствуют»[1].

Можно согласится с мнением ученого, особенно, если учитывать то, что зачастую невозможно вычислить субъекта, нарушившего права на неприкосновенность частной жизни, дабы применить к нему меры ответственности. Отсюда следует, что основной задачей правотворчества становится минимизация негативных последствий незаконного распространения информации о частной жизни гражданина. Так, существенным видится уже упоминавшееся нами положение ст. 152.2 проекта ГК РФ о возможности обращения в суд с требованием об изъятии носителей информации из оборота и их уничтожении без какой бы то ни было компенсации. Полагаем, что данное положение следовало бы дополнить указанием на возможность потребовать удалить информацию с Интернет сайтов, распространивших информацию о частной жизни лица, без его согласия. Если же подобное требование невозможно заявить ввиду отсутствия

[1] Донцова Ю. Приватность в сети // ЭЖ-Юрист. – 2011. – № 33. – С. 5.

владельца соответствующего сайта, логичным видится подача искового заявления с требованием обязать интернет провайдера ограничить доступ к сайтам, на которых распространена соответствующая информация.

Еще одной проблемой в регулировании неприкосновенности частной жизни является так называемый спам. Деятельность по рассылке спама связана с выяснением электронных адресов граждан, что естественным образом угрожает неприкосновенности частной жизни. Рассматривая указанную проблему С.В. Солгалов полагает, что «учитывая тот факт, что спам распространяется с помощью сетей связи, дать определение этого термина в Федеральном законе от 7 июля 2003 г. № 126 «О связи». Также следует предусмотреть возможную криминализацию спама в административном и уголовном порядке. Необходимо ввести ответственность за сопутствующие распространению спама деяния: сбор адресов для рассылки спама и распространение программ для его рассылки. Причем указанные нормы должны касаться не только рассылок через Интернет, но и иных средств передачи данных (например, через мобильные услуги)»[1].

К.С. Аверьянова, изучая проблемы охраны частной жизни, считает, что «при современных информационных технологиях, всеобщей компьютеризации, распространении сети Интернет, активном внедрении в жизнь социальных сетей, актуальным является введение в ст. 137 УК такого квалифицирующего признака, как распространение сведений о частной жизни с использованием сети Интернет»[2].

Р.В. Маркарьян обосновано замечает, что «одним из аспектов защиты информационной безопасности граждан, тесно примыкающим также к проблемам охраны правопорядка и неприкосновенности частной жизни, является необходимость законодательного запрета на такой вид «сетевого хулиганства», который заключается в рассылке нежелательной рекламы (спам) в тысячи и миллионы адресов пользователей Интернета. Наряду с моральным ущербом «сетевые хулиганы» приносят также существенный материальный ущерб в виде несанкционированного использования сетевых ресурсов третьих лиц. Соответствующие положения могут быть закреплены, например, в законодательных актах об административных нарушениях»[3].

Предложения ученных сводятся к ужесточению ответственности за нарушение неприкосновенности частной жизни. Однако по нашему мнению, в первую очередь, следует продумать гражданско-правовой механизм защиты права на неприкосновенность частной жизни гражданина в сети Интернет. Применение мер административной или уголовной ответственности носит карательный характер и во многом зависит от действий государственных органов.

---

[1] Солгалов С.В. Законодательное обеспечение права на неприкосновенность частной жизни // Право и экономика: Сб. научных трудов. Вып. 4. – М.: Изд-во МосГУ, 2010. – С. 3.

[2] Аверьянова К.С. Нарушение неприкосновенности частной жизни // VII студенческая заочная научно-практическая конференция «Научное сообщество студентов XXI столетия». – 2013. – С. 18.

[3] Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации // Международное публичное и частное право. – 2011. – № 4. – С. 20 – 22.

По нашему же мнению, первоочередным является компенсация вреда, причиненного лицу, распространением информации о его частной жизни, что может быть обеспечено преимущественно гражданско-правовыми средствами. Следует максимально расширить возможности пострадавшего защищать нарушенное право, что может быть достигнуто в рамках гражданского судопроизводства. Кроме того, проще всего добавить ещё одну статью в КоАП РФ и таким образом как бы защитить права граждан. Однако, данные изменения, на наш взгляд, не только не обеспечат защиты прав граждан, но и не будут эффективны ввиду сложности применения санкции. Лица, рассылающие спам или публикующие сведения о частной жизни граждан, как правило не оставляют сведений о своем месте жительства и не сообщают свои контактные данные.

Подводя итог всему вышеизложенному, следует признать, что в настоящий момент не существует специальных норм, регулирующих отношения по защите неприкосновенности частной жизни в сети Интернет. Представляется, что подобные нормы необходимы ввиду уникальности такого явления как Интернет. Звучат предложения о распространении на Интернет законодательства, регулирующего отношения, связанные со СМИ[1]. Считаем, что подобные меры не будут эффективными, ввиду того, что Интернет более глобальное и хаотичное явление нежели средства массовой информации. Следует пойти по пути расширения возможности защиты нарушенного права самим гражданином в рамках гражданского судопроизводства, дополнить соответствующими положениями ст. 152.2 проекта ГК РФ. Только подобные меры позволят оперативно реагировать на нарушение неприкосновенности частной жизни гражданином.

[1] Беляева. Н. Г. Право на неприкосновенность частной жизни и доступ к персональным данным // Правоведение. – 2001. – № 1. – С. 112.

Комаров И.М.

О СИСТЕМЕ ПРОЦЕССА ДОКАЗЫВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация: в статье на основе системного подхода раскрывается содержание процесса доказывания по уголовному делу, как на стадии его предварительного расследования, так и судебного разбирательства.

Ключевые слова: доказывание по уголовному делу, уголовное судопроизводство.

Abstract. The process maintenance proving on criminal case approaches on the basis of the system in this article. It *becomes apparent* in the stage of preliminary investigation and also judicial proceedings reveals.

Key words: proving on criminal case, criminal legal proceedings.

Досудебное производство и судебное разбирательство по уголовному делу непосредственно связано с процессом доказывания, которым называется деятельность органов дознания, предварительного следствия, прокуратуры и суда по собиранию, исследованию, оценке и использованию доказательств о факте совершенного преступления. Установить факт преступления – значит доказать, что преступление действительно было совершено[1].

Доказательствами является фактический материал, которым досудебное производство и судебное разбирательство оперируют в процессе расследования и разрешении уголовных дел и, на основании которых в указанных стадиях следователем (судьей) решаются все вопросы существа этих дел. Доказывание как познание истины по уголовному делу наряду с требованиями текущего законодательства подчиняется определенным логическим правилам и системным законам. Как всякий процесс познания доказывание по делу – это мыслительная деятельность следователя (досудебное производство), государственного обвинителя и судьи (судебное разбирательство) над собранным доказательственным материалом и в то же время «деятельность, совокупность действий, совершаемых следователем и судьей, направленная на собирание и проверку доказательств»[2].

Одним из важных способов и средств обеспечения этой деятельности являются версии. Именно их построение и проверка правомочными субъектами доказывания в процессе досудебного производства и судебного разбирательства обеспечивает принятие единственного в соответствии с процессуальной стадией окончательного процессуального решения, которое может быть выражено в обвинительном заключении и приговоре.

Проверка версий осуществляется следователем (государственным обвинителем, судьей) посредствам собирания (проверки) доказательств виновности (невиновности) лица привлеченного к уголовной ответственности на основе разрешенных уголовно-процессуальным законодательством способов и средств.

---

[1] Строгович М.С. Курс советского уголовного процесса. Т.1. М., 1968 – С. 287.

[2] Старченко А.А. Логика судебного исследования. Госюриздат, 1958 – С. 34.

Фактически на указанных уголовно-процессуальных стадиях осуществляется один и тот же процесс доказывания, но в различных формах. Причем на стадии судебного разбирательства и государственный обвинитель и суд, в большей степени призваны проверить в соответствии с уголовно-процессуальными требованиями объективность доказательств виновности подсудимого, добытых в процессе предварительного расследования.

В итоге, эта деятельность должна отражать системную связь конечных результатов предварительного расследования и судебного разбирательства. Установление системной связи доказательств виновности лица, привлеченного к уголовной ответственности, служит основанием для вынесения в отношении него судом обвинительного приговора. В случае отсутствия этой связи приговор должен быть оправдательным.

Данный процесс в судебном разбирательстве протекает в соответствии со сложившимися научными положениями системного подхода.

Одно из популярных определений системы гласит – ею является совокупность элементов, находящихся в отношениях и связях между собой и образующих определенную целостность, единство[1]. Оно принадлежит И.В. Блаубергу и Э.Г. Юдину, которые ввели в оборот и основные принципы системного подхода в познании исследуемых объектов, процессов и явлений – целостность, типы связей, среди них системообразующие структура и организация, цель и целесообразный характер, поведение, самоорганизация, функционирование и развитие[2].

В соответствии со спецификой процессуально-криминалистических аспектов доказывания определения принципов системного подхода и системы процесса доказывания в целом должны быть интерпретированы к предмету статьи.

С учетом этого, первоначально, следует определиться с типами связей, возникающими в системе процесса доказывания по уголовному делу. Их объясненное наличие между доказательствами, добытыми в процессе предварительного расследования и судебного разбирательства (элементами системы доказывания) и образует важнейший принцип всех систем – целостность.

В криминалистике, с учетом ее особой объектной природы, исследованы различные виды связей, обуславливающих прикладной характер положений этой науки. Среди них можно назвать причинно-следственные, временные, пространственные, логические и организационные связи, косвенные, прямого и обратного направления, дедуктивные, индуктивные, закономерные, случайные связи, связи однозначные (многозначные), непосредственные, многоступенчатые, соответствия и функциональные, связи принадлежности вещей.

Все перечисленные виды связей тем или иным образом встречаются в системе процесса доказывания по уголовному делу. Однако анализ материалов уголовных дел, рассмотренных с обвинительным приговором в районных судах Белгорода свидетельствует о том, что доказательства двух подсистем всей системы процесса доказывания (предварительного расследования и судебного раз-

---

[1] Философский энциклопедический словарь / Редкол.: С.С. Аверинцев, и др. М.,: Сов. Энциклопедия. 1989 – С. 215.

[2] Становление и сущность системного подхода». М.: Наука, 1973 – С. 18.

бирательства) строятся преимущественно на причинно-следственных, пространственно-временных и логических связях, а также связях косвенных, прямого и обратного направления.

На вдаваясь в объяснение и характеристику связей, которыми должны быть обеспечены собственно доказательства виновности обвиняемого и подсудимого на предварительном расследовании и в судебном разбирательстве кратко попытаемся отобразить содержание связей указанных подсистем и системы процесса доказывания по уголовному делу.

Причинно-следственные, пространственно-временные и логические связи отвечают за сохранение закономерностей обнаружения, фиксации, изъятия, исследования, оценки и использование следов преступления (преступника) на основе деятельности следователя по их отображению в результатах проведенных следственных действий. Полученные таким образом доказательства преступления сохраняются в уголовном деле, а затем приводятся в систему в обвинительном заключении, в качестве версии предварительного расследования, объясняющей событие происшедшего преступления. В судебном разбирательстве данные связи реализуются на основе исследования судом доказательств, содержащихся в обвинительном заключении, которые представляет и защищает прокурор, поддерживающий государственное обвинение.

Данная деятельность государственного обвинителя не может быть в полной мере осуществлена без сохранения и учета логических связей доказательств обвинительного заключения, доказательств добытых в ходе судебного разбирательства, а также связей этих групп доказательств между собой. Нарушение логики доказывания судебного разбирательства полностью или частично влечет за собой негативные последствия, которыми могут быть как частичное, так и полное оправдание подсудимого.

Система доказательств предварительного расследования, также как и доказательств судебного разбирательства основана на классификационных подходах к ним, которые определены уголовным процессом и криминалистикой. Наряду с прямыми обвинительными доказательствами, большое значение в системе процесса доказывания по уголовному делу принадлежит косвенным обвинительным доказательствам, а они основываются на соответствующих видах связей. Если эти связи достаточно прочны, то косвенные обвинительные доказательства могут играть решающую роль при вынесении судом первой инстанции обвинительного приговора. Иллюстрационным примером этого может служить практически любое уголовное дело о преступлении, совершенном в условиях неочевидности в ситуациях расследования и судебного разбирательства, когда обвиняемый воспользовался своим правом, предусмотренным ст. 51 Конституции РФ. Косвенные связи в известном смысле то же, что и связи принадлежности вещей.

Связи прямого и обратного направления как в системе процесса доказывания в целом, так и в формирующих ее подсистемах, обусловлены содержанием собранных и зафиксированных в протоколах следственных действий доказательств. Их содержание основано на процедурах последовательного получения доказательств преступления, то есть, нельзя, например, назначить дактилоско-

пическую экспертизу, прежде чем в распоряжение предварительного расследования не поступят отпечатки пальцев рук человека изъятые в ходе того или иного следственного действия, а также идентифицирующие их образцы отпечатков пальцев рук подозреваемых лиц. Получение этих образцов также должно пройти соответствующие процессуальные процедуры изъятия. Результаты данного дактилоскопического исследования, признаются судебным доказательством в процессе судебного разбирательства на основе проверки судом обратной связи посредствам обозрения в ходе судебного разбирательства материалов уголовного дела и установления, таким образом, законности получения данного доказательства в процессе предварительного расследования. Определение связей прямого и обратного направления в системе процесса доказывания предполагает также наличие логических и организационных связей, за содержание которых отвечает также субъект доказывания.

Однако, несмотря на необходимый характер всех приведенных видов связей главной системаобразующей связью, объединяющей подсистемы предварительного расследования и судебного разбирательства в единую систему процесса доказывания, являются корреляционные связи (связи сосуществования) всех доказательств совершенного преступления. Своим содержанием они обеспечивают целостность данной системы и на этой основе возможность постановления судом обвинительного приговора по делу.

Системаобразующее значение корреляционных связей заключается в том, что они обеспечивают непротиворечивое уголовно-процессуальным нормам и криминалистическим рекомендациям существование всех доказательств добытых в процессе предварительного расследовании, проверенных в судебном разбирательстве и принятых судом в качестве судебных доказательств для вынесения обвинительного приговора. Отсутствие данного вида связей между какимилибо элементами системы процесса доказывания по уголовному делу (элементами ее подсистем) требует от следователя и судьи действий по гармонизации указанных подсистем и системы процесса доказывания в целом. Она может быть выражена, например, в отказе суда признать судебным доказательством какие-либо сведения, добытые в процессе предварительного расследования, проведении судебно-процессуальных действий по ходатайству сторон или инициативе суда для установления фактов, которые могут повлиять на принятие законных процессуальных решений и пр.

Дедуктивные и индуктивные связи системы процесса доказывания представляют собой методологический блок логических приемов обеспечивающих построение и проверку версий предварительного расследования и судебного разбирательства. Версия предварительного расследования, выраженная в обвинительном заключении, также в значительной степени основана на связях этого вида, а в случае подтверждения этой версии в судебном разбирательстве они повторяются в обвинительном приговоре суда, чем обеспечивают со своей стороны целостность системы процесса доказывания по уголовному делу.

Закономерные типы связей, обеспечивающие целостность системы процесса доказывания, первоначально представлены в подсистеме предварительного расследования и обеспечивают своим существованием криминалистичес-

кие процессы собирания, исследования, оценки и использования доказательств. В судебном разбирательстве эти типы связей, находя свое подтверждение, формируют со своей стороны систему процесса доказывания. При этом в обеих подсистемах значительная часть закономерных связей обеспечена связями непосредственного характера, наличие которых указывает на прямые доказательства виновности привлеченного к уголовной ответственности лица.

Любой сложившейся системе процесса доказывания по уголовному делу должны соответствовать однозначные и многозначные связи между доказательствами. Основанием этому является, на наш взгляд, невозможность осуществления процесса доказывания, как в ходе предварительного расследования, так и судебного разбирательства только на основе применения закономерностей линейных систем. То есть процесс доказывания это не примитивная причинно-следственная связь, когда появление одного доказательства порождает связь и появление другого доказательства, что в конечном итоге обеспечивает принятия окончательного процессуального решения. Представляется, что любое доказательство может быть закономерно связано и порождает как одно последующее, так и множество других доказательств по расследуемому преступлению. Поэтому связи в системе процесса доказывания всегда представлены как однозначными, так и многозначными отношениями.

Наличие функциональных связей обеспечивает системе процесса доказывания целостность за счет объективности принятия как промежуточных, так и окончательных процессуальных решений. Основой этому служит выполнение определенных уголовно-процессуальных функций сторонами защиты и обвинения на стадиях предварительного расследования и судебного разбирательства.

Заканчивая анализ связей, обеспечивающих принцип целостности системе процесса доказывания, хотелось отметить, что, по нашему мнению, данной системе не присущи случайные связи, так как это противоречило бы уголовно-процессуальным и криминалистическим закономерностям, на основе которых собираются, исследуются, оцениваются и используются судебные доказательства.

Можно попытаться продолжить анализ связей, которые обеспечивают осуществление предварительного расследования и судебного разбирательства и формируют наряду с другими факторами целостную систему процесса доказывания по уголовному делу. Однако, на наш взгляд, даже приведенный беглый анализ связей предварительного расследования и судебного разбирательства указывает на целостность их как подсистем системы процесса доказывания, которую с учетом формально-логических правил, теоретически также можно считать целостной.

И.В. Блаубергом и Э.Г. Юдиным принцип целостности в системном подходе к исследованию тех или иных объектов, процессов и явлений раскрывается также на основе «структуры и организации, цели и целесообразного характера, поведения, самоорганизации, функционирования и развития».

Относительно нашего объекта исследования – системы процесса доказывания по уголовному делу, можно сказать, что ее структура и организация определены действующим уголовно-процессуальным законодательством, цели связаны с процессуально-криминалистической природой доказывания, а целе-

сообразный характер в данной системе отсутствует полностью, так как целесообразность ни коим образом не может подменять законность в деятельности следователя на стадии предварительного расследования и судьи на стадии судебного разбирательства. Связи поведения объяснены нами в настоящей статье через функциональные связи с учетом выполнения следователем (судьей) своих уголовно-процессуальных функций.

Функционирование и развитие, как типы связей системного подхода существуют как в подсистемах предварительного расследования и судебного разбирательства, так и в системе процесса доказывания по уголовному делу до пределов решения той или иной уголовно-процессуальной задачи на основе криминалистической деятельности следователя в границах принятой им процессуальной формы.

Раскрыв, таким образом, содержание системного подхода к доказыванию по уголовному делу, можно дать собственно определение системы процесса доказывания по уголовному делу, на наш взгляд она представляет собой целостность, единство совокупностей подсистем: доказательств добытых следователем в ходе производства предварительного расследования и доказательств, установленных судом в процессе судебного разбирательства в первой инстанции, которые находятся в непротиворечивых отношениях и связях, чем обеспечивают принятие процессуально уполномоченными лицами правильных (промежуточных и окончательных) судебно-процессуальных решений по делу.

Подходы к такому пониманию системы процесса доказывания по уголовному делу в практической деятельности в состоянии обеспечить принятие судом первой инстанции справедливых процессуальных решений.

Косолапова Н.А.

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ЖЕСТОКИМ ОБРАЩЕНИЕМ С ЖИВОТНЫМИ, С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-РЕСУРСОВ

Аннотация. Данная работа посвящена способам предупреждения преступлений, связанных с жестоким обращением с животными, в сети Интернет.

Ключевые слова: гуманность, жестокое обращение, животные, предупреждение преступлений, Интернет-реклама с животными.

Abstract. This article represents the ways of the prevention of the crimes connected with cruelty to animals on the Internet.

Key words: humanity, cruelty, animals, prevention of crime, Internet advertising allowed.

В самых разных регионах планеты все чаще происходят трагические события, которые говорят об одном: нам пора выстраивать новые отношения с окружающим миром. Попытки обращаться с природой с позиции силы приводят к отрицательным последствиям. Это доказывает и история человечества. Поэтому проблема жестокого обращения с животными за последние несколько лет перешла на международный уровень.

По тому, как люди относятся к животным, можно судить об общем уровне развития общества. Оправдание или просто не осуждение жестокости здесь деформирует и общее понятие гуманности, и ее значение как принципа уголовной политики. А значит, меры по защите животных можно считать одним из важных шагов в профилактике и других более тяжких преступлений.

Взаимосвязи жестокого обращения с животными с другими преступлениями, как правило, более тяжкими посвящены работы В. Китаевой, А. Плешакова, С. Щербы, а также этой проблемой занимаются и в ГНЦ СиСП им. В.П. Сербского.

Тем не менее, проблемы предупреждения преступлений, предусмотренных ст. 245 УК РФ, в настоящее время остаются одними из наименее изученных. Это обусловлено тем, что жестокое обращение с животными относится к преступлениям небольшой тяжести, поскольку наказание за его совершение не превышает двух лет лишения свободы. Именно по этой причине расследованию и предупреждению преступлений, относящихся к указанной категории, зачастую не уделяется достаточного внимания, тем более, что общий уровень преступности в России столь велик, что правоохранительные органы не успевают должным образом расследовать преступления, имеющие среднюю степень тяжести, а также тяжкие и особо тяжкие преступления.

В настоящее время актуальность данной темы обусловлена проблемой роста жестокости по отношению к животным, предусмотренной ст. 245 УК РФ. Так количество вынесенных обвинительных приговоров по данной категории дел выросло за 2012 г. на 18%[1].

[1] Сайт РосПравосудия. URL: http://rospravosudie.com/category-245-ch-1-s (дата обращения: 10.02.2013).

На наш взгляд, такую ситуацию отчасти обусловливает развитие Интернет-ресурсов и доступность информации, пропагандирующей жестокое обращение с животными.

Все чаще в Интернете можно встретить сайты, где публикуются картинки и ролики, изображающие жестокие убийства и истязания животных, а также приводятся советы, как отравить собаку, кошку и т.д.

Распространение и популярность в Интернете роликов о жестоком обращении с животными существует, потому что на нее есть спрос. Объяснить подобную ситуацию можно следующими факторами:

- безопасность – работа с такой информацией не связана с риском;
- анонимность – просмотр ее носит «обезличенный» характер;
- доступность – ресурс, содержащий жестокое обращение с животными, доступен в любое время;
- удобство пользования – достаточно найти необходимый сайт и пройти на нем регистрацию/авторизацию;
- «терапевтическое» воздействие – у людей с различными отклонениями психического развития просмотр подобной информации может вызвать чувство облегчения;
- чувство общности с другими людьми – раньше то, что они могли воспринимать как собственный недостаток, теперь с учетом знакомства и общения с другими «заинтересованными» воспринимается как норма.

Поскольку сеть таких сайтов построена на принципе самоорганизации, контролировать их деятельность очень сложно, а наказания за такую пропаганду в РФ не предусмотрено. В УК РФ нет нормы, касающейся запрета на пропаганду. Получается, что сегодня привлечь к ответственности человека, выложившего видеоролик со сценами насилия над животным, не представляется возможным. Даже если он будет задержан, доказать тот факт, что он убил животное – очень сложно. Он может сказать, что просто снимал это видео, но сам не убивал.

Сейчас из-за повышенного внимания и увеличения интереса к данной проблеме, связанных с рассмотрением дел так называемых «дог-хантеров», такие сайты стали работать скрытно, они существуют под закрытыми разделами. Но зайти на форумы или на страницы людей, жестоко обращающихся с домашними животными, не так уж сложно. Они работают как виртуальный круг по интересам, где получить необходимую информацию можно, заплатив определенную сумму за регистрацию или даже без уплаты таковой. Определить сайты, содержащие жестокое обращение с животными, можно по названию, например, «Pokysov.net» или «Vreditelyam.net». Несколько таких сайтов могут находиться под управлением одного человека. *Например, «kalashnikov.guns.ru», «talks.guns.ru» и «tantal.kalashnikov.guns.ru». В этом случае заказчиком, плательщиком или активным пользователем всех этих Интернет-ресурсов является один и тот же источник, находящийся в определенном месте и работающий на нескольких компьютерах, связанных внутренней сетью.* Такая организация позволяет их сравнить с платными сайтами детской порнографии,

которые на сегодняшний день, не смотря на борьбу с ними, все еще представляют угрозу для общества.

Необходимо учесть тот факт, что видеоролики и изображения жестокого обращения с животными используются не только преступниками, но и различными организациями по защите животных. В современной действительности зоозащитники также активно используют Интернет-ресурсы для пропаганды положительного отношения к окружающей среде и животным. Защитники животных нередко сами снимают и распространяют в сети документальные фильмы о фактах жесткого обращения с животными.

Часто сайты, призывающие к жестокому обращению с животными и борющиеся с таковым, используют одни и те же видеоматериалы. Таким образом, возникает потребность в установлении признаков таких роликов и права на их использование, доступ и распространение. Обязательным должны быть комментарии происходящего в видеоролике или пояснительные надписи к фотографиям жестокого обращения с животными, направленные вызвать у воспринимающего чувство отвращения, нежелания поступать противоправно в отношении к животному и обществу в целом, а также должны воспитывать чувство ответственности за приручённое животное, учить жить в гармонии с природным миром. Видеоролики и изображения, не имеющие таких пояснений, должны быть запрещены к просмотру. Отсюда, возникает еще одна проблема – это огромный массив информации, непрерывно обновляющийся в сети Интернет, и отследить его полностью, к сожалению, не представляется возможным.

Также хотелось бы отметить, что в сети Интернет появилось много рекламы, в которой животные рекламируют не только корма и биодобавки, но и белье, одежду и обувь. Как правило, условия, в которых находится животное во время съемок, не соответствуют нормам гуманного обращения с животными. Примером может послужить Интернет-реклама шведской страховой компании Folksam, на съемках которой под котами, изображающими прыжок с парашютом, находился включенный вентилятор, пугающий своим шумом животных.

На основании изучения данной проблемы способами предупреждения данного преступления в сети Интернет, на наш взгляд, являются:

- необходимость разработки нормы закона, касающуюся запрета пропаганды жестокости в Интернете, которая позволила бы свести к минимуму возможность распространять подобную информацию в сети;
- введения требования наличия комментария воспитательного характера к изображающим жестокое обращение с животными видеороликам и фотографиям;
- создание Интернет-порталов и сайтов зоозащитных движений с обязательным разделом, содержащим нормы международного законодательства и законодательства РФ о жестоком обращении с животными, а также научную литературу по данной тематике (например, форум «Правовой отдел Антидогхантера» на сайте «antidogxanter.ucoz.ru»);
- запрет на использование в Интернет-рекламе животных, за исключением рекламы кормов и аксессуаров для животных.

Костин А.А.
Костина О.В.

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОСУЩЕСТВЛЕНИЯ ТАМОЖЕННОГО АДМИНИСТРИРОВАНИЯ

Аннотация. В статье рассмотрены основные направления совершенствования таможенного администрирования в Таможенном союзе ЕврАзЭС с использованием информационных технологий.

Ключевые слова: информационные технологии, интеграция, Таможенный союз, таможенное администрирование.

Abstract. The article describes the main trends of the customs administration in the EurAsEC Customs Union with the use of information technology.

Key words: information technology, the integration of the Customs Union, the customs administration.

В условиях растущего уровня глобализации мировой экономики развитие государств в значительной степени определяется теснотой международных экономических связей, ростом взаимного экспорта и импорта, взаимными прямыми инвестициями, которые повышают эффективность общественного производства и ведут к региональной экономической интеграции. Процесс формирования региональных интеграционных объединений обычно опирается на договорно-правовую базу – целые группы стран на основе взаимных соглашений объединяются в региональные межгосударственные комплексы, проводят совместную торговую политику.

Наиболее распространены в современном мировом сообществе интеграционные группировки, находящиеся на таких стадиях своего развития как зона свободной торговли либо таможенный союз.

Начиная с 2010 г. полноценно функционирует Таможенный союз ЕврАзЭС, объединяющий на постсоветском пространстве Россию, Белоруссию и Казахстан.

Переход Российской Федерации на инновационный принцип государственного развития, предполагает применение информационных технологий в органах государственной власти, деятельность которых сопряжена с необходимостью обработки и анализа большого объема разнородной информации, на современном этапе особенно актуально. Именно информационные технологии являются одним из основных факторов, определяющих тенденции развития ФТС России и инструментов таможенного администрирования[1].

Согласно определению, принятому ЮНЕСКО, информационные технологии – это комплекс взаимосвязанных научных, технологических, инженерных

[1] Александров Д.Л. Информационные технологии в таможенных услугах и их проявление в экономической эффективности таможенных операций // Вестник Российской таможенной академии. 2012. № 3. С. 59 – 64.

дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации с помощью вычислительной техники, и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы[1].

ФТС России, как и любая другая государственная структура, ориентирована на внедрение перспективных технологий с целью повышения эффективности своего функционирования. Одним из инструментов реализации таких технологий и являются информационные технологии. Разработка и внедрение информационных технологий в сфере таможенного дела – своевременный и необходимый процесс, который позволяет повысить качество и оперативность работы таможенных органов, особенно после вступления России во Всемирную торговую организацию, что обусловливает необходимость обеспечения нового уровня информатизации таможенной службы России[2].

В этих условиях Правительством Российской Федерации был утвержден План мероприятий «Совершенствование таможенного администрирования»[3], суть которого состоит в том, чтобы максимально упростить порядок перемещения товаров и транспортных средств через таможенную границу Таможенного союза при их ввозе в РФ и вывозе из нее. Реализация положений Плана позволит усовершенствовать таможенные операции и процедуры, сделает их более простыми, быстрыми, прозрачными и менее затратными с одновременным повышением эффективности таможенного контроля за счет применения современных информационных технологий и смещения его акцентов на этап после выпуска товаров.

Проведение указанных мероприятий рассчитано на период до 2018 г. Приоритетной задачей «дорожной карты» является повышение к 2018 году позиции России в рейтинге Doing business по показателю «Международная торговля» с 160 до 17 (данный рейтинг выбран в качестве контрольных показателей успешной реализации «дорожной карты». Он составляется ежегодно Всемирным банком, а позиции стран в нем ранжируются в зависимости от доступности той или иной страны для ведения бизнеса).

Согласно «дорожной карте» предполагается разработать и реализовать технологию автоматической регистрации таможенной декларации, поданной в электронном виде.

Интересным нововведением представляется внедрение в 2018 г. технологии автоматического (без участия должностных лиц таможенных органов) принятия решения о выпуске товаров при подаче декларации в электронном виде.

---

[1] Информация и информатика: информационные технологии [Электронный ресурс]. – Режим доступа: http://www.bibliotekar.ru/rInform/7.htm.

[2] Наше будущее – перспективные таможенные технологии [Электронный ресурс]. – Режим доступа: http://dvtu.customs.ru/index.php?option=com_ content&view=article&id=9927:2012-09-27-03-05-23&catid=49:press-cat&Itemid=107.

[3] Об утверждении плана мероприятий («дорожной карты») «Совершенствование таможенного администрирования»: Распоряжение Правительства РФ от 29.06.2012 № 1125-р.

При этом срок выпуска товара составит не более 20 минут. В настоящее время по общим правилам, установленным таможенным законодательством Таможенного союза, выпуск должен быть завершен не позднее одного рабочего дня, следующего за днем регистрации таможенной декларации.

К 2014 г. планируется отказаться от дублирования электронных документов бумажными. Однако это коснется только тех товаров (транспортных средств), которые не идентифицированы как рисковые поставки, требующие дополнительной проверки документов на бумаге.

Между тем в настоящее время в Евразийской экономической комиссии проводится разработка Основных направлений совершенствования таможенного администрирования в Таможенном союзе в 2012-2015 годах[1]. Необходимость такого документа обусловлена требованиями времени, когда для дальнейшего системного и комплексного развития таможенного администрирования требуется сформулировать перспективные цели и задачи, продумать механизмы их правового и информационно-технического обеспечения, механизмы межведомственного взаимодействия.

Основные направления включают в себя дальнейшее развитие электронного декларирования, внедрение автоматического выпуска, развитие информационного межведомственного взаимодействия, сокращение сроков и количества документов, глубокую дифференциацию участников ВЭД, развитие института уполномоченного экономического оператора, дальнейшее развитие принципа «двух служб» на границе и другие предложения. В результате реализации Основных направлений должен быть создан баланс между эффективностью таможенного контроля и упрощением таможенных формальностей.

Таким образом, с учетом работы, проводимой в странах Таможенного союза (например, Дорожная карта совершенствования таможенного администрирования в Российской Федерации, программы развития таможенных служб в Республике Беларусь и Республике Казахстан) было принято решение о подготовке Основных направлений в целом для Таможенного союза. Наличие таковых направлений необходимо для чёткой постановки задач при разработке нормативных актов и международных соглашений, а также для того, чтобы ориентироваться на них в повседневной работе, придерживаясь выработанной стратегии.

Реализация таможенной службой поставленной государством задачи по созданию стабильных и благоприятных условий для развития внешней торговли и проведения эффективного таможенного контроля не может быть эффективно осуществлена без внедрения и использования современных информационных технологий, необходимость применения которых обусловлена быстрым увеличением объемов международной торговли, усложнением ее структуры.

В таможенной службе России ведется постоянная работа по внедрению и адаптации современных инструментов таможенного администрирования и кон-

[1] Основные направления совершенствования таможенного администрирования в Таможенном союзе в 2012-2015 годах [Электронный ресурс]. – Режим доступа: http://www.tsouz.ru/db/dta/Documents/Functions2012.pdf.

троля, основанных на информационных технологиях и международных нормах, среди которых:

– использование информационных технологий при совершении таможенных операций (электронное декларирование и информирование по каналам связи и через Интернет (ЭД 1 и ЭД 2));

– разработка новых программных продуктов, обеспечивающих защиту, полноту и конфиденциальность обрабатываемых данных;

– система управления рисками;

– внедрение электронной подписи;

– модернизация информационной сети ЕАИС таможенных органов;

– разработка Концепции создания Интегрированной информационной системы внешней и взаимной торговли Таможенного союза.

На фоне стремительного прогресса информационного общества, постоянного усиления процессов глобальной интеграции и широкого применения информационных технологий в государственном аппарате, в рамках реализации Федеральных целевых программ[1] Правительство РФ ставит перед ФТС России задачу совершенствования таможенных операций и процедур. Для решения данной задачи необходимо внедрение информационных технологий и использование электронных способов передачи информации.

Таким образом, для дальнейшего системного и комплексного развития таможенного администрирования требуется сформулировать перспективные цели и задачи, продумать механизмы их правового и информационно-технического обеспечения, механизмы межведомственного взаимодействия. При этом информационным технологиям отводится значительная роль, так как их эффективное внедрение в будущем будет способствовать существенному сокращению сроков осуществления таможенных операций и таможенного контроля; автоматизации многих процессов, касающихся взаимодействия участников ВЭД с таможенной службой России, а также самой таможенной службы с иными органами исполнительной власти; повышению качества предоставления таможенных услуг; упрощению обеспечения соответствия информационных систем таможенной службы России с информационными системами зарубежных стран.

---

[1] См. например, Государственная программа «Информационное общество (2011-2020 годы)» [Электронный ресурс]. – Режим доступа: http://fcp.economy. gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2011/369/, О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (вместе с «Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года»): Распоряжение Правительства РФ от 17.11.2008 № 1662-р.

Коцюмбас С.М.

К ВОПРОСУ МЕТОДИКИ УСТАНОВЛЕНИЯ ЛИЦ, ПРИЧАСТНЫХ К СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. В статье исследуются проблемы установления лиц совершивших преступления в сфере компьютерной информации.

Ключевые слова: расследование преступлений, неправомерный доступ к компьютерной информации.

Abstract. The paper investigates the problems of identifying the persons committed crimes in the sphere of computer information.

Key words: investigating crimes, illegal access to computer information.

Преступления в сфере компьютерной информации на сегодняшний день представляют реальную угрозу не только отдельным пользователям электронно-вычислительной техники, но и в целом национальной безопасности страны, поскольку они все больше приобретают транснациональный организованный характер, а наносимый ими вред порой с трудом поддается подсчету.

Внедрение безбумажных технологий и средств вычислительной техники в управленческую и производственную деятельность позволяет «криминальным элементам» обладающих специальными познаниями в области компьютерных технологий, без особых физических усилий, а зачастую и финансовых затрат путем нажатия «пары клавиш» или ввода в программу технического устройства вредоносной программы, совершать преступления против собственности, неприкосновенности частной жизни, авторских и смежных прав и т.п.

Специфичность преступлений в сфере компьютерной информации обусловлена использованием при их совершении высоких технологий и других новейших достижений мировой науки и техники, необходимостью обладания определенным уровнем специальных познаний, что с учетом высокой латентности этих преступлений существенно затрудняет их выявление и фиксацию, а также организацию противодействия им, включая их пресечение и предупреждение.

Неправомерный доступ к закрытой компьютерной системе или сети является технологически весьма сложным действием, совершить которые могут только специалисты, имеющие достаточно высокую квалификацию.

Поэтому установление и поиск лиц, совершивших неправомерный доступ к компьютерной информации, следует начинать с технического персонала пострадавших компьютерных систем или сетей (разработчиков соответствующих систем, их руководителей, операторов, программистов, инженеров связи, специалистов по защите информации и других).

Следственная практика показывает, что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен.

Установлению причастности конкретного лица к несанкционированному доступу к компьютерной информации могут способствовать различные обна-

руживаемые иногда при осмотре компьютера и его компонентов материально – фиксированные отображения (например, следы пальцев рук, биологические следы, отдельные рукописные записи на тех или иных носителях).

Для их исследования назначаются криминалистические экспертизы – дактилоскопическая, почерковедческая, технико-криминалистическая, биологическая.

Чтобы выявить лиц, обязанных обеспечивать соблюдение режима доступа к компьютерной системе или сети, необходимо, прежде всего, ознакомиться с имеющимися инструкциями, устанавливающими полномочия должностных лиц, ответственных за защиту информации.

При допросе лиц, обслуживающих компьютерную систему, можно установить, кто запускал нештатную программу, было ли это зафиксировано каким-либо образом. Следует также выяснить, кто увлекается программированием, учится или учился на компьютерных курсах.

При этом к допросу по нашему мнению обязательно необходимо привлекать специалиста обладающего познаниями в области компьютерных технологий, что безусловно поможет следователю который в большинстве случаев не обладает необходимыми познаниями и навыками, полно и всесторонне провести допрос заподозренного лица.

У лиц, заподозренных в неправомерном доступе к компьютерной информации, при наличии достаточных оснований производится обыск или выемка, в ходе которых могут быть обнаружены: компьютеры разных конфигураций, принтеры, средства телекоммуникационной связи с компьютерными сетями, дискеты, диски, магнитные ленты, содержащие сведения, могущие иметь значение для дела (в том числе коды, пароли, идентификационные номера пользователей конкретной компьютерной системы, также данные о ее пользователях).

Обыск и выемка, как и осмотр места происшествия по уголовным делам о преступлениях в сфере компьютерной информации, безусловно, имеют свои особенности и существенные различия, однако общая цель указанных следственных действий (обнаружение, фиксация и изъятие доказательств совершенного преступления) обуславливает схожесть в методике и тактике их проведения.

Применительно к компьютерным преступлениям обыск и выемка производятся чаще всего, когда имеются сведения о лицах, причастных к их совершению, способах, средствах или месте преступного посягательства с использованием компьютерных технологий и вероятном местонахождении доказательств. При проведении обыска и выемки (в отличие от осмотра места происшествия) круг поиска доказательств сужен не только до конкретного помещения, где находится компьютерная техника, но зачастую до отдельного компьютера или устройства, содержащего конкретную информацию и иные следы преступления.

Методика и тактика проведения обыска и выемки при расследовании преступлений в сфере компьютерной информации имеют свои особенности и отличаются от аналогичных следственных действий при расследовании других преступлений.

Это обусловлено не только опасностью умышленного уничтожения информации, имеющей доказательственное значение, еще не выявленными соучастниками преступления, либо иными заинтересованными лицами среди персонала по месту работы подозреваемого или его близких по месту жительства, но и вероятностью неосторожного поведения следователя и других членов следственно-оперативной группы, которые в результате неправильного и неквалифицированного обращения с программно-аппаратными средствами могут повредить информацию либо уничтожить следы.

Одним из важнейших условий проведения обыска (выемки) является строгое соблюдение установленных правил обращения с компьютерной техникой и носителями информации, технически грамотное проведение поиска электронных доказательств, иной нужной информации. В ходе обыска (выемки) также следует обращать внимание на литературу, методические материалы по компьютерной технике и программированию.

При решении следственной задачи по установлению лиц, виновных в создании, использовании и распространении вредоносных программ для ЭВМ, необходимо учитывать, что вредоносную программу может создать человек, обладающий навыками в обращении с компьютером и написании программ. Лучше всего это могут сделать опытные программисты, но они, как правило, не участвуют в их распространении. Поэтому при установлении лица, создавшего вредоносную программу, необходимо продолжить следственную и оперативно-розыскную работу по выявлению лиц, ее распространявших.

Оперативная информация о лицах, участвующих в совершении компьютерных преступлений, сосредоточивается в специальных подразделениях по борьбе с преступлениями в сфере высоких технологий МВД и ФСБ России, куда надлежит обращаться с соответствующими поручениями в тех случаях, когда оно не подключено к расследованию преступления на стадии возбуждения уголовного дела.

Наибольшую общественную опасность в этой связи представляют опытные компьютерные взломщики, так называемые «хакеры», которые являются высококвалифицированными специалистами в области компьютерных технологий.

Нередко преступления данной категории совершаются группой лиц, т.е. «хакер» создает вредоносные программы, а остальные члены группы обеспечивают его деятельность в материально-техническом и информационном отношениях.

В мировой практике борьбы с компьютерными преступлениями известны случаи осуществления «хакерами» связей с организованной преступностью, когда преступные сообщества выступают в роли заказчиков компьютерных махинаций, обеспечивая «хакеров» необходимой техникой, организуя прикрытие, снимая через подставных лиц деньги в банковских компьютерных системах.

Поиск лиц, причастных к использованию вредоносных программ, требует значительных затрат времени и средств, проведения по указанию следователя оперативно-розыскных мероприятий.

Задержание подозреваемого после его установления должно быть произведено незамедлительно, чтобы не допустить уничтожения компрометирующих материалов. В случае, если вредоносная программа является компьютерным

вирусом, от быстроты задержания зависят масштабы возможного распространения вируса и причинения ущерба.

Органу дознания целесообразно дать поручение выявить и проверить лиц, ранее привлекавшихся к ответственности за такое же преступление.

В отношении каждого из заподозренных в совершении преступления лица необходимо установить:

– относимость к категории лиц, ответственных за информационную безопасность и надежность работы компьютерного оборудования, компьютерной системы или сети;

– образование (общее и специальное);

– специальность;

– стаж работы по специальности и на данной должности, прежнее место работы и должностные обязанности;

– уровень профессиональной квалификации;

– конкретные обязанности по обеспечению информационной безопасности;

– причастность к разработке, внедрению компьютерной системы или сети;

– наличие и объем доступа к базам и банкам данных;

– данные, характеризующие лицо по месту работы и жительства с учетом специфики данных преступлений;

– наличие домашнего компьютера и оборудования к нему, уровень навыков обращения с ним и познаний в области информационных технологий.

Все это устанавливается посредством допросов подозреваемого и свидетелей, проведения экспертиз, истребования соответствующих документов, осмотра компьютера, оборудования к нему и иных носителей информации.

В настоящей статье, с учетом ее рамок, обозначены лишь некоторые сложные вопросы, связанные с установлением лиц причастных к совершению преступлений исследуемой категории. Однако, на наш взгляд, данная проблема является актуальной для правоприменительной практики и требует более глубокой научной проработки.

Куксин И.Н.

ПОСЯГАТЕЛЬСТВО НА КОНСТИТУЦИОННЫЕ ЛИЧНЫЕ ПРАВА И СВОБОДЫ В СЕТИ «ИНТЕРНЕТ»: ПРАВОВОЙ АСПЕКТ

Аннотация: В статье раскрываются основные направления правового регулирования в сфере распространения информации через информационно-коммуникационные сети. Особое внимание уделяется анализу правовых форм защиты чести, достоинства и деловой репутации от распространения компрометирующих материалов в сети «Интернет».

Ключевые слова: конституционные права, честь, достоинство, деловая репутация, распространение, разглашение, Интернет-сайт, порочащие сведения, правовая форма защиты.

Abstract. The article describes the main areas of legal regulation in the sphere of distribution of information through information and communication networks. Special attention is paid to the analysis of the legal forms of protection honor, dignity and business reputation from distribution of compromising materials in the Internet.

Key words: constitutional rights, honor, dignity, reputation, distribution, disclosure, website, defamation, legal form of protection.

За последние годы в средствах массовой информации, в том числе и в сети «Интернет» появляется все больше информации, содержание которой свидетельствует не только о вторжении в частную жизнь человека, но и затрагивает честь[1], достоинство[2] и деловую репутацию[3] человека. Из единичных случаев это превратилось в повседневное явление. Наиболее распространено неправомерное вторжение в личную жизнь политиков, депутатов, спортсменов, артистов. Известный случай, когда группа представителей шоу-бизнеса обратилась за защитой в Комитет Государственной Думы по информационной политике, информационным технологиям. По их словам журналисты замучили своей назойливостью: следят, подглядывают, проникают в жилище, выспрашивают соседей, набиваются на интервью, снимают на фото– видеокамеры «из-за угла»[4].

Особенно участились случаи посягательств с помощью компьютерной сети «Интернет» на такие конституционные права и свободы человека как честь, достоинство, деловая репутация граждан. Примерами таких посягательств могут служить сотни гражданских и уголовных дел[5], которые совершены посредс-

---

[1] Честь – общественно-моральное достоинство, то, что вызывает и поддерживает общее уважение, чувство гордости. – Толковый словарь русского языка. – М.: ООО «Издательство Оникс»: ООО «Издательство «Мир и Образование», 2009. С. 1302.

[2] Достоинство – совокупность свойств, характеризующих высокие моральные качества, а также сознание ценности этих свойств и уважения к себе. – Там же. С. 275.

[3] Репутация деловая – создавшееся общее мнение о достоинствах и недостатках кого-чего-нибудь. – Там же. С. 1003.

[4] Шкель Т. Автограф на поправках. – Российская газета, 2013, 15 февраля. С.5.

[5] Так, 28-летний житель одного из сел Кировского района, Приморского края из личных неприязненных отношений к бывшей возлюбленной разместил в Интернете несколько её фотоснимков, на которых она изображена в обнаженном виде. Злоумышленник действовал тайно и думал, что его поступок останется безнаказанным. Режим доступа: http://primamedia.mobi/news/show.php?id=140019&p. (Дата обращения 19.02.2013) Абаканским следственным отделом СК России по Хакасии возбуждено уголовное дело в отношении 23-летнего местного жителя. С 20 сентября по 26 октября 2012 года подозреваемый, желая

твом возможностей глобальной сети «Интернет». Эти и подобные явления, свидетельствуя о нанесении ущерба охраняемым законом интересам личности, общества и государства, требуют пересмотра действующего законодательства, особенно в области гражданского и уголовного права в части, касающейся регулирования общественных отношений, связанных с названными конституционными правами.

Очевидно, что реализация конституционного принципа о признании, соблюдении и защите прав и свобод человека и гражданина, как обязанности государства, требует правового уточнения таких формулировок как «свобода слова», «свобода средств массовой информации», «недопущение цензуры». Сегодня общество осознало, что право на защиту своей чести и своего доброго имени, должно быть подкреплено действенным, четко прописанным в законодательстве механизмом защиты указанных прав. Любая компрометирующая информация, «выпущенная» в Интернет, несравненно более опасна, чем опубликованная в «самых массовых» СМИ. Поэтому она должна пресекаться правовыми мерами действующего законодательства.

Российское законодательство содержит несколько форм юридической защиты чести и достоинства от посягательств в сети «Интернет». Остановимся лишь на тех из них, которые представляются наиболее значимыми и требуют дальнейшего законодательного совершенствования.

Конституционно-правовая форма защиты личных прав и свобод. Конституция Российской Федерации заложила юридическую основу такой защиты, которая детализируется и дополняется другими отраслям права. Так, согласно ее ст. 21 достоинство личности охраняется государством. Ничто не может быть основанием для его умаления. Провозглашено также право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23). Приведенные основания, закрепленные в Конституции России и направленные на защиту чести и достоинства, в том числе от посягательства с использованием ресурсов глобальной сети «Интернет», получают дальнейшую реализацию, прежде всего, в гражданском, уголовном и административном судопроизводстве.

Гражданско-правовая форма защиты личных прав и свобод. Основанием обращения в судебные органы за защитой чести и достоинства от посягательства с использованием ресурсов глобальной сети «Интернет», является ст. 150 Гражданский кодекс РФ (далее – ГК РФ). Гражданин вправе требовать по суду опровержения той информации, которая порочит[1] (унижает) его честь и доброе

причинить нравственные страдания своей знакомой, с которой некоторое время поддерживал близкие отношения, разместил ее фотографии, где она изображена в обнаженном виде, в социальных сетях. – Режим доступа: http://xakac.info/news/2012103027732. (Дата обращения 19.02.2013).

[1] Порочащими являются сведения, содержащие утверждения о нарушении гражданином или юридическим лицом действующего законодательства, совершении нечестного поступка, неправильном, неэтичном поведении в личной, общественной или политической жизни, недобросовестности при осуществлении производственно-хозяйственной и предпринимательской деятельности, нарушении деловой этики или обычаев делового

имя, деловую репутацию либо вторгается в частную жизнь, личную и семейную тайну. Закон допускает защиту чести и достоинства гражданина и после его смерти.

Учитывая общедоступность сети «Интернет» и стремительный рост количества ее пользователей, сегодня особенно актуальными являются вопросы защиты таких ценностей как достоинство личности, личной неприкосновенности, чести и доброго имени, деловой репутации, которые каждому человеку очень дороги. За стремительностью развития сети «Интернет» не должно отставать и законодательство. Именно поэтому внесен ряд существенных поправок в ГК РФ, направленных на защиту нематериальных благ. Так, в подготовленном законопроекте, который рассматривается Государственной Думой ст. 150 ГК РФ дополнена частью третьей, в которой сказано: «В случаях, когда того требуют интересы гражданина, принадлежащие ему нематериальные блага могут быть защищены, в частности, путем признания судом факта нарушения его личного неимущественного права, публикации решения суда о допущенном нарушении, а также путем пресечения или запрещения действий, нарушающих или создающих угрозу нарушения личного неимущественного права либо посягающих или создающих угрозу посягательства на нематериальное благо»[1]. Такое дополнение в ГК РФ будет защищать не только знаменитостей, но и обычного человека. Поэтому любые подглядывания, подслушивания, фотографирования «из-за угла», размещение позорящей информации в сети «Интернет» будет решительно пресекаться с помощью судебных процедур. В таких и подобных случаях суд своим решением может запретить подобные действия. Приведенное дополнение в ГК РФ даст возможность эффективнее защищать нематериальные блага граждан.

Реализация приведенного законопроекта вызовет у суда определенную сложность. Но как отметил председатель Комитета Государственной Думы по гражданскому, уголовному, арбитражному и процессуальному законодательству П. Крашенинников: «Не все наши законы начинают работать сразу, некоторые законы у нас получаются на вырост»[2].

Гражданский кодекс РФ должен соответствовать духу времени. Нормы, которые регулируют частную жизнь граждан, были приняты давно (1994 г.). За это время бурными темпами развивается сеть «Интернет». На конец лета 2010 г. в России 43 млн. человек, что составляет 30% от общей численности на-

---

оборота, которые умаляют честь и достоинство гражданина или деловую репутацию гражданина либо юридического лица. – См.: постановление № 3 Пленума Верховного Суда РФ от 24 февраля 2005 г. «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Бюллетень Верховного Суда РФ, 2005. № 4. С. 5.

[1] Проект ФЗ № 47538-6 «О внесении изменений в Гражданский кодекс Российской Федерации, отдельных законодательных актов Российской Федерации и о признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации». – Режим доступа: www/rg/ru/art/732414 (дата обращения: 17.02.2013).

[2] Куликов В. Частная нечастная жизнь. – Российская газета, 2013, 5 февраля. С. 9.

селения, имеют выход в Интернет и являются его пользователями[1]. Опасность сети «Интернет» заключается в том, что она доступна широкой аудитории, а поэтому заложенная в нем компрометирующая информация может храниться годами[2]. В итоге какая-нибудь древняя негативная информация или фотография может загубить человеку карьеру, повлиять на его личную жизнь. Чтобы этого избежать, в указанном законопроекте содержится следующее дополнение к ч. 5 ст. 152 ГК РФ: «Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети «Интернет», гражданин вправе требовать удаления соответствующей информации, а также опровержения указанных сведений способом, обеспечивающим доведение опровержения до пользователей сети».

В судебной практике, как правильно отмечает Колоколов Н.А., одной из проблем является установление круга лиц, которые подлежат ответственности за моральный вред и материальный ущерб потерпевшему[3]. Возможность анонимного присутствия в сети «Интернет» позволяет скрыть подлинное имя автора, разместившего компрометирующую информацию. Особенно, когда речь идет о сайтах, где размещаются мнения посетителей. Каждый последующий посетитель имеет возможность познакомиться с мнением предыдущего. Найти автора, который высказал мнение унижающее честь или достоинство того или иного лица не представляется возможным. В таких случаях речь может идти только о собственнике зарегистрированного сайта. Однако зачастую ими могут быть иностранные компании, что значительно усложняет возможность защиты нарушенных прав[4]. Чтобы компрометирующая информация не хранилась долгое время, в ГК РФ внесена поправка к ч. 8 ст. 153 ГК РФ следующего содержания: «Если установить лицо, распространившее сведения, порочащие честь, достоинство или деловую репутацию гражданина, невозможно, гражданин, в отношении которого такие сведения распространены, вправе обратиться в суд с заявлением о признании распространенных сведений не соответствующими действительности (ч.8 ст. 152 ГК РФ).

---

[1] Тридцатый выпуск регулярного бюллетеня «Интернет в России». Вып. 30. Лето 2010 г. URL. Режим доступа: http:// bd.fom.ru/ pdf/ kratkaya_ versiya_ otcheta_ leto2010.pdf. По данным «Яндекс», полугодовая аудитория Рунета превышает 34 миллиона человек, что составляет 30% от населения России старше 18-ти лет. Режим доступа: http://sozdanie-saytov.com/posetiteli-saytov-socialnyh-setey (дата обращения: 18.02.2013).

[2] Об усиливающейся опасности глобальной сети «Интернет» для интересов общества свидетельствует тот факт, что правительство США в 2012 г. учредило государственную награду – медаль, за успешную борьбу против киберпреступности. Президент РФ Путин В.В., выступая на расширенной коллегии ФСБ, «призвал как можно скорее сформировать систему обнаружения, предупреждения и отражения компьютерных атак на информационные ресурсы России» // Российская газета, 2013, 15 февраля. С.2.

[3] Колоколов Н.А. Ответственность за клевету и оскорбление: проблемы судебной практики // Уголовный процесс. 2008. №2. С. 26.

[4] Алавердов О.С. Распространение компрометирующих сведений в глобальной сети Интернет: уголовно-правовой аспект // Вестник Адыгейского государственного университета. Серия 1: регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2009. №3. С. 181 179-182.

Таким образом, удалить не только порочащую информацию из сети «Интернет», но и любые не соответствующие действительности сведения о гражданине можно будет через суд.

Уголовно-правовая форма защиты личных прав и свобод. Наиболее общественно опасные действия по распространению компрометирующих материалов, посягающих на личные права и свободы, признаются преступлениями и соответственно закреплены в Уголовном кодексе РФ (далее – УК РФ). Количество таких составов преступлений относительно велико, и разграничиваются они в Особенной части УК РФ в зависимости от тех общественных отношений, на которые они посягают: честь и достоинство личности ст. 128.1 («Клевета»); конституционные права граждан (ст. 137 УК РФ «Нарушение неприкосновенности частной жизни»); семья (ст. 155 УК РФ «Разглашение тайны усыновления (удочерения)»); экономические отношения (ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»); конституционные основы безопасности государства (ст. 283 УК РФ «Разглашение государственной тайны»); правосудие (ст. 298.1 УК РФ «Клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, судебного пристава», ст.310 УК РФ «Разглашение данных предварительного расследования»); порядок управления (ст. 319 УК РФ «Оскорбление представителя власти»).

Анализируя указанные составы преступлений с позиции объективной стороны, все они представляют собой активные действия, выражающиеся в форме распространения и (или) разглашения. Например, в ч. 1 ст. 128.1 УК РФ сказано: «Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающего его репутацию».

Под распространением сведений, порочащих честь и достоинство личности или деловую репутацию граждан и юридических лиц, следует понимать «опубликование таких сведений в печати, трансляцию по радио и телевидению, демонстрацию в кинохроникальных программах и других средствах массовой информации, распространение в сети Интернет, а также с использованием иных средств телекоммуникационной связи, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение, в той или иной, в том числе устной, форме хотя бы одному лицу»[1].

В ряде статей УК РФ законодатель использует термин «разглашение». По смысловой нагрузке этот термин близок к термину «распространение», однако между ними имеется принципиальное различие в субъекте. Последний, нарушает не только нормы уголовного права, но и обязанность по неразглашению сведений, относящихся к категории охраняемых законом тайн, например, усыновления (удочерения), государственной тайны, предварительного расследова-

[1] См.: п.7 постановления № 3 Пленума Верховного Суда РФ от 24 февраля 2005 г. «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Бюллетень Верховного Суда РФ. 2005. № 4. С.4-5.

ния. Таким образом, разглашение отличается от распространения субъектом, который относится к категории специального субъекта преступления.

Лица, которые преследуют цель довести ту или иную информацию до широкого круга через сеть «Интернет», прибегают к форме распространения. Для квалификации преступных действий по УК РФ значение имеет не только форма распространения компрометирующих сведений, но и способ. Так, в ч.2 ст. 128.1 УК РФ «Клевета»[1] содержится такой квалифицирующий признак как «клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации».

Публичность в данном случае следует толковать как показ, публичное сообщение для всеобщего сведения в местах, где присутствует значительное число лиц. Так, ст. 319 УК РФ «Оскорбление представителя публичной власти» предполагает именно публичное оскорбление представителя власти при исполнении им своих должностных обязанностей или в связи с их исполнением.

Если речь идет о публичном распространении компрометирующей информации, затрагивающей честь, достоинство, деловую репутацию или частную жизнь физических или юридических лиц в сети «Интернет», то возникает вопрос: относится ли Интернет-сайт к одной из форм СМИ? Ответ на поставленный вопрос содержится в ст. 2 Федерального закона «О средствах массовой информации». Федеральным законом от 14.06. 2011 года № 142-ФЗ была дополнена ст. 2 «О средствах массовой информации» следующим положением: «под сетевым изданием понимается сайт в информационно-телекоммуникационной сети «Интернет», зарегистрированный в качестве средства массовой информации в соответствии с настоящим Законом»[2]. Следовательно, Интернет-сайт относится к средствам массовой информации, при условии, что он таковым зарегистрирован в соответствии с законом о СМИ.

Ныне действующий УК РФ нуждается в кардинальной переработке. По мнению председателя Ассоциации Юристов России П. Крашенинникова, – «Уголовный кодекс РФ не сегодня и не вчера перестал быть Кодексом как таковым. Он стал сводом законов об уголовном праве. И если Общая часть кодекса выглядит более или менее сносно, то Особенная – статьи, описывающие конкретные составы преступлений: хулиганство, убийство и другие – не выдерживает никакой критики[3]. Сложившаяся ситуация вполне объяснима. Разработка ныне действующего УК РФ в середине 90-х гг. XX в. не имела выверенной социологической и криминологической базы, не имела системного общего и конкретного прогноза возможных позитивных и негативных последствий действия УК РФ. За эти годы в действующий УК РФ внесено более 3 тыс. измене-

---

[1] Статья введена Федеральным законом от 28 июля 2012 г. № 141-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты российской федерации» // Собрание законодательства Российской Федерации. 2012. № 10. Ст. 1162.

[2] Федеральный закон «О средствах массовой информации» от 27.12 1991 г. № 2124-1 в ред. ФЗ от 21.07.2011 № 252-ФЗ, от 28.07.2012 № 133-ФЗ. Режим доступа: http://www.consultant.ru/popular/smi/ – (Дата обращения 21.02.2013)

[3] Уголовный кодекс перечитают // Российская газета – Неделя. 2011, 16 декабря.

ний и дополнений[1]. Оценивая состояние действующего УК РФ, необходимо выработать новую концепцию, на основе которой разработать уголовное законодательство, которое бы отвечало современным требованиям развития российского общества. Эта задача завтрашнего дня. А что касается борьбы с противоправными действиями через сеть «Интернет», то сегодня ряд статей УК РФ нуждаются в дальнейшем совершенствовании. Так, ч. 2 ст. 128.1 УК «Клевета», по мнению автора, необходимо сформулировать в следующей редакции: «Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации, в том числе размещенная на Интернет-сайтах, разосланная по электронной почте, а равно с использованием программ передачи мгновенных сообщений». В подобной редакции нуждаются и другие статьи УК РФ.

Изложенное показывает, что российский законодатель, исходя из потребностей судебной практики, используя новые теоретические разработки ученых, практиков, вносит соответствующие изменения, дополнения, поправки в нормы действующего законодательства с тем, чтобы конституционные права граждан были надежно защищены.

[1] Лебедев В. Судя по всему // Российская газета. 2013, 19 февраля.

Лагуточкин А.В.

НЕКОТОРЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СЕТИ ИНТЕРНЕТ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Аннотация. В статье рассматриваются проблемы осуществления оперативно-розыскных мероприятий в Интернет. Проводится краткая характеристика правового обеспечения оперативно-розыскных мероприятий в Интернет.

Ключевые слова: оперативно-розыскные мероприятия, Интернет.

Abstract. The problems of the search operations to the Internet. A brief description of legal support search operations on the Internet.

Keywords: search operations, the Internet.

Современное состояние информационной сферы характеризуется стремительным ростом объемов распространяемой информации, в том числе посредством ее распространения в цифровом пространстве сети Интернет. Как известно, Интернет представляет уникальные возможности для общения, перемещения больших объемов информации, осуществления покупок и т.д.

По данным статистических центров на конец 2012 года зафиксировано 2,2 млрд. пользователей E-mail по всему миру. Ежедневно расходится около 144 млрд. электронных писем. Важнейшей частью интернета являются его пользователи, которых на конец 2012 года было насчитано 2,4 млрд. Мобильный рынок уже давно неразрывно связан с Интернетом, где в 2012 году было зафиксировано 6,7 млрд. подключений к сервису мобильной связи[1]. Что касается России, то в последние годы происходит стремительный рост числа пользователей российского сегмента сети Интернет. Согласно результатам исследования «Российского рынка интернет-торговли: товары 2012», проведенного агентством РБК.research, весной 2013 года уровень проникновения интернета составит 63,6%, а в 2018 году он превысит отметку в 80%[2].

В представленных современных преобразованиях преступность также трансформировалась, обрела новые возможности криминальной деятельности в информационном пространстве сети Интернет и посредством его использования. Это отмечает и выступивший на коллегии МВД России в феврале 2012 года, Д.А. Медведев, который отметил, что «...мир меняется, он стал абсолютно глобальным, это создаёт и свои сложности. Поэтому нам нужно уделять внимание и той преступности, которая совершается в информационном пространстве, самой разной. Этим занимаются все государства. Существуют и факты коррупции, и хищений через «электронные деньги» с использованием возможностей Интернета. В Сети можно встретить не только финансовых аферистов, но и торговцев наркотиками, тех, кто совершает другие преступления»[3].

Современный криминальный мир уже не мыслит своего преступного функционирования без Интернета, с помощью которого осуществляется:

- удаленная связь между преступными группировками различной направленности;

---

[1] http://www.fight.org.ua/publications/statistika-internet-v-2012-godu.html

[2] http://www.bizhit.ru/index/users_count/0-151

[3] http://президент.рф/новости/14474

- обмен преступным опытом;
- привлечение соучастников готовящихся преступлений, криминальный поиск жертвы и орудий;
- сбыт имущества, добытого преступным путем;
- осуществление расчетно-денежных операций между лицами в условиях подготовки и совершения преступлений;
- совершение преступлений посредством использования сетевого информационного пространства.

Изложенное выше является поводом для применения правового инструментария в противодействии представленным современным угрозам. К этому «набору инструментов», конечно, необходимо отнести оперативно-розыскные мероприятия (далее ОРМ), представленные Федеральным законом «Об оперативно-розыскной деятельности»[1].

В теории ОРД и в практике оперативных подразделений ОРМ всегда являлись наиболее действенными элементами в борьбе с преступностью, важной частью которых, являлась негласность их проведения. Однако современность диктует необходимость осмысления их применения в противодействии новым видам преступлений, совершенным в информационном пространстве сети Интернет или с его использованием.

Большая часть ОРМ может применяться субъектами оперативно-розыскной деятельности (далее – ОРД) в условиях непосредственности их применения. Конечно, важно отметить тот факт, что сотрудники оперативных подразделений ОВД сегодня не боятся использовать информационное пространство сети Интернет для решения частных и иных задач ОРД. Однако в этом направлении есть проблемы субъективного и объективного характера, которые необходимо решать в ближайшее время. Известно, что оперативный сотрудник в условиях осуществления личного сыска в информационном пространстве сети Интернет должен владеть навыками и умениями уверенного пользователя. Однако уровень подготовки оперативных сотрудников для работы в сетевом информационном пространстве крайне полярен и неодинаков, чаще готовность ограничивается знаниями, приобретенными в процессе пользования информационных сетей в условиях самообучения. К тому же в ОВД существует дефицит специалистов рассматриваемого направления ввиду высокой востребованности в иных сферах деятельности, в том числе деятельности хозяйствующих субъектов, где ресурсы для привлечения подобных лиц играют не последнюю роль. Курсы повышения квалификации сотрудников оперативных подразделений, а также специализация на данном направлении вуза МВД России в должной мере не решают поставленных в этом направлении задач и требуют от системы подготовки специалистов нового подхода.

Среди объективных проблем можно в большей степени выделить техническую, связанную с оснащенностью необходимыми для работы ресурсами. Возвращаясь к коллегии МВД в 2012 года можно отметить, что Д.А. Медведев указал: «...стоит задача приобретения высококлассной техники. На эти цели не следует жалеть денег». Мы разделяем его позицию. Действительно, не каждый отдел полиции оснащен современными компьютерами, не говоря уже о необхо-

[1] См.: Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

димом высокоскоростном доступе в сеть Интернет. Особо стоит остановиться на последнем. Для доступа в Интернет оперативные сотрудники в большей части используют личные ресурсы, при условии покрытия сети через Wi-Fi[1], или сотовых операторов через модем, причем похвастаться высокой скоростью 4G[2] могут лишь крупные города, а что касается районов и сельской местности – это несбыточная мечта. Помимо этого, предоставление корпоративного Интернета может исключить вопросы, связанные с легитимностью полученных доказательств в сети, который, как уже было указано, осуществляется за счет использования частного трафика предоставляемого доступа (из личных средств оперативного работника).

Любое оперативно-розыскное мероприятие, в том числе осуществляемое в информационном пространстве посредством сети Интернет, должно иметь свои правовые основания. Общеизвестно, что на законодательном уровне данные основания закреплены в ст. 7 ФЗ «Об оперативно-розыскной деятельности». При этом, мы видим проблемы поведения оперативно-розыскных мероприятий, осуществляемых личным сыском в сети Интернет.

Так, сложность вызывает отсутствие в нормативно-правовом блоке единого понятийного аппарата терминологии, применяемых в использовании техники и программирования. Довольно сложно перечислить всю терминологию деятельности, однако есть необходимость на нормативном уровне раскрыть ряд терминов, которые позаимствованно вошли в обиход жизни граждан и активно используются в русском языке, такие как: онлайн, аккаунт, логин, сервер, IP-адресс, скриншот и др. Это достаточно упростит нормативное описание событий, явлений, действий в процессе обеспечения решения правоохранительных задач.

Помимо этого, осуществляя ОРМ, оперативный сотрудник рискует перейти пределы охраняемых конституционных прав граждан. Как известно, в России законодательно граница прав на информацию неразрывно связана с собственником информации, ее характером и местонахождением компьютера, на котором находится (может находиться) значимая информация, причем последнее наиболее важно в определении необходимости получения судебного разрешения на ее получение.

В настоящее время идут споры о том, что Конституция РФ помимо гарантий защиты личной информации, находящейся на жестком диске компьютера пользователя, свое действие распространяет и на отдельные сегменты в сети Интернет, где присутствует «личное информационное пространство» пользователя. Данная обеспокоенность граждан понятна, ведь в Интернете концентрируется очень большое количество информации, связанной с личной жизнью граждан: это и дневники (блоги), и частные СМИ, и личные странички в социальных сетях, и много другое. Любое мнение, произведение, текст, картинка, ви-

---

[1] Wireless Fidelity – высокая точность беспроводной передачи данных, соответствующее стандарту IEEE 802.11.

[2] *Fourth generation* – «четвёртое поколение» – поколение мобильной связи, особенно отличающееся широкой полосой передачи данных (высокой скоростью). К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с подвижным и 1 Гбит/с – стационарным абонентам.

део в Интернете доступны неограниченному кругу лиц в силу самого устройства среды. И что любопытно, пользователь сети Интернет, передавая информацию неопределенному кругу лиц для размещения на сервере, полагая о ее публичности, требует ограничить доступ к ее содержанию.

Прямой законодательный акт, регулирующий правоотношения в сети Интернет, отсутствует, однако некоторые аспекты, которые можно отнести к защищаемым интересам граждан, регулируется иными правовыми актами.

Так, в результате внесения изменений в уголовно-процессуальное законодательство в 2010 году п. 24.1 ст. 5 посредством использования ст. 186 УПК РФ[1] частично определяет охраняемые законом элементы частной жизни граждан в сети Интернет, преодоление которых возможно по судебному решению, такие как: информация о соединениях между абонентами и (или) абонентскими устройствами – сведения о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведения о номерах и месте расположения приемопередающих базовых станций. Исходя из вышеизложенного, а также анализа правовых актов, судебной защите подлежат сведения, находящиеся в информационном пространстве сети Интернет, такие как: содержание переписок между абонентами сети, трафик соединений контактных номеров, а также финансовых расходов абонента в сети и др.

Особо хотелось бы выделить Федеральный закон[2], вокруг поправок в который, до сих пор ведутся ожесточенные споры о правомерности их введения по вопросу ограничения доступа к противоправной информации в сети Интернет. Это Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». В результате принятия поправок[3] с 1 ноября 2012 года создана новая саморегулируемая организация, в обязанности которой входит следить за контентом в сети. *Так,* мониторингом сети занимается оператор, которого определил специальный орган, уполномоченный правительством (Роскомнадзор). При обнаружении противоправного контента Роскомнадзор уведомляет об этом владельца сайта и хостинг-провайдера. Если владелец сайта не удалит опасный контент в течение суток, это в течение следующих суток должен сделать хостинг-провайдер. В случае если данная информация осталась не вырезанной – сайт или страница сайта – вообще IP-адрес включается в «черный» реестр, где размещается эта опасная информация с целью его блокировки. Проблема, которая осталась, – это нерешенный спор о том, по IP или по URL должна проходить блокировка.

Сейчас в едином реестре информации, которая запрещена к распространению в России, уже более 200 сайтов. За неделю работы Роскомнадзора (с 01 ноября 2012 года) зафиксировано почти семь тысяч обращений. После первич-

---

[1] Федеральный закон от 01 июля 2010 г. № 143-ФЗ О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

[2] Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию».

[3] Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации».

ной аналитики они переданы в Госнаркоконтроль, Роспотребнадзор и Роскомнадзор на экспертизу. Самый большой объем таких обращений передан в Госнаркоконтроль – 199. Основная часть поступивших заявлений содержит ссылки на ресурсы, где торгуют наркотическими и психотропными препаратами. Роспотребнадзор получил для экспертизы 72 обращения о пропаганде суицидального поведения[1]. Представляемая в ОВД информация от Роскомнадзора о противоправных явлениях в сетях подлежит обязательной проверке, в том числе, с использованием ОРМ в информационном пространстве сети Интернет.

В заключении необходимо указать на то, что техническое совершенствование, качественное изменение преступности, изменения ее организационного и правового характера позволяют говорить о назревшей необходимости создания нормативно-правовой базы, регулирующей сферу отношений в информационном пространстве сети Интернет, а также обновления правовых актов, регламентирующих оперативно-розыскную деятельность на законодательном и ведомственном уровнях. И что важно, в условиях глобализации информационного пространства сети Интернет данные изменения ничтожны в том случае, если представленные обновления коснутся только России. В настоящее время ни в одной из стран мира нет кодифицированного законодательства, регулирующего правоотношения в сети Интернет. Необходимо выходить с предложением о принятии международного акта, определяющего: механизм противодействия незаконным действиям в сети Интернет, компетенцию субъектов борьбы, потенциально опасные угрозы и другие факторы.

Современные глобальные компьютерные сети являются новым объектом оперативно-розыскного воздействия, на что указывают присутствие криминальной составляющей в процессах, связанных с их функционированием; наличие в глобальных сетях источников оперативно значимой информации; развитые механизмы обеспечения анонимности при использовании сетей; влияние нормального функционирования сетевых объектов на безопасность общества; надгосударственный характер глобальных сетей, способствующий совершению трансграничных преступлений; выявленные обстоятельства криминального плана, связанные с особенностями сетевой среды.

[1] http://www.rg.ru/2012/11/06/saiti-site-anons.html

Лиликова О.С.

БИЛЕТ ЧЕРЕЗ ИНТЕРНЕТ: ОСОБЕННОСТИ ПРИОБРЕТЕНИЯ ЭЛЕКТРОННОГО БИЛЕТА

Аннотация. Статья посвящена новому способу приобретения билета через Интернет на воздушном транспорте (электронному билету). Рассматривается сущность электронного билета и его возможности, в отличие от бумажных бланков. Определяются преимущества использования технологии электронного билета как для пассажира, так и для авиакомпаний (перевозчика).

Ключевые слова: договор воздушной перевозки, электронный билет.

Abstract. Article focuses on a new way of purchasing tickets through the Internet in air transport (e-ticket). The essence of e-ticketing and its capabilities, as opposed to paper-based forms. Determined the benefits of using technology as an e-ticket for passengers and for airlines (carrier).

Key words: the contract of air transportation, the electronic ticket.

Сегодня переход на электронные билеты лежит в основе общемировой стратегии по упрощению бизнеса и сокращению расходов в воздушно-транспортной отрасли. Во всем мире авиакомпании активно внедряют электронные билеты. В идеале электронное оформление предполагает, что пассажир заказывает билет в сети Интернет и оплачивает его в безналичном порядке. На вокзале или в аэропорту пассажир просто предъявляет документ, удостоверяющий личность, и получает распечатку электронного билета по установленной форме. Данный способ удобен как для пассажиров, так и для перевозчиков. Даже у самого рассеянного гражданина подобный билет не будет забыт дома, а перевозчики, конечно, выигрывают экономически (затраты на электронный билет значительно меньше, чем на бумажный).

По заявлению Международной Ассоциации гражданской авиации (IATA), с 1 июня 2008 года весь мир пассажирских авиаперевозок перешел на электронную систему регистрации и продажи билетов и отказался от оформления билетов в бумажном виде. В России электронный авиабилет узаконен Приказом министра транспорта РФ от 8 ноября 2006 года «Об установлении формы электронного пассажирского билета и багажной квитанции в гражданской авиации»[1]. Федеральным законом от 1 декабря 2007 г. № 314-ФЗ «О внесении изменений в статью 105 Воздушного кодекса РФ»[2] в ст. 105 Воздушного кодекса РФ были внесены изменения. В частности, был на законодательном уровне закреплён электронный билет.

Согласно данным документам, электронный билет в нашей стране получил возможность на существование, однако не все категории пассажиров смогут воспользоваться его преимуществами. Обычному туристу, отправляющемуся на отдых за границу в Грецию или в Хорватию за свои кровные денежки,

---

[1] Приказ Минтранса РФ от 08.11.2006 г. № 134 «Об установлении формы электронного пассажирского билета и багажной квитанции в гражданской авиации» // Российская газета. – № 22. – 02.02.2007.

[2] Федеральный закон от 01.12.2007 г. №314 «О внесении изменений в статью 105 Воздушного кодекса РФ» // Собрание законодательства РФ. – 2007. – №49. – Ст.6075.

электронный билет оформят без проблем. А вот страдальцу-командировочному все же придется наведаться в офис авиакомпании и получить в дополнение к электронному билету бумажный или контрольно-кассовый чек, который будет подтверждать факт оплаты (и который в дальнейшем ему пригодится для отчетности перед работодателем). То есть электронный билет в России используется в достаточно усеченном варианте. Введение электронно-бумажного билета полезно компаниям, которые в основном занимаются перевозками «частников» — они действительно смогут снизить свои расходы на оформление билетов. Если же компания специализируется на перевозке командированных пассажиров, то ей на практике узнать о достоинствах электронного билета не придется — бумажной волокиты меньше не станет.

Билет, багажная квитанция, иные документы, используемые при оказании услуг по воздушной перевозке пассажиров, могут быть оформлены в электронном виде (электронный перевозочный документ) с размещением информации об условиях договора воздушной перевозки в автоматизированной информационной системе оформления воздушных перевозок.

При использовании электронного перевозочного документа пассажир вправе потребовать, а перевозчик или действующее на основании договора с перевозчиком лицо при заключении договора перевозки или регистрации пассажира обязаны выдать заверенную выписку, содержащую условия соответствующего договора воздушной перевозки, из автоматизированной информационной системы оформления воздушных перевозок.

Особенность электронного билета состоит в том, что его можно заказать только в том случае, когда весь перелет обслуживает одна авиакомпания. Это обусловлено тем фактором, что информацию такого билета, могут счесть не все авиакомпании, а только та, которая продает его. Преимуществ у таких билетов – очень много. Например – их потерять невозможно, так как вся информация данного билета, находится в компьютере авиакомпании. Такой билет снабжает вас гибкостью перелета, т.е. намного легче будет изменить дату вылета или возвращения. Купить такой билет вы сможете крайним сроком – за тридцать минут до начала регистрации. Преимущество, также состоит и в том, что у вас не будет необходимости предоставлять билет, в случае внесения каких-то изменений или корректировок. Такой билет может быть оплачен третьими лицами, что избавит Вас от необходимости простаивания очередей за бумажным билетом.

Уже давно авиакомпании осуществляют продажу авиатранспортных услуг в традиционных кассах. Широкое участие в продажах билетов принимают и туристические агентства. Кроме того, много билетов сбывается с помощью современных автоматизированных систем бронирования (АСБ), предоставляющих информацию о расписании рейсов авиаперевозчиков, свободных местах и тарифах, и с помощью которых потребители могут осуществлять бронирование авиатранспортных услуг. АСБ помогает им производить бронирование и оформление билетов, предоставляет информацию об ассортименте других услуг, связанных с путешествиями и отдыхом. Оформление авиабилетов попрежнему в основном производится через агентов, хотя объем продаж с помощью Интернета растет невероятно.

Практика показывает, что при совершении покупки билета через Интернет потребители услуг авиакомпаний менее защищены, чем при приобретении бумажного билета по традиционным каналам.

На данный момент развития Интернета функции поиска, которые обычно выполняются агентами от имени и по поручению потребителей, частично переходят к потребителям, самостоятельно наводящим справки через различные веб-сайты для получения желаемой информации о рейсах и тарифах. Если традиционные АСБ являются всеобъемлющими и достоверными источниками информации о воздушных сообщениях, то этого, к сожалению, нельзя сказать о веб-сайтах, которые не могут быть абсолютно независимыми от АСБ и могут содержать информацию, за достоверность которой трудно поручиться, поскольку неизвестны принципы и правила, регулирующие составление информации, размещаемой на веб-сайтах.

Однако веб-сайты предоставляют потребителям возможность познакомиться с большим разнообразием новой, постоянно обновляемой информации о дополнительных вариантах авиапутешествий, эксклюзивных Интернет-тарифах и аукционных тарифах. Но разобраться в ней посетителям веб-сайтов далеко непросто, так как требует от них обладания определенными навыками работы с такой информацией в Интернете.

Другой проблемой для потребителей является раскрытие личных данных в Интернете. Осуществляя покупку билета традиционным путем, потребитель сообщает необходимые личные данные только агентам. Эта информация является конфиденциальной и не подлежит публичному распространению. А при покупке билета через Интернет дело обстоит по другому. Сообщая данные по Интернету, потребитель не защищен от того, что они не будут доступны для третьих лиц и не использованы в преступных или хулиганских целях.

Известно, что для защиты пользователей от неполной и вводящей в заблуждение информации, а также укрепления доверия пользователей, некоторые государства принимают меры по охране прав потребителей и принимают законы о защите прав потребителей при совершении ими сделок, осуществляемых через Интернет. Ложные веб-сайты, ложное расписание рейсов, ложные льготные акции и другие формы ложной информации, распространяемой недобросовестными конкурентами могут быть причиной многих правовых, экономических, финансовых и иных конфликтов. Вполне вероятно, что потребитель может свои недоразумения с покупкой электронного билета через веб-сайты обратить против перевозчика и потребовать от него компенсации за причиненный как материальный, так и моральный вред. В связи с этим возникает проблема решения новых вопросов ответственности перевозчика, которых раньше не было, но возникших в связи с продажей электронных билетов[1].

Если техническая сторона вопроса электронного оформления билетов через Интернет практически решена, то этого нельзя сказать о юридическом обеспечении такой деятельности. Внедрение электронных билетов в практику ме-

[1] Мосашвили В. В. Правовые аспекты внедрения и использования электронного билета Российскими авиаперевозчиками. // Право. – 2007. – №6. –С.13-14.

ждународных воздушных перевозок привело к возникновению новых правовых проблем, которые ранее не решались ни международным, ни национальным правом. В частности, российские законы ориентированы на регулирование исключительно бумажных билетов и только их признают в качестве законных средств регулирования финансовых отношений между перевозчиком и пассажиром. Поэтому без легализации электронного билета и признания его законным документом расчетов невозможно перейти к его масштабному использованию. Чтобы устранить существующие преграды на пути использования электронного билета, предстоит серьезное реформирование национального законодательства.

Техническая эволюция в сфере организации продаж и бронирования авиабилетов на мировом рынке авиаперевозок ставит новые проблемы, ранее не решавшиеся национальным законодательством. Использование для сохранения записей о пунктах отправления и назначения электронного оборудования ставит задачу выработки критериев соответствия применяемой для этих целей техники. В национальном плане она может быть решена путем принятия технического регламента в соответствии с Федеральным законом «О техническом регулировании». Закон позволяет российским перевозчикам работать на опережение, разработать и принять такой регламент, с такими параметрами соответствия, которые наиболее общим образом отвечают прагматическим интересам российских перевозчиков при переходе к продажам и бронированию электронных билетов.

При выдаче пассажиру электронного билета договор воздушной перевозки считается заключенным так же, как и при выдаче пассажиру бумажного билета.

Рассмотрим заключение договора воздушной перевозки с электронным билетом.

1. Во-первых, пассажир обращается к перевозчику или агенту перевозчика непосредственно или посредствам телефона или Интернета.

2. Во-вторых, перевозчик или агент перевозчика выясняют наличие свободных мест на воздушном судне и сообщает об этом пассажиру.

3. В-третьих, перевозчик или агент перевозчика разъясняют пассажиру условия договора воздушной перевозки пассажира и при согласии пассажира с условиями договора воздушной перевозки пассажир вносит плату согласно тарифу за услугу воздушной перевозки. После чего получает электронный билет, что по сути своей является записью в реестре перевозочных документов перевозчика.

Подчеркнем, что в прошлом и настоящем международное право, национальное право и обычаи делового оборота определяют и признают традиционный бумажный билет как перевозочный документ, удостоверяющий факт заключения договора международной воздушной перевозки. Электронные билеты также должны быть признаны и узаконены в качестве перевозочных документов. Предварительный мониторинг российского законодательства, регулирующего применение авиабилетов, показывает, что для обеспечения перехода к электронным билетам необходимо будет дополнить действующее законодате-

льство новыми положениями. При этом следует учитывать, что на данном этапе переход к новой перевозочной документации касается только международных воздушных перевозок, а не внутренних. Это обстоятельство позволяет не трогать действующее законодательство, регулирующее внутренние перевозки, и целиком и полностью сосредоточиться на внесении новых изменений, дополняющих законы в соответствии с требованиями Монреальской конвенции[1]. В конце 2012 г. РФ ратифицировала Монреальское соглашение, в соответствии с которым существенно увеличены лимиты ответственности авиакомпаний перед пассажирами при выполнении международных рейсов и снимает ограничения по компенсациям за потери багажа и ущерб здоровью клиентов.

Таким образом, электронный авиабилет – это очень удобно, и не только в способе заказа, но и в его использовании. Такой вид билета, обладает рядом преимуществ, наверное, именно поэтому, его популярность растет так быстро и стремительно.

[1] Конвенция для унификации некоторых правил международных воздушных перевозок (заключена в г. Монреале 28.05.1999г.) // СПС «Консультант Плюс».

Ляхова А.И.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АДВОКАТСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья раскрывает проблему обеспечения информационной безопасности адвокатской деятельности в Российской Федерации. Автор рассматривает меры по обеспечению информационной безопасности адвокатской деятельности как необходимое условие сохранения адвокатской тайны и теории юридического процесса, которая обеспечивает эффективность исследования юридического процесса как общеправовой категории.

Ключевые слова: адвокатура, адвокатская деятельность, информационная безопасность, информационное пространство, адвокатская тайна.

Abstract. The article reveals the problem of information security law in the Russian Federation. The author considers the measures to ensure the security of advocacy as a necessary condition for maintaining secrecy law and the theory of the legal process, which ensures the efficiency of the legal research process as a general legal category.

Key words: advocacy, advocacy, information security, information space, attorney secrets.

В последнее время во всем мире наблюдается быстрый переход от общества индустриального к обществу информационному. Уровень развития информационного пространства и его защищенности оказывает существенное влияние на развитие политических, социальных, экономических процессов а также на обороноспособность государства и состояние правоохранительной системы. Единое информационное пространство представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей[1].

В Российской Федерации на сегодняшний день сформировалось единое развитие информационное пространство, в связи, с чем является необходимым развитие системы нормативного правового регулирования отношений в области информатизации. Юридическая поддержка открытости государственных информационных ресурсов является необходимой предпосылкой обеспечения интеграции единого информационного пространства России с европейским и мировым информационным пространством.

Важное значение в сфере развития информационного законодательства следует уделить вопросам формирования законодательства в области регулирования создания и использования информационного компонента адвокатской деятельности.

Отправной точкой при разработке законодательства в области защиты

[1] Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов [Электронный ресурс]// sbras.nsc.ru/win/laws/russ_kon.htm.

информации является четкое уяснение роли и места системы защиты информации в деятельности адвокатского образования и в сфере обеспечения его безопасности в целом. Защита информации является одним из элементов общей политики адвокатского образования в области безопасности, которая охватывает более широкий круг вопросов, начиная от подбора на работу сотрудников, не обладающих статусом адвоката, сохранности информации сообщаемой доверителем в ходе беседы с адвокатом до использования средств защиты информации и предотвращения возможной утечки информации за при использовании информационных правовых систем и Интернет-ресурсов. Элементы общей системы безопасности адвокатской деятельности должны быть взаимосвязаны и согласованы.

Меры по обеспечению информационной безопасности адвокатской деятельности должны осуществляться по следующим направлениям:

предотвращение распространения и утечки информации;

предотвращение угрозы информационной безопасности личности, обратившейся за юридической помощью;

предотвращение несанкционированных действий по уничтожению, искажению, копированию, блокированию информации, составляющей адвокатскую тайну;

предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы адвокатского образования;

защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, лиц обратившихся за юридической помощью;

сохранение секретности, конфиденциальности документированной информации в адвокатском образовании;

подготовку сотрудников и их обучение для обеспечения режима информационной безопасности в адвокатском образовании.

Объектом обеспечения информационной безопасности в адвокатской деятельности является:

1) адвокатская тайна (факт обращения к адвокату, включая имена и названия доверителей; все персональные данные клиентов; все доказательства и документы, собранные адвокатом входе подготовки к делу; сведения, полученные адвокатом от доверителей; информация о доверителе, ставшая известной адвокату в процессе оказания юридической помощи; содержание правовых советов, данных непосредственно доверителю или ему предназначенных; все адвокатское производство по делу; условия соглашения об оказании юридической помощи, включая денежные расчеты между адвокатом и доверителем; любые другие сведения, связанные с оказанием адвокатом юридической помощи)[1];

---

[1] Кодекс профессиональной этики адвоката [Электронный ресурс]: принят Всероссийским съездом адвокатов 31 января 2003г.: в ред. от 5 апреля 2003г. // Справочная правовая система «Консультант Плюс». Разд. «Законодательство». Информ. банк «Версия Проф».

2) коммерческая тайна (сведения об обороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредитов организации (пассивы и активы); сведения о рыночной стратегии фирмы, об эффективности коммерческой деятельности фирмы; обобщенные сведения клиентах и других партнерах, состоящих в деловых отношениях с организацией; обобщенные сведения о внутренних и зарубежных фирм как потенциальных конкурентах, оценка качества деловых отношений с конкурирующими предприятиями; сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с клиентами; сведения о методах расчета, структуре, уровне реальных цен на услуги и размеры скидок; сведения о порядке и состоянии организации защиты коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме[1]);

3) персональные данные работников (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, уровень квалификации, доход, наличие судимостей и некоторая другая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника[2].

Адвокатским сообществом выработаны некоторые практические меры по защите информации, составляющей предмет адвокатской тайны. Так например адвокатам рекомендуется: общаться с доверителем в помещениях, позволяющих сохранять конфиденциальность; в телефонных разговорах с доверителем не использовать «громкую» телефонную связь; для защиты от прослушивания использовать разные SIM-карты или телефонные аппараты; при обсуждении особо важных дел выключать сотовый телефон и вынимать из него батарею питания; уничтожать документы и информацию, в хранении которых нет необходимости; для защиты информации, содержащейся в компьютере адвоката.

Особое внимание в рекомендациях по защите информации в сфере адвокатской деятельности уделяется организации компьютерной безопасности: адвокатам рекомендуется установить периодически изменяемые пароли и систематически тестировать компьютер на предмет выявления попыток незаконного проникновения; особое внимание уделить локальной сети, а также получению и отправке информации через Интернет, контролю за безопасностью электронной почты; компьютер, в котором хранится вся информация, создаваемая в адвокатском образовании, или сервер, разместить в отдельном помещении с особым доступом – защитой от вторжения, а наиболее важную информацию хранить на сервере в зашифрованном виде; принимать меры к тому, чтобы исключить возможность доступа к содержимому компьютеров, на которых работают адвока-

---

[1] Столяров, Н.В. Разработка системы защиты конфиденциальной информации/ Н.В.Столяров [Электронный ресурс]// 4Delo.ru Библиотека.– (http://www.4delo.ru/inform/articles/).

[2] Цыпкин, А.Л. Адвокатская тайна/ А.Л.Цыпкин [Электронный ресурс]// Russian-lawyers.ru..– (http://russian-lawyers.ru/files/cypkin.doc).

ты, всех остальных лиц (защита информации может быть обеспечена путем специальных шифровальных программ, например PGP (Pretty Good Privacy), которая доступна на сайте www.pgp.com).

Кроме того, рекомендуется всех работников адвокатских образований при принятии их на работу предупредить о недопустимости разглашения адвокатской тайны и проинструктировать, как следует организовать работу на своем рабочем месте, чтобы информация не могла попасть к посторонним; информировать всех работников адвокатских образований о том, что истребование от них, так же как и от адвоката, сведений, связанных с оказанием юридической помощи, не допускается; уделять особое внимание защите сведений, известных сетевому администратору и бухгалтеру.

Однако все рекомендации, выработанные адвокатским сообществом в сфере обеспечения информационной безопасности адвокатской деятельности носят только рекомендательный характер и в настоящее время отсутствуют четкие нормативные предписания, раскрывающие содержания понятия «адвокатская тайна», определение ценности защищаемой информации, комплекса мер по поддержанию необходимого уровня защиты информации, отсутствует четкая законодательная регламентация мер по поддержанию необходимого уровня защиты информации, не определены полномочия и условия ответственности за обеспечение установленного режима информационной безопасности.

Правовая основа единого информационного пространства призвана регулировать отношения производителей и потребителей информации, обеспечивать координацию действий органов государственной власти в едином информационном пространстве и гарантировать соблюдение конституционных прав и свобод граждан и организаций, в том числе и в сфере адвокатской деятельности и обеспечения реализации адвокатской тайны.

Мамин А.С.
Остапюк В.Г.

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ, СВЯЗАННЫХ С ЗАЩИТОЙ ЛИЧНОЙ (ПЕРСОНАЛЬНОЙ) ИНФОРМАЦИИ

Аннотация. В статье представлены основные проблемы связанные с правовым регулированием отношений связанных с защитой личностных прав граждан на информацию.
Ключевые слова: личные права граждан, персональная информация
Abstract. The paper presents the main issues related to the legal regulation of relations connected with the protection of personal rights of citizens to information.
Key words: individual rights, personal information.

Реализация прав человека, прежде всего личных, как основополагающих для всех других, невозможна без информации, которая является необходимым условием реализации группы личных прав.

За минувшее десятилетие в России было принято значительное число нормативных актов, в том числе федеральных законов, указов Президента и постановлений Правительства Российской Федерации, которые целиком посвященных вопросам регулирования общественных отношений, возникающих в процессе создания, преобразования и потребления информации, так и затрагивающих информационные отношения в области личной информации. Но далеко не все персональные данные являются конфиденциальными. Многочисленные энциклопедии персоналий, профессиональные персональные справочники, адресные книги и т.п. – это персональные данные, которые обнародуются по согласию субъекта.

Законодательное регулирование сбора и использования персональных данных обусловлено защитой неприкосновенности частной жизни как базового конституционного принципа, однако особый механизм правового регулирования сбора, использования, распространения персональных данных возник, как указывалось выше, в связи с повсеместным созданием в органах власти и организациях автоматизированных баз персональных данных.

С развитием научно-технического прогресса, с приходом компьютерной эры неизмеримо возросло значение защиты права на неприкосновенность частной жизни в информационной сфере. С одной стороны, в условиях повсеместного внедрения информационных технологий добавился доступ людей к информации, что способствует осуществлению права индивида на свободу информации. С другой стороны, доступ физических лиц к базам персональных данных усиливает риск вторжения в сферу частной жизни и нарушения права на ее неприкосновенность. Таким образом, информационные и телекоммуникацион-

ные технологии предельно обострили правовые проблемы, связанные с дилеммой «раскрытие информации – защита частной жизни»[1].

Информация (от латинского informatio – ознакомление, разъяснение, изложение) представляет собой сведения (сообщения, данные) независимо от формы их представления. Информация в современном мире стала наиважнейшим ресурсом, который влияет на уровень развития всех сфер человеческой жизни. Экономические и политические отношения под воздействием информационного развития получают новые перспективы.

Итак, нужно ли защищать информацию о конкретном человеке, которая позволяет его идентифицировать?

Для большинства людей этот вопрос уже не стоит. Законодательство многих стран, прежде всего Конституции, содержат принципы защиты неприкосновенности частной жизни, защиты личной тайны, «prïvecy», запрет на сбор информации о человеке без его согласия. Жизнь человека в информационном мире неизбежно делает его более прозрачным для государства и общества. Именно развитие информационно-телекоммуникационных технологий, внедрение их во все сферы жизни общества и государства, перевод многочисленных картотек в цифровую форму побудили людей задуматься о защите этой весьма чувствительной информации. Новые технологии, с одной стороны, существенно упростили сбор, обработку, хранение, передачу данных, а с другой – создали очевидные угрозы их незаконного оборота, что приводило к нарушениям прав личности[2].

В Российской Федерации правовым фундаментом, регулирующим отношения в области информации, является ряд статей Конституции РФ (в частности, ст. ст. 23, 24, 29, 44)[3]. Так, например, в соответствии со ст. 24 Конституции РФ, определяется что: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Запрет сбора информации о частной жизни и оперирования полученными сведениями охватывает как обширную сферу неофициального общения лица, так и его внутренний духовный мир. Этот запрет является составной частью характеристики качества жизни в обществе, показателем степени автономности и свободы индивида по отношению к обществу и государству. Речь идет о событиях прошлой и настоящей жизни человека, значимых для него фактах, действиях и решениях, наконец, о свойствах и переживаниях, присущих самой личности (в некоторых законодательных актах говорится об интимных сторонах жизни),

---

[1] Филатов С. Правовое обеспечение защиты личной и семейной тайны в компьютерной информации // Право и жизнь. 2005. N 89(12).

[2] В.В. Дятленко, Е.К. Волчинская Законодательство о защите персональных данных: проблемы и решения // Информационное право. 2006. № 1.

[3] Конституция Российской Федерации от 12 декабря 1993 года // Российская газета. – 25 декабря 1993 года. №237.

отделенных от аспектов его бытия, непосредственно включенных в процессы государственной или общественной жизни[1].

Очевидно, что человек как социальный элемент, находящийся постоянно в отношениях с другими людьми, организациями, органами власти, не может не сообщать о себе персональные данные, оставаясь инкогнито в этих отношениях. В каких-то ситуациях он сам определяет, какие персональные данные ему сообщить, а в каких-то (чаще всего в отношениях с государством) он вынужден сообщать требуемые персональные данные для того, чтобы взамен государство обеспечило его права, предоставило услуги.

Другим не менее важным нормативно-правовым актом, регулирующим более детально данную сферу, стал Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» который был принят 27 июля 2006 г[2]. Данный нормативно правовой акт регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений в области охраны результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации. Закрепляется принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом. При этом существует ограничение доступа к информации, которое может устанавливаться только федеральными законами.

Персональные данные могут охраняться и охраняются в настоящее время различными режимами ограниченного доступа (см.: Закон РФ «О государственной тайне», Федеральный закон «О коммерческой тайне» и др.). Например, в режиме государственной тайны охраняются персональные данные ряда лиц, имеющих доступ к государственным секретам. В режиме коммерческой тайны могут охраняться персональные данные авторов «ноу-хау», используемых в производстве. В режиме профессиональной тайны охраняется информация персонального характера, характеризующая пользователей предоставляемых услуг (врачебная тайна, нотариальная, адвокатская, банковская, тайна усыновления и т.п.). В режиме личной тайны – сведения об особенностях личности, ее пристрастиях, привычках, интересах. В режиме семейной тайны – сведения о взаимоотношениях членов семьи, в том числе родственных.

Таким образом, персональные данные – это вид сведений, непосредственно связанных с личностью, а не режим конфиденциальности этих сведений.

Помимо этого, можно привести иные нормативно-правовые акты которые также регулируют отношения в данной области: Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральный закон от 27 декабря 1991 г. № 2124-1 «О средствах массовой инфор-

---

[1] Научно-практический комментарий к Конституции Российской Федерации (Отв. ред. В.В.Лазарев) – Система ГАРАНТ, 2003.

[2] Российская газета от 29 июля 2006 г. № 165.

мации» (в ред. от 27 июля 2006 г.), Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (в ред. от 9 июля 1997 г.).

Действующее законодательство устанавливает ответственность за нарушения связанных с получением, использованием, информации относящейся к личной. Так, глава 13 Кодекса РФ об административных правонарушениях устанавливает ответственность за административные правонарушения в области связи и информации. *В соответствии со ст.* 13.11. КоАП РФ устанавливается ответственность за: «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»[1]. За данное правонарушение предусматривается ответственность в виде штрафа.

Помимо административной ответственности существует и уголовная ответственность, которая также регулирует данную сферу отношений. Так, Уголовный кодекс РФ в главе 19 «Преступления против конституционных прав и свобод человека и гражданина» определяет ответственность за нарушение норм Конституции РФ. Например, в соответствии со ст. 137 УК РФ «Незаконное собирание 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 и наказываются штрафом в размере до двухсот тысяч рублей»[2].

Таким образом, подводя итог можно констатировать, что интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на ее использование в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, гарантирующей личную безопасность. Помимо всего прочего, необходимо не забывать о санкции, которая может наступить за нарушение действующего законодательства в области охраны личной информации.

---

[1] Кодекс Российской Федерации Об Административных Правонарушениях от 30.12.2001 N 195-ФЗ // Собрание законодательства РФ», 07.01.2002, N 1 (ч. 1), ст. 1.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 года N 63-ФЗ // Собрание законодательства РФ», 17.06.1996, N 25, ст. 2954.

Митякина Н.М.
Федорященко А.С.

НЕКОТОРЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ЗАКЛЮЧЕНИЯ ПРЕДПРИНИМАТЕЛЬСКИХ ДОГОВОРОВ В СЕТИ ИНТЕРНЕТ

Аннотация. В данной статье авторами предпринимается попытка обобщить основные проблемные вопросы правового регулирования заключения предпринимательских договоров с помощью сети Интернет, предлагаются пути решения выявленных проблем и противоречий современного российского законодательства.

Ключевые слова: Интернет, предпринимательский договор, форма договора, электронная подпись

Abstract. In this article, authors try to summarize major issues of legal regulation of the conclusion of business contracts with the help of the Internet, offer solutions to the identified problems and contradictions of contemporary Russian law.

Key words: Internet, a business contract, a contract form, electronic signature.

За развитием современных информационных технологий неизбежно следует их внедрение не только в науку и технику, но и в систему правоотношений, в том числе в практику товарооборота и заключения сделок. Динамика развития рынка и рыночных связей, мобильность субъектов предпринимательских правоотношений приводит к тому, что использование традиционных способов заключения договоров (составление бумажного документа) становится все более «неудобным» и постепенно оттесняется новыми возможностями, которые предоставляет Интернет.

В связи с этим возникает проблема адекватного правового регулирования заключения сделок с использованием электронных средств. Особенно это касается вопросов соблюдения письменной формы сделки и ее подписания.

В юридической литературе неоднократно обращалось внимание на трудность соблюдения требований законодательства при заключении сделок в сети Интернет[1].

Основу правовой регламентации в рассматриваемой сфере, безусловно, составляет Гражданский кодекс, который в ст. 160 указывает, что сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, или должным образом уполномоченными ими лицами; использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

Таким образом, Гражданский кодекс, указывая на возможность использо-

[1] Наумов В.Б. Право и Интернет: очерки теории и практики. М., 2002; Степанов В.С. Договоры в сети Интернет: теория и практика // Цивилистические записки: Межвуз. сб. науч. трудов. Вып. 2. М., 2002.

вания аналога собственноручной подписи, ставит такую возможность в зависимость от конкретного указания в законе либо от наличия соглашения сторон.

Представляется, что такая формулировка закона создает определенные препятствия для широкого использования электронных документов в сфере заключения договоров.

Перечень нормативных актов, предусматривающих случаи, когда возможно использование электронной подписи либо иного аналога собственноручной подписи, не такой уж и большой. В частности, в настоящее время ряд нормативных актов регламентирует использование электронной подписи в процессе расчетов между банками, например: Положение Центрального банка РФ «О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России»[1].

Основной документ, регулирующий отношения, возникающие при применении информационных технологий – Федеральный закон «Об информации, информационных технологиях и о защите информации»[2] (ст. 11) – содержит норму, в соответствии с которой в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами. То есть данная статья не содержит указания на случаи, когда возможно применение электронной подписи или иного аналога собственноручной подписи для заключения договора, а предусматривает такую возможность для обмена документами.

И здесь следует согласиться с выводом И.А. Соболь, что «с сожалением приходится констатировать, что перечисленные законодательные положения являются весьма значимыми для электронного документооборота, но не для совершения сделок в электронной форме»[3].

Регламентировать использование электронной подписи призван Федеральный закон «Об электронной подписи»[4]. Статья первая данного закона гласит, что закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий. То есть, рассмат-

---

[1] Положение Центрального банка РФ от 23 июня 1998 г. № 36-П «О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России» // Вестник Банка России. 1998. № 61.

[2] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

[3] Соболь И.А. Гражданско-правовая защита сделок, заключенных с использованием сети Интернет // Общество и право. 2011. № 3. С. 156.

[4] Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СЗ РФ. 2011. № 15. Ст. 2036.

риваемый акт регулирует использование только электронных подписей и не касается применения кодов, паролей, ключей и т.д. Их использование при заключении договоров остается за рамками правового регулирования на законодательном уровне.

Упоминание не электронной подписи, а других электронных аналогов собственноручной подписи в ГК удалось найти только в ч. 3 ст. 847. В соответствии с ним, договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (п. 2 ст. 160) кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом. Но, как видим, данная статья не говорит о заключении договора с использованием кодов и паролей, а предусматривает лишь возможность распоряжения средствами банковского счета (при этом указывает, что использование кодов и паролей должно быть предусмотрено в договоре). Вследствие этой ситуации наиболее распространенным способом подписи электронных документов (в том числе договоров) в настоящее время выступает электронная подпись.

Даже поверхностный анализ Федерального закона «Об электронной подписи» позволяет говорить о его недостаточности для правового регулирования заключения гражданско-правовых сделок.

И здесь можно выделить ряд проблем. Во-первых, на наш взгляд, данный закон регулирует порядок использования электронной подписи, но не случаи возможного ее применения.

Во-вторых, и это главное, что закон предусматривает возможность совершения электронной подписи на сделке, но в нем не говорится о возможности использования электронных средств для фиксации содержания самой сделки.

Статья 2 ФЗ «Об электронной подписи»: электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. То есть электронная подпись позволяет идентифицировать подписывающее лицо, а не сам документ.

Поэтому трудно согласиться с выводом, что законом создан механизм, позволяющий защитить электронный документ от подделки и от внесения в него несанкционированных изменений, а также идентифицировать лицо, подписавшее этот документ[1].

Поэтому важным вопросом (хотя уже больше процессуального характера), связанным с заключением сделки в электронной форме, является вопрос о достоверности информации, содержащейся в электронном документе. В этой связи Ю.Ф. Вацковский обоснованно предлагает обратить внимание на зарубежный опыт, в частности на принятый в Англии в 1968 г. Закон о доказательст-

[1] Комментарий к Гражданскому кодексу Российской Федерации. Часть первая: учеб.-практич. комментарий (постатейный) / Е.Н. Абрамова, Н.Н. Аверченко, Ю.В. Байгушева и др.; под ред. А.П. Сергеева. М.: Проспект, 2010. С. 429.

вах по гражданским делам, который содержит требования, предъявляемые к компьютерным доказательствам. Прежде всего, согласно этому Закону утверждения, содержащиеся в документе, произведенном при помощи компьютера, допускаются в качестве доказательства заявляемого факта, в отношении которого было бы допустимо прямое устное показание, если соблюдены следующие условия:

1) документ, содержащий это утверждение, был произведен компьютером в тот период, когда этот компьютер регулярно использовался для сохранения и обработки информации в целях любой деятельности, осуществлявшейся в течение указанного периода;

2) в течение этого периода в обычном порядке указанной деятельности в компьютер регулярно передавалась информация, подобная той, которая содержится в утверждении, либо подобного вида, из которого она была произведена;

3) в течение существенной части этого периода компьютер исправно работал, а если в этот период и возникали неисправности, то они не влияли на производство документа либо на точность его содержания, и

4) информация, содержащаяся в утверждении, воспроизводит или выведена из информации, переданной в компьютер в обычном режиме в процессе указанной деятельности[1].

Рассмотренные выше правовые проблемы, как правило, не влияют на развитие Интернет-торговли в сфере потребительских правоотношений. Современный потребитель при покупке через Интернет обычно не задумывается о том, что возможно ему придется отстаивать свои интересы в суде и перспективах доказывания наличия договора, либо, если и думает об этом, то полагается на удачу и считает возможным «рискнуть» некоторой суммой сделки. В предпринимательской же сфере (особенно в международном аспекте) циркулируют значительные финансовые потоки, и «рисковать», заключая недостаточно урегулированные законом электронные сделки, в этой области контрагенты не намерены.

Поэтому, в заключение рассмотрения заявленной темы, можно сформулировать некоторые основные проблемные вопросы правового регулирования, которые создают определенные трудности и препятствия для широкого применения сети Интернет для заключения предпринимательских договоров.

1. Ограничительная формулировка статьи 160 ГК РФ, позволяющая использовать электронную подпись и иные аналоги собственноручной подписи только в случаях и порядке, предусмотренных правовыми актами или соглашением сторон.

2. Пробельность правового регулирования использования не электронных подписей, а других аналогов собственноручной подписи: кодов, паролей, ключей и т.д.

3. Отсутствие правового регламентации возможности использования электронных средств для фиксации содержания самой сделки.

---

[1] Вацковский Ю.Ф. Доменные споры. Защита товарных знаков и фирменных наименований. М.: Статут, 2009. С. 145.

Названные и многие другие правовые проблемы, связанные с заключением предпринимательских договоров в сети Интернет, на наш взгляд, возможно решить путем принятия закона «Об электронной торговле». Учитывая, что использование Интернет напрямую затрагивает не только внутрироссийский рынок, но и сферу международных коммерческих отношений, строить такой закон целесообразно с учетом международных соглашений.

Еще в 1996 г. Комиссией ООН по праву международной торговли (ЮНСИТРАЛ) был разработан Типовой закон об электронной торговле[1], на основе которого многие страны разработали и приняли свои аналогичные законы. В 2008 году Межпарламентской Ассамблеей государств-участников СНГ был принят Модельный закон об электронной торговле[2]. Целью данного Модельного закона является правовое обеспечение условий для электронной торговли на основе признания электронных сообщений, включая:

– закрепление прав и обязанностей лиц, осуществляющих электронную торговлю;

– определение правил совершения сделок с использованием электронных сообщений, подписанных аналогами собственноручной подписи;

– формирование правовой основы государственного регулирования и поддержки электронной торговли;

– защиту прав и законных интересов граждан и юридических лиц, участвующих в электронной торговле (ст. 1).

Принятие данного Модельного закона в общем свидетельствует, что Российская Федерация постепенно продвигается к принятию собственного Федерального закона «Об электронной торговле», который, на наш взгляд, и будет способен разрешить противоречия и устранить несовершенства действующего законодательства в области заключения предпринимательских договоров в сети Интернет.

---

[1] Типовой закон ЮНСИТРАЛ об электронной торговле (Принят в г. Нью-Йорке 28.05.1996 – 14.06.1996 на 29-й сессии ЮНСИТРАЛ) // Комиссия ООН по праву международной торговли. Ежегодник. 1996 год. Т. XXVII.– Нью-Йорк: Организация Объединенных Наций, 1998. С. 319-323.

[2] Модельный закон об электронной торговле (Принят в г. Санкт-Петербурге 25.11.2008 Постановлением 31-12 на 31-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2009. № 43. С. 268-293.

Мишакин А.В.

ВЛИЯНИЕ ИНТЕРНЕТА НА РАЗВИТИЕ ИНСТИТУТА УСЫНОВЛЕНИЯ

Аннотация. В статье рассмотрены вопросы влияния интернет-ресурсов на развитие института усыновления как на одну из самых острых проблем на данном этапе развития Российской Федерации.

Ключевые слова: усыновление, информационные технологии, базы данных, интернет-ресурс.

Abstract. The paper deals with the influence of online resources for the development of the Institute of adoption as one of the most acute problems in the present stage of development of the Russian Federation.

Key words: adoption, information technology, database, web site.

База данных детей-сирот – основной источник информации о детях, оставшихся без попечения родителей и нуждающихся в усыновлении или опеке.

Именно в банк сирот обращаются люди, получившие одобрение как кандидаты в усыновители от органов опеки и попечения.

Порядок деятельности банка данных детей-сирот, нуждающихся в усыновлении, регламентирован Федеральным законом от 16.04.2001 № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей»[1] и устанавливает порядок формирования и использования государственного банка данных о детях, оставшихся без попечения родителей.

С полным текстом закона о банке данных детей-сирот (и с рядом других нормативных актов и документов) можно ознакомиться на соответствующих интернет-ресурсах – например, «усыновите.ру». Наше внимание будет направлено на рассмотрение сущности так называемой «базы усыновления» в интернет-ресурсах, а также порядка обращения в соответствующие органы исполнительной власти, какие документы необходимо представить и какую информацию предоставляет потенциальным усыновителям база данных детей-сирот.

Собственно база данных детей на усыновление представляет собой информационные ресурсы, сформированные на федеральном или региональном уровне (соответственно, будут именоваться региональный или федеральный банк данных сирот) и информационные технологии, при помощи которых осуществляется поиск, сбор, хранение и предоставление будущим усыновителям документированной информации о детях, оставшихся без родителей.[2]

Во исполнение указанного Закона Постановлением Правительства РФ от 4 апреля 2002 г. № 217 «О государственном банке данных о детях, оставшихся без попечения родителей, и осуществлении контроля за его формированием и

[1] Федеральный закон от 16.04.2001 № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей»// Собрание законодательства РФ. 2001. № 17. Ст. 1643.

[2] http://insomnia.com.ua/article/vliyanie-interneta

использованием»[1] установлена процедура формирования банка данных, документирования информации о детях, подлежащих устройству на воспитание в семьи, о гражданах, желающих принять таких детей, определены правила и порядок предоставления гражданам конфиденциальной информации о детях, подлежащих семейному устройству, определен механизм пополнения банка данных.

Документированная информация о детях-сиротах в базе данных должна быть полной, достоверной и стандартизированной по единому образцу. Также информация банка данных о детях, нуждающихся в опеке и гражданах, желающих усыновить ребенка, должна быть защищена от хищения, подделки и несанкционированного доступа.

Сведения о детях из базы данных предоставляют гражданам органы исполнительной власти – региональный или федеральный оператор государственного банка данных детей-сирот. А информацию о детях, оставшихся без родителей, операторам банка данных предоставляют органы опеки и попечительства на местах.

Необходимо отметить, что размещение информации в базе данных не освобождает органы опеки и попечительства от обязанностей по устройству детей-сирот на воспитание. Обратимся к порядку обращения в банк усыновления.

Если кандидат в усыновители получил положительное заключение и встал на учет в ООП, он может ознакомиться с информацией о детях-сиротах, находящихся в ведении данного органа опеки и попечительства и получить направление для посещения ребенка.

Если будущий усыновитель не смог подобрать ребенка для усыновления по месту жительства, он имеет право обратиться к региональному или федеральному оператору государственного банка данных.

Для того, чтобы гражданам, желающим усыновить ребенка, банк данных выдал информацию, необходимо представить соответствующему оператору следующие документы:

- ✓ паспорт гражданина РФ;
- ✓ заявление о желании принять ребенка на воспитание с просьбой ознакомиться с информацией о детях, соответствующих его пожеланиям;
- ✓ анкету гражданина, желающего усыновить ребенка;
- ✓ заключение ООП о возможности гражданина быть усыновителем.

Все эти документы должны быть рассмотрены в срок, не превышающий 10 дней, после чего оператор предоставляет гражданину сведения о ребенке, в соответствии с пожеланиями усыновителя.

Если гражданин согласен усыновить предложенного ребенка, то оператор банка данных выдает направление на встречу. Если сведения о представленных

---

[1] Постановление Правительства РФ от 04.04.2002 № 217 «О государственном банке данных о детях, оставшихся без попечения родителей, и осуществлении контроля за его формированием и использованием»// Собрание законодательства РФ. 2002. № 15. Ст. 1434.

в базе данных детях-сиротах не соответствуют пожеланиям гражданина, то гражданин имеет право подать просьбу о продолжении поиска. Также важно учитывать информацию о детях, которые нуждаются в усыновление, это полные данные о этническом происхождении, состоянии здоровья, физическом и умственном развитии и особенностях характера ребенка. К анкете ребенка в банке данных детей на усыновление прилагается также фото ребенка.

Необходимо заметить, что размещенная в банке данных полная информация о детях, оставшихся без попечения родителей, является конфиденциальной.

Операторы государственного банка данных и органы опеки и попечительства имеют право публиковать частичную информацию о детях, нуждающихся в усыновлении, на публичных ресурсах, однако при этом должна быть исключена любая возможность идентификации личности ребенка и его родственников.

Российских сирот стали усыновлять через Интернет. Малыши все чаще находят новых родителей в сети Интернет. По словам экспертов, стоит детскому дому завести свою веб-страничку, как количество потенциальных усыновителей возрастает в три-четыре раза. Интернет дает шанс обрести семью даже, казалось бы, обреченным на сиротство тяжелобольным малышам.

Уже сейчас слово «усыновление» вводится в интернет-поисковики более 14 тыс. раз за месяц. А на сайт при Минобрнауки, где содержится информация о 163 тыс. сиротах, ежедневно заходит более двух тыс. посетителей. Руководитель Школы приемных родителей Алексей Рудов, отмечает что виртуальное пространство оказывает настолько большое влияние на пользователей, что посетители сайта, посвященного сиротам, решают стать приемными мамами и папами, даже если раньше об этом и не задумывались.

Всемирная паутина помогает обрести семью и другой «сложной» категории – тяжелобольным малышам, а также малышам, состоящим друг с другом в родстве, т.е. сестрам и братьям, когда усыновление одного без другого невозможно.

Министерство образования и науки полагает, что в ближайшее время, а именно в 2013 году, начнет работать новая система, которая будет обновляться каждые три дня, но эта инициатива пока находится на уровне планов. В целях оказания методической помощи органам исполнительной власти субъектов Российской Федерации Минобрнауки России направляет Рекомендации по организации и осуществлению деятельности по опеке и попечительству в отношении несовершеннолетних в субъекте Российской Федерации.[1]

Руководители детских домов уверены в том, что статистику усыновления можно было бы улучшить, если бы было постоянное финансирование информационной поддержки сайтов. Сейчас же информация в виртуальном детдоме

---

[1] Письмо Минобрнауки РФ от 25.06.2007 № АФ-226/06 «Об организации и осуществлении деятельности по опеке и попечительству в отношении несовершеннолетних» // Вестник образования. 2007. № 16.

обновляется редко, а фотографии одиноких малышей очень плохого качества. К тому же к доброму делу уже успели подключиться мошенники, которые вполне могут дискредитировать затею. По официальной статистике в прошлом году новую семью обрело более 7,6 тыс. сирот. По прогнозам экспертов, их количество будет только увеличиваться. За последний год в стране появилась новая тенденция: детей, оставшихся без родителей, стали усыновлять одним кликом мышки. Будущих мам и пап привлекает удобство системы: не нужны долгие поездки в другой город, достаточно просто зайти на сайт, ввести требуемые параметры – и несколько кандидатур уже есть. К тому же анонимность Интернета подкупает: можно спокойно выяснить все, что надо для усыновления, спокойно обдумать свое решение, не давая преждевременных обещаний. Если после личной встречи с сиротой потенциальный родитель обязан дать ответ в десятидневный срок, то при поиске ребенка через сайт никаких временных ограничений не существует[1].

Итак, важное практическое значение имеет закрепление на законодательном уровне положений о реализации возможности усыновления через сеть интернет.

Признание приоритетности права ребенка на семью означает признание факта необходимости совершенствования и развития механизмов не только законодательства, но механизмов информационного обеспечения будущих родителей информацией о детях, которые попали в трудную жизненную ситуацию и нуждаются в усыновлении.

[1] http://www.probirka.org/usynovlenie/3180-otkuda-berutsya-deti-na-usinovlenie.html

Москаленко С.А.

КРИЗИСНЫЕ ЦЕНТРЫ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ПРАВ ЖЕНЩИНЫ И РЕАЛИЗАЦИИ ПРИНЦИПА ГЕНДЕРНОГО РАВЕНСТВА

Аннотация. В статье представлен анализ создания и развития Кризисных центров помощи женщинам в России, с учетом зарубежного опыта. Детально рассматриваются социально-незащищённые группы женщин, такие как – матери-одиночки, женщины-инвалиды, вдовы, женщины, подвергшиеся психофизическому насилию и другие, нуждающиеся в квалифицированной помощи специалистов разных областей. Представленный анализ показал, что опыт создания кризисных центров более характерен для институтов гражданского общества, нежели публичных властных структур, в частности на муниципальном уровне.

Ключевые слова: кризисные центры, женщины, гендерное равенство, помощь, матери-одиночки, защита прав и интересов, насилие, семья, общество, реабилитация, женщины-инвалиды, несовершеннолетние матери, благотворительное учреждение, гражданское общество.

Abstract. The analysis of the creation and development of crisis centers for women in Russia, with the foreign experience. Provides details of socially vulnerable groups of women, such as – single mothers, women with disabilities, widows, women victims of violence and other psychophysical in need of professional assistance of specialists in different areas. This analysis showed that the experience of a crisis center more characteristic of civil society than the public authorities, particularly at the municipal level.

Key words: crisis centers, women, gender equality, support, single mothers, the protection of rights and interests, violence, family, society, rehabilitation, women with disabilities, teenage mothers, charities, civil society.

Права женщин нуждаются в правовой регламентации и обеспечении, поскольку исторически женщины являются более угнетенными по сравнению с мужчинами, а также в силу физиологических особенностей женского организма и выполнения важнейшей функции материнства.

Несмотря на формально определенное в Конституции России равенство прав и свобод мужчины и женщины (ч. 3 ст. 19)[1], аналогичного фактического состояния не достигнуто. Исходя из этого, целесообразно обратиться к рассмотрению обеспечительных инструментов субъективных прав женщин, которые в итоге не только позитивно повлияют на правозащитную среду в целом, но также будут способствовать действительной реализации принципа равенства прав и свобод мужчины и женщины в различных областях.

Итак, в рамках данной работы исследовательское внимание обращено на кризисные центры помощи женщинам. Таковые осуществляют свою деятельность в различных формах. Наиболее распространенные из них: телефонная линия доверия, очное консультирование специалистами в конкретной области

[1] Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ и от 30 декабря 2008 г. № 7-ФКЗ) // Российская газета. – 1993, 25 декабря; 2009, 21 января.

(психологами, врачами, педагогами, юристами), групповые занятия (психотерапия) и группы взаимной поддержки.

Существует и такая форма помощи, как «шелтеры» – широкая сеть специальных учреждений для пострадавших от насилия в семье. Здесь, если в семье создалась нетерпимая ситуация, женщина может укрыться вместе с детьми. Например, в США деятельность «шелтеров» – одна из самостоятельных специализированных программ помощи жертвам насилия. Как правило, это далеко отстоящие от центра города небольшие уютные здания, адрес которых держится в секрете. Режим здесь свободный, некоторые женщины даже продолжают работать в период пребывания в «шелтере». Все построено на принципах самообслуживания; женщины обеспечены бесплатным питанием и медицинской помощью. Средняя наполняемость «шелтеров» составляет 30–50 человек, а продолжительность пребывания в них – от 2 до 5 недель. Одна из главных задач сотрудников служб помощи потерпевшим – психологическая реабилитация и правовая помощь; здесь подробно разъясняются права женщины и ребенка, а в случаях неизбежности развода оказывается практическая помощь[1].

В Российской Федерации также получила распространение практика создания таких кризисных центров. В 1997 г. по данному поводу даже было принято Постановление Минтруда РФ от 10 июля 1997 г. № 40, которое утверждало Примерное положение о Кризисном центре помощи женщинам (далее – Положение)[2]. Оно определило кризисный центр помощи женщинам (далее – Центр) как учреждение государственной (муниципальной) системы социального обслуживания населения, предназначенное для оказания женщинам, находящимся в кризисной ситуации, социальной помощи различных видов.

По Положению Центр создается, реорганизуется и ликвидируется местными органами исполнительной власти по согласованию с соответствующими территориальными органами социальной защиты населения. Участие органов социальной защиты населения субъектов Российской Федерации в деятельности Центров определено как координационное и организационно-методическое.

Центр организуется и содержится за счет средств, предусмотренных бюджетами субъектов Российской Федерации, местными бюджетами, а также за счет доходов от хозяйственной и иной деятельности Центра и других внебюджетных поступлений.

Положение предъявило требование к размещению Центра в специальных помещениях, которые должны соответствовать реализации цели и задач этого учреждения и располагать всеми необходимыми видами коммуникаций (отопление, водопровод, канализация, электричество, газ, радио, телефон и пр.), отвечать санитарно-гигиеническим нормам, противопожарным требованиям.

---

[1] Егорова М.Б., Спиридонова Г.И. Кризисные центры как форма помощи подвергшимся насилию в семье // http://www.rusnauka.com/1_NIO_2013/Psihologia/7_124924.doc.htm

[2] Бюллетень Минтруда РФ. – 1997. – № 8. Минюстом РФ отказано в регистрации данного документа (Бюллетень Минюста РФ. – 1998. – № 5-6; письмо Минюста РФ от 15 мая 1998 г. № 3272-ПК).

Статусно Центр является юридическим лицом, имеет собственное имущество, самостоятельный баланс, печать, бланк со своим наименованием, открывает счета в банках (включая валютные), в том числе внебюджетный счет для поступления средств от предприятий и организаций, общественных объединений и граждан.

Целью создания Центра является оказание психологической, юридической, педагогической, социальной и др. помощи женщинам, находящимся в кризисном и опасном для физического и душевного здоровья состоянии или подвергшимся психофизическому насилию.

Основными задачами Центра в этой связи являются: создание необходимых условий для обеспечения максимально полной социально-психологической реабилитации и адаптации в обществе, семье; привлечение различных государственных органов и общественных объединений к решению вопросов социальной помощи женщинам, оказавшимся в трудной жизненной ситуации, и координация их деятельности в этом направлении.

Деятельность Центра направлена на: выявление совместно с государственными органами и общественными объединениями (органами и учреждениями образования, здравоохранения, внутренних дел, по делам молодежи, занятости, миграции, комитетами Общества Красного Креста, ассоциациями многодетных, неполных семей, обществами инвалидов и другими) женщин, остро нуждающихся в незамедлительной социальной защите и помощи; предоставление клиентам Центра необходимых социальных услуг разового или постоянного характера; поддержка женщин в решении проблем мобилизации их собственных возможностей и внутренних ресурсов по преодолению сложных жизненных ситуаций; социальный патронаж женщин, нуждающихся в социальной помощи, реабилитации и поддержке, предоставление временного приюта; повышение стрессоустойчивости и психологической культуры населения, особенно в сфере межличностного, семейного, родительского общения; помощь женщинам в создании в семье атмосферы взаимопонимания и взаимного уважения, благоприятного микроклимата, преодолении конфликтов и иных нарушений супружеских и внутрисемейных отношений; социально-психологическая помощь женщинам в социальной адаптации к изменяющимся социально-экономическим условиям жизни; рекламно-пропагандистская работа (распространение информации о задачах и перечне услуг, оказываемых Центром, пропаганда в местных средствах массовой информации о деятельности Центра).

В качестве субъектов, которым Центр оказывает социальные услуги определены следующие категории женщин: подвергшиеся психофизическому насилию; потерявшие родных и близких (вдовы); имеющие детей-инвалидов; женщины-инвалиды; одинокие матери с несовершеннолетними детьми; несовершеннолетние матери; беременные женщины, в т.ч. несовершеннолетние и одинокие; женщины из неполных семей; находящиеся в предразводной и послеразводной ситуации; находящиеся в конфликте с семьей; находящиеся в отпуске по уходу за ребенком; самостоятельно проживающие выпускницы детских домов и школ-интернатов; женщины, вышедшим на пенсию и испыты-

вающим психологический дискомфорт, в т.ч. одинокие пожилые женщины, брошенным детьми.

Отмечено, что Центр может оказывать социальные услуги женщинам как обратившимся по собственной инициативе, так и по направлению органов системы социальной защиты населения, образования, здравоохранения, внутренних дел, по труду и занятости, миграции и других.

Социальные услуги оказываются Центром, как правило, бесплатно, но по решению руководства Центра и местной администрации отдельные виды социальных услуг могут предоставляться за плату. Денежные средства, взимаемые за предоставление этих социальных услуг, зачисляются на счет Центра и направляются на его развитие, улучшение социального обслуживания клиентов сверх выделяемых ассигнований по бюджету.

Положительной чертой рассматриваемого документа следует считать определенную в нем структуру подразделений Центра. Так, Центр может иметь отделение дневного пребывания и стационарное отделение.

Первое предназначается для: диагностики состояния женщин; разработки мероприятий по реабилитации женщин и координации их выполнения; оказания экстренной психологической помощи по телефону доверия; организации поэтапного выполнения мероприятий по реабилитации женщин; оказания женщинам медико-социальной, психолого-педагогической, юридической, бытовой помощи; проведения досуговых мероприятий (в т.ч. с целью профилактики); индивидуальной работы с клиентами по предупреждению и избавлению от вредных привычек, по подготовке к созданию семьи и рождению ребенка; консультирования по медико-социальным вопросам (планирование семьи, современные средства контрацепции, гигиена питания и жилища, избавление от избыточного веса, вредных привычек, сексуальные расстройства, психосексуальное развитие и др.); содействия в направлении в специализированные учреждения лиц, требующих лечения в специализированных учреждениях органов здравоохранения.

Стационарное отделение создается для пребывания в нем женщин и обеспечивает бытовые, психологические и прочие условия их жизнедеятельности на срок не более двух месяцев.

Основными направлениями деятельности отделения являются: обеспечение доступной, своевременной и эффективной помощи женщинам, нуждающимся во временном приюте; оказание квалифицированного и разностороннего (психологического, педагогического, медицинского, юридического и др.) консультирования в зависимости от конкретных причин социальной дискомфортности; проведение индивидуальных диагностических бесед с целью выявления актуальных проблем и степени психологического стресса, помощь в их разрешении, педагогической коррекции, медико-социальной адаптации и реабилитации; предоставление бесплатного питания; содействие в принятии юридического решения об изменении или создании новых условий дальнейшей жизнедеятельности женщин в семье, на работе или иной среде жизнедеятельности; привлечение к сотрудничеству организаций, индивидуальных лиц, способных оказать моральную, методическую или финансовую поддержку.

В Положении также определены сроки пребывания женщин в Центре – в зависимости от конкретных обстоятельств и индивидуальных особенностей обратившихся за помощью женщин, но не более двух месяцев. При этом оказание помощи женщинам осуществляется в любое время суток.

Независимо от места жительства любая женщина в Центре может получить первичную консультацию специалистов.

Отметим, что указанное Положение было утверждено только в 1997 г., а многие Центры создавались до принятия этого акта, в силу чего по юридической природе эти структуры являются институтами гражданского общества. Уточним, что и в настоящее время количественно число общественных кризисных центров преобладает над муниципальными. Данную ситуацию, на наш взгляд, можно объяснить доверием женщин именно общественным организациям, так как небезызвестны факты бездействия представителей публичных властных структур. Также немаловажным здесь является механизм обращения и последующей процедуры оказания помощи – в общественных организациях он менее формализован.

В целом, все-таки следует отметить тенденцию создания муниципальных и общественных кризисных центров в различных регионах Российской Федерации. Для подтверждения приведенного тезиса представим некоторый опыт деятельности таких Центров.

Например, с 21 октября 2012 г. в городе Старый Оскол Белгородской области действует Кризисный центр помощи женщинам, оказавшимся в трудной жизненной ситуации. Центр как некоммерческая общественная организация был создан при участии администрации Старооскольского округа и духовенства города.

Данный проект впервые реализовывается в городе Старый Оскол.

На момент открытия в нем находилось трое женщин с младенцами.

За время работы Центр доказал свою эффективность, появились первые положительные результаты: отец признал родившегося ребенка и забрал женщину и малыша домой; постепенно налаживаются отношения с родственниками у других молодых мам.

Как правило, женщинам, которые оказались в непростой жизненной ситуации, кроме психологической и материальной поддержки, требуется помощь в оформлении необходимых документов для получения предусмотренных выплат по рождению ребенка, бесплатного питания на детей. В настоящее время руководители Кризисного центра продумывают варианты оформления женщинам-матерям временной регистрации, чтобы они могли получать социальные выплаты и пособие на детей, а в дальнейшем устроить ребенка в детский и сад и найти работу[1].

В качестве положительного опыта следует привести деятельность Кризисной службы помощи женщинам города Лангепас Тюменской области. Инициатива создания этой структуры принадлежала администрации города, от

[1] http://www.beleparh.ru/index.php/novosti/57-drugie-novosti/2043-krizisnyj-tsentr-pervye-polozhitelnye-rezultaty

имени которой выступало муниципальное учреждение «Центр по проблемам семьи». Финансирование ее осуществляется городским бюджетом.

Сведения, полученные в органах внутренних дел г. Лангепаса, показали, что каждый день три-четыре женщины обязательно обращаются в правоохранительные органы с просьбой защитить их от домашнего насилия. Кроме того, социальные службы обладали достаточной информацией о том, что в городе имеются неблагополучные семьи, где женщины с детьми часто подвергаются насилию со стороны мужей, есть семьи, где не складываются взаимоотношения между мужем и женой, детьми и стариками-родителями.

Благодаря инициативе населения и активности мэра в 1997 г. в Лангепасе был создан муниципальный Кризисный центр. Он включает в себя две службы – телефон доверия и убежище для женщин, переживших домашнее насилие. В убежище (это уютная пятикомнатная квартира, адрес которой не сообщается в целях безопасности жертв насилия и персонала приюта) одновременно могут укрыться от семейных проблем семь человек. Женщинам здесь созданы все необходимые для проживания условия.

Максимальный срок пребывания был увеличен с семи дней до четырнадцати, так как одной недели для решения конфликта явно не достаточно. В некоторых случаях срок пребывания может быть продлен.

Одним из направлений работы Кризисного центра является подготовка и распространение брошюр «Личная безопасность женщин и девушек». Специально для проведения лекций в органах внутренних дел сотрудники Центра составили памятку для полицейского «Что делать, если к Вам обратилась женщина, пережившая насилие».

Основную помощь женщинам оказывают социальные работники и психологи Кризисного центра. Иногда при необходимости привлекаются работники здравоохранения, образования и сотрудники органов внутренних дел. Существенным недостатком в работе Центра, по мнению его заведующей И. А. Миланович, является отсутствие юриста и невозможность оказания квалифицированной юридической помощи. Следующим шагом в совершенствовании деятельности Кризисного центра будет привлечение юристов и создание в нем специализированной бесплатной юридической консультации[1].

Следует также указать на деятельность Кризисного центра для женщин «Приют» в городе Мурманск (неправительственная благотворительная организация в форме общественного учреждения) с 20 апреля 1997 г. Он учрежден Конгрессом женщин Кольского полуострова и группой женщин-добровольцев «Телефона доверия для женщин», который работал на общественных началах с весны 1995 г. Центр имеет собственное помещение, приобретенное на средства гранта.

Открытие Кризисного центра – результат российско-норвежского партнерств женских неправительственных организаций Мурманска и Тромсе.

Основные задачи центра: предоставлять убежище женщинам в возрасте от 18 до 55 лет, в случае необходимости и женщинам с детьми, на период от 1

[1] http://soc-work.ru/article/650

до 7 суток; вести просветительскую работу среди населения; вести телефонное консультирование; предоставлять женщинам полную информацию о социальной, психологической, юридической и медицинской помощи.

Для продолжения работы по предотвращению домашнего насилия, начатой в 1996 г. Екатеринбургский Женский Центр открыл в 1998 г. Кризисный Центр «Екатерина». В мае 1998 г. центр стал членом Российской Ассоциации Женских Кризисных Центров, а с мая 2000 г. в Центре начал работу телефон доверия. В это же время центр начал предоставлять юридические и психологические консультации женщинам, попавшим в кризисные ситуации, и регулярно проводит группы поддержки для женщин.

В рамках рассматриваемых укажем и Женский Кризисный Центр «Майя», который начал свою работу в октябре 1999 г. и был официально зарегистрирован как неправительственная правозащитная организация в мае 2000 г. Центр является членом Российской Ассоциации Женских Кризисных Центров и Сети Кризисных Центров Баренц региона. Сеть объединяет муниципальные и общественные кризисные центры для женщин в Швеции, Норвегии, Финляндии и Северо-западном регионе России.

Основные направления деятельности центра: проведение информационных кампаний с целью предотвращения торговли людьми; повышение осведомленности о проблеме насилия над женщиной; оказание помощи женщинам в защите их прав и интересов; предоставление юридических и психологических консультаций жертвам; поддержка женских инициатив и взаимодействие с неправительственными правозащитными организациями и государственными структурами региона; создание и поддержка базы данных организаций и служб, которые могут предоставить помощь и поддержку клиентам кризисного центра.

Кризисный центр тесно сотрудничает с общественными организациями и муниципальными службами, такими как Центр социальной помощи населению, приют для женщин и детей, Республиканский центр социальной поддержки семьи и детей «САМПО» и др. Центр заключил кооперативные соглашения с Министерством Внутренних дел Карелии, Городским комитетом по международным связям, Государственным университетом Петрозаводска и другими организациями для реализации совместных проектов и оказания консультативной помощи.

Приведенные кризисные центры составляют далеко неисчерпывающий перечень подобного рода организаций в Росси и своим опытом доказывают необходимость создания таковых по всей стране. Несмотря на то, что на данном этапе деятельность Центров носит специализированный характер (предотвращение насилия над женщинами), полагаем, что эти организации могут быть и универсальными в контексте обеспечения прав женщин.

Представленный анализ показал, что опыт создания кризисных центров более характерен для институтов гражданского общества, нежели публичных властных структур, в частности на муниципальном уровне. Полагаем, сложившаяся ситуация не является основанием для ее принципиальной корректировки, так как институты гражданского общества в этой части более востребованы у населения. Вместе с тем, считаем, есть направления и для совершенствования:

утверждение Положения о кризисных центрах помощи женщинам на уровне Правительства Российской Федерации, как органа государственной власти универсальной межотраслевой компетенции. Такое предложение связываем с тем, что ныне действующее Положение 1997 г. не зарегистрировано в Минюсте, поэтому у граждан, не обладающих специальными юридическими знаниями, данный факт вызывает сомнения относительно правоприменения; активизация деятельности по созданию муниципальных кризисных центров помощи женщинам. Не случаен именно данный уровень, так как органы местного самоуправления – наиболее близки к населению и призваны максимально быстро и эффективно решать по существу вопросы своей юрисдикции; в целях упорядочивания и унификации деятельности общественных кризисных центров помощи женщинам, представляется целесообразным принятие рамочного положения на федеральном уровне относительно указанных структур; обязательное наличие юриста или юридической службы в рассматриваемых Центрах; заключение соглашений о сотрудничестве между кризисными центрами помощи женщинам (муниципального и общественного характерами) с публичными властными структурами для своевременного решения вопросов, находящихся в ведении органов государственной власти и местного самоуправления; популяризация и информирование населения о деятельности кризисных центров помощи женщинам, в том числе посредством создания специальных сайтов в сети Интернет.

Насонова В.А.

ОБЗОР ПРАВОВЫХ ОСНОВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье рассмотрены правовые основы защиты персональных данных в информационных системах.

Ключевые слова: персональные данные, информационная система персональных данных, защита информации, классы информационных систем персональных данных.

Abstract. This paper examines the legal framework for the protection of personal data in information systems.

Key words: personal data, personal data information systems, information security, the classes of information systems of personal data.

Последние десятилетия с развитием информационно-телекоммуникационных систем вопросы защиты информации и регулирование сетевых ресурсов приобретают все большие масштабы. С учетом роста проблем, связанных с использованием сетей наряду с развитием технических аспектов формируется и законодательство. Так, например, в закон о защите детей от вредоносной информации[1] могут быть внесены поправки, обязывающие провайдеров информировать покупателей о системах родительского контроля при продаже пакета подключения. Все так же, непростым вопросом, остается защита персональных данных от утечки в информационных системах.

Российское законодательство в сфере защиты персональный данных (ПДн) предлагает следующие основные нормативно-правовые акты, без учета ведомственных:

- Федеральный закон от 27.06.2006 №152-ФЗ (ред. От 25.07.2011) «О персональных данных». Закон регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и доступ к таким персональным данным;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

[1] ФЗ РФ от 29.12.2010 № 436-ФЗ (ред. 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» – Российская газета, № 297, 31.12.2010.

- Приказ ФСТЭК, ФСБ и МинИнформСвязи от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства РФ 18.09.2012 № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Федеральная служба по техническому и экспортному контролю России (ФСТЭК) в области персональных данных формирует следующие нормативно-методические документы:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Настоящая «Базовая модель...» содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия для нарушения безопасности персональных данных, которое ведет к ущербу жизненно важных интересов личности, общества и государства;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методика предназначена для использования при проведении работ по обеспечению безопасности ПДн при их обработке в следующих автоматизированных информационных системах персональных данных (ИСПДн): государственных или муниципальных ИСПДн; ИСПДн, создаваемых и эксплуатируемых предприятиями, организациями и учреждениями независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением; ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд;
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Положение устанавливает основные принципы, ор-

ганизационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации;

- Руководящий документ Защита информации. Специальные защитные знаки. Классификация и общие требования. Руководящий документ устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки;
- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90. Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.
- «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Руководящий документ устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.
- Руководящий документ Защита от несанкционированного доступа к информации. Термины и определения. Документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
- Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». Положение устанавливает единый на территории Российской Федерации порядок исследований и разработок в области: защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от несанкционированного доступа; создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения информации за счет НСД, в том числе программных и технических средств защиты информации от НСД; -создания программных и технических средств защиты информации от НСД в составе систем защиты секретной информации в создаваемых АС;
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа, являющейся частью общей проблемы безопасности информации.

• Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. приказом Государственной технической комиссии при Президенте РФ от 27.10.1995 № 199). Положение устанавливает организационную структуру Системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации. В приложениях к настоящему Положению приведены перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации, сертификата и лицензии на применение знака соответствия.

• Приказ Федеральной службы по техническому и экспортному контролю от 5.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, или лицом, которому на основании договора оператор поручает обработку персональных данных.

После вступления в силу требований закона «О защите персональных данных», согласно которым личные сведения сотрудников, посетителей или клиентов, такие как ФИО, дата и место рождения, адрес и другие данные, должны быть защищены от несанкционированного доступа. Для исполнения требований закона все организации, оперирующие персональными данными, должны принять ряд организационных мер, а также использовать сертифицированные средства защиты.

Исходя из приведенных выше нормативных правовых актов при обработке персональных данных в информационной системе должны быть выполнены следующие действия:

• проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и передачи их лицам, не имеющим права доступа к такой информации;

• своевременное обнаружение фактов несанкционированного доступа к персональным данным;

• недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

• возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль за обеспечением уровня защищенности персональных данных.

Все указанные требования по обеспечению защиты обрабатываемых персональных данных должны выполняться в соответствии с классификацией таких систем. Порядком определены 4 класса информационных систем персональных данных (ИСПДн):

- класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Классификация ИСПДн осуществляется с учетом категорий ($Х_{ПД}$) и объема обрабатываемых персональных данных ($Х_{НПД}$)

- категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 – обезличенные и общедоступные персональные данные.

В соответствии с объемом обрабатываемых в ИСПДн персональных данных разбит на три группы:

- группа 1 – более чем 100 000 субъектов;
- группа 2 – от 1000 до 100 000 субъектов;
- группа 3 – менее чем 1000 субъектов.

$Х_{ПД}$	Группа 1	Группа 2	Группа 3
категория 4	К4		
категория 3	К2	К3	
категория 2	К1	К2	К3
категория 1	К1		

По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Класс информационной системы определяется в соответствии с представленной таблицей на следующей странице.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности, защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий.

К специальным информационным системам ИСПДн относятся:

- информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов ПДн;
- информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

Количество субъектов ПДн в системе (Хнпд) Категория обрабатываемых ПДн (Хпд)	Хнпд = 1			Хнпд = 2				Хнпд = 3	
	Более 100 000 ПДн	В объеме РФ	В объеме субъекта РФ	От 1000 до 100 000 ПДн	В объеме отрасли	В объеме органа власти	В объеме муницип. образования	До 1000 ПДн	В объеме одной организации
Хпд= 1 (расовая, нац. принадлежность…)	**К1**								
Хпд = 2 (ПДн субъекта, позволяющие идентифицировать и получить допол. инф.)	**К1**			**К2**				**К3**	
Хпд = 3 (ПДн, позволяющие идентифицировать)	**К2**			**К3**					
Хпд = 4 (обезличенные и общедоступ ПДн)	**К4**								

Применительно к специальным информационным системам после определения класса системы оператором должна быть разработана модель угроз безопасности персональных данных с использованием методических документов, разрабатываемых в соответствии с пунктом 2 постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и проведена оценка актуальности угроз. По результатам оценки требования по защите информационных системах персональных данных от различных угроз могут быть скорректированы по сравнению с типовыми.

После реализации комплекса мер по защите ПДн, с учетом класса ИСПДн и в соответствии с правовым актами и методическими документами, проводится проверка соответствия ИСПДн требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия, т.е. производится документальное оформление оценки соответствия ИСПДн.

В зависимости от класса ИСПДн устанавливается следующий порядок оценки защищенности:

- К1 и К2 – Оценка соответствия путём обязательной сертификации (аттестации);
- К3 – Оценка соответствия осуществляется по выбору оператора (сертификация или декларирование соответствия);
- К4 – Оценка соответствия не регламентируется и осуществляется по решению оператора ПДн.

По результатам проверки соответствия, для классов К1, К2 и в некоторых случаях К3 выдается «Аттестат соответствия» (сертификат) ИСПДн заявленному классу, для класса К3 и по решению оператора для класса К4 делается Декларация о соответствии характеристик ИСПДн предъявляемым к ней требованиям.

Таким образом, вступившие в силу нормативные правовые акты и иные руководящие документы, регламентируют порядок технической защиты персональных данных.

Невыполнение требований соответствующих правовых актов и нормативных документов ФСБ и ФСТЭК может привести к негативным последствиям для юридических и физических лиц, таким как выплата штрафов, а при определенных условиях возможно приостановление действия или аннулирование лицензий на деятельность по работе с персональными данными.

Технические средства защиты для защиты информационных систем персональных данных должны подбираться с учетом требований регуляторов и класса ИСПДн.

Средства защиты персональных данных должны иметь сертификат по существующим РД уровня «конфиденциально». Также для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации, в том числе и встроенных в общесистемное и прикладное программное обеспечение), должен быть обеспечен соответствующий уровень контроля отсутствия в нем недекларированных возможностей.

Никонова Л.И.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОЛОДЁЖИ: ЗАКОНОДАТЕЛЬНЫЙ ОПЫТ ФРГ

Аннотация. В статье представлен законодательный опыт регулирования вопросов обеспечения информационной безопасности несовершеннолетних в ФРГ. На основе действующего законодательства Германии проанализированы конституционно-правовые гарантии и организационные механизмы защиты детей и молодёжи от негативного влияния информации, которая может причинить вред физическому и психическому здоровью, нравственному, духовному и социальному развитию молодого поколения.

Ключевые слова: информационная безопасность, органы контроля, информация, оказывающая негативное влияние на молодёжь, федеральный закон, государственный договор.

Abstract. The article deals with law-making experience of regulation of providing information security of young people in FRG. Constitutional and legal guarantees and organizational mechanisms of protecting young people and children from negative informational impact which can do harm to physical and mental health , ethical , intellectual and social development of young generation are analyzed on the basis of current legislation of FRG.

Key words: information security, inspection authorities, information making an impact on young people, national law, state treaty.

В сентябре 2012 г. в Российской Федерации вступил в силу Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1]. Как указано в пояснительной записке к законопроекту: актуальность этого нормативного акта «объясняется особой уязвимостью детей, которые в условиях интенсивного развития новых информационных технологий (Интернета, мобильной и иных видов электронной связи, цифрового вещания) в наибольшей степени подвержены негативному информационному воздействию»[2].

Важность данного вопроса давно признана и международным, и российским законодательством (ст. 13, 17 Конвенции ООН о правах ребенка 1989 г.[3], Доктрина информационной безопасности Российской Федерации от 3 сентября 2000 г. № Пр-1895[4], ст. 14 Федерального закона «Об основных гарантиях прав ребенка в Российской Федерации» 1998 г. и др.)[5].

---

[1] Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изм. и доп. от 28 июля 2012 г.) // Собрание законодательства РФ. – 2011. – № 1. – Ст. 48; www.garant.ru

[2] Пояснительная записка к проекту Федерального закона «О защите детей от информации, наносящей вред их здоровью, нравственному и духовному развитию» [Электронный ресурс] //Законодательство и практика масс-медиа. – 2005. – № 4. – Режим доступа: http://law.edu.ru/doc/document.asp?docID=1224620

[3] Конвенция о правах ребенка. Одобрена Генеральной Ассамблеей ООН 20 ноября 1989 г. (вступила в силу для СССР 15 сентября 1990 г.) // Сборник международных договоров СССР. – 1993. – Выпуск XLVI; www.garant.ru

[4] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09 сентября 2000 г. № Пр-1895) // Российская газета. – 2000. – № 187, 28 сентября.

[5] Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (ред. от 3 декабря 2011 г. с изм. и доп. от 01 сентября 2012 г.) // Собрание законодательства РФ. – 1998. – № 31. – Ст. 3802.

Однако до принятия ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в России должным образом не обеспечивалась охрана публично-правовых интересов несовершеннолетних от деструктивного информационного воздействия на них СМИ. И поэтому в отличие от стран Европы и США Российская Федерация почти не имеет опыта правовой защиты информационной безопасности детей. В этой связи особый интерес для исследования представляют конституционно-правовые гарантии и организационные механизмы защиты несовершеннолетних от информации, которая может причинить вред их здоровью и нравственности, действующие в Германии, имеющей значительный практический опыт в данной сфере.

Осознавая значимость и важность защиты и охраны детей и молодежи от негативного влияния информации, поступающей через СМИ, регулирование данного вопроса в Германии осуществляется на конституционном уровне. Статья 5 Основного закона ФРГ 1949 г., провозглашая право каждого «свободно выражать и распространять свое мнение устно, письменно и посредством изображения, а также беспрепятственно черпать информацию из общедоступных источников», вместе с тем очерчивает границы и устанавливает пределы этих прав, которые в соответствии с ч. 2 этой же статьи «указываются предписаниями общих законов, законодательных положений об охране молодежи и правом на честь личности»[1].

Конституции большинства федеральных земель Германии так же содержат положения о том, что одной из основных задач федеральных органов власти земли является защита несовершеннолетних от агрессивного и негативного воздействия на них информации. Поэтому в учредительных актах земель содержатся императивные предписания о соблюдении каждым человеком ограничений, установленных законом об охране молодежи. Например, ст. 18 Конституции земли Гессен гласит, что лицо, нарушающее законы об охране молодежи не может ссылаться на право свободного выражения мнений, распространения научных и художественных произведений и свободу информации[2].

До 2003 г. в ФРГ государственная политика по защите молодежи от негативного воздействия СМИ регулировалась двумя законами: Законом о правовой защите молодежи в общественных местах (Gesetz zum Schutze der Jugend in der Öffentlichkeitc) 1951 г.[3] и Законом о распространении вредной для молодёжи печатной литературы и информации на прочих носителях (GjSM) (Act To

---

[1] Конституции зарубежных государств: Великобритания, Франция, Германия, Италия, США, Япония, Бразилия: учеб. пособие / сост. сб., пер., авт., введ. и вступ. В.В. Маклаков. –7-е изд. перераб и доп. – М.: Изд. Волтерс Клувер, 2010. – С. 169.

[2] Конституция земли Гессен от 1 декабря 1946 г. [Электронный ресурс] // Конституции государств (стран) мира. – Режим доступа: http://worldconstitutions.ru/archives/225

[3] Gesetz zum Schutze der Jugend in der Öffentlichkeit/Закон о правовой защите молодежи в общественных местах Bundesgesetz// Dezember 1951, (BGBl. I S. 936)

Regulate The Dissemination of Writings and Media Contents Harmful to Young Persons) 1953 г. [1]

В соответствии со ст. 1 Закона GjSM 1953 г. все материалы, которые способны нанести ущерб нравственности детей и подростков, включались в специальный список. Критериями включения информационных материалов в список являлись: пропаганда войны и подстрекательство к насилию, приуменьшение пагубного характера смерти, разрушений и бедствий; пропаганда нацистской идеологии, расовой ненависти, милитаризма; дезориентация в сексуально-этическом плане и порнография.

На средства массовой информации (газеты, журналы, производителей книжной продукции, аудио или видеокассет, кинофильмов и др.), чья информационная продукция попала в список опасной для детей и подростков, налагались ограничения. Такие материалы запрещалось предлагать, продавать, давать напрокат или хранить за пределами торговых помещений, в розничной торговле, в киосках или других торговых точках, в библиотеках или читальных залах; распространять с помощью электронных информационных и коммуникационных служб или каким-либо иным способом, осуществлять их публичную презентацию и рекламу.

С 1 апреля 2003 г. в ФРГ действует новый федеральный Закон об охране молодёжи (Jugendschutzgesetz -JuSchG)[2] куда частично вошли нормы Закона о распространении вредной для молодёжи печатной литературы и информации на прочих носителях (GjSM) 1953 г.

Одновременно с ним вступил в силу, заключенный в 2002 г. премьер-министрами земель и Федеральным правительством, Государственный договор о защите подростков от негативного влияния масс-медиа (Jugend Medien Schutz Vertrag (JMStV))[3], который создал единую правовую систему в ФРГ по защите юношества в сфере электронных СМИ (интернет, телевидение, радио).

До этого частное телерадиовещание в землях ФРГ контролировалось специализированными земельными ведомствами по делам СМИ, учрежденными в каждой федеральной земле, осуществляющими лицензирование вещания и контроль за соблюдением частными вещателями условий лицензий и законодательства при подготовке программ[4].

Владельцы частных каналов должны были соблюдать нормы Государственного договора об информационных и телекоммуникационных службах, за-

---

[1] Act to regulate the dissemination of writings and media contents harmful to young persons (Gesetz uber die Verbreitung jugendgefahrdender Schriften und Medieninhalte, GjSM). URL: – Режим доступа: http://www.iuscomp.org/gla/.

[2] Jugendschutzgesetz (JuSchG) vom 23. Juli 2002 (BGBl. I S. 2730, 2003 I S. 476), geandert durch Artikel 3 des Gesetzes vom 31. Oktober 2008 (BGBl. I S. 2149)// http://www.bmfsfj.de/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/juSchGrussisch,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf

[3] Jugend Medien Schutz Vertrag (JMStV) Juli 2002 (BGBl. I S. 2730, 2003 I S. 476)

[4] Кобзева, С.В. Сравнительно-правовой анализ регулирования оборота вредной информации в телерадиовещании и кинопрокате [Электронный ресурс]// Юридическая библиотека «Юристлиб», 2010. http://www.juristlib.ru/book_8849.html

ключенного правительством ФРГ с представителями средств массовой информации от 1 августа 1997 г. (Informations und Kommunikationsdienste Gesetz)[1]. В случае особо грубых нарушений закона соответствующее земельное ведомство имело право отобрать лицензию у той или иной телерадиокомпании. Таким образом, правовые основы и компетенция контролирующих органов не были едиными для всех немецких земель.

В настоящее время в соответствии с федеральным Законом об охране молодёжи (Jugendschutzgesetz) и Государственным договором о защите подростков от негативного влияния масс-медиа (Jugend Medien Schutz Vertrag (JMStV) установлены единые правовые стандарты для федеральных и земельных ведомств.

Государственный договор определят, что противозаконно распространение той информации, которая запрещена Уголовным Кодексом ФРГ, а именно, порнографии (§ 184 УК ФРГ) и изображения насилия (§131 УК ФРГ). Кроме того, поставщики услуг масс-медиа обязаны создать условия для того, чтобы дети соответствующего возраста не могли получить доступ к контенту, способному нанести вред их развитию. Соблюдение этих требований возможно посредством использования системы размещения программ в сетке вещания в зависимости от контента либо посредством других мер, например таких, как блокирующее контент программное обеспечение.

Общественно-правовые организации, вещание которых распространяется на территорию более чем одной земли, обязаны иметь штатного работника, на которого возложена ответственность за обеспечение защиты и безопасности детей[2].

Органом, контролирующим информацию, оказывающую негативное влияние на молодёжь, на уровне Федерации является Федеральное ведомство по проверке материалов, вредных для молодежи (Federal Department for Media Harmful to Young Persons или Bundesprüfstelle für jugendgefährdende Medien (BPjM), созданное еще в 1954 г. в Бонне. При назначении состава сотрудников данного ведомства по Закону об охране молодёжи (Jugendschutzgesetz) 2003 г. непосредственное участие принимает Министерство по делам семьи, престарелых, женщин и молодежи.

В соответствии с § 19 раз. 4 Закона Германии о защите молодежи Министерство по делам семьи, престарелых, женщин и молодежи назначает Председателя контрольного органа и экспертов в области изобразительного искусства, литературы, книготорговли и издательского дела; представителей добровольных молодёжных и общественных организации; представителей педагогических коллективов; служителей церкви, еврейской общины и других религиозных общин и т.д. Также в состав этого Федерального ведомства входят по одному

---

[1]Informations und Kommunikationsdienste Gesetz Bundesgesetzblatt 1997 I 1870. URL: http://www.iuscomp.org/gla/

[2] Ефимова, Л.Л. Опыт Германии по защите детей от вредной информации / Л.Л. Ефимова // Правовые и криминологические проблемы защиты прав несовершеннолетних Ч. 1. Академия Генеральной прокуратуры РФ. – М., 2008. – С. 73.

представителю от каждой федеральной земли, назначаемые соответствующим земельным правительством.

Согласно абз. 5 § 19 раз. 4 Закона возглавляемый Председателем Совет (из 12 членов) 2/3 выносит решение об отнесении представленного в Федеральное ведомство материала к опасным или угрожающим развитию молодёжи и вносит его в список.

Список носителей информации, оказывающих негативное влияние на молодёжь, делится на четыре части (абз. 2 § 18 Jugendschutzgesetz):

Часть А (публичный список носителей информации).

Часть В (публичный список носителей информации, распространение которых категорически запрещено). В него включаются носители информации, если они содержат материалы антиконституционных организаций, пропагандирующие идеи национал-социализма, расизма, прославляющие насилие, приуменьшающие его пагубное влияние и т.д., и все что запрещено § 86, § 130, § 130а, § 131, § 184а, § 184б и § 184в Уголовного кодекса ФРГ.

В часть С (закрытый список носителей информации) включаются те носители информации, которые не включены в часть А.

Часть D (закрытый список носителей информации, распространение которых категорически запрещено).

Периодические издания могут вноситься в этот список на срок от 3 до 12 месяцев. Но в законе сделано исключение для ежедневных газет и политических журналов, также запрещено «индексировать» носители информации, посвященные искусству и науке.

Рассматривая соотношение свободы творчества и вреда, который может быть причинен молодежи по ее вине, О.В. Пристанская пишет, что эта проблема в Германии «решается на основе взвешивания указанных правовых ценностей. Наряду с компетентной профессиональной оценкой художественной ценности произведения предписывается «принимать во внимание и реальное влияние произведения искусства», а также то, что «несовершеннолетние могут видеть его по-другому, нежели взрослые». Если будет установлено, что вред для молодежи перевешивает чашу весов, то произведения искусства можно включать в список запрещенных для распространения среди молодежи материалов»[1].

Самостоятельно Федеральный ведомство (§ 21) действовать не может, оно начинает делопроизводство, только тогда, когда ему будет подано соответствующее заявление. По абз. 2 § 21 право подать такое заявление имеют: Федеральное министерство по вопросам семьи, пожилых людей, женщин и молодёжи; высшие органы по делам молодёжи федеральных земель; центральный ор-

[1] Пристанская, О.В. Международно-правовые основы защиты детей от информации, наносящей вред их здоровью, нравственному и духовному развитию // Правовые и криминологические проблемы защиты прав несовершеннолетних. Ч. I: Сб. науч. тр. / [О.В. Пристанская и др.]; Акад. Ген. прокуратуры РФ. – М., 2008. – С. 69.

ган надзора федеральных земель по охране молодёжи в области СМИ; управления по делам молодёжи федеральных земель; местные управления по делам молодёжи[1].

Еще одним органом, осуществляющим контроль за поставщиками услуг масс-медиа, действующим на федеральном уровне является Комиссия по защите молодежи в электронных СМИ. Комиссия состоит из 6 директоров органов земель по контролю за деятельностью СМИ и 6 экспертов, назначенных федеральным правительством и правительствами земель.

В ноябре 2003 г. Комиссия по защите молодежи и органы федеральных земель, контролирующие СМИ, утвердили основные правила защиты детей от негативной информации и одобрили «Положение об обеспечении защиты детей при цифровом распространении программ частного телевидения», которым устанавливается обязательность специального кодирования сигнала цифрового телевидения. Наблюдение за деятельностью вещателей и поставщиков услуг теле-медиа осуществляют соответствующие органы земель по контролю в сфере СМИ (Государственный договор 2003 г.) [2]. Они же в соответствии с абз. 2 §14 Закона Германии о защите молодежи проводят индексацию фильмов, кинопрограмм и игровых программ:

1. «Разрешено без возрастного ограничения»;
2. «Детям до 6 лет не разрешается»;
3. «Детям до 12 лет не разрешается»;
4. «Лицам до 16 лет не разрешается»;
5. «Лицам до 18 лет не разрешается».

Кроме земельных органов, контролирующих СМИ, право осуществлять индексацию имеют организации добровольного самоконтроля.

Федеральные органы власти земли имею право принимать нормативные акты, касающиеся деятельности таких саморегулируемых организаций. Необходимо отметить, что для реализации своих функций этим организациям нужно пройти обязательную сертификацию. Сертификат выдается организации, удовлетворяющей критериям ст. 19 (3) Jugend Medien Schutz Vertrag (JMStV) на четыре года и может быть продлен Комиссией по защите молодежи в электронных СМИ. Комиссия может также и отозвать сертификат, если орган саморегулирования не отвечает установленным требованиям.

---

[1] Jugendschutzgesetz (JuSchG) vom 23. Juli 2002 (BGBl. I S. 2730, 2003 I S. 476), geandert durch Artikel 3 des Gesetzes vom 31. Oktober 2008 (BGBl. I S. 2149)// http://www.bmfsfj.de/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/juSchGrussisch,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf

[2] Ефимова, Л.Л. Опыт Германии по защите детей от вредной информации / Л.Л. Ефимова // Правовые и криминологические проблемы защиты прав несовершеннолетних Ч. 1. Академия Генеральной прокуратуры РФ.– М., 2008. – С. 73.

Так, с 2004 г. в Германии действует негосударственная «Ассоциация добровольного мониторинга провайдеров мультимедийных услуг»[1], выполняющая функции саморегулирующего органа. Большинство поисковых систем, включая Google, Lycos Europe, MSN Deutschland, AOL Deutschland, Yahoo!, T-Online и T-info, присоединились к соглашению «Добровольный самоконтроль для мультимедийных сервис-провайдеров» (Voluntary Self-Control for Multimedia Service Providers)[2]. Эти организации фильтруют Интернет-сайты на основе списка, который создается Федеральным ведомством[3].

Таким образом, информационная безопасность молодежи в Германии обеспечивается посредством детально разработанной системы законодательных актов федерального уровня, внутригосударственных договоров и регионального законодательства.

[1] Association for the Voluntary Self-Monitoring of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter – FSM) – Режим доступа: www.fsm.de/en/

[2] Voluntary Self-Control for Multimedia Service Providers. Complaint Rules for the Association Freiwillige Selbstkontrolle Multimedia e.V. Status: 4 May 2004 – http://www.fsm.de/en/Complaint_Rules

[3] Кобзева, С.В. Модели защиты прав несовершеннолетних в сети интернет: мировой опыт и рекомендации для России / Доклад на X Международной конференции «Право и Интернет» [Электронный ресурс] – Режим доступа: http://www.ifap.ru/pi/10

Новикова А.Е.

РОЛЬ МЕЖОТРАСЛЕВОЙ КОНВЕРГЕНЦИИ В РАЗВИТИИ КАТЕГОРИИ «РИСК»

Аннотация. В данной работе представлен авторский анализ развития категории риск в различных областях гуманитарных знаний. Круг исследований, занимающихся рисками в целом и разработкой способов снижения их уровней или сглаживанием негативных последствий, чрезвычайно широк и охватывает самые разнообразные направления знаний. При этом с развитием цивилизации становится все более очевидным, что интерес к фактору риска не только не ослабевает, а, наоборот, набирает силу. На основе проведенного исследования автором предложено общие концептуальные положения, раскрывающие смысл и содержание категории риск, считать базисом разрабатываемой теории правозащитных рисков.

Ключевые слова: риск, вероятность, неопределенность, философия, социология, экономика.

Abstract. This paper presents the author's analysis of the risk categories in different areas of human knowledge. Range of studies dealing with risk management in general, and developing ways to reduce their levels or offset the negative consequences, is extremely wide and covers a variety of areas of knowledge. In this case, the development of civilization is becoming increasingly clear that the interest in the risk factor is not only not diminished, but rather, is gaining momentum. Based on the research the authors proposed a common conceptual provisions on the meaning and content of the risk categories, consider a basis to develop the theory of human rights risks.

Key words: risk, chance, uncertainty, philosophy, sociology and economics.

Современное российское общество характеризуется достаточной степенью самостоятельности и инициативности граждан в различных сферах. Естественно, что всякая деятельность вынуждает идти на риск для достижения определенной цели.

Риск относится к тем категориям, которые, во-первых, имманентно сопровождают жизнь человека; во-вторых, связаны практически со всеми сферами жизнедеятельности; в-третьих, исследуются разными областями знаний; в-четвертых, довольно активно расширяют масштабы своего проявления. Риски разной природы могут способствовать нейтрализации или усилению последствий друг друга[1].

Таким образом, риск представляет собой явление, с которым человек сталкивается постоянно и в этой связи вынужден с ним считаться. Он настолько широко распространен в обществе, насколько велик круг направлений действий, осознанно осуществляемых человеком, и количество обстоятельств, которые воспринимаются людьми как способные отклонить фактические результаты их действий от намеченных. Не случайно, поэтому круг исследований, занимающихся рисками и разработкой способов снижения их уровней или сглаживанием их негативных последствий, чрезвычайно широк и охватывает самые разнообразные направления знаний. При этом с развитием цивилизации стано-

[1] Бутяев А.Г. Макроэкономические детерминанты государственной политики России по минимизации интеграционных экономических рисков. Монография. – Ростов-на-Дону: Ростиздат, 2007. – С. 19.

вится все более очевидным, что интерес к фактору риска не только не ослабевает, а, наоборот, набирает силу. Данное обстоятельство, на наш взгляд, логично вытекает из самой природы риска как явления, имеющего не только объективную, но и субъективную природу. Если объективно фактор риска обуславливается неопределенностью как неизбежным свойством окружающей человека реальности, то субъективная природа фактора риска определяется тем, что оценить вероятность тех или иных результатов, просчитать шансы на удачу или неудачу может только наделенный сознанием субъект. Как подчеркивает Н. Луман, «Сам по себе внешний мир не знает никакого риска, ибо ему неведомы ни различия, ни ожидания, ни оценки, ни вероятности ...»[1]. Но если риск – это субъективное ощущение и субъективная оценка опасности, то неизбежность усиления фактора риска следует уже из тог, что всякое увеличение накопленного знания автоматически ведет к расширению непознанного. Весьма убедительным в этом отношении представляется использование одной из наиболее известных и одновременно древних философских моделей – так называемой «сферы Аристотеля»[2]. Внутренность этой сферы, ее объем символизирует накопленное знание, а ее поверхность – это неизвестное, что окружает человека. Чем больше человек узнает, тем больше радиус этой сферы и ее площадь и тем, соответственно, больше и разнообразнее объемы окружающего неизвестного. поскольку неизвестное практически всегда воспринимается человеком как потенциальная угроза, то и круг осознаваемых рисков не может не расширяться. Кроме того, сама повседневная практика существования человеческого общества дает колоссальное количество подтверждений того, что никакие успехи в области науки, техники, медицины, страхового дела ни в состоянии устранить из жизни людей этот тревожащий фактор. Более того, именно при современном, самом высоком за всю историю человечества, уровне развития науки и техники пришло осознание того, что сам факт существования человеческой цивилизации – это область глобального риска, и у человечества нет способа защиты от него.

Данный тезис подчеркивает необходимость специального изучения сущности феномена риска с учетом его видовых особенностей для более результативной минимизации негативных последствий.

О риске сегодня говорят специалисты самых разных дисциплин, соответственно, существует многообразие подходов к определению риска с учетом сферы исследования и приложения.

С философской точки зрения «риск» – это возможность возникновения неблагоприятных и нежелательных последствий деятельности самого субъекта[3].

---

[1] Луман Н. Понятие риска // THESIS. – 1994. – № 5. – С. 139.

[2] Братимов О.В., горский Ю.М., Делягин М.Г., Коваленко А.А. Практика глобализации: игры и правила новой эпохи. – М.: ИНФРА-М, 2000. – С. 77.

[3] Алехнович С.О. К вопросу об изменении подходов к теории и практике национальной безопасности // Международное публичное и частное право. – 2007. – № 4.

Для социологической науки также характерно обращение к исследованию категории «риск» в специальном преломлении с использованием прилагательного «социальный».

А. Л. Благодир отмечает, что все социальные риски оказывают непосредственное влияние на возникновение материальных отношений (как страховых, так и нестраховых), которые реализуются через определенные виды правоотношений[1].

В психологии понятие риска как опасности, возможного наступления вредных последствий терминологически определяется через группы риска[2].

Естественным можно считать пристальное внимание к данной проблематике ученых-экономистов, так как риски, имеющие экономическое содержание способны оказывать существенное влияние на развитие общества.

В специальной экономической литературе представлены следующие точки зрения относительно рисков. Первая и наиболее многочисленная состоит в том, что он не рассматривается как экономическая категория[3]. Так, риск – фундаментальная, стержневая экономическая категория либерального общества, основным условием существования которого является свободный рыночный механизм[4]. Я. М. Магазинер считал риск настолько важным для права, что определял само право через понятие риска: «...все... право есть не что иное, как система распределения рисков, которая изменяет и направляет стихийно складывающееся их распределение на основе естественных законов экономики»[5].

Вторая точка зрения признает частные случаи влияния риска на экономическое поведение (асимметрия информации, эффект владения – утверждение о том, что человек ценит сегодняшнее имущество и доход гораздо выше, чем возможные имущество и доход в будущем)[6]. В соответствии с третьей точкой зрения риск рассматривают как категорию, влияющую на цену капитала, т.е. не самостоятельную, а входящую в состав затрат на капитал[7].

Уточним, что в рамках заявленной науки некоторыми авторами риск определяется как опасность наступления непредсказуемых и нежелательных для субъекта предпринимательской деятельности последствий его действий[8]. Другие экономисты, например, А. Г. Каратуев отмечает, что риск – это потенци-

---

[1] Благодир А.Л. Социальные риски как обстоятельства, влекущие возникновение социально-обеспечительных отношений // Социальное и пенсионное право. – 2011. – № 1. – С. 5-12.

[2] См.: Корнилова Т.В., Григоренко Е.Л., Смирнова С.Д. Подростки группы риска. – СПб: Питер, 2005. – С. 5.

[3] Ховард К., Эриашвили Н.Д., Никитин А.М. Экономическая теория. – М.: ЮНИТИ-ДАНА, 2000.

[4] См.: Танаев В.М. Понятие «риск» в Гражданском кодексе Российской Федерации // Актуальные проблемы гражданского права / Под ред. С.С. Алексеева. – М., 2000. – С. 9.

[5] Магазинер Я.М. Общая теория права на основе советского законодательства // Правоведение. – 1999. – № 1. – С. 136.

[6] Курс экономической теории. – Киров: АСА, 2005. – С. 188, 194.

[7] Ковалев В.В. Введение в финансовый менеджмент. – М.: Финансы и статистика, 2001. – С. 646.

[8] См.: Экономика предприятия / Под ред. Н.А. Сафронова. – М.: Юристъ, 1998. – С. 535.

альная возможность наступления неблагоприятного для хозяйствующего субъекта события, как правило, несущего финансовые потери[1].

Таким образом, исходя и представленных позиций видно, что в вопросе определения экономического содержания категории «риск» отсутствует унифицированных подход.

В экономической науке также распространено исследование рисков в связи с их видовым многообразием. Так, экономисты выделяют финансовый риск, определяя его как вероятность наступления ущерба в результате каких-либо операций в финансово-кредитной и биржевой сферах, совершения операций с ценными бумагами, то есть риск, который следует из природы финансовых операций. К финансовым рискам относится кредитный риск, процентный риск, валютный риск, риск упущенной финансовой выгоды[2].

Уточним, что в современной науке имеется тенденция появления терминов, описывающих риски в смежных областях знаний. Так, по мнению, А. К. Есаяна, основным фактором, сдерживающим экономический прогресс государств-участников СНГ, ЕврАзЭС, ШОС, является геополитический риск и отсутствие его явного и прямого законодательного регулирования. При этом «геополитическим риском названа возможность ухудшения геополитического положения государства и нации, снижение жизненной энергии этноса по любым из возможных причин»[3].

Геополитические риски являются стратегическими и глобальными по масштабам ущерба. В перспективном, текущем, оперативном управлении экономической сферой государства они тесно пересекаются и могут рассматриваться как политические и страновые[4]. Политические риски проявляются в изменении (улучшении или нарушении) условий производственно-торгового процесса по причинам, определяемым деятельностью органов государственного управления. Страновой риск может быть структурирован на риски конвертируемости валюты, трансферта или моратория платежа[5].

Представленный перечень понимания риска в различных отраслях не является исчерпывающим. В совокупности, полагаем, данная теоретико-концептуальная база является одним из направлений познания категории «риск» в целом, а также его отдельных разновидностей, в том числе и юридической природы. Считаем, что приведенные тезисы в перспективе можно считать частью разрабатываемой теории правозащитных рисков

---

[1] См.: Каратуев А.Г. Финансовый менеджмент. – М.: ФБК-Пресс, 2001. – С. 378.

[2] См.: Экономика предприятия / Под ред. Н.А. Сафронова. – М.: Юристъ, 1998. – С. 537.

[3] Глущенко В.В. Глущенко В.В. Теория государства и права: системно-управленческий подход. – Железнодорожный: ООО НПЦ «Крылья», 2000; Глущенко В.В. Управление рисками. Страхование. – Железнодорожный: ТОО НПЦ «Крылья», 1999.

[4] Кузнецов В.Н. Глобальная структурная гуманитарная революция XXI века: геокультурный, социологический аспект: Доклад весенней научной сессии авторов и участников научно-издательского проекта «Безопасность Евразии». Москва. 30 мая 2006 г.

[5] Глущенко В.В. Право как инструмент снижения инвестиционных рисков национальной экономики в условиях глобализации // Законодательство и экономика. – 2006. – № 9.

Олейник Н.Н.,
Олейник А.Н.

К ПРОБЛЕМЕ ВЗАИМООТНОШЕНИЙ ГОСУДАРСТВА И ЛИЧНОСТИ В КОНТЕКСТЕ ГЕНЕЗИСА ПОКОЛЕНИЙ ПРАВ ЧЕЛОВЕКА

Аннотация. В статье раскрывается взаимодействие государства и личности в контексте развития института прав человека и гражданина. Обобщается и анализируется процесс возникновения и развития теории и практики четырех поколений прав человека.

Ключевые слова: личность, человек, права человека, поколение прав человека, естественные права, личные права, гражданские права.

Abstract. The article reveals the interaction between the state and the individual in the context of the development of the institution of human rights and civil rights. Compile and analyze the origins and development of the theory and practice of four generations of human rights.

Key words: personality, people, human rights, the generation of human rights, natural rights, individual rights, civil rights.

Взаимодействие государства и личности пронизывает всю историю существования человечества. Еще древнегреческие мыслители, создавая концепции идеальных государств и обществ, прежде всего, выделяли соотношение государства, общества и личности. Они указывают, что именно благодаря государству и обществу человек вообще становится «личностью». Вступая в жизнь, человек осваивает сначала определенный минимум знаний, профессиональные навыки, а затем приобретает совокупность статусов в экономике, культуре, политике. При этом личность характеризуется совокупностью осваиваемых социальных связей; через объем знаний, опыта, профессиональных ориентаций, индивидуальных особенностей, мировоззренческий потенциал и т.п. Таким образом, если понятие «человек» – биологическое, то «личность» – безусловно, социальное явление.

Вместе с формированием понятия «личность» в научный оборот вводится понятие «права человека», которые и отображают развитие прав личности в обществе и государстве. В результате научной систематизации прав человека в историческом ключе и появилась теория трех поколений прав человека. В начале XXI века некоторые исследователи начинают выделять четвертое поколение[1].

Термин «права человека» сравнительно новый. Его стали использовать после Второй мировой войны, когда в 1945 г. была создана Организация Объединенных Наций. И тогда вводится и другой термин – «естественные права». Таким же образом было заменено более раннее выражение «права мужчины», так как оно не учитывало права женщин[2].

Специалисты по правам человека прослеживают историческое происхождение этой концепции еще со времен Древней Греции и Рима. Тогда она была

[1] Скакун О. Ф. Теорія держави і права (Енциклопедичний курс). / О.Ф. Скакун. – Х.: «Еспада«Ай Бі», 2006. – С. 211.

[2] Уетсон Бернс Г. Права людини / Бернс Г. Уетсон // Права людини: концепції, підходи, реалізація: пер. з англ. / Під ред. Б. Зізік. – К.: вид-во «Ай Бі»,2003. – С. 13.

тесно связана с доктринами естественного права греческого стоицизма. Эта была философская школа, основанная Зеноном с Китиона, который считал, что всю вселенную пронизывает универсальная творческая сила. Поэтому поведение человека необходимо рассматривать согласно законам природы и согласовывать с ними[1]. Эллинистический стоицизм существенно повлиял на формирование и распространение римского права, можно сказать, что он предусматривал существование естественного права и отвечал jus gentium («права народов») – универсальному праву, которое выходило за границы прав гражданства. Например, римский юрист Ульпиан считал, что естественное право – это право, которое дается от природы, а не от государства. И оно дается всем человеческим существам, независимо от того римские ли они граждане или нет[2].

Однако доктрины естественного права стали тесно связывать с либеральными политическими теориями о правах человека лишь во времена позднего средневековья. Для того чтобы идея о правах человека, то есть о естественных правах, как общая социальная потребность и реальность, постоянно доминировала, должны были состояться фундаментальные изменения в убеждениях и практике общества, что произошло в период Возрождения и упадка феодализма. То есть, начиная с XIII в. до начала буржуазных революций. Это было связано с тем, что сопротивление религиозному догматизму и политико-экономической рабской зависимости постепенно стало трансформироваться в либеральные понятия свободы и равноправия, особенно относительно владения и пользования собственностью, лишь тогда по-настоящему были заложены основы, понятия, которые мы сегодня называем правами человека. В течение этого периода состоялся переход от обязанностей естественного права к правам естественного права[3].

Однако, лишь в XVII и XVIII вв. была разработана модернистская концепция естественного права, которая предусматривала наделением всех людей естественными правами. В ее разработке особый вклад внесли такие философы, и просветители нового времени как Джон Локк, Шарль Монтескье, Вольтер и Жан-Жак Руссо. Наибольшее влияние на развитие этой концепции, по нашему мнению оказало творчество Дж. Локка. В своих произведениях, связанных с революцией 1688 г. в Англии («Славной революцией»), он последовательно доказывал, что каждой личности принадлежат определенные права (поскольку она, как человеческое существо, существовала в «естественном состоянии» еще до того, как человечество стало гражданским обществом). Основными среди этих прав, по мнению названного мыслителя, являются право на жизнь, свободу и собственность; что после наступления гражданского общества (в соответствии с «общественным соглашением»), человечество отказа-

---

[1] Чанышев А.Н. Курс лекций по древней и средневековой философии: Учеб. пособие для вузов. / А.Н. Чанышев. – М.: Высшая школа, 1991. – С. 130-131.

[2] Хрестоматия по истории государства и права зарубежных стран (Древность и Средние века) / Составитель: В. А. Томсинов. – М.: Издательство ЗЕРЦАЛО, 1999. – С. 182.

[3] Уетсон Бернс Г. Права людини / Бернс Г. Уетсон // Права людини: концепції, підходи, реалізація: пер. з англ. / Під ред. Б. Зізік. – К.: вид-во «Ай Бі»,2003. – С. 14.

лось в пользу государства не от самых прав, а лишь от реализации этих естественных прав. И что неспособность государства обеспечить эти зарезервированные права (государство само обязалась обеспечить интересы своих граждан) порождает право на соответствующую народную революцию[1]. Вместе с Ш. Монтескье Дж. Локк также разработал концепцию разделения власти на три ветви: законодательную, исполнительную и судебную. Что касается прав человека, то Ш. Монтескье считал, что "свобода есть право делать все, что дозволено законами"[2]. Это определение не потеряло свою актуальность и сегодня.

Многие философы нового времени, опираясь на учение Локка и других ученых-обществоведов разных направлений мысли и имея большую веру в здравый смысл, решительно критиковали религиозный и научный догматизм, нетерпимость, цензуру и социально-экономические ограничения. Они стремились действовать на основе универсальных справедливых принципов, которые гармонично руководят одновременно природой, человечеством и обществом, а теория неотчуждаемых «прав человека» стала их основными этическими и социальными пастулатами.

Не удивительно, что все эти либерально-интеллектуальные поиски имели большое влияние на западный мир конца XVIII – начала XIX вв. Вместе с практическим примером Английской революции 1688 г. и Билля о правах, который стал ее результатом, они содействовали логическому обоснованию революционной волны, которая к тому времени охватила западную цивилизацию и особенно Северную Америку и Францию. Томас Джефферсон, который изучал Дж. Локка и Ш. Монтескье утверждал, что его соотечественники – «свободные люди. Они претендуют на права, которые вытекают с естественного права, а не являются подарком верховного судьи»[3]. Эта ж идея была закреплена в Декларации независимости, провозглашенной тринадцатью американскими колониями 4 июля 1776 г. В ней подчеркивалось: «мы считаем очевидной истиной, что все люди созданы равноправными, что они наделены Богом определенными не отчуждаемым правами, к числу которых относятся жизнь, свобода и стремление к счастью.»[4]. Маркиз де Лафайет – близкий друг Джорджа Вашингтона и который делил с ним трудности американской войны за независимость, – повторил лозунги английской и американской революций в Декларации прав человека и гражданина Франции от 26 августа 1789 г. Подчеркивая, что «люди рождаются и остаются свободными и равными в своих правах», в этой декларации провозглашалось: «цель каждой политической ассоциации состоит в сохранении естественных и неотъемлемых прав человека»[5]. Декларация определяла эти права как «Свободу, Собственность, Безопасность и Сопротивление

---

[1] Локк Дж. Сочинения: В 3-х т. / Локк Дж. – М.: Мысль, 1988. – Т. 3. – С. 264-267.

[2] Монтескье Ш.Л. Избранные произведения. / под ред. М.П. Баскина. – М.: гос. изд-во пол. лит-ры, 1955. – С. 289-291.

[3] Уетсон Бернс Г. Указ. соч. – С. 15.

[4] Хрестоматия по истории государства и права зарубежных стран (Новое и Новейшее время) / Составитель: Н. А. Крашенинникова. – М.: Издательство ЗЕРЦАЛО, 1999. – С. 132-133.

[5] Там же. – С.88-89.

притеснениям». В понятие «свобода» она включала свободу слова, свободу объединений, религиозную свободу и свободу от своевольного ареста и тюремного заключения (словно опережая Билль о правах (1791 г.)[1], принятый в дополнение к Конституции Соединенных Штатов 1787 г.)[2].

Можно подытожить, что традиции прав человека продукт своего времени. Они отображают процессы исторической непрерывности и изменений и, как предмет кумулятивного опыта, помогают предоставить им содержание и форму. Таким образом, чтобы лучше понять формы и законный объем прав человека полезно проанализировать основные школы, которые определили традиции прав человека, начиная с периода Возрождения.

Особенно полезным в этом отношении являются понятия и понимание связи «трех поколений прав человека». Этот *термин ввел в 1970-х гг.* Карел Васак, *чешский юрист и первый генеральный секретарь Международного института прав человека в г. Страсбурге (Франция)*[3]. Три поколения прав человека, по его мнению, соотносятся с тремя идеалами Французской революции: свободой, равенством и братством[4]. Модель Васака, конечно лишь упрощенное отображение чрезвычайно сложного исторического периода, но дает возможность создать систему развития прав человека в контексте развития государства и общества.

Первое поколение гражданских и политических прав ведет свое начало от указанных выше реформистских теорий XVII и XVIII вв., связанных с Английской и особенно с Американской и Французской буржуазно-демократическими революциями. Первое поколение включает личные права, вытекающие из естественных прав и созданных на основе позитивного права политических прав. Они находят свою конкретизацию в законодательстве первых буржуазно-демократических государств. Речь идет о личных (гражданских) и политических правах: право на свободу вероисповедания, на участие в управлении государственными делами, на равенство перед законом и судом, на жизнь, свободу и безопасность лица, от своевольного (незаконного) ареста, задержание. Эти права закрепили так называемую "негативную свободу" – т.е. они обязали государство воздерживаться от вмешательства в сферу личной свободы. Это, например, хорошо отображено коротким утверждением, которое приписывается Х. Л. Менкену – «любое правительство, конечно ж выступает против свободы»[5]. Таким образом, до этого первого поколения относятся заявленные права, изложенные в статьях 2-21 Общей Декларации прав человека принятой ООН 10

---

[1] Там же. – С.153-155.

[2] Хрестоматия по истории государства и права зарубежных стран под ред. З.М. Черниловского. – М.: Юридическая литература, 1984. – С. 189-199.

[3] Vasak K. Human Rights: A Thirty-Year Struggle: the Sustained Efforts to Give Force of the Universal Declaration of Human Rights // UNESCO Courier, 1977. Nov.

[4] Vasak K. Pour une troisieme generation des droits de l'homme // Studies and Essays on International Humanitarian Law and Red Cross Principles / Ed. by C. Swinarski. Hague, 1984. – P. 837, 839.

[5] *Mencken H.L.* A Mencken Chrestomathy. N.Y.: Alfred A.Knopf, 1949. – P. 145.

декабря 1948 г.[1]. К первому поколению прав также можно отнести право на собственность. И любая попытка лишить человека собственности является незаконным действием. Каждое из этих прав отстаивало интересы, за которые велась борьба во время Американской и Французской буржуазных революций, а также интересы, важные для развития капиталистического общества. Однако в этой концепции первого поколения главным есть понятие свободы – щита, который защищает личность (или группу лиц) от злоупотреблений и плохого отношения к ним политических властей. Эта основная правовая ценность в наше время записана в конституциях более чем 180 стран – о есть практически во всех действующих конституциях мира[2]. Эти права закреплены в большинстве международных деклараций и соглашений, которые касаются прав человека принятых после Второй мировой войны. Это – западная либеральная концепция прав человека, которую иногда представляют в романтическом свете, как триумф индивидуализма Гоббса-Локка над статизмом Гегеля.

Второе поколение экономических, социальных и культурных прав ведет свое начало от социалистической традиции, которая возникает среди сенсимонистов во Франции в начале XIX в. Эти права сформировались в процессе борьбы народов мира за улучшение своего экономического уровня (конец XIX – начало XX ст.) – к ним относятся социально-экономические права. Они впервые были закреплены также в конституциях социалистических стран. К ним относятся право на работу, образование, отдых, на защиту материнства, детства.

Исторически эта традиция противопоставляется первому поколению гражданских и политических прав. Второе поколение прав человека воспринимается в более положительном («право на»), чем в негативном («свобода от») плане. Эти права требуют вмешательства государства в обеспечение равного участия всех людей в производстве и распределении соответствующих ценностей. Показательными для характеристики данной модели являются права человека, изложенные в статьях 22-27 Декларации ООН принятой 10.12.1948 г., такие как право на социальную безопасность, право на работу и защиту от безработицы, право на отдых и досуг, в том числе на периодический оплачиваемый отпуск, право на достойный уровень жизни, соответствующий здоровью и благополучию самого лица и его семьи, право на образование и право на защиту научной, литературной и художественной продукции деятельности человека и др.

Однако, как все гражданские и политические права первого поколения неверно характеризовать их как «негативные права». Объяснять это тем, что все права, которые принадлежат ко второму поколению экономических, социальных и культурных прав, в сущности, не могут иметь понятия «положительные права». Например, право на свободный выбор занятости, право создавать профессиональные союзы и принимать участие в них, право свободного участия в культурной жизни общества в своей основе не требуют положительных действий государства для обеспечения удовлетворения этих прав. Однако, большин-

[1] Всеобщая декларация прав человека от 10 декабря 1948 г. / Голос України від 10.12.2008 – № 236.

[2] Уетсон Бернс Г. Указ. соч. – С. 21.

ство прав второго поколения, в соответствии с некоторыми критериями справедливого распределения благ, требуют определенного государственного вмешательства о выделении необходимых ресурсов. Ведь эти права относятся к категории скорее материальных, чем нематериальных ценностей. Таким образом, права второго поколения в своей основе являются требованиями социального равенства. Интернационализация этих прав состоялась с определенным опозданием, частично из-за социалистического влияния в нормативной сфере международных отношений. Но с выходом на глобальную арену стран Третьего мира, которые действовали под лозунгом «революций больших ожиданий», эти права начали интенсивно развиваться.

В конце концов, третье поколение солидарных прав базируется на двух предыдущих поколениях прав, связывает их между собой и по-новому их концептуализирует. Однако лучше всего рассматривать это поколение как продукт в стадии формирования – результат одновременного подъема и упадка наций-государств второй половины XX века. Третье поколение прав получило свое выражение в статье 28 Общей Декларации прав человека ООН, которая провозглашает, что «каждый имеет право на общественный и международный порядок, в котором права, изложенные в этой Декларации, могут быть полностью реализованы»[1]. Третье поколение охватывает ныне шесть вышеуказанных прав. Три из них отображают появление национализма в странах Третьего мира и их требований относительно перераспределения власти, богатства и других важных ценностей: право на политическое, экономическое, социальное и культурное самоопределение; право на участие и получение прибылей от «общего наследства человечества» (общее околоземное пространство; научная, техническая и другая информация и прогресс; культурные традиции, памятки и памятники). Следующие заявленные права третьего поколения – право на мир, право на здоровую и сбалансированную окружающую среду и право на гуманитарную помощь в случае различных катастроф – дают нам возможность понять, что нации-государства неспособны эффективно решать наиболее сложные проблемы самостоятельно без участия международного сообщества в современном мире.

Все шесть вышеизложенных прав – коллективные права, которые требуют общих усилий всех социальных сил на планетарном уровне. Однако каждое из них выявляет как индивидуальную, так и коллективную сторону. Например, обеспечение нового международного экономического порядка, который устранит препятствия на пути экономического и социального развития заявленных прав, можно считать коллективным правом всех стран и народов (особенно развивающихся стран). Можно также утверждать, что получение пользы от политики развития, которая базируется на удовлетворении людских материальных и нематериальных нужд, это индивидуальное право всех людей. Когда, например, право на самоопределение и право на гуманитарную помощь находит свое отображение, как на законодательном, так и на моральном уровне, большинство из этих солидарных прав по своему характеру скорее желательны, чем обеспечены

[1] Всеобщая декларация прав человека от 10 декабря 1948 г. / Голос України від 10.12.2008 – № 236.

судебной властью, и имеют лишь неоднозначный юридический статус международных норм прав человека.

Таким образом, на разных этапах современной истории – после «буржуазных» революций XVII и XVIII вв., социалистических революций XX в. и антиколониальных революций, которые начались вскоре после окончания Второй мировой войны, – содержание прав человека определялось в общих чертах. Новое содержание прав человека развивалось путем расширения и добавления. Отображая развитие осознания того, какие именно ценности в разные исторические периоды требовали самого большого поощрения и защиты, история содержания прав человека также показывает периодические требования всего человечества о непрерывности и стабильности.

Между двумя первыми и третьим поколениями прав человека есть взаимозависимость, осуществляемая через принцип: реализация коллективных прав не должна ограничивать права и свободы личности.

В XXI в. продолжается процесс возникновения и закрепления новых прав личности, поэтому некоторые исследователи выделяют и четвертое поколение прав человека[1]. Объясняется это тем, что вместе с развитием и углублением права на информационное пространство нашей планеты, на предоставления различных услуг, основанных на интеллектуальных информационных технологиях (в том числе новейших различных технологичных исследований). Так в технологиях связи, использование глобальной сети «Интернет», обеспечение информационных отношений внутри страны и за рубежом, расширяет коллективные права человека. Активно началось становление прав человека, связанных с научными открытиями в области микробиологии, медицины, генетики и т.п. Эти права – результат вмешательства в психофизиологическую сферу жизни человека (например, право человека на искусственную смерть (эвтаназия), право женщины на искусственное оплодотворение и вынашивание ребенка для другой семьи и др.). Эти права тоже имеют границы. Например, во многих странах введен запрет клонирования человека и установлены другие правовые границы по отношению к другим правам этого поколения прав.

Нельзя утверждать, что каждое из этих четырех поколений прав одинаково приемлемо для всех, или что они или их отдельные элементы всегда и всюду находят одинаковое положительное отношение. Например, некоторые защитники прав первого поколения склонны исключать права второго и третьего поколения из своего определения прав человека вообще (или, по крайней мере, называют их второстепенными). В то же время многие ученые не признают появление четвертого поколения прав. В частности, это объясняется сложностью, которая возникала в процессе реализации этих прав. Приверженцы прав первого поколения, которые доказывают их особую значимость, вытекающую из естественного права и традиции невмешательства в их реализацию государства, небезразличны к мысли, что права человека в своей основе независимы от гражданского общества и являются индивидуалистическими, то есть только они составляют классические права личности. И наоборот, защитники прав второго,

[1] Скакун О. Ф. Указ. соч. – С. 213-214.

третьего и четвертого поколений считают, что права первого поколения, по крайней мере, на уровне общей практики, уделяют недостаточное внимание материальным потребностям людей и используются несправедливыми национальными, транснациональными и международными общественными институциями в качестве легитимизирующих инструментов и это «буржуазная иллюзия». Подобным образом, не исключая права первого поколения со своего определения прав человека, они по обыкновению предоставляют этим правам низкий статус и, соответственно, трактуют их как хронологически отдаленные цели, достижения которых возможно лишь после постепенного осуществления фундаментальных экономических и социальных преобразований, которые полностью будут реализованы лишь в далеком будущем.

В конце концов, ни один из механизмов прав человека, на сегодняшний день действующих или предложенных, ничего не говорят о легитимности или упорядочении прав, которых они касаются, за исключением прав, которые по международному соглашению определены как неотъемлемые и потому они являются более фундаментальными чем иные (например, свобода от своевольного или незаконного лишения жизни, свобода от пытки и нечеловеческого или унизительного отношения и наказания, свобода от рабства, свобода от тюремного заключения за долги). Вероятно, когда вопрос касается проблемы осуществления заявленных прав, среди юристов, философов, политологов и других обществоведов не существует единой мысли относительно их легитимности и иерархии.

Таким образом, легитимность прав личности и заявленные среди них приоритеты определяются контекстом определенной эпохи. Поскольку люди в разных частях планеты отстаивают и уважают те или иные права человека в соответствии с различными процедурами и практикой, эти вопросы целиком зависят от времени, места, обстоятельств, уровня кризиса и других причин. При этом взаимоотношения государства и личности в историческом генезисе через поколения права человека свидетельствуют, что по мере развития прав личности их количество и распространение в различные сферы общественной и социальной жизни, по нашему мнению, только увеличивается. Об этом убедительно свидетельствует и появление третьего и четвертого поколений прав человека. С другой стороны гармоническое развитие личности возможно только в правовом демократическом государстве и в развитом гражданском обществе.

Список литературы

1. Всеобщая декларация прав человека / Голос України від 10.12.2008 – № 236.
2. Локк Дж. Сочинения: В 3-х т. / Локк Дж. – М.: Мысль, 1988. – Т. 3. – 668 с.
3. Монтескье Ш.Л. Избранные произведения. / под ред. М.П. Баскина. – М.: гос. изд-во пол. лит-ры, 1955. – 843 с.
4. Скакун О. Ф. Теорія держави і права (Енциклопедичний курс). / О.Ф. Скакун. – Х.: «Еспада«Ай Бі», 2006. – 776 с.
5. Уетсон Бернс Г. Права людини / Бернс Г. Уетсон // Права людини: концепції, підходи, реалізація: пер. з англ. / Під ред. Б. Зізік. – К.: вид-во «Ай Бі»,2003. – 262 с.
6. Хрестоматия по истории государства и права зарубежных стран под ред. З.М. Черниловского. – М.: Юридическая литература, 1984. – 472 с.

7. Хрестоматия по истории государства и права зарубежных стран (Древность и Средние века) / Составитель: В. А. Томсинов. – М.: Издательство ЗЕРЦАЛО, 1999. – 480 с.

8. Хрестоматия по истории государства и права зарубежных стран (Новое и Новейшее время) / Составитель: Н. А. Крашенинникова. – М.: Издательство ЗЕРЦАЛО, 1999. – 592 с.

9. Чанышев А.Н. Курс лекций по древней и средневековой философии: Учеб. пособие для вузов. / А.Н. Чанышев. – М.: Высшая школа, 1991. – 512 с.

10. Mencken H.L. A Mencken Chrestomathy. N.Y.: Alfred A.Knopf, 1949. – 627 p.

11. Vasak K. Human Rights: A Thirty-Year Struggle: the Sustained Efforts to Give Force of the Universal Declaration of Human Rights // UNESCO Courier, 1977. Nov.

12. Vasak K. Pour une troisieme generation des droits de l'homme // Studies and Essays on International Humanitarian Law and Red Cross Principles / Ed. by C. Swinarski. Hague, 1984.

Петрова Н.А.

ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОГО КОНТРОЛЯ В СЕТИ ИНТЕРНЕТ КАК ФАКТОР ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ

Аннотация. Противодействие распространению экстремизма в сети-Интернет, как защита прав граждан и юридических лиц в сфере интернет-услуг.

Ключевые слова: информационная безопасность, информационное пространство, информационные технологии, киберпреступность, экстремистская деятельность (экстремизм); материалы экстремистской направленности.

Abstract. Counteraction to distribution of extremism is in the Internet, as a protection of rights for citizens and legal entities in the field of internet-services.

Key words: information security, information space, information technology, cyber crime, extremist activity (extremism), and materials of an extremist.

Телекоммуникационные и компьютерные системы стали неотъемлемой частью всех сфер деятельности людей и государства. Однако, разработав глобальную компьютерную сеть и службы телекоммуникации для своих нужд, люди даже не предполагали, что со временем это станет объектом злоупотребления и начнет причинять им вред. Возрастающая роль информационной сферы, которая является системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, военной и других составляющих национальной безопасности Российской Федерации. В связи с этим информационная безопасность приобретает все бóльшую значимость в общей системе обеспечения национальной безопасности Российской Федерации в целом. Криминогенная обстановка однозначно свидетельствует о том, что информационная сфера с ее специфическими особенностями является весьма привлекательной для преступников. Специфика телекоммуникационной инфраструктуры такова, что весьма существенный ущерб ей можно нанести внезапно, минимальными силами и средствами, находясь практически вне зоны реальной досягаемости.

Особо следует отметить устойчивую тенденцию к укреплению международных связей преступных группировок и трансграничность самих преступных посягательств. Понятие киберпреступности имеет международное значение и означает совершаемые людьми преступления, в процессе которых информационные технологии используются в преступных целях. Уровень развития этого вида преступлений напрямую зависит от степени развитости информационных технологий и глобальных сетей, а также открытости доступа к ним. ***Киберпреступность*** охватывает и компьютерную преступность в целом и связанные с ней события. ***Киберпреступлением*** принято считать уголовно наказуемые действия, подразумевающие несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных. При этом компьютер выступает в качестве предмета преступления, а информационная безопасность – объекта.

В значительной части выявляемых киберпреступлений либо субъект, либо объект, либо предмет преступного посягательства находятся в географических пространствах различных государств, что, с одной стороны, затрудняет работу правоохранительных органов отдельно взятой страны, а с другой – способствует поиску взаимовыгодных и взаимоприемлемых условий кооперации и сотрудничества, способствуя формированию единой системы противодействия современным вызовам и угрозам.

К числу их преступлений можно отнести взлом паролей, распространение вредоносных программ, рассылка спама, кражи информации, касающейся любой деятельности человека, распространение клеветы, порнографии, материалов, которые могут повлечь межрелигиозную или национальную вражду и тому подобное.

Подобные преступления имеют несколько особенностей, которые очень затрудняют борьбу с ними. Это чрезвычайная завуалированность, нанесение ущерба в особо крупных размерах, высокий профессионализм преступников, отсутствие национальных границ и общей правовой базы для лиц, которые совершают подобные преступления. В связи с развитием виртуальных сетей, практически любой пользователь, имеющий доступ к этим сетям может сравнительно легко и беспрепятственно осуществить любое покушение на информацию, касающуюся каждого из нас, чем может повлечь тяжелые последствия.

В зависимости от того, с какой целью ***киберпреступник*** использует компьютерные системы, можно выделить три основных типа киберпреступлений:

– компьютерные преступления, когда компьютер используется как предмет преступления, т.е. неразрешенный доступ к информации, кража важной информации, повреждение и уничтожение информации и т.д.;

– действия, в которых компьютер выступает в роли орудия преступления, например, электронные хищения;

– преступления, при которых компьютер выполняет роль интеллектуальных средств, к примеру, создание порнографических сайтов и размещение соответствующей информации, которые могут повлечь межрелигиозную или национальную вражду (экстремистская деятельность) и тому подобное.

Так, к числу действий экстремистского характера современное российское законодательство относит возбуждение расовой, национальной или религиозной розни; пропаганду исключительности, превосходства либо неполноценности человека по признаку его расовой, национальной, религиозной или языковой принадлежности или отношения к религии; нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его расовой, национальной, религиозной или языковой принадлежности или отношения к религии.

Основным нормативным документом, в котором определяются правовые и организационные основы противодействия экстремистской деятельности, а также устанавливается ответственность за ее осуществление, является Федеральный закон №114-ФЗ от 25 июля 2002 года (в редакции Федерального зако-

на от 29.04.2008 №54-ФЗ) «О противодействие экстремистской деятельности»[1]. В этом законе дается конкретное определение таким понятиям, как экстремистская деятельность (экстремизм); экстремистская организация; экстремистские материалы.

По официальным оценкам ежегодно МВД России выявляет около 150 ресурсов, содержащих материалы экстремистской направленности. Больше всего подобных сайтов было обнаружено в российском сегменте сети, их оказалось более 70. В России борьбой с киберпреступлениями занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел. Мониторингом интернет-простанства круглосуточно занимаются специализированные подразделения МВД России, в соответствие с законодательством закрываются сайты с негативным контентом, а лиц, размещающих на них информацию, привлекают к уголовной ответственности. Однако около 15% закрытых сайтов появилось вновь под другими именами на хостинговых ресурсах как российских, так и зарубежных провайдерах. Чаще всего сайты, вытесненные из российского сегмента сети, мигрируют в другие страны. Поэтому повышение уровня международного сотрудничества в данной сфере представляется весьма актуальным[2].

Все это указывает на необходимость правового регулирования вопросов установления ответственности за совершение противоправных деяний в глобальных информационно-телекоммуникационных системах. В настоящее время правовой базой противодействия экстремизму являются: Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»[3]. Так, этим законом устанавливается запрет на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность (п.6 ст.10).

Нормативное правовое регулирование информационной безопасности России образуется совокупностью норм федерального законодательства, законодательства субъектов Российской Федерации, общепризнанных принципов и норм международного права, регулирующих защищаемые от угроз общественные отношения в информационной сфере. Осуществление международного информационного обмена диктует необходимость использования соответствующих межгосударственных конвенций, договоров и иных нормативных правовых актов данной сферы.

---

[1] О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002г.№114-ФЗ//Собрание законодательства Российской Федерации.2002.№30.Ст.3031.

[2] Проблемы противодействия экстремизму: материалы научно-практической конференции, – Белгород, 2009. 224 с.

[3] Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. №149-ФЗ//Собрание законодательства Российской Федерации.2006. №31 (ч.1).Ст.3448.

Организация системы информационной безопасности также является важной составляющей правового обеспечения. Важнейшими требованиями, предъявляемыми к информационной безопасности, являются: своевременность, надежность, эффективность, бесперебойность. От их соблюдения при правовом регулировании напрямую зависят обеспечение нормального кругооборота информационных потоков, устойчивость функционирования системы государственного управления, основанная на электронном документообороте, обеспечение подтверждения достоверности и подлинности электронных документов, правовой режим информации ограниченного доступа, обеспечение доступа к публичной информации, борьба с киберпреступностью, защита критически важных объектов и др.

Для эффективной борьбы с киберпреступностью необходимо детально изучить ее специфику и виды распространения. Необходимо по возможности объединить и достигнуть координации в действиях всех силовых и правоохранительных систем каждой из стран, вплоть до ограничения доступа к информации в сети Интернет. Это поможет повысить безопасность информационного пространства каждого из отдельных государств.

В связи с возникшей необходимостью государство обязано контролировать содержание информации, размещенной в компьютерных сетях, предусмотреть нормы, регулирующие права и обязанности пользователей сети Интернет, их ответственность.

По мнению Т.А. Поляковой, в законодательстве Российской Федерации для пресечения распространения противоправной информации целесообразно предусмотреть возможность аннулирования лицензии провайдера, размещающего сайты экстремистского характера, после вынесения соответствующего предупреждения и внесения сведений об аннулировании лицензии в реестр, а также лишения таких провайдеров права в дальнейшем на участие в конкурсе на право оказания услуг связи. При этом необходимо установление ответственности провайдеров за размещение в компьютерных сетях материалов, признанных экстремистскими по решению суда или возобновление деятельности сайта, закрытого по мотивам размещения экстремистских материалов, а также возможность административного приостановления деятельности интернет-провайдера, допускающего размещение материалов противоправного характера[1].

[1] Полякова Т.А. Вопросы ответственности за использование информационно-телекоммуникационных систем в террористических и экстремистских целях.//Российский следователь.2008.№1//СПС «Консультант Плюс».

Пономаренко О.М.

ОСОБЕННОСТИ ЗАКЛЮЧЕНИЯ СЕМЕЙНЫХ ДОГОВОРОВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СЕТЕЙ

Аннотация. В докладе рассмотрены особенности заключения семейных договоров с использованием электронных сетей, изложены возможности заключения таких договоров в устной и письменной форме. Исследуется проблема использования в качестве подписи аналога собственноручной подписи лица.

Ключевые слова: семейный договор, форма договора, электронная подпись, субсидиарное применение гражданского законодательства, аналог собственноручной подписи.

Abstract. This article discusses the features of the conclusion family contracts through electronic networks. The possibilities of such contracts in oral and written form. We study the problem of using as a signature analogue of signature of the person.

Key words: family contract, the contract form, electronic signature, Subsidiary application of civil law, similar to a handwritten signature.

За последнее время в регулировании семейных отношений произошли коренные изменения, связанные, прежде всего, с расширением диспозитивности в семейно-правовом регулировании. Это выразилось в том, что закон перестал рассматриваться в качестве единственно возможного регулятора семейных отношений. За их участниками было признано право на саморегулирование.

В этой связи в семейном праве появился новый институт – семейный договор и перед наукой возникла необходимость в разработке теории семейного договора. Стоит отметить, что и теория и законодательство относительно семейных договоров находятся в зародышевом состоянии. Но, тем не менее, уже сейчас можно наметить некоторые тенденции и проблемы, связанные с договорным регулированием семейных отношений. Так, необходимо обратить внимание на то, что в семейном законодательстве практически отсутствуют общие положения о семейных договорах, а нормативные конструкции отдельных их видов разработаны недостаточно. В этой связи применение положений ГК к регулированию семейных отношений, особенно, в отношении семейных договоров, является необходимым. Учитывая это, и украинский и российский законодатель допускают возможность субсидиарного применения гражданского законодательства к регулированию тех семейных отношений, которые не урегулированы СК, с учетом специфики последних.

В этой связи, хотелось бы обратить внимание на проблему возможности и особенностях заключения семейных договоров через сеть интернет. Этот вопрос на сегодняшний день является как нельзя актуальным. Это обусловлено тем, в современных условиях огромное количество членов семьи, особенно бывших членов семьи, живут в разных городах, разных государствах, на разных континентах. В тоже время, вопросы, связанные с решением многих семейных проблем, зачастую требуют немедленного разрешения. В этой связи как раз и

возникает вопрос о том, а возможно ли заключить семейный договор через интернет?

Так как особенности заключения семейных договоров не предусмотрены ни СК Украины, ни СК РФ, возникает необходимость в применении нормативных предписаний гражданского законодательства.

Известно, что существуют две возможные формы договора – устная и письменная (простая и требующая нотариального удостоверения). Форма договора выбирается самостоятельно сторонами, что является одним из проявлений принципа свободы договора. Стоит, однако, отметить, что законодатель в некоторых случаях ограничивает свободу в вопросе выбора формы договора тем, что посредством императивных норм закрепляет требования к форме конкретного договора. Так, например, в отношении брачного договора, алиментных договоров и СК Украины, и СК РФ предусматривают письменную форму, требующую нотариального удостоверения. В таких случаях, стороны не могут отступить от нормативных предписаний под страхом признания сделки недействительной. Таким образом, можно сделать вывод, что члены семьи имеют право заключить семейный договор в любой форме, если это не противоречит требованиям семейного законодательства.

Представляется, что семейные договоры чаще, чем остальные гражданские договоры заключаются в устной форме. Стоит отметить, что в устной форме семейные договоры заключаются, как правило, в тех случаях, когда между членами семьи существуют бесконфликтные, мирные отношения. Такие соглашения зачастую в теории семейного права именуются договоренностями, хотя по существу они являются договорами, так как направлены на возникновение, изменение или прекращение семейных прав и обязанностей. В тоже время, их необходимо отличать от семейных соглашений, направленных на урегулирование бытовых отношений. Отличие семейного договора от «бытового» соглашения следует проводить по направленности на возникновение юридических прав и обязанностей. Среди них только лишь договор порождает юридические последствия.

Устные семейные договоры могут быть двух видов. Во-первых, семейные договоры, связанные с реализацией личных неимущественных прав, например, соглашение о выборе имени ребенку, соглашение о выборе методов воспитания ребенка, соглашение о выборе воспитательного или образовательного учреждения и т.п. Во-вторых, договоры, направленные на осуществление имущественных прав, например, договор о порядке использования общего или личного имущества, договор о расходовании общих или личных доходов членов семьи и т.п.

Гражданским законодательством предусмотрены два случая, когда договор может быть заключен в устной форме. Во-первых, устно могут заключаться сделки, которые полностью исполняются в момент их совершения. Необходимо отметить, что семейные отношения носят длящийся характер, а поэтому, сделки, полностью исполняемые в момент заключения для семейного права, как

правило, не характерны. Во-вторых, сделки на исполнение договора, заключенного в письменной форме, могут по договоренности сторон исполняться устно, если это не противоречит договору или закону.

Кроме того, на основании анализа нормативных предписаний, можно сделать вывод о том, что в устной форме могут заключаться и другие договоры, при наличии в совокупности двух условий: во-первых, законодательством предусмотрена письменная форма конкретного договора; во-вторых, актами гражданского законодательства не предусмотрено признание таких сделок недействительными в случае несоблюдения письменной формы.

Такой вывод сделан в связи с тем, что единственным негативным последствием несоблюдения простой письменной формы в таких случаях является невозможность доказывания факта совершения сделки и ее условий свидетельскими показаниями.

В устной форме, безусловно, не могут совершаться сделки, требующие нотариального удостоверения или государственной регистрации, а также те сделки, несоблюдение письменной формы которых влечет признание их недействительными.

С учетом сказанного, можно сделать вывод, что в устной форме может быть заключена любая сделка, за исключением сделок, которые в соответствии с требованиями законодательства должны быть нотариально удостоверены или подлежат государственной регистрации, а также сделок, для которых законом предусмотрена недействительность за несоблюдение письменной формы.

В устной форме договора существуют как положительные, так и отрицательные стороны. Стоит отметить, что характерной чертой семейных договоров, заключаемых в устной форме, является то, что между сторонами (членами семьи) существуют доверительные отношения. Такие соглашения относятся к разряду фидуциарных сделок, а, следовательно, стороны стремятся к упрощенной процедуре заключения, что как нельзя больше соответствует устной форме. Преимущества устной формы договора как раз и состоят в простоте и отсутствии формальностей процедуры заключения.

Однако, устной форме присущи также и негативные черты, которые выражаются, прежде всего, в сложностях доказывания факта заключения договора и его содержания. Такая необходимость появляется при наличии спора, когда наличие доказательств приобретает первостепенное значение. Именно потенциально высокий риск недоказуемости факта заключения устного договора и его условий нивелируют позитивные стороны такой формы и придают определенный риск подобным договорам.

Таким образом, наибольшую практическую значимость для устной формы договора приобретают доказательства, особенно в тех случаях, когда в соответствии с требованием закона договор должен был быть заключен в простой письменной форме. Наиболее распространенным видом таких доказательств на практике, как правило, являются письменные доказательства. Однако, необходимо особо отметить, возможность использования в качестве доказательств

данные интернет ресурсов. Так, переписка по электронной почте, видео и аудио разговоры в программах skype, facetime и других аналогичных программах в полной мере могут быть использованы как доказательства факта заключения семейного договора и его условий. Таким образом, можно сделать вывод о том, что заключение семейного договора посредством сети интернет нейтрализует негативные стороны устной формы договора.

В простой письменной форме заключается большинство семейных договоров. Необходимо отметить, что в ст. 8 СК Украины сформулировано общее правило о том, что лица, которые проживают одной семьей, а также родственники по происхождению, отношения между которыми не урегулированы СК, могут урегулировать своих семейные (родственные) отношения посредством договора, который должен быть заключен в письменной форме.

Кроме того, в соответствии со ст. 208 ГК Украины в письменной форме должны заключаться сделки: во-первых, между юридическими лицами; во-вторых, между юридическими и физическими лицами; в-третьих, между физическими лицами на сумму, превышающую в 20 и более раз необлагаемый налогом минимум доходов физических лиц; в-четвертых, в случаях, когда актами гражданского законодательства предусмотрена письменная форма.

В этой связи можно сделать вывод о том, что, в простой письменной форме могут быть заключены любые семейные договоры, для которых законодательством не предусмотрено обязательное нотариальное удостоверение.

Следует отметить, что особенностью письменной формы является то, что в этом случае договор рассматривается в качестве документа. А поэтому заключение договора в письменной форме сопровождается определенными формальностями.

Так, большое значение для такой формы имеет процедура оформления документа. В соответствии со ст. 207 ГК Украины возможны несколько вариантов соблюдения простой письменной формы. Во-первых, содержание сделки может быть зафиксировано в одном или нескольких документах. Во-вторых, содержание сделки может быть зафиксировано в письмах, телеграммах, которыми обменялись стороны. В-третьих, воля сторон может быть выражена с помощью телетайпного, электронного или иного технического средства связи.

Следующим обязательным компонентом любого документа является подпись. В соответствии с ч. 2 ст. 207 ГК Украины и ч. 1 ст. 160 ГК РФ сделка считается совершенной в письменной форме, если она подписана сторонами.

Предназначение подписи заключается в том, чтобы, во-первых, идентифицировать лицо, подписывающее договор; во-вторых, подтвердить целостность данных, содержащихся в документе.

Если при заключении договора присутствуют обе стороны, то собственноручно подписать договор не составляет труда. Однако, современные условия жизни зачастую не позволяют лицам лично присутствовать при заключении договора. Кроме того, бурное развитие электронных технологий делает такое присутствие необязательным. При признании за договором, заключенным с

помощью телетайпного, электронного или иного технического способа связи качеств письменной формы сделки, логично возникает вопрос о способе подписания такого электронного документа.

Учитывая необходимость применения электронных технологий, в том числе и в сфере документооборота, законодатель предусматривает возможность подписания сделки с использованием аналогов собственноручной подписи. К ним, в частности, относятся, воспроизведение подписи с помощью способов механического и другого копирования; электронно-числовой подписи и др. В этой связи хотелось бы обратить внимание на то, что законодатель не предусматривает исчерпывающего перечня аналогов собственноручной подписи, что, безусловно, является позитивным подходом и в полной мере соответствует методу диспозитивности частного права. Такая законодательная формулировка дает возможность сторонам договора самостоятельно определить, что может быть использовано в качестве аналога собственноручной подписи.

Необходимо отметить, что и в ГК Украины и в ГК РФ предусмотрены условия, при которых допускается использование для подписи сделки аналога собственноручной подписи. В результате сравнительного анализа статьи 160 ГК РФ и статьи 207 ГК Украины можно сделать вывод о некоторых отличиях в законодательствах обоих государств. Общим является то, что закрепляется правило о возможности использования в качестве подписи аналога собственноручной подписи только в трех случаях: во-первых, в случаях, установленных законом; во-вторых, в случаях, установленных актами гражданского законодательства (иными правовыми актами); в-третьих, в случаях, установленных соглашением сторон. Помимо этого, в ст. 206 ГК Украины к соглашению об использовании в качестве подписи аналога собственноручной подписи предъявляются определенные требования. Во-первых, такое соглашение должно быть заключено в письменной форме. Во-вторых, в соглашении должны содержаться образцы соответствующего аналога их собственноручных подписей. Представляется, что подобная детализация в ГК Украины вполне оправдана и имеет свои положительные стороны.

Необходимо отметить, что подписание договора посредством использования электронной (электронно-цифровой) подписи является наиболее урегулированным в законодательствах обоих государств. Отношения, связанные с получением и использованием электронной (электронно-числовой) подписи и в Украине и в РФ регулируются отдельными законами. В соответствии с законом РФ «Об электронной подписи» под электронной подписью понимается информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Закон Украины «Об электронной цифровой подписи» различает электронную подпись и электронную цифровую подпись. Под электронной подписью понимаются данные в электронной форме, которые добав-

ляются к другим данным или логично с ними связаны и предназначены для идентификации подписанта этих данных. Под электронной же цифровой подписью понимается вид электронной подписи, полученной по результатам криптографического преобразования набора электронных данных, который добавляется до этого набора или логично с ним соединяется и дает возможность подтвердить его целостность и идентифицировать подписанта.

Необходимо отметить, что процедура оформления электронной подписи в обоих государствах достаточно формализована, поэтому считаю, что получение такой подписи имеет смысл только в том случае, если субъект работает с большим объемом электронной документации. К таким субъектам, как правило, относятся субъекты предпринимательской деятельности. Для физических же лиц, которые хотят заключить семейный договор посредством электронных технологий, приобретение электронной подписи, на сегодняшний день, нецелесообразно. Для заключения разового договора, к числу которых, можно отнести и договоры, регулирующие семейные отношения, необходимо использовать иные аналоги собственноручной подписи. При этом в договоре должно быть указано, что определенное обозначение (например, электронный адрес сторон, ник и др.) является аналогом собственноручной подписи. В этой связи, необходимо отметить, что в качестве электронной подписи может быть использован и видеофайл, транслирующий чтение стороной договора вслух. Такой файл должен рассматриваться как часть договора, заключаемого в электронной форме.

Хотелось бы обратить внимание на то, что в качестве одного из недостатков электронного договора является сложность в идентификации подписанта. Именно поэтому, как уже отмечалось, законодательством и предусмотрена достаточно сложная процедура получения электронной подписи. Однако, специфика семейных договоров заключается в том, что они заключаются между членами семьи (бывшими членами семьи), то есть между людьми, которые хорошо друг друга знают, поддерживают общение, в том числе и посредством электронной переписки. Именно поэтому при идентификации стороны семейного договора, как правило, не возникает сложностей. В этой связи, можно сделать вывод о том, что семейные договоры могут быть заключены в электронной форме и подписаны с использованием аналога собственноручной подписи.

В тех же случаях, когда законодатель требует нотариального удостоверения договора, при заключении договора должны присутствовать или лично стороны, или их представители. А поэтому такие сделки подписываются только посредством собственноручной подписи стороны (представителя, рукоприкладчика). Таким образом, заключение семейного договора, требующего нотариального удостоверения через интернет на сегодняшний день невозможно.

Вышеизложенное позволяет прийти к выводу о том, что, во-первых, по общему правилу, семейные договоры могут быть заключены посредством сети интернет. Во-вторых, при заключении семейного договора в устной форме информация в электронной форме рассматривается как доказательство факта со-

вершения сделки и ее условий. В-третьих, при заключении семейного договора в простой письменной форме с использованием электронных средств, необходимо подписание такого документа посредством аналога собственноручной подписи сторон. При этом, электронная подпись при заключении семейного договора, как правило, не используется. Стороны самостоятельно выбирают обозначения, которые ими будут восприниматься в качестве подписи. В-четвертых, так как при нотариальном удостоверении сделки должны лично присутствовать или стороны, или их представители, заключение семейного договора, требующего нотариального удостоверения в электронной форме невозможно.

Пономаренко Ю.А.

НЕКОТОРЫЕ ВОПРОСЫ НАКАЗУЕМОСТИ «КОМПЬЮТЕРНЫХ»ПРЕСТУПЛЕНИЙ ПО ЗАКОНОДАТЕЛЬСТВУ УКРАИНЫ

Аннотация. Доклад посвящён проблемным вопросам установления и назначения наказания за совершение преступлений в сфере информационных технологий.

Ключевые слова: наказание; пенализация преступлений; назначение наказания.

Abstract. The report focuses on issues of concern to establish and punishment for crimes committed in the area of information technology.

Key words: punishment; penalize crimes; sentencing.

Бурное развитие информационных технологий в конце XX – в начале XXI веков породило множество ранее не известных видов общественных отношений, связанных с созданием, изменением, хранением, распространением, передачей, уничтожением etc информации на электронных носителях. В свою очередь это вызвало к жизни целый пласт нормативно-правовых предписаний, направленных на урегулирование указанных процессов. Появление новой сферы урегулированных правом общественных отношений создало и предпосылки для появления нового сегмента в структуре преступности, а именно – преступлений в сфере информационных технологий или, как их зачастую называют, «компьютерных» преступлений.

Реакцией государств на такого рода деяния стало введение в уголовные законы отдельных статей или целых разделов, в которых устанавливается уголовная ответственность за подобные деяния. Например, в различные разделы Особенной части УК Германии были введены отдельные параграфы, в которых установлена ответственность за те или иные «компьютерные» преступления (§ 202a, § 263a, § 303a, § 303b); в УК России включена отдельная глава 28 УК «Преступления в сфере компьютерной информации»; в Украине – раздел XVI Особенной части Уголовного кодекса 2001 г. (далее – УК), который называется «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи».

Для целей данного доклада мы рассматриваем в качестве «компьютерных» только преступления, предусмотренные разделом XVI Особенной части УК, и не рассматриваем иные виды преступлений, которые направлены против других объектов, но могут быть совершены с использованием компьютерной техники, информационных технологий, в том числе и Интернет-ресурсов (в частности: нарушение равноправия граждан (ст. 161 УК), мошенничество (ст. 190 УК), изготовление или распространение материалов, пропагандирующих культ насилия или жестокости, нетерпимость либо дискриминацию (ст. 300 УК) либо порнографических материалов (ст. 301 УК), разглашение государственной тайны (ст. 328 УК) и т.п.).

Итак, в 6 статьях раздела XVI УК содержится 12 санкций, из которых 6 установлены за основные составы преступлений и 6 – за квалифицированные. Привилегированных составов преступлений в разделе XVI УК не содержится.

Виды и размеры наказаний, установленных в санкциях данного раздела, свидетельствуют о том, что 5 из этих преступлений являются преступлениями небольшой тяжести, 3 – средней тяжести, 4 – тяжкими. Особо тяжких «компьютерных» преступлений уголовное законодательство Украины не предусматривает.

Из 12 санкций раздела XVI УК 7 являются альтернативными (в том числе 6 санкций установленных за основные составы преступлений), остальные 5 – безальтернативными (все они установлены за квалифицированные составы преступлений). Во всех безальтернативных санкциях установлено исключительно лишение свободы на определённый срок. Данный вид наказания вообще является наиболее часто используемым в санкциях за «компьютерные» преступления: вместе с альтернативными санкциями он, в общем, предусмотрен в 9 случаях. Сроки лишения свободы устанавливаются достаточно разнообразные: от 1 года до 2 лет (в ч. 1 ст. 361^1 и ч. 1 ст. 361^2 УК); от 1 года до 3 лет (в ч.1 ст. 361 и ч. 2 ст. 362 УК); от 1 года до 5 лет (ч. 2 ст. 361^1 и ч. 2 ст. 363^1 УК); от 2 до 5 лет (ч. 2 ст. 361^2 УК) и от 3 до 6 лет (ч. 2 ст. 361 и ч. 3 ст. 362 УК). Вторым по частоте использования является основное наказание в виде штрафа – он предусмотрен в 6 альтернативных санкциях. Его размер составляет либо от 500 до 1000 необлагаемых налогом минимумов доходов граждан (в ч. 1 ст. 361^1, ч. 1 ст. 361^2, ст. 363, ч. 1 ст. 363^1 УК) либо от 600 до 1000 н.м.д.г. (в ч. 1 ст. 361 и ч. 1 ст. 362 УК). Кроме того, в 4 санкциях содержится основное наказание в виде ограничения свободы (на срок от 1 года до 3 лет в ст. 363 и ч. 1 ст. 363^1, на срок от 1 года до 5 лет в ч. 2 ст. 363^1 и на срок от 2 до 5 лет в ч. 1 ст. 361 УК); в двух – в виде исправительных работ (в традиционном размере – на срок до двух лет (в ч. 1 ст. 361^1 и ч. 1 ст. 362 УК). Иных видов основных наказаний в санкциях раздела XVI УК не содержится.

Из 12 санкций раздела XVI УК 6 являются кумулятивными, поскольку содержат дополнительное наказание в виде лишения права занимать определённые должности или заниматься определённой деятельностью (в ч. 1 ст. 361 УК на срок от 1 года до 2 лет, в иных случаях – на срок от 1 года до 3 лет). В 5 из этих санкций данный вид наказания является обязательным, в 1 – факультативным. Иных видов дополнительных наказаний в санкциях данного раздела не содержится, хотя в 10 из них предусмотрена т.н. «специальная конфискация», а именно конфискация «программных или технических средств», принадлежащих виновному лицу и использованных при совершении конкретного преступления. Некоторые украинские криминалисты полагают, что данная мера воздействия является не внесённым в систему наказаний отдельным видом наказания. Однако согласиться с таким утверждением не представляется возможным, поскольку, во-первых, система наказаний носит закрытый характер, а, во-вторых, специальная конфискация не всегда обладает признаками вида наказания.

По данным Единого государственного реестра судебных решений (http://reyestr.court.gov.ua/) по состоянию на 01.03.2013 судами Украины вынесено 49 приговоров, которыми 54 лица были осуждены за совершение 66 «компьютерных» преступлений. В том числе: за несанкционированное вмешатель-

ство в работу ЭВМ, автоматизированных систем, компьютерных сетей и сетей электросвязи (ст. 361 УК) лица осуждались 36 раз (в т.ч.: по ч. 1–23 раза; по ч. 2–13 раз); за создание с целью сбыта либо сбыт вредоносных программ или технических средств, предназначенных для несанкционированного вмешательства в работу ЭВМ (ст. 361^1 УК) – 8 раз (все по ч. 1); за несанкционированное распространение информации с ограниченным доступом, хранящейся в ЭВМ, в автоматизированных системах или компьютерных сетях (ст. 361^2 УК) – 10 раз (в т.ч.: по ч. 1–7 раз; по ч. 2–3 раза); за несанкционированные действия с информацией, обрабатываемой в ЭВМ, автоматизированных системах или компьютерных сетях (ст. 362 УК) – 10 раз (в. т.ч.: по ч. 1 – 2 раза; по ч. 2 – 1 раз; по ч. 3–7 раз); за нарушение правил эксплуатации ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи, или порядка защиты обрабатываемой информации (ч. 2 ст. 363 УК) – 1 раз; за воспрепятствование работе ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи путём массового распространения сообщений электросвязи (ч. 1 ст. 363^1 УК) – 1 раз. Не подвергая анализу нерепрезентативные случаи осуждения по ч. 2 ст. 361^2, ч.ч. 1 и 2 ст. 362, ст.ст. 363 и 363^1 УК, обратим внимание на виды и размеры основных наказаний, назначенных при осуждении за иные «компьютерные» преступления.

Так, по ч. 1 ст. 361 УК, в санкции которой установлены основные наказания в виде штрафа от 600 до 1000 н.м.д.г. или ограничения свободы на срок от 2 до 5 лет, или лишения свободы на срок до 5 лет, суды назначали такие меры наказания:

а) лишение свободы – 7 раз (в т.ч.: на срок 1 год – 6 раз; на срок 2 года – 1 раз). Во всех случаях осуждённые были освобождены от его реального отбывания с испытанием (ст. 75 УК);

б) ограничение свободы на минимальный срок в 2 года – 5 раз и всякий раз осуждённый также освобождался от его отбывания с испытанием;

в) штраф – 11 раз и этот вид наказания всегда исполняется реально, если только не поглощается иным более строгим видом наказания при его назначении по совокупности преступлений либо приговоров. По данной статье штраф 5 раз назначался в минимальном размере, предусмотренном санкцией (600 н.м.д.г.), 1 раз – чуть выше медианы санкции (14000 грн, что соответствует 823,5 н.м.д.г.), остальные 5 раз – ниже низшего предела на основании ст. 69 УК.

По ч. 2 ст. 361 УК, в санкции которой предусмотрено безальтернативное основное наказание в виде лишение свободы на срок от 3 до 6 лет, суды во всех 13 случаях назначали минимальный срок лишения свободы (3 года) и в 12 случаях освободили осуждённых от отбывания этого наказания с испытанием. Лишь один раз назначенное наказание было обращено к исполнению.

По ч. 1 ст. 361^1 УК, в санкции которой предусмотрены альтернативные основные наказания в виде штрафа в размере от 500 до 1000 н.м.д.г. или исправительных работ на срок до 2 лет, или лишения свободы на тот же срок, суды 6 раз назначали различные сроки лишения свободы (в основном – 1 год), но каждый раз освобождали от его отбывания с испытанием. Дважды был назначен штраф: один раз в размере 600 н.м.д.г., другой – ниже низшего предела (250 н.м.д.г.).

При осуждении по ч. 1 ст. 361^2 УК, предусматривающей в качестве альтернативных основные наказания в виде штрафа в размере от 500 до 1000 н.м.д.г. или лишения свободы на срок до 2 лет, одно лицо было освобождено от назначения наказания (ч. 4. ст. 74 УК), пяти был назначен штраф (трём – по 500 н.м.д.г., одному – 600 н.м.д.г., одному – 50 н.м.д.г., т.е. ниже низшего предела). Ещё один осуждённый был приговорён к 1 году и 6 мес. лишения свободы, но освобождён от его отбывания с испытанием.

Наконец, по ч. 3 ст. 362 УК, санкция которой содержит безальтернативное основное наказание в виде лишения свободы на срок от 3 до 6 лет, шести осуждённым было назначено это наказание (четверым – по три года, двоим – по четыре), но все они были освобождены от его отбывания с испытанием. Ещё одному осуждённому на основании ст. 69 УК был назначен иной более мягкий вид наказания – штраф в размере 50 н.м.д.г.

Таким образом, при осуждении с назначением наказания за совершение «компьютерных» преступлений, предусмотренных ч.1 ст. 361, ч. 1 ст. 361^1 и ч. 1 ст. 361^2 УК, в санкциях которых содержатся альтернативные наказания в виде штрафа и лишения свободы, суды в 51,35 % случаев назначали лишение или ограничение свободы, но освобождали осуждённых от реального отбывания наказания с испытанием (ст. 75 УК), в остальных 48,65 % – назначали штраф. Причём последний вид наказания в 44,44 % случаев его применения определялся в минимальном предусмотренном санкцией размере; в 16,67 % – в размере выше минимума, но меньше максимума санкции; в остальных 38,89 % – ниже низшего предела, установленного в санкции. При осуждении по ч. 2 ст. 361 и ч. 3 ст. 362 УК, санкции которых предусматривают безальтернативное основное наказание в виде лишения свободы, суды Украины в 90 % случаев назначали лишение свободы (как правило, в минимальном предусмотренном санкцией размере), но с освобождением от его отбывания с испытанием. В 5 % случаев (1 раз) на основании ст. 69 УК был назначен штраф как иной более мягкий вид наказания, ещё в 5 % (1 раз) – назначенное наказание в виде 3 лет лишения свободы было обращено к реальному исполнению.

Достаточно редким является применение судами дополнительного наказания в виде лишения права занимать определённые должности или заниматься определённой деятельностью. Так, при осуждении по ч. 1 ст. 361 УК, в санкции которой данное наказание является факультативным, оно было назначено лишь в 3 случаях из 23 (13,04 %); при осуждении по ч. 2 ст. 361 УК, где лишение права является обязательным дополнительным наказанием, оно было назначено в 4 случаях из 13 (30,77 %). Ни разу не зафиксировано назначение этого вида наказания как дополнительного на основании ч. 2 ст. 55 УК за те «компьютерные» преступления, в санкциях за которые оно не предусмотрено.

Оценивая в целом современное состояние пенализации «компьютерных» преступлений, следует отметить следующее. Во-первых, она является достаточно суровой, о чём свидетельствует чрезмерное использования в санкциях лишения свободы и его достаточно длительные сроки (в трёх случаях – до 5 лет, в двух – до 6 лет). Представляется, что применение такой меры наказания к лицам, имеющим известный уровень знаний и способностей в сфере информа-

ционных технологий, зачастую может иметь негативный социальный эффект. Кроме того, следует обратить внимание на тот факт, что в данном разделе УК, который не содержит ни одного насильственного преступления, имеется лишь одна санкция (ч. 1 ст. 362 УК), не содержащая ни лишения, ни ограничения свободы. Наконец, об излишнем использовании в санкциях данного раздела наказания виде лишения свободы красноречиво свидетельствуют данные судебной статистики. Во-вторых, явно необоснованным является установление в этих санкциях архаичного наказания в виде исправительных работ, поскольку они должны отбываться по месту работы осуждённого, то есть во многих случаях именно там, где и было совершено «компьютерное» преступление. Возможно, именно поэтому данный вид наказания и не нашёл широкого применения в практике применения статей о «компьютерных» преступлениях. В-третьих, нельзя признать обоснованным отказ от использования в этих санкциях таких эффективных основных видов наказания как лишение права занимать определённые должности или заниматься определённой деятельностью и общественные работы. Достаточно эффективной заменой лишению свободы во многих санкциях могли бы стать арест и ограничение свободы. В-четвёртых, недостаточно использован потенциал штрафа, причём и как основного, и как дополнительного вида наказания. Прежде всего, современная редакция ст. 53 УК позволяет существенно увеличить суммы штрафа, в тех случаях, когда он предусмотрен de lege lato. Хотя судебная практика пока вполне обходится нынешними размерами штрафа, однако определённый «запас» его суммы не будет лишним для случаев совершения «компьютерных» преступлений повышенной степени общественной опасности. Кроме того, de lege ferenda штраф мог бы быть установлен как основное наказание в большем количестве санкций, а в некоторых – мог бы стать дополнительным наказанием взамен т.н. «специальной конфискации».

Изложенное позволяет заключить, что и догматический, и эмпирический анализ санкций статей раздела XVI УК свидетельствуют, с одной стороны, о значительно завышенной степени суровости установленных в них наказаний, с другой – о недостаточном использовании возможностей целого ряда видов наказания, альтернативных лишению свободы. Представляется, что в дальнейшем уголовное законодательство Украины должно пойти по пути известного смягчения и дифференциации ответственности за совершение этих преступлений. Однако то или иное реформирование законодательно определяемого уровня наказуемости может иметь место лишь на основании единой теоретической модели пенализации преступлений. Разработка же последней является одной из наиболее насущных задач уголовно-правовой науки.

Прокопенко А.Н.
Дрога А.А.

ЗАЩИТА СВЕДЕНИЙ СОСТАВЛЯЮЩИХ ПРОФЕССИОНАЛЬНУЮ ТАЙНУ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СОТРУДНИКАМИ ПОЛИЦИИ

Аннотация. Статья посвящена рассмотрению вопросов касающихся защиты конфиденциальных данных сотрудниками полиции, в правовом и техническом контексте.
Ключевые слова: профессиональная тайна, служебная тайна, конфиденциальная информация, защита информации, органы внутренних дел.
Abstract. The article deals with the issues relating to the protection of confidential data by the police, the legal and technical context.
Key words: professional secrecy, official secrets, confidential information, information security, internal affairs bodies.

Изменения, произошедшие в нашей стране и в мире в последние двадцать лет, выдвинули на первый план вопросы информационного обеспечения, информационного обслуживания и защиты информации. За счет развития Интернет информация стала общедоступной, появилась возможность ее передачи на неограниченные расстояния в практически любых объемах и в реальном масштабе времени. В результате доступ любого человека к различным информационным ресурсам значительно упростился.

Увеличение количества процессов обмена информацией неизбежно приводит к тому, что общедоступными становятся сведения, которые имеют ограниченный доступ. Это наносит серьезный ущерб не только отдельным гражданам и организациям, но и безопасности государства.

Служебная тайна сотрудника полиции представляет собой особый режим информации с ограниченным доступом. С такими режимами информации как адвокатская тайна, врачебная тайна, тайна нотариальных действий и др., ее объединяет то, что все они являются видами конфиденциальной информации, различающимися по свойствам субъекта, осуществляющего охрану сведений.

Все рассуждения о защите информации, являющейся профессиональной тайной, без нормативного закрепления такого понятия являются очень условными. Другими словами, они могут с таким же успехом быть отнесены к обеспечению безопасности любого вида конфиденциальной информации.

Без определения перечня сведений, составляющих профессиональную тайну в органах внутренних дел, закрепленного на законодательном уровне, можно лишь рассуждать об обеспечении режима конфиденциальности сведений, представляющих государственную тайну, либо об обеспечении защиты персональных данных, которые могут быть частью каждого из вышеназванных видов тайн.

В отличие от установления режима государственной и служебной тайны режим конфиденциальности профессиональной тайны устанавливается обладателем сведений, составляющих такую тайну, который и предпринимает правовые, организационные, технические и иные меры по охране ее конфиденциальности.

На наш взгляд полиция в своей деятельности руководствуется двумя принципами: соблюдение требований законодательства и выполнение поставленных перед собой целей деятельности. Этими же принципами нужно руководствоваться при обеспечении защиты любой информации в органах внутренних дел[1].

Каждый сотрудник полиции должен в связи с выполнением своих служебных обязанностей, а именно обеспечивать конфиденциальность профессиональной тайны и персональных данных граждан:

- знать и соблюдать требования по получению, обработке, передаче, хранению, получению сведений, составляющих профессиональную тайну, предусмотренные нормативными правовыми актами;
- принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами;
- не использовать без разрешения обладателя сведения, составляющие профессиональную тайну, в целях, не связанных с осуществлением своих должностных обязанностей;
- незамедлительно сообщать об утрате или несанкционированном уничтожении сведений, составляющих профессиональную тайну, своему непосредственному руководителю. А также об иных обстоятельствах, создающих угрозу сохранению конфиденциальности таких сведений.

Сложности в защите конфиденциальных данных (профессиональной тайны) сегодня заключаются не столько в технической плоскости (как защитить), сколько в организационной. Для того чтобы информация была надежно защищена, важно всего один раз написать политику информационной безопасности и внедрить процесс мониторинга ее соблюдения и актуализации. Озаботиться охраной данных нужно уже сейчас. Если дожидаться, пока будет утвержден федеральный закон о профессиональной тайне, пока выйдут подзаконные акты, устанавливающие способы защиты информации, может быть потеряно очень много сведений.

В настоящее время в МВД России происходит унификация существующего программного обеспечения и обеспечивается информационное взаимодействие с другими министерствами и ведомствами. Это связано с переходом на предоставление государственных услуг и исполнение государственных функций в электронном виде федеральными органами исполнительной власти.

Для обработки, накопления, размножения или передачи служебных сведений ограниченного распространения в МВД России используются средства компьютерной техники и электронной оргтехники при условии соблюдения организационных мер, а также применения сертифицированных программных и программно-аппаратных средств, ограничивающих свободный доступ информации в соответствии с требованиями секретного приказа МВД России, регламентирующего меры по технической защите информации в органах внутренних

[1] А. Н. Прокопенко, А. А. Дрога Правовое регулирование оборота информации, относящейся к служебной и профессиональной тайне в органах внутренних дел // монография. – Белгород: Бел ЮИ МВД России, 2011

дел Российской Федерации и внутренних войсках Министерства внутренних дел Российской Федерации.

Сведения, отнесенные к профессиональной тайне, также как и секретная информация, могут являться предметом заинтересованности со стороны различного рода разведывательных служб и криминальных кругов. Поэтому ее безопасность должна носить комплексный характер, предусматривающий создание следующих подсистем защиты, включая и ее правовой контекст:

- защиты от утечки по акустическим и виброакустическим каналам;
- защиты от утечки по цепям электропитания;
- предотвращения использования телефонов сотовой связи;
- разграничения доступа к ресурсам корпоративной сети;
- защиты от несанкционированной звукозаписи;
- обнаружения источников радиоизлучения и видеокамер;
- контроля и управления доступом в помещение, сигнализации и др.

Для планирования и проведения мероприятий по технической защите информации составляющую профессиональную тайну, включая и секретную информацию, необходимо провести категорирование объектов, содержащих данную информацию, и их техническую паспортизацию.

К охраняемой информации среди прочих относят информацию о частной жизни физического лица и персональные данные, коммерческую и профессиональную тайну.

Основным вопросом для владельцев информационных систем остается способ организации информационного обмена между находящимися в разных зданиях сегментами информационных систем, с другими информационными системами, а также с удаленными пользователями.

Для работы с информационными системами, обрабатывающими охраняемую информацию, принято использовать выделенные каналы передачи данных. Подключение информационных систем, обрабатывающих охраняемую информацию, к сетям общего пользования, в том числе к глобальной сети Интернет, запрещается.

Для обеспечения передачи охраняемой информации с использованием сетей общего пользования рекомендуется применять выделенные компьютеры. Данные компьютеры не имеют подключения к локальной сети передачи данных, на них запрещается обрабатывать охраняемую информацию в открытом виде, передача данных должна осуществляться в зашифрованном виде, перенос которых осуществляется с применением съемных носителей.

Эффективность решения задач по обеспечению информационной безопасности на современном уровне во многом определяется оптимальностью поддерживающей инфраструктуры, основными элементами которой являются подразделения защиты информации. В связи с этим проводится работа, направленная на совершенствование организационно-штатной структуры подразделений защиты информации на всех уровнях системы МВД России, укрепление кадро-

вого потенциала и развитие системы профессиональной подготовки специалистов по защите информации[1].

В настоящее время ведется работа по совершенствованию информационных систем и продуктов в МВД России, что должно положительно повлиять на обеспечение сохранности конфиденциальной информации (в том числе профессиональной тайны) сотрудниками ОВД. Так обозначены основные направления внедрения информационных технологий в деятельность МВД России на 2012-2014 годы[2]:

- завершение создания интегрированной мультисервисной телекоммуникационной сети (далее ИМТС) и обеспечение подключения к ней 100% объектов МВД, в том числе обеспечение доступа к сервисам ИМТС с мобильных устройств;
- проектирование и разработка типового унифицированного программно-технического решения обеспечения деятельности органов внутренних дел на региональном и территориальном уровне;
- дальнейшее совершенствование систем автоматизированных банков данных общего пользования ОВД и создание единой системы доступа к содержащимся в них данных, в т.ч. на межведомственном уровне;
- создание единой системы центров обработки данных для централизации всех информационных ресурсов МВД России и обеспечения функционирования типового программного обеспечения;
- разработка общей политики и общих требований, задачи по обеспечению защиты конкретных систем решаются в рамках реализации отдельных систем и приложений;
- создание центра управления и обеспечения эксплуатации Системы.

В заключении хотелось бы отметить, что организационные и технические меры защиты профессиональной тайны, при обработке в информационных системах, должны составлять единый комплекс. Данным вопросам уделено довольно много внимания в специальной технической литературе и посвящено большое количество научных исследований и технических изысканий в нашей стране и мире.

---

[1] Чирков К.А. О перспективах развития защиты информации в системе МВД России // Информационные технологии, связь и защита информации МВД России. 2011. №1.

[2] См.: Приказ МВД России от 30 марта 2012 г. № 205 «Об утверждении концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012 – 2014 годах».

Прохорова М.В.

СРЕДСТВА ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ И СТЕПЕНЬ ИХ ЭФФЕКТИВНОСТИ

Аннотация. В статье содержаться современные методы и средства защиты, проблемы и рекомендации по выбору подходящей антивирусной защиты, а также произведена оценка эффективности представленного защитного комплекса в целом.

Ключевые слова: вредоносное программное обеспечение, средства борьбы с компьютерным мошенничеством, брандмауэры; антивирусные программы, их проблемы.

Abstract. The article contained modern methods and means of protection, challenges and recommendations for choosing a suitable anti-virus protection, and evaluated the effectiveness of the protective presented in whole.

Key words: malware, anti-fraud computer, firewall, anti-virus, their problems.

В нашу жизнь все настойчивей вливаются и прочно закрепляют свои позиции, так называемые, информационные технологи. Не так давно, мы и помыслить не могли, что наступит век виртуального реальности, компьютерных сетей, сотовой связи, где мы уже не мы без мобильного телефона, ПК, ноутбука или планшета. Изначально, это были скорее предметы роскоши, теперь – необходимость.

Появление такого рода новшеств существенно упростило нашу жизнь. Что обуславливает вовлечение огромной массы людей, их вложений, и как следствие «любителей легкой наживы». А компьютерные сети просто клондайк для недобропорядочных пользователей.

Статистика показывает, что количество совершаемых преступлений в сфере компьютерной информации неумолимо растет, несмотря на законодательно закрепленную ответственность за преступления в данной сфере. Например, в соответствии со ст. 273 УК РФ создание, использование, или распространение вредоносных компьютерных программ, либо иной компьютерной информации заведомо предназначенных для несанкционированного уничтожении, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации влечет наказание в виде лишения свободы до четырех лет и т.д.

Правоохранительные органы пытаются адекватно реагировать, но борьба с последствиями куда более эффективна в тандеме с профилактикой преступлений в обозначенной выше области. Поэтому постараемся разобраться, и предложить наиболее приемлемые пути решения этой проблемы.

Анализ различных источников показал, что к определению вредоносного программного обеспечения (ВПО) или вредоносной программы авторы подходят неодинаково, рассмотрим некоторые из них. В Уголовном кодексе в редакции от 07.07.2003 дано следующее определение вредоносному программному обеспечению: ВПО – это программа для электронно-вычислительной машины (ЭВМ) или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ и их

сети[1]. Представители Лаборатории Касперского определяют «вредоносное ПО» следующим образом: «к ВПО относятся сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие какой-либо вред компьютеру, на котором они запускаются, или другим компьютерам в сети»[2]. Доктор Веб и вовсе не дает определения, а лишь перечисляет и описывает программы и технологии, относящиеся к этой категории. Также известны два основных способа проникновения вредоносных программ в систему: социальная инженерия (от анг. «social engineering») и технические приемы внедрения вредоносного кода в заражаемую систему без ведома пользователя[3].

Как же обезопасить себя от подобного рода посягательств.

Выделяют три группы средств борьбы с компьютерным мошенничеством и методов обеспечения безопасности от вредоносного ПО: юридические, образовательные и технические. Юридические включают в себя нормативно-правовую базу государства, и формы ее применения в данной сфере. На основе образовательных и технических методов, а также, исходя из известных способов заражения систем, Microsoft Corporation предлагает следующие рекомендации по обеспечению безопасности ПК и информации на нем:

1. Создать защиту для своего ПК:

1.1.Установить антивирусные и антишпионские программы из надежных источников (MS предлагают свои варианты таких программ, или же рекомендуют выбрать источник из списка их партнеров);

1.2.Регулярное обновление ПО (в данном случае противодействие не должно отставать от действия, в противном случае заражение неизбежно);

1.3.Использовать надежные пароли и хранить их в секрете – не менее 14 символов обеспечит более или менее надежный уровень защиты (простое правило, но им часто пренебрегают);

1.4.Не отключать брандмауэр. Тут следует пояснить, что это такое и зачем он нужен. Брандмауэр – это специальная программа или устройство, которое позволяет блокировать попытки хакеров, вирусов, и червей получить доступ к вашему ПК через Интернет. Операционные системы Windows 7, Windows Vista и Windows XP SP2 и выше содержат встроенный брандмауэр, который включен по умолчанию.

1.5.Соблюдать осторожность при использовании флеш-накопителей.

2. Не соглашаться на загрузку, предлагаемую вредоносным ПО:

2.1.С осторожностью относиться к вложенным файлам и ссылкам в электронной почте, мгновенных сообщениях и публикациях в социальных сетях, даже если отправитель вам известен.

---

[1] Уголовный Кодекс Российской Федерации от 13.06.1996 №63-ФЗ, редакция от 07.07.2003 г. [Электронный ресурс] // КонсультантПлюс [сайт]. – Режжим доступа: URL: http://base.consultant.ru

[2] Глоссарий [Электронный ресурс] // Securelist [сайт]. – Режим доступа: URL: http://www.securelist.com

[3] Вредоносные программы [Электронный ресурс] /DrWEB Антивирус [сайт]. – Режим доступа: URL: http://vms.drweb.com/malware/

2.2.Не нажимайте кнопки «Согласен», «ОК», или «Я принимаю» в баннерной рекламе, в неожиданных всплывающих окнах или предупреждениях на сайтах, которые кажутся незнакомыми;

2.3.Загружайте ПО только на сайтах, которым вы доверяете. С осторожностью относитесь к «бесплатным» загрузкам медиа-информации[1].

Этих же рекомендаций придерживается и Лаборатория Касперского.

Что касается конкретно антивирусных программных средств, необходимо отметить, что при их выборе необходимо учитывать:

– уровень детектирования вредоносных программ;

– частота и регулярность выхода обновлений;

– возможность корректного удаления вирусного кода из системы;

– ресурсоёмкость;

– возможность использования двойной защиты от разных производителей;

– умение защищать не только от уже известных, но и от новых вирусов и троянских программ.

Из выше перечисленных критериев вытекают следующие проблемы:

– появление вредоносных программ растет количественно и усложняется качественно, не каждой антивирусной компании под силу держать такой темп, и удержать позиции на этом рынке, любая задержка чревата пользователю их услуг определенными негативными последствиями, что неизбежно приводит к упадку спроса на данную продукцию.

– изначально ВПО писалось, как правило, студентами, самоучками, подростками-хулиганами, что говорит об их простоте и относительно небольшой опасности. А что мы видим теперь, по данным «Лаборатории Касперского» около 75% вирусов написано лицами, имеющими специальную подготовку и исключительно в криминальных целях, что значительно повышает сложность их обнаружения и предотвращение инфицирования ими, а также значительную степень их опасности для пользователя. Следовательно, необходима своевременная и эффективная защита, которую обеспечить в силах далеко не все производители антивирусов.

– возможность изъятия и уничтожения вредоносного кода из зараженной системы корректно, тоже задача не из легких. Сложность состоит в том, что составляющие ВПО предпринимают определенные действия, чтобы скрыть в первую очередь сам факт своего присутствия в системе, а также может встраиваться в нее настолько глубоко, что иногда невозможно его удаление без утраты зараженного объекта в целом.

– сложность в сбалансированности производительности и полноценной защиты. Тут необходимо расставить приоритеты, что важнее высокая производительность или надежная защита, а может несложно найти компромисс. Быстродействие антивирусной программы, как правило, говорит о ее ненадежности. А вот низкая скорость работы, не гарантирует ее качества.

---

[1] Методы улучшения защиты от вредоносного ПО и безопасности компьютера [Электронный ресурс] // Центр безопасности Microsoft [сайт]. – Режим доступа: URL: http://www.microsoft.com/ru-ru/security/pc-security/protect-pc.aspx

– несовместимость различных антивирусных программ или их технологическая несовместимость, и как следствие невозможность в большинстве случаев создания «двойной защиты», т.е. установки двух и более антивирусных программ от разных производителей[1].

Как же выбрать подходящий антивирус, самый надежный советчик – компетентное тестирование, проводимое различными компьютерными изданиями, но, к сожалению, их не там много. Для проведения подобных исследований необходимо определенное оборудование, специально обученный персонал, помещение, и т. д. Увы, не каждое издание способно себе такое позволить.

Таким образом, становится ясно, что эффективность различных способов борьбы с вредоносным вмешательством и средств защиты от него по отдельности, достаточно высока, но недостаточна для создания полноценной защиты от преступного посягательства на компьютерную информацию. Куда выше уровень надежности обеспечит комплекс описанных выше методов. Ни полноценная правовая база, ни технические, технологические новшества не обезопасят вас в полном объеме, если вы лично не позаботитесь об этом. А что для этого необходимо, разумеется, соответствующая информационная база (которой сейчас изобилует Интернет), достаточно высокий уровень ваших знаний, использование выше описанных рекомендаций по обеспечению защиты своего ПК, регулярного ознакомления с рекомендациями производителей антивирусов. Повышение уровня личной ответственности, своевременная осведомленность о новинках и угрозах в данной сфере, принятия максимума мер по обеспечения защиты ЭВМ и информации, находящейся на ней, обеспечит спокойное существование не только самому пользователю, но и создаст определенные сложности злоумышленникам, что в свою очередь притормозит рост преступности в данной сфере. Именно борьба на всех уровнях (пользователь, органы правопорядка, производители антивирусных программ), способна обеспечить необходимый уровень безопасности от подобного рода посягательств, а также предотвратить в определенной мере наступление серьезных последствий.

[1] Качество антивирусной защиты и проблемы антивирусных программ [Электронный ресурс] // Securelist [сайт]. – Режим доступа: URL: http://www.securelist.com

Романенко Р.В.
Степанюк О.С.

АНАЛИЗ ПОНЯТИЯ «КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ»

Аннотация. В статье анализируется отечественное уголовное законодательство о защите компьютерной информации, разбираются основные понятия, данные в гл. 28 УК РФ.
Ключевые слова: глобализация, компьютерная информация, информационная безопасность, информационные преступления.
Abstract. The paper analyzes the domestic criminal legislation to protect computer information, understand the basic concepts, the data in Sec. 28 of the Criminal Code.
Key words: globalization, computer information, information security, information crimes.

В условиях формирования глобального информационного общества огромное значение придается вопросам обеспечения безопасности, в частности, противодействию преступным посягательствам в сфере обращения цифровой информации.

Всеобщая информатизация общества обострила указанную проблему и вызывает острую необходимость разработки соответствующей государственной политики.

Так, Совет Безопасности Российской Федерации к числу основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации отнес проблему нормативно-правового регулирования отношений в области борьбы с преступлениями в сфере информационно-коммуникационных технологий[1].

В последние 15 лет в России успешно развиваются новые виды систем обращения цифровой информации, в число которых входят: мобильная, спутниковая, цифровая связь, а также различные системы персональной беспроводной связи.

Опасность преступлений в сфере цифровой информации обусловливается и определенным ростом их количества, сложной «технической латентностью» составов. Так, по мнению У.В. Зининой, реальная статистика раскрываемых преступлений в сфере компьютерной информации в России искажена в результате не всегда правильного применения в следственной и судебной практике гл. 28 УК РФ, в том числе из-за расширительного толкования элементов содержащихся в ней составов преступлений и фактического непонимания технических реалий[2].

---

[1] Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. Утв. исполняющим обязанности Секретаря Совета Безопасности Российской Федерации, председателя научного совета при Совете Безопасности Российской Федерации 7 марта 2008 г. URL: http://www.scrf.gov.ru/documents/94.html (дата обращения: 12.02.2013).

[2] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Автореф. дис. ... канд. юрид. наук. М., 2007. С. 13

Внедрение компьютеров в особо важные сферы жизни общества вызвало необходимость усиления уголовно-правовой охраны компьютерной информации от преступных посягательств. Так как после принятия Уголовного кодекса Российской Федерации 1996 года, в который была введена глава 28, предусматривающая ответственность за преступления в сфере компьютерной информации, прошел значительный период времени, удалось выявить некоторые ее недостатки. Федеральным законом от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» предусмотрена новая редакция всех трех статей главы 28 УК РФ, однако, по нашему мнению, законодатель недостаточно полно и технически верно отобразил понятие самой «компьютерной информации». Ранее понятие компьютерной информации приходилось трактовать исходя из диспозиции ст. 272 УК РФ как «информацию на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети». При этом содержание самого понятия «информация» законодатель в УК РФ не раскрывал. Теперь же примечание к ст. 272 УК РФ содержит определение этого понятия, где под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Понятие информации как «сведений, сообщений, данных независимо от формы их представления» было введено Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации». Развивая положения вышеназванного нормативно-правового акта, законодатель указывает, что, будучи представленными в форме электрических сигналов, сведения, сообщения и данные становятся компьютерной информацией.

Таким образом, под защиту уголовного закона попала и та информация, которая еще не зафиксирована на каком-либо носителе или устройстве, а находится в процессе передачи. Это должно расширить сферу применения данной статьи. Однако информация, передаваемая по беспроводным и оптическим каналам связи, не будет являться объектом уголовно-правовой охраны, т.к. не подпадает под определение электрических сигналов при трактовке этого термина с точки зрения физики. В связи с этим использование такого термина, как «электрический сигнал», лишь вводит в заблуждение и поэтому нуждается в дальнейшем разъяснении или замене более подходящим термином. Сходной позиции придерживается и Верховный Суд Российской Федерации, который в официальном отзыве от 7 апреля 2011 г. № 1/общ-1583. «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» отмечает, что предложенный в примечании к ст. 272 УК РФ термин «электрический сигнал» не вносит достаточной ясности в определение понятия и требует дополнительного пояснения»[1].

[1] Официальный сайт компании «Консультант Плюс». URL: http://base.consultant.m/cons/cgi/online.cgi?req=doc;base=PRJ;n=87058 (дата обращения: 12.02.2013).

В заключение Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05.07.2011 «На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» (к первому чтению)» данная позиция получила развитие. Более того, там указывается, «что понятие компьютерной информации отсутствует в федеральных законах, а в предлагаемой дефиниции неясен смысл термина «электрические сигналы». Представляется необходимым уточнить данную формулировку. Понятие компьютерной информации дается в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (от 1 июня 2001 г.). Согласно пункту «б» статьи 1 названного Соглашения компьютерная информация – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»[1]. Предложения о заимствовании понятия компьютерной информации из этого Соглашения высказывались и ранее[2]. Ввиду недостаточной ясности термина «электрический сигнал», который используется в настоящее время в определении компьютерной информации в примечании к ст. 272 УК РФ, вышеназванное предложение о заимствовании этого определения из Соглашения вновь может стать предметом научной дискуссии.

В связи с вышеизложенным нами предлагается решить существующее противоречие следующим образом: понятие «компьютерная информация» следует заменить на понятие «электронная информация», так как компьютерная информация является одним из видов электронной информации. Кроме того, ввиду недостаточной ясности термина «электрический сигнал», который используется в настоящее время для раскрытия понятия «компьютерной информации» (электронной информации) в примечании к ст. 272 УК РФ, представляется необходимым изменить существующее законодательное определение и изложить его в следующем виде: «Под электронной информацией понимаются сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи». Видится, что предложенные изменения могли бы способствовать более широкому применению как ст.272 УК РФ, так и норм главы 28 УК РФ, что поспособствует решению сложившихся в законе противоречий, устранению судебных ошибок и правовых коллизий.

---

[1] Официальный сайт компании «Консультант Плюс». URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=90718 (дата обращения: 12.02.2013).

[2] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: Автореф. дис. ... канд. юрид. наук. М., 2005. С. 8.

Семенов Р.И.

ОСОБЕННОСТИ СИСТЕМНОГО СУБЪЕКТНОГО КОНТРОЛЯ В СФЕРЕ ЗАЩИТЫ ПРАВ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Аннотация: В данной статье рассматривается вопрос защиты детей от информации, причиняющей вред их здоровью и развитию, а также субъекты, противодействующие неблагоприятному Интернет контенту.

Ключевые слова: контроль Интернет пространства, защита детей, национальная безопасность государства, субъекты контроля.

Abstract: This paper addresses the issue of protecting children from information harmful to their health and development, as well as subjects that oppose unfavorable Internet content.

Key words: control of the Internet space, protection of children, national security state, the regulated community.

Согласно Национальной стратегии действий в интересах детей на 2012 – 2017 годы[1], в последнее десятилетие обеспечение благополучного и защищенного детства стало одним из основных государственных приоритетов России. Проблемы подрастающего поколения и пути их решения нашли свое отражение в Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, Концепции демографической политики Российской Федерации на период до 2025 года. Долгожданным и вполне логичным стало появление первого в своем роде законодательного акта, достаточно подробно регулирующего информационную сферу жизни, прямо затрагивающую интересы детства – Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»[2].

Широкое распространение передовых компьютерных технологий, открытость информационного пространства привели к незащищенности детей перед лицом телекоммуникационной сети Интернет. Приобрели более громкое звучание такие проблемы как – торговля детьми, детская порнография, проституция, в сети все чаще появляются подробнейшие обзоры информации, популяризирующей наркотизацию общества. Существует значительное число сайтов, посвященных суицидам, которые доступны подросткам в любое время. Помимо порнографии, педофилии в Интернете существует еще одна немаловажная угроза для несовершеннолетних пользователей – многочисленные экстремистские направления – как политического, так и религиозного характера. Важной целью является создание возможностей для их отслеживания. Для этого государству требуется, прежде всего, отлаженная система мониторинга контента, что становится задачей для органов и сотрудников, обладающих профессиональными знаниями в данных областях. Для компаний, отвечающих за поставку

[1] Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы» // Собрание законодательства РФ. – 2012. – № 23. Ст. 2994.

[2] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета. – 2010. – № 297.

услуг коммуникаций, повышается ответственность и ужесточается контроль за добросовестностью проводимых мер по сведению к нулю таких проявлений. И наконец, на первые места выходит проблема территориальности, то есть, если Интернет ресурс зарегистрирован за пределами государства, предъявить ему обвинение из России, зачастую, не представляется возможным.

Исходя из вышеперечисленного, законодатель начинает формировать базу национальной безопасности государства, закладывает основы создания четкой и выверенной политики в области духовно-нравственного воспитания детей, вводит ограничения или даже запрет на использование в средствах массовой информации определенных программ и зрелищ, которые пропагандируют насилие, жестокость и антиобщественное поведение. Национальная стратегия в качестве мер противодействия подобному негативному влиянию Интернет ресурсов предусматривает: блокирование информационных каналов проникновения в детско-подростковую среду элементов криминальной психологии, создание как государственных, так и общественных экспертиз детского Интернет контента, обучение детей определенным правилам безопасного для них поведения на просторах Интернет сети и защиты от возникновения различного рода зависимостей[1]. Были определены границы ответственности Интернет провайдеров, администраций социальных сетей, телекоммуникационных компаний за те услуги, которые они предоставляют. Так, Государственная Дума 15 февраля 2013 года приняла поправки в КоАП Российской Федерации, которые обозначили рамки административной ответственности лиц, предоставляющих доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, в местах, доступных для детей.

Статьи 20-21 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» разделили органы, осуществляющие такую защиту в пределах своей компетенции, на два типа – государственные и общественные. К государственным относятся федеральные органы исполнительной власти и органы исполнительной власти субъектов Российской Федерации. На практике этим органом является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), осуществляющая функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации[2], а также осуществляющая процедуру лицензирования, ре-

---

[1] Концепция формирования национального плана (Стратегии) действий в интересах детей Российской Федерации (проект) // www.council.gov.ru/kom_home/ccf_educ/analytics/item2373.html: 01.03.2013

[2] Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 26.10.2012) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») // Российская газета. – 2009. – № 49.

гистрации и стандартизации в сфере массовой информации. В субъектах действуют региональные управления (например, управление Роскомнадзора по Белгородской области). Из наиболее ярких первичных мер по обеспечению деятельности Роскомнадзора в исследуемой области следует отметить создание «Единого реестра доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено». Это «творение» ведомства направлено на общественное участие в данной проблеме, так как заявку на включение конкретного сайта в ряды нежелательных может оставить любой посетитель с указанием причины.

К иным функциям Федеральной службы относятся:

-разработка и реализация единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию;

– разработка и реализация федеральных целевых программ обеспечения информационной безопасности детей, производства и оборота информационной продукции для детей;

– установление порядка проведения экспертизы информационной продукции, предусмотренной Федеральным законом[1].

К органам и лицам, прямо не указанным в законе, но в силу своей деятельности участвующим в контроле за информационным пространством в сфере обеспечения интересов детей относятся также правоохранительные органы Российской Федерации, Уполномоченный по правам ребенка при Президенте Российской Федерации[2], Общественная палата Российской Федерации[3] и их региональные представители, а также органы местного самоуправления, в пределах своей компетенции осуществляющие контроль и надзор в сфере распространения информации, способной нанести вред здоровью и развитию несовершеннолетних[4]. Эти субъекты являются, с одной стороны, связующим звеном государственных контролирующих органов с общественными, а с другой, – выполняют самостоятельные функции по надзору за безопасностью детей на Интернет пространстве. Например, Уполномоченный по правам ребенка наделяется широким комплексом контрольных и надзорных функций по проведению проверок деятельности федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, а также должностных лиц и получении от них соответствующих разъяснений, а также по привлечению в установленном порядке для осуществления экспертных и научно-

---

[1] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета. – 2010. – № 297.

[2] Указ Президента РФ от 01.09.2009 № 986 «Об Уполномоченном при Президенте Российской Федерации по правам ребенка» // Собрание законодательства РФ. – 2009. – № 36. Ст. 4312.

[3] Федеральный закон от 04.04.2005 № 32-ФЗ (ред. от 06.12.2011) «Об Общественной палате Российской Федерации» // Российская газета. – 2005. – № 70.

[4] Безугленко О.С. Классификация субъектов защиты несовершеннолетних от воздействия вредной информации // Информационное право. – 2011. – № 2. С. 9 – 12.

аналитических работ, касающихся защиты прав ребенка, научных и иных организаций, а также ученых и специалистов, в том числе на договорной основе[1]. В этой связи заслуживает особого внимания деятельность Уполномоченного по правам ребенка города Санкт-Петербурга, которая в своих докладах неизменно касается данной проблематики[2]. В обеспечении своей деятельности неоднократно принималось участие в заседаниях Общественного Совета при прокуратуре Санкт-Петербурга, на которых данная тема стала переходить из плоскости теории в плоскость реальных практических контрмер.

При поддержке Комитета по образованию Санкт-Петербурга, Комитета по вопросам законности, правопорядка и безопасности были проведены исследования, согласно которым:

– 60,2% несовершеннолетних сталкивались с информацией противоправного или сексуально-эротического содержания случайно;

– 42,6 % сталкивались случайно со сценами насилия.

Столкнувшись с противоправной информацией, 61,4% подростков сообщают о них:

– 56% друзьям;

– 34% родителям и другим родственникам.

В случае наступления негативных последствий для ребенка (психологической травмы или физического насилия) в результате Интернет-знакомства, только каждый третий обратился за помощью[3].

Из приведенной статистики, можно сделать выводы о недостаточной пока степени участия государственных и общественных организаций в проблеме защиты детей от некачественного Интернет контента. На данный момент вопрос чаще рассматривается и решается на внутрисемейном уровне, поскольку не все граждане осведомлены о деятельности организаций, занимающихся попытками «вылечить» Интернет пространство.

Зарегистрированные в установленном Федеральным законом порядке общественные объединения и иные некоммерческие организации в соответствии с их уставами, а также граждане также вправе осуществлять в соответствии с законодательством Российской Федерации общественный контроль за соблюдением требований законодательства в области защиты несовершеннолетних от воздействия информации, способной нанести вред их здоровью и развитию. Наибольшую известность среди подобных организаций приобрели межрегиональная правозащитная организация «Сопротивление», Центр безопасного Интернета в России, Фонд «Дружественный Рунет», региональная общественная организация «Центр социальных программ в сфере благополучия населения «Время жить». К крупным Интернет ресурсам, занимающимся непосредствен-

---

[1] Безугленко О.С. Классификация субъектов защиты несовершеннолетних от воздействия вредной информации // Информационное право. – 2011. – № 2. С. 9 – 12.

[2] Ежегодный доклад Уполномоченного по правам ребенка в Санкт-Петербурге за 2011 год // www.do.znate.ru/docs/index-23797.html?page=17: 28.02.2013

[3] Там же.

ной помощью государственным органам, следует отнести «Лигу безопасного Интернета».

К функциям общественного контроля можно отнести:

– противодействие распространению опасного контента в сети;

– объединение профессионального сообщества, участников Интернет рынка для выработки механизмов саморегуляции сообщества;

– оказание реальной помощи детям и подросткам, которые прямым или косвенным образом стали жертвами распространения опасного контента в сети Интернет;

– оказание содействия государственным структурам в борьбе с владельцами Интернет ресурсов, занимающимися созданием и распространением опасного контента: детская порнография, пропаганда наркомании, насилия, фашизма и экстремизма;

– участие в разработке законодательных инициатив, направленных на ликвидацию опасного контента в сети Интернет[1].

Таким образом, можно сделать следующие выводы: одним из наиболее приоритетных направлений в сфере защиты детей, является повышение ответственности Интернет провайдеров, администраций социальных сетей, телекоммуникационных компаний за те услуги, которые они предоставляют, а также установление четких границ такой ответственности, появление обязанности авторизации пользователей сети Интернет, для идентификации личности. А консолидации государственных и общественных субъектов контроля за проведением этих мер поможет обеспечить воспитание несовершеннолетних в духе полноценного нравственного развития.

[1] Лига безопасного Интернета // www.ligainternet.ru/liga/about.php: 24.02.2013

Синенко В.С.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-ИНФОРМАЦИИ КАК ДОКАЗАТЕЛЬСТВА ПО ГРАЖДАНСКИМ И АРБИТРАЖНЫМ ДЕЛАМ

Аннотация. В данной статье указано на отдельные проблемные вопросы, связанные с использованием информации, полученной в сети Интернет, в качестве доказательства по делу.

Ключевые слова: интернет-информация, доказательство, гражданский процесс.

Abstract. The article pointed out some problems connected with the use of information obtained from the Internet, as evidence in the case.

Key words: Internet information, evidence, civil procedure.

Доказывание обстоятельств, имеющих знание по делу, в гражданском процессе возможно только с помощью таких средств доказывания, которые прямо предусмотрены в абз. 2 ч.1 ст.55 Гражданского процессуального кодекса РФ (далее – ГПК РФ). В частности, доказательственные сведения «могут быть получены из объяснений сторон и третьих лиц, показаний свидетелей, письменных и вещественных доказательств, аудио– и видеозаписей, заключений экспертов».

Причем перечень средств доказывания, предусмотренный в указанной статье, является исчерпывающим. Такая законодательная конструкция вызывает определенные трудности в правоприменительной практике, связанные с возможностью использования фактических данных полученных из иных средств доказывания.

Например, результаты несудебной экспертизы могут быть приобщены к делу только в качестве письменных доказательств. Это связано с тем, что заключение эксперта, предусмотренное в качестве средства доказывания в ст. 55 ГПК РФ, может являться таковым, только если оно получено по результатам проведения судебной экспертизы. Причем возможность использования в процессе результатов несудебной экспертизы в качестве письменных доказательства является единственной, чтобы бы их хоть как то можно было бы приобщить к делу. Однако, несмотря на то, что в конечном итоге заключения несудебных экспертиз все же рассматриваются в качестве доказательств, их использование в качестве письменных не является верным в силу того, что имеется существенная специфика в оценке письменных доказательств и заключений эксперта.

Кроме того, данная ст.55 ГПК РФ не предусматривает в качестве средства доказывания консультации специалиста, хотя возможность привлечения специалиста для дачи разъяснений и консультаций прямо предусмотрена ст.188 ГПК РФ. Это также не позволяет рассматривать информацию, полученную от специалиста в качестве доказательства.

Более логичным в этом плане выглядит подход, отраженный в ч.2 ст.64 Арбитражного процессуального кодекса РФ (далее – АПК РФ). В качестве доказательств данное положение допускает письменные и вещественные доказательства, объяснения лиц, участвующих в деле, заключения экспертов, консультации специалистов, показания свидетелей, аудио– и видеозаписи, иные до-

кументы и материалы. Как видно, данный перечень не является исчерпывающим, поскольку включает в себя фразу о возможности использования «иных документов и материалов». Под ними в ст.89 АПК РФ понимаются любые сведения, зафиксированные как в письменной, так и в иной форме. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном АПК РФ.

Правильность такого подхода к установлению перечня средств доказывания связана с тем, что «жизнь не стоит на месте». Развитие технических возможностей сохранения и передачи информации (особенно последнего времени) требует учета в правовом регулировании процесса доказывания. В конечном итоге, это, конечно, требует специального прямого нормативного регулирования, но, как минимум, законодательство не должно создавать препятствий в использовании современных достижений науки и техники.

Особенная актуальность этого связана с тем, что огромное количество информации последнего времени преобразовано в цифровую форму, и находится в глобальной сети Интернет и максимально доступно любому заинтересованному пользователю. Причем подобная информация может не просто иметь доказательственное значение в процессе, но и некоторые правонарушения совершаются непосредственно в сети Интернет. Например, распространение сведений, порочащих честь и достоинство гражданина; распространение сведений, составляющих тайны личной жизни; незаконное использование товарных знаков; нарушение авторских прав и другие. В связи с этим возникает потребность использования информации, которая имеет цифровую форму.

Проблемы использования данных, не имеющих обычного материального (письменного) носителя, стали возникать еще в 70-е годы прошлого столетия. Одним из первых нормативно-правовых актов в отечественном праве были инструктивные указания Госарбитража СССР от 29 июня 1979 г. «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники»[1]. Согласно п.1 данных указаний, такие документы должны приниматься органами арбитража на общих основаниях в качестве письменных доказательств. В п.9 дополнительно имеется разъяснения о том, что «данные, содержащиеся на техническом носителе (перфоленте, перфокарте, магнитной ленте, магнитном диске и т.п.), могут быть использованы в качестве доказательств по делу только в случаях, когда они преобразованы в форму, пригодную для обычного восприятия и хранения в деле». Однако ни о способах преобразования, ни о конкретной форме, с помощью которой могло бы быть обеспечено их хранение в деле в данных указаниях не говорится. Проблемы преобразования в форму, пригодную для обычного воспри-

[1] Инструктивные указания Госарбитража СССР от 29.06.1979 г. №И-1-4 «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники» // СПС Консультант Плюс: Законодательство.

ятия актуальны и в настоящее время. Более того, сегодня данные вопросы особенно актуальны в силу причин, изложенных выше.

Представление необходимой доказательственной информации необходимо уже на этапе подачи искового заявления. Учитывая, что информация, имеющаяся на соответствующем веб-сайте, в любой момент может быть удалена или изменена, возникает необходимость обеспечения доказательства, а именно фиксация наличия соответствующей информации на определенном сайте в определенный момент времени. В силу этого вопрос фиксации данного факта и преобразование информации в форму, пригодную для обычного восприятия, иногда должен решаться еще на досудебном этапе.

В настоящее время правом обеспечения доказательств согласно ст.102 Основ законодательства о нотариате обладают нотариусы. Однако ни в этом нормативном акте, ни в каком-либо другом, нет четко установленного регламента обеспечения информации, имеющейся в сети Интернет. В научной литературе имеются описания данной процедуры, которая фактически реализуется на практике.

Так, А.А. Вайшнурс описывает процедуру нотариального обеспечения доказательств с помощью Интернета, которая уже в настоящее время используется в практике. В частности, автор поясняет, что на имя нотариуса подается заявление (запрос) о заверении правонарушающей информации, в котором заинтересованное лицо просит удостоверить факт нахождения такой информации по определенному адресу в сети Интернет. В данном запросе необходимо обозначить цель обеспечения доказательств, адрес интернет-страницы, реквизиты документа, а также желательно указать заголовок текста или графической информации, ее месторасположение на интернет-странице, конкретные цитаты, которые будут использованы в иске, жалобе или заявлении. При этом целесообразно описать последовательность действий, которые должен совершить нотариус для получения экранного изображения интересующей страницы[1]. В. Погуляев, в свою очередь, определяет порядок действий по обеспечению доказательств следующим образом. Заинтересованное в обеспечении доказательств лицо обращается в нотариальную контору с соответствующим заявлением. Нотариус осматривает содержимое сайта в присутствии заявителя и, как правило, еще двух-трех лиц. Убедившись в наличии на Web-странице соответствующего материала, нотариус делает распечатку страницы и составляет протокол с описанием результатов осмотра, в котором указывается: дата и место производства нотариального действия; фамилия, инициалы нотариуса, дата и номер приказа органа юстиции о назначении его на должность, нотариальный округ или наименование государственной нотариальной конторы; сведения о заинтересованных лицах, участвующих в производстве нотариального действия; обнаружен-

[1] Вайшнурс А.А. Обеспечение и сбор доказательств с помощью Интернета. Процессуальный статус доказательств, полученных с помощью Интернета // Вестник Высшего Арбитражного Суда Российской Федерации. 2003. №3 (124). С. 142-148.

ные обстоятельства. Протокол подписывается нотариусом, всеми участвующими при производстве обеспечения доказательств лицами, скреплялся печатью нотариуса и сшивался вместе с распечаткой Web-страниц в единый документ. К нему также следует приложить и носитель электронной записи с копией всего сайта или его отдельных страниц.[1]

Несмотря на, казалось бы, относительную простоту данной процедуры, придание информации соответствующей формы требует и определенных реквизитов. В противном случае могут возникнуть затруднения с признанием данных доказательств допустимыми.

Изложенное позволяет утверждать о необходимости нормативного закрепления процедуры обеспечения доказательств в виде информации, содержащейся в сети Интернет. Причем это желательно сделать на уровне закона, например, в качестве дополнений к ГПК РФ и АПК РФ.

[1] Погуляев В. Правонарушения в сети Интернет // ЭЖ-Юрист. 2004. №12.

Скворцова Т.В.

ДИСТАНЦИОННЫЙ ТРУД С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-РЕСУРСОВ

Аннотация. Статья посвящена анализу нового вида занятости в РФ – дистанционному труду с использованием Интернет – ресурсов.

Ключевые слова: дистанционный труд, «телеработа», надомник.

Abstract. The paper analyzes a new type of employment in the Russian Federation – remote work with the Internet – resources.

Key words: remote work, «telecommuting», outworker.

Стремительное развитие общественной жизни и информационных технологий воздействуют на принципы организации производства и трудовые взаимоотношения. Новые способы делового сотрудничества и социальные коммуникации воздействуют на трудовую сферу, вызвав появление новых эффективных форм занятости.

Кроме того, существенные сдвиги в рыночной экономике и ее динамичное развитие заставляют последовательно изучать и формировать различные оптимизационные модели управления трудовыми ресурсами.

Среди новых форм занятости большие перспективы имеет дистанционный труд. На сегодняшний день это самая быстроразвивающаяся форма занятости.

Термин «дистанционный труд», или «теледоступ» (от англ. telecommuting – дистанционное присутствие) впервые был предложен американцем Джеком Найллсом в 1970-х для обозначения дистанционной работы по договору, а позднее труд вне офисных стен начали называть «телеработой».[1] Таким образом, можно сказать о том, что понятия «удаленный труд», «телеработа», «дистанционный труд» являются синонимами.

Джек Найллс не просто ввел термин «телеработа» в оборот, он разработал революционную для своего времени концепцию. Работая над программой по снижению транспортных расходов для сотрудников, он предложил никому никуда не ездить. Связь между работником и работодателем поддерживалась через Интернет – так они и получали задания, и передавали результаты своего труда. Первоначально телеработа была антикризисной мерой, позволяющей сократить издержки на топливо.

Что касается терминологии, то согласиться с тем, что дистанционный труд и телеработа одно и то же, на наш взгляд не правильно. Ведь дистанционный труд – ситуация, когда место работы отдалено от работодателя или заказчика, при этом неважно, посредством чего происходит взаимодействие между ними – сети Интернет, письмами, периодическими походами в офис и т. д. Те-

[1] Бобровникова М. Правовое регулирование дистанционного труда в зарубежном законодательстве // Сравнительное трудовое право 2011. №5. С 18.

леработа – вид дистанционного труда, при котором выполнение работы происходит посредством сети Интернет. Надомничество также является разновидностью дистанционного труда. При такой констатации выбивается из колеи ситуация привлечения членов семьи надомника к выполнению работы. Однако такой признак трудовых отношений как личностный характер работы не всегда корректно употреблять в отношении надомника, как раз в этом проявляется двойственный, смешанный характер отношений с надомником.

На сегодняшний день гл.49 ТК РФ «Особенности регулирования труда надомников» не соответствует сложившимся отношениям в сфере дистанционного труда: в ней речь идет о надомниках, которые осуществляют работу в сфере материального производства дома. Согласно статье 310 ТК: «Надомниками считаются лица, заключившие трудовой договор о выполнении работы на дому из материалов и с использованием инструментов и механизмов, выделяемых работодателем либо приобретаемых надомником за свой счет».[1]

Таким образом, можно сделать вывод о том, что в российском трудовом законодательстве существует пробел: фактически сложившиеся трудовые отношения с дистанционными работниками остаются неурегулированными нормами права. Кроме того, анализ отечественной литературы по проблеме дистанционной занятости показывает отсутствие фундаментальных научных трудов по данной проблеме.

Между тем данное определение понятия «надомник» не учитывает складывающуюся в экономике и на рынке труда ситуацию, при которой в условиях быстрого развития информационных технологий и сферы услуг появляются новые формы трудовых отношений. В условиях появления новых информационных технологий многие виды нематериальных работ и услуг работник может выполнять вне территории работодателя, производя продукцию не только материального производства.

В первую очередь к таким видам работ относятся работы, выполняемые на персональном компьютере работника. К ним относятся работы, связанные с разработкой и сопровождением программных средств, многие виды консалтинговых и сервисных услуг, осуществляемых при условии наличия доступа к сети Интернет и мобильной связи. Для выполнения данных работ не требуется присутствие работника на отдельно выделенном ему работодателем рабочем месте при условии наличия у работника указанных технических средств и возможностей[2].

Дистанционный труд имеет ряд преимуществ и недостатков для работников. Наиболее очевидные преимущества – это баланса между работой и отдыхом; отсутствие производственных и личностных конфликтов на работе; возможность работать по специальности сразу на нескольких работодателей; минимизация дополнительных расходов. Недостатками являются отвлекающие факторы, которые могут отрицательно сказаться на качестве и сроках выполнения работы (дети, домашние дела); отсутствие возможностей для профессиона-

---

[1] Трудовой кодекс РФ от 21 декабря 2001г №197-ФЗ. // Собрание законодательства РФ. 2002. №1. (ч. 1). Ст. 3.

[2] Джиоев С.Х Правовое регулирование дистанционного труда// Законы России: опыт, анализ практика. 2012. № 10. С 24.

льного общения и обмена мнениями с коллегами; отсутствие профессионального и карьерного роста, профессиональной конкуренции.

Кроме того, есть плюсы и минусы применения дистанционного труда для работодателей. Так к плюсам модно отнести: экономию на расходах, связанных с арендой, коммунальными платежами, экономию на оргтехнике, налоговых отчислениях, соцпакете (работники реже уходят на больничные), возможность платить меньшую заработную плату, чем сотруднику, работающему в офисе. К минусам относятся: отсутствие закрепленных обязанностей и рычагов влияния на работников, невозможность контроля за деятельностью работника, отсутствие стационарного офиса негативно сказывается на имидже компании, эффективность работы зависит только от профессионализма удаленного работника, так как у него нет возможности взаимодействовать с коллегами и структурными подразделениями.

Неурегулированность вопросов, связанных с дистанционным трудом, в том числе отсутствие правовых оснований для заключения трудового договора с применением электронной подписи, приводит к тому, что значительное количество граждан, при фактически складывающихся трудовых отношениях, лишены возможности легального трудоустройства.

На рассмотрении Госдумы находится проект федерального закона № 88331-6 «О внесении изменений в Трудовой кодекс Российской Федерации и статью 1 Федерального закона «Об электронной подписи». Проект подготовлен с целью правового регулирования труда работников, работающих вне места расположения работодателя и уже прошел первое чтение, а в настоящее время депутаты готовятся ко второму.

Некоторые изменения, предлагаемые законопроектом необходимо тщательно доработать.

Во-первых, при определении понятия «дистанционный работник» не ясно о каких работниках идет речь, о тех, которые заключили трудовой договор с использованием информационно-коммуникационной сети «Интернет» или же о тех, которые выполняют свою трудовую функцию с использованием сети «Интернет».

Во-вторых, законопроект предлагает по желанию работника вносить сведения о дистанционной работе в трудовую книжку путем внесения дополнения в ст. 66 ТК РФ. Однако это положение является особенностью регулирования труда дистанционных работников и должно располагаться в соответствующей главе ТК РФ.

В-третьих, нуждаются в согласовании наименование и содержание новой статьи 312^2 ТК РФ, поскольку в наименовании говорится об особенностях заключения трудового договора с дистанционными работниками, а в части второй содержится порядок не только заключения, но и изменения трудового договора.

В-четвертых, из положений законопроекта не ясно как дистанционный работник будет реализовывать предоставляемые ему гарантии (например, при

предоставлении отпуска, при временной нетрудоспособности и т.д.), а также как будут применяться положения будущего федерального закона при осуществлении на территории Российской Федерации трудовой деятельности иностранным гражданином. Кроме того, положение новой статьи 312^4 ТК РФ о том, что дистанционные работники распределяют свое рабочее время и время отдыха по своему усмотрению, некорректно по отношению к такому виду времени отдыха, как отпуск. Вряд ли имелось в виду, что работник по своему усмотрению может считать себя находящимся в отпуске, или что он может отказаться от очередного оплачиваемого и иных видов отпусков.[1]

Также в законопроекте целесообразно было бы урегулировать такие вопросы как реализация дистанционными работниками права на объединение, включая право на коллективные переговоры; установить особенности порядка выплаты заработной платы дистанционным работникам и действия в отношении дистанционных работников гарантий при направлении их в служебные командировки и другие служебные поездки; установить особенности порядка применения к дистанционным работникам мер дисциплинарного воздействия, включая увольнение.

Итак, из вышеизложенного видно, что правовое регулирование дистанционного труда является важной инновацией для российского общества, которая необходима в первую очередь в современных технологических отраслях, предполагающих высокую мобильность и творческую активность работников. Введение в трудовое законодательство норм по дистанционной занятости должно предоставить России хорошие конкурентные преимущества по привлечению высококвалифицированной рабочей силы и в результате стать основой для технологического и экономического роста.

[1] Заключение комитета по труду, социальной политике по проекту ФЗ №88331-6 «О внесении изменений в Трудовой кодекс РФ и статью 1 ФЗ «Об электронной подписи» – об особенностях правового регулирования труда работников, выполняющих работу вне места расположения работодателя.

Табунщиков А.Т.

ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ПРОВАЙДЕРОВ ЗА НАРУШЕНИЕ АВТОРСКИХ И СМЕЖНЫХ ПРАВ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье предпринята попытка выявить правовые проблемы гражданско-правовой ответственности провайдеров за нарушении авторских и смежных прав в сети Интернет. Анализируется действующее российское гражданское законодательство и опыт применения института ответственности Интернет-провайдера в области нарушении авторских и смежных прав в развитых мировых правопорядках.

Ключевые слова: авторские и смежные права, вред, деликт, Интернет, интеллектуальная собственность, обязательства из причинения вреда.

Abstract. The paper attempts to identify the legal issues of civil responsibility of providers for infringement of copyright and related rights on the Internet. Ana-lysed the current Russian civil legislation and experience of the Institute's internet service provider liability in violation of copyright and related rights in the developed world order.

Key words: copyright and related rights, harm, tort, internet, intellectual propertytion, the obligations of the injury.

Современные общественные отношения складываются под влиянием научно-технических достижений, особое место среди которых занимает Интернет. Россия, являясь субъектом международного права, обязана в условиях развития глобального информационного пространства принять все меры по обеспечению эффективной охраны авторских и смежных прав в сети Интернет.

Нарушения авторских и смежных прав в сети совершаются как в отношении личных неимущественных прав, так и в отношении прав на использование охраняемых объектов. Как отмечает Н.И. Федоскина, такие нарушения обладают определенной спецификой, выражающейся, в частности, в сложности контроля над использованием размещенных объектов, в особенностях пресечения совершаемых нарушений[1]. Особые трудности вызывает и проблема установления того, кто именно является нарушителем, а так же в каком объеме осуществляется незаконное использование.

Доступ к Интернету, передача информации обеспечиваются с помощью услуг поставщиков интернет-услуг (провайдеров). Как справедливо подмечено в юридической литературе, в странах Европы, в Великобритании и США, правообладатели все чаще требуют возложения на Интернет-провайдера ответственности в связи с нарушением авторских и смежных прав, осуществляемым его клиентами[1]. Во-первых, воздействие на деятельность провайдера позволяет пресечь большой объем нарушений и требует меньших затрат, чем предъявление претензий к отдельным нарушителям – пользователям сети. Во-вторых, провайдер обладает значительными финансовыми возможностями для удовлет-

[1] Федоскина Н.И. Условия гражданско-правовой ответственности интернет-провайдеров за нарушение авторских и смежных прав // Право и экономика. – 2007. – №9. – С.38.

[1] Чернышова А.А. Ответственность провайдера за нарушение авторских прав в сети Интернет // Правовые вопросы связи. – 2011. – № 1. – С.36.

ворения потенциального взыскания[2]. Таким образом, в развитых мировых правопорядках, подчеркивается бесспорность факта ответственности провайдеров за нарушение авторских и смежных прав в сети Интернет. В юридической литературе отмечается и то, что фактическим нарушителем, исходя из анализируемой отечественной и зарубежной судебной практики, является не провайдер, а пользователь сетевого ресурса, но обращение взыскания на имущество провайдера представляет собой наиболее эффективный способ защиты нарушенных прав[3]. Аргументируется данная позиция еще и тем, что не всегда удается установить истинного нарушителя права в силу многочисленности пользователей сети Интернет. Последнее предположение представляется несколько спорным, поскольку идентифицировать субъекта можно и по закрепленному за ним статическому IP-адресу. Присвоенный постоянный (статический) IP-адрес в соответствии с договором пользователя с провайдером позволяет установить пользователя именно через организацию, которая предоставила ему такую услугу. Также через провайдера услуг связи можно установить и владельца динамического IP-адреса в определенный промежуток времени. Такая информация хранится в лог-файлах компьютеров провайдера, в которых указываются дата соединения, время установления и прекращения соединения, IP-адрес, назначенный пользователю[4].

В российской цивилистической науке также высказываются предложения о необходимости привлечения к гражданско-правовой ответственности Интернет-провайдера за незаконное использование в сети объектов авторских и смежных прав[5]. Следует отметить, что по такому же пути идет и отечественный законодатель дополняя часть IV ГК РФ новой ст. 1253.1 об особенностях ответственности информационного посредника за нарушение интеллектуальных прав в сети Интернет[1]. Информационным посредником предлагается считать лицо, осуществляющее передачу материала в сети Интернет или предоставляющего возможность размещения материала в этой сети (Интернет-провайдер). Провайдер будет нести ответственность на общих основаниях, при наличии вины, с учетом особенностей, установленных в п.п. 2 и 3 ст. 1253.1 ГК РФ. Информационный посредник, осуществляющий передачу материала в сети Интернет, не

---

[2] Федоскина Н.И. Условия гражданско-правовой ответственности интернет-провайдеров за нарушение авторских и смежных прав // Право и экономика. – 2007. – №9. – С.39.

[3] Чернышова А.А. Ответственность провайдера за нарушение авторских прав в сети Интернет // Правовые вопросы связи. – 2011. – № 1. – С.36.

[4] Милашева В.А. Неправомерный доступ к компьютерной информации в сетях ЭВМ // Правовые вопросы связи. – 2006. – №1. – С.36.

[5] Липкес А.М. Правовые вопросы использования авторских произведений в Интернете: Дисс... к.ю.н. – М. 2006. – С.13; Невзоров И.В. Проблемы региональной разобщенности гражданско-правового регулирования деятельности в сети Интернет // Правовые вопросы связи. – 2006. – №2. – С.22; Симкин Л. Как бороться с «сетевыми» пиратами // Российская юстиция. – 2002. – №7. – С. 62; Федоскина Н.И. Условия гражданско-правовой ответственности интернет-провайдеров за нарушение авторских и смежных прав // Право и экономика. – 2007. – №9. – С.39; Чернышова А.А. Ответственность провайдера за нарушение авторских прав в сети Интернет // Правовые вопросы связи. – 2011. – № 1. – С.36. и др.

[1] Проект ГК РФ (часть четвертая) // СПС Консультант Плюс: Версия проф.

несет ответственности за нарушения интеллектуальных прав, произошедшие в результате такой передачи, при соблюдении следующих условий: информационный посредник не изменяет указанный материал после его получения, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала; информационный посредник не знал и не должен был знать о том, что использование соответствующего результата интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего такой результат или средство индивидуализации, является неправомерным (п. 2. ст. 1253.1 ГК РФ).

Информационный посредник, предоставляющий возможность размещения материалов в сети Интернет, также освобождается от ответственности за нарушения интеллектуальных прав, произошедшие в результате размещения в сети Интернет материала третьим лицом или по его указанию, при соблюдении следующих условий: информационный посредник не знал и не должен был знать о том, что использование соответствующего результата интеллектуальной деятельности или средства индивидуализации, содержащегося в таком материале, является неправомерным; информационный посредник в случае получения письменного заявления правообладателя о нарушении интеллектуальных прав в результате размещения такого материала в сети Интернет своевременно принял необходимые и достаточные меры по устранению последствий нарушения интеллектуальных прав, предусмотренные законодательством об информации (п. 3. ст. 1253.1 ГК РФ).

Роль Интернет-провайдера в механизме защиты авторских и смежных прав определяется не только возможностью привлечения его к гражданско-правовой ответственности, но и возможности пресекать незаконную деятельность в сети путем отказа в доступе пользователям – нарушителям[2].

Согласно общим положениям о деликтной ответственности, ответственность за нарушение авторских и смежных прав возлагается на провайдера исключительно при наличии его вины, в иных случаях ответственность несет иное лицо (пользователь)[3]. Как считает Г.И. Сытенко привлечение пользователей к ответственности представляется нецелесообразным и проблематичным в силу закрытости таких сетей от лиц, не получающих услуги от конкретного провайдера, а также вследствие отсутствия в России развитого в Европе и США механизма проверки домашних компьютеров. Кроме того, правовая культура, имеющая место в нашей стране в настоящее время, не позволит ввести какие-либо механизмы ответственности пользователей в силу хотя бы широты охвата круга лиц, являющихся потенциальными нарушителями[1].

В свою очередь А.А. Чернышева, в целях наиболее эффективной защиты

---

[2] Федоскина Н.И. Условия гражданско-правовой ответственности интернет-провайдеров за нарушение авторских и смежных прав // Право и экономика. – 2007. – №9. – С.39.

[3] Чернышова А.А. Ответственность провайдера за нарушение авторских прав в сети Интернет // Правовые вопросы связи. – 2011. – № 1. – С.37.

[1] Сытенко Г.И. Актуальные вопросы регулирования отношений по охране авторского и смежных прав в сети Интернет. // Культура: управление, экономика, право. – 2010. – №2. – С. 8.

правообладателей предлагает предусмотреть в соответствии со ст. 1080 ГК РФ солидарную ответственность провайдера и пользователя, тем самым оба лица будут нести ответственность за свои противоправные действия, если таковые имели место[2]. Автор считает, что подобная ответственность возможна в случае установленной вины как пользователя, так и провайдера, причем вина последнего может выражаться через определение «лицо знало или должно было знать о противоправности действий абонента». Кроме того, субъект, возместивший правообладателю заявленное им требование, получает право регресса к солидарному с ним должнику. Объем регрессного возмещения может в окончательном варианте определяться судом, исходя из степени вины должника с учетом требований разумности и справедливости. Несмотря на указание в литературе на отсутствие необходимости привлекать к ответственности пользователя, А.А. Чернышева считает данные действия целесообразными, способствующими уменьшению нарушений авторских прав[3].

Отдельного внимания заслуживает проблема касающаяся существования многочисленных сайтов – торрент-трекеров. Суть функционирования которых сводится к тому, что торрент-трекеры не хранят те файлы, которыми обмениваются пользователи, они только дают ссылки на источник информации а закачка происходит напрямую между пользователями. Администрациями подобных сайтов предусмотрена процедура урегулирования споров с правообладателями в случае получения претензий по поводу авторских прав на контент, однако это не восстанавливает нарушенные права и не предотвращает нарушения исключительных прав в будущем. Основной проблемой воздействия на таких правонарушителей является еще и то, что в большинстве своем торрент-трекеры зарегистрированы в других государствах, где и находятся их серверы, а свою деятельность в России они осуществляют посредством трассировки через иные зарубежные государства[4].

Согласно п. 34 Постановления Пленума Верховного Суда Российской Федерации и Пленума Высшего Арбитражного Суда Российской Федерации №5/29 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» от 26 марта 2009 г[1]., нарушением исключительного права на произведение признается изготовление одного экземпляра произведения или более, осуществленное с контрафактного экземпляра либо при неправомерном доведении до всеобщего сведения (в том числе при неправомерном размещении в сети Интернет).

В свою очередь, допускается без согласия автора или иного правообладателя воспроизведение, осуществляемое только гражданином и только в личных

---

[2] Чернышова А.А. Ответственность провайдера за нарушение авторских прав в сети Интернет // Правовые вопросы связи. – 2011. – № 1. – С.37.

[3] Там же. – С. 38.

[4] Сытенко Г.И. Актуальные вопросы регулирования отношений по охране авторского и смежных прав в сети Интернет. // Культура: управление, экономика, право. – 2010. – №2. – С. 9.

[1] Постановление Пленума Верховного Суда РФ №5, Пленума ВАС РФ №29 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» от 26 марта 2009 г. // Российская газета. – 2009. – 22 апреля.

целях, под которыми по смыслу ст. 1273 ГК РФ понимается последующее некоммерческое использование соответствующего экземпляра для удовлетворения собственных потребностей или потребностей обычного круга семьи этого гражданина (который определяется судом с учетом конкретных обстоятельств рассматриваемого дела).

При нарушении авторских и смежных прав потерпевшее лицо может воспользоваться общими способами защиты гражданских прав, предусмотренными в ст. 12 ГК РФ, и специальными, в частности, закрепленными в ст. 1250 – 1253 ГК РФ. В соответствии со ст. 1301 ГК РФ, в случаях нарушения исключительного права на произведение автор или иной правообладатель наряду с использованием других применимых способов защиты и мер ответственности, установленных настоящим Кодексом (статьи 1250, 1252 и 1253), вправе в соответствии с пунктом 3 статьи 1252 настоящего Кодекса требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации: в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда; в двукратном размере стоимости экземпляров произведения или в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения. В случае нарушения личных неимущественных прав автора их защита осуществляется, в частности, путем признания права, восстановления положения, существовавшего до нарушения права, пресечения действий, нарушающих право или создающих угрозу его нарушения, компенсации морального вреда, публикации решения суда о допущенном нарушении (1251 ГК РФ).

Тонков Е.Е.
Пожарова Л.А.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ОХРАНЫ ДОСТОИНСТВА ЛИЧНОСТИ В УСЛОВИЯХ МОДЕРНИЗАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ

Аннотация. В публикации раскрыты основные положения, связанные с обеспечением достоинства личности в условиях модернизации отношений в развивающемся обществе.
Ключевые слова: Достоинство личности, модернизация общественных отношений.
Abstract. The publication on the key provisions relating to the dignity of the individual in terms of modernization of relations in a developing society.
Key words: Human dignity, the modernization of public relations.

Какие бы мы законы ни изобрели и какие бы лучшие образцы Запада мы ни приняли, они могут свободно зачахнуть в той атмосфере административного произвола, которая господствует в настоящее время.

Г.Ф. Шершеневич

Размышления и теоретические обобщения авторов статьи исходят из потребности осмысления и критической оценки деятельности современного Российского государства, базовым постулатом которой является приоритет человека, его прав и свобод (ст. 2 Конституции Российской Федерации) в совокупности с государственными гарантиями их защиты (ст. 45-46), подкрепленными соответствующей обязанностью, адресованной государству.

Процесс реализации данной обязанности инициировал принятие в нашей стране законодательных норм, касающихся защиты отдельных прав или категорий лиц; наделения правозащитными полномочиями публичных структур и учреждения специализированных органов; введения новых, более выдержанных в правозащитном смысле процедур и уточнения действующих; активного включения в международную систему защиты прав и основных свобод человека.

Однако предпринятые меры не достигли того правозащитного результата, который бы в полной мере соответствовал «духу и букве» Конституции. Практика современного государственно-правового строительства показывает, что проблема повышения эффективности правозащитной деятельности в нашей стране, обеспечения охраны достоинства личности, остается злободневной.

Более того, по словам С.С. Алексеева, в России происходит «суровое явление – это крушение права в его общецивилизационном, высоком значении. И это должно быть большой тревогой для общества. Потому что крушение права означает, что общество теряет одну из важнейших ценностей цивилизации, которая может вывести его на новые ступени прогресса» [1].

[1] Алексеев С.С. Право – одно из самых высоких достижений человеческой цивилизации // Закон. – 2009. – № 7. – С. 16.

Население страны во многом разделяет опасения ученых по поводу несостоятельности представителей власти на местах консолидировать общество для решения то и дело возникающих острых проблем, о чем свидетельствует количественный рост обращений граждан в федеральные публичные структуры.

В результате нестабильной экономической обстановки, вызванной мировым финансово-экономическим и системным кризисом, паралича господствовавшей ценностной парадигмы видимого всеобщего благоденствия государственные органы оказались не готовы к защите предложенных эталонов поведения и тех идеалов, которые были навязаны рыночной вседозволенностью и начинают разрушаться.

Кризис наглядно продемонстрировал, что институциональная система России буквально пронизана дефектами, а уроки из прошлого власть предержащими не извлечены.

Как иронично и прогностически точно подчеркнул И.А. Исаев еще несколько лет назад, «амбициозная убежденность современной политико-правовой науки в чистом рационализме своих категорий и понятий в жизни постоянно сталкивается с неизвестно откуда возникающими феноменами иррационального и стихийного»[1].

Отметим, что проблеме защиты прав человека систематическое внимание уделяется главой государства в ежегодных посланиях. Являясь, в том числе, принципиальным правозащитным ориентиром для всех публичных структур, даже послания Президента, к сожалению, не стали фактором существенного изменения отношения к правам человека и необходимости их соблюдения и защиты. Сложившуюся ситуацию можно считать вполне закономерным результатом сформировавшейся на постсоветском пространстве научно-правовой традиции, которая существовала и продолжает во многом главенствовать с советских времен. Функции государства в их традиционном «наборе» по-прежнему рассматриваются как способы или средства воздействия государства на общественные процессы и поведение людей. Такие представления последовательно отражают присущую советскому строю идеологию верховенства государства над личностью, которой отводилось место объекта воздействия со стороны государственных органов.

Наша страна, к сожалению, не является ни колыбелью теории правового государства, ни полигоном для убедительного освоения ее практики. Его идеи, возникнув во времена античности, научное оформление получили в известных работах Ж.Ж. Руссо, теории общественного договора, трудах немецких философов и правоведов. В России же до сих пор отсутствуют фундаментальные исследования, посвященные правовому государству и правозащитной деятельности, хотя в Конституции РФ закрепляется характеристика правового государства и его элементов.

Не случайно даже Председатель Конституционного Суда страны, избран-

[1] Исаев И.А. Власть и закон в контексте иррационального. – М.: Юрист, 2006. – С. 8.

ный недавно на очередной срок полномочий, размышляя о влиянии социально-государственного кризиса на правовую систему, озадачился вопросом, куда сегодня движется Россия – к праву или хаосу[1].

Все это подчеркивает потребность обеспечения новым методологическим инструментарием проблемы реализации государством своей конституционной обязанности защищать права и свободы человека и гражданина, охранять его достоинство. Одним из них может стать, по нашему мнению, выделение в качестве самостоятельной правозащитной функции государства. Предложенный вариант находится в русле прогрессивной тенденции к детализации функций государственной деятельности и соответственно усложнению их классификации. Указанная тенденция не является случайной, а сформировалась в результате развития всей государственности, в частности, усложнения государственной деятельности по масштабности и содержанию задач и функций, демократизации общества, возрастания роли правительственных органов всех звеньев и т.д.

Нетрудно заметить, что озвученный руководством страны курс на модернизацию общественных отношений сопровождается очевидным усилением значимости четкого функционирования государственной власти. Возрастание доли участия государства в экономике рассматривается как вынужденная антикризисная мера и пока, несмотря на высказываемые некоторыми политиками и учеными опасения, не означает свертывания рыночных реформ.

Государственная власть как социальный феномен характеризуется особым статусом в силу известных особенностей ее субъекта, выделяющих государство из других институтов общества, поэтому только расширение диапазона ее влияния может обеспечить макроэкономическую стабильность и сбалансированность бюджета. Используя авторитет и силу публичной власти, административный ресурс аппарата, государственный механизм выполняет роль мощного активатора общественной жизни, способного организовать эффективное управление обществом, реализацию социальных обязательств, создание стимулов для развития частного сектора и повышения деловой активности.

Политико-правовая модернизация во многом затрагивает тем или иным образом практически все формы общественной жизни и предполагает необходимость переосмысления сложившихся позиций и точек зрения на новой методологической основе. Эта потребность объясняется тем, что созданная при социализме теория правового регулирования не в состоянии объяснить происходящие перемены в политической и правовой системе. Политико-правовая модернизация является одновременно и содержательной характеристикой всей правовой системы общества. Если в 90-х гг. XX века мы наблюдали разрушение монополии государственной собственности и сопровождение этого процессом приватизации, ухудшение общего экономического положения страны, в результате чего произошло снижение уровня жизни значительной части населения, то в настоящее время осуществляется перераспределение прав собственности при очевидном государственном вмешательстве в этот процесс.

Очевидно, что государство пока не справляется с возложенными на него

[1] Зорькин В. Россия: движение к праву или хаосу? // Российская газета. – 2012. – 26 января.

функциями, а его контрольно-надзорная деятельность также не отвечает философии осуществляемых реформ. Поэтому совершенствование государственной деятельности в процессе модернизации должно осуществляться координированно, на основе единой концепции, с учетом взаимозависимости функций государства, хотя они отличаются друг от друга содержанием и, соответственно, характером действий, способов, методов, средств их реализации, а также направленностью юридических процедур и последовательностью их использования.

Модернизация создает предпосылки для формирования новых отношений, преодоления кризиса и стабилизации экономического положения. Трансформация природы отношений собственности неизбежно влечет за собой видоизменение отношений правового регулирования. Государственная деятельность в условиях рыночной экономики не может осуществляться в тех же юридических формах и пределах, что и прежде.

Как подчеркивает Н.И. Матузов, в решении вопроса о сущности права, правовой системы необходима уверенность в определении границ собственно права и правил другой природы, действующих в обществе, четко знать, где кончается правовое поле и начинается неюридическое пространство[1].

Поэтому главной задачей ближайшего будущего является адаптация политической, социально-экономической и правовой систем к новой ситуации. Модернизация юридических форм осуществления функций государства, их совершенствование могут придать необходимый динамизм и результативность действиям органов власти по преодолению кризиса, становятся одним из определяющих факторов развития демократии, становления гражданского общества, построения правового государства.

Новая правовая перспектива не может основываться на простой совокупности юридических норм и рациональности создающего их государства вне практики правовой коммуникации, обеспечиваемой с помощью функций государственной деятельности. Наряду с расширением сферы деятельности государства, изменения его направленности в сторону обеспечения прав и свобод человека и гражданина, возникает необходимость в уточнении функций современного социального государства.

При таком подходе возможны дальнейшие теоретические и конституционно-отраслевые разработки сущности и содержания функций государства с учетом его модернизации; уточнение приоритетных направлений деятельности государства и его органов в сфере защиты прав человека; развитие конституционной системы и структуры такой защиты; выработка критериев участия публичных структур в реализации правозащитной функции государства. Эти и иные возможности, опосредованные обособлением и развитием правозащитной функции государства, могут позитивно сказаться на состоянии защиты прав человека в России.

Решающее значение имеет переосмысление фундаментальных правовых подходов к взаимоотношениям государства и личности, гражданина и права. Устаревшие идеологические стереотипы до настоящего времени превалируют в

[1] См.: Матузов Н.И. Актуальные проблемы теории права. – Саратов, 2003. – С. 103.

общественном правосознании, что не способствует современному пониманию сущности функций государства и юридических форм государственной деятельности как способа обеспечения приоритета прав человека в сфере публичной власти. Хотя активных дискуссий по этой проблеме в научных кругах сегодня практически нет, единое мнение так и не сложилось, что дает нам основания на собственное представление о ней.

Особое значение имеют новые подходы к оценке и формированию государственной деятельности. В любом государстве, как и в любой науке, должен существовать основной, ведущий методологический подход. Не единый и обязательный для всех, а преобладающий, доминирующий, выступающий базой методологического инструментария той или иной науки[1].

В ряде диссертационных работ затрагивались вопросы конституционной обязанности Российского государства охранять права и свободы граждан (С.Н. Бочарова), функции охраны прав и свобод личности в современном Российском государстве (А.В. Сим), конституционно-правового механизма защиты основных прав человека и гражданина в Российской Федерации и ее субъектах (К.Д. Шаймарданов), правозащитной функции государства (М.А. Беспалова).

Вместе с тем, проблема охраны достоинства личности в условиях современных преобразований в Российской Федерации, несмотря на ее безусловную научно-практическую актуальность и значимость, объектом самостоятельного исследования не становилась. В специальной юридической литературе не акцентировалось внимание ни на теоретических аспектах проблемы, ни на прикладных вопросах, ориентированных на анализ обеспечения охраны достоинства личности публичными институтами.

Мы рассматриваем публично-правовые отношения, складывающиеся в связи с реализацией Российской Федерацией своей обязанности защищать права и свободы человека и гражданина, с учетом развития ее конституционных параметров в условиях современных процессов модернизации.

До настоящего времени в научной среде не сложилось однозначное представление о методологии исследования проблемы. Изменившиеся экономические, политические и социокультурные условия неизбежно обусловливают перенос акцентов с интересов общества на интересы личности. Это существенно влияет на саму парадигму управления обществом, инициируя трансформацию его целей, содержания, технологии, активизирует инновационные процессы, которые требуют осмысления и обоснования на теоретико-методологическом уровне.

В начале века нынешнего российское общество не осознавало всех масштабов опасности, которую несет расширение неконтролируемого рыночного пространства. Общественное мнение в отношении значимости государственного управления, укрепления так называемой «вертикали власти» длительное время не формировалось или произвольно складывалось в искаженном виде, пока социально-экономические проблемы не затронули интересы активной час-

---

[1] См.: Сырых В.М. Методология юридической науки: состояние, проблемы, основные направления дальнейшего развития // Методология юридической науки: состояние, проблемы, перспективы: Сб. ст. Вып. 1 / Под ред. М.Н. Марченко. – М., 2005. – С. 15–44.

ти населения страны.

Выступления политиков, руководителей органов законодательной и исполнительной властей, ученых, представителей творческой интеллигенции, в которых была представлена вызывающая тревогу объективная картина развития ситуации в стране, обращалось внимание на необходимость принятия экстренных мер по усилению государственной власти, не смогли своевременно консолидировать общество для реального решения возникших проблем.

На наш взгляд, в современном цивилизованном демократическом государстве, к числу которых стремится принадлежать и Россия, обеспечение охраны достоинства личности должно приобрести характер тенденции. На это указывают, во-первых, положения международных актов в части, касающейся защиты прав человека; во-вторых, нормы новых конституций, в той или иной степени отражающих обязанность государства защищать права и свободы человека; в-третьих, признание юрисдикции международных правозащитных органов, опосредующее ответственность государства, допустившего нарушение прав и свобод человека.

Международные источники, поддерживающие данную тенденцию, имеют как декларативный, так и конвенционный характер. При этом уровень уважения к первым подчеркивает, по мнению автора, добровольность участия государств в обособлении их правозащитной функции. Особого внимания в данном аспекте заслуживает Декларация о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы (1998 г.), согласно которой именно государство несет основную ответственность и обязанность поощрять и защищать права человека и основные свободы.

Исследование доктринальных и конституционно-отраслевых подходов к защите государством нарушенных прав и свобод позволяет уточнить применительно содержание универсальных принципов деятельности государства, систематизировать конституционные параметры достоинства личности, выделить ее детерминанты.

Высоко оценивая преимущества свободного рынка и демократических устоев, следует понять, что формирование гражданского общества, реальной демократии, создание правового государства подразумевают господство права, Конституции и закона. Сильное государство, соответствующее современному характеру и структуре общества, должно располагать не менее эффективной методологией и реальным инструментарием, позволяющими осуществлять надежное противостояние возникающим угрозам.

В России законодателем созданы необходимые фундаментальные основы для реализации демократических правовых принципов. Теперь необходимо сформулировать четкую концепцию природы и содержания процесса реального обеспечения конституционных прав человека и гражданина в современных условиях с выходом на практические рекомендации правового регулирования соответствующего спектра проблем.

Трубников В.М.

К ВОПРОСУ О ПОНЯТИИ ОСНОВАНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Аннотация. Автор предлагает отказаться от законодательного определения понятия основания уголовной ответственности и обосновывает необходимость изменения ч. 1 ст. 2 УК Украины в такой редакции: «Основанием уголовной ответственности является совершение лицом деяния (действия или бездействия) общественно опасного, виновного и противоправного, т. е. преступления, признаки которого предусмотрены в конкретной статье Особенной части Кодекса».

Ключевые слова: уголовная ответственность, свобода воли, детерминизм, материализм, правонарушение, преступление, состав преступления.

Abstract. The author proposes to abandon the legal definition of criminal responsibility and reason justifies the need to amend Part 1 of Art. 2 of the Criminal Code in the following wording: "The basis of criminal responsibility is the person committing an act (action or inaction) of a socially dangerous, guilty and illegal, that is, the crime, the signs of which are provided in a specific article of the Code."

Key words: criminal responsibility, free will, determinism, materialism, offense, offense, an offense.

Проблему уголовной ответственности принято рассматривать в уголовном праве на базе философского учения о свободе воли и обусловленности любых человеческих поступков, в том числе, преступлений.

С точки зрения философии, основанием уголовной ответственности (юридической ответственности) является свобода воли лица, его способность самостоятельно выбирать способ поведения: ответственность наступает потому, что лицо, хотя и могло выбрать путь, одобряемый обществом и государством, дозволенный законами, всё же выбрало путь преступления, причиняющий вред правам и законным интересов других индивидов и общества в целом. Если нет свободы выбора поведения, не может быть и уголовной ответственности.

Считается, что общество и государство имеет право упрекать и отсюда привлекать к уголовной ответственности граждан на том основании, что каждый человек награждается от природы сознанием и волей, которые позволяют ему понимать действие уголовно-правовых запретов и соотносит свое поведение в соответствии с их требованиями. Но для привлечения лица к уголовной ответственности этого недостаточно. Нужно выяснить: имело ли данное лицо реальную возможность не нарушать требования уголовного закона, и вообще, в какой степени человек свободен в выборе своего поведения, он должен воздержаться от совершения преступления или совершение преступления для него фатальное обстоятельство.

Спор о наличии или отсутствии у человека свободы выбирать линию поведения многие века ведется по двум направлениям: детерминизме или индетерминизме.

Философы детерминистской школы предлагали различные основания для применения мер юридической ответственности к лицу, совершившему преступление. Представители французского материализма рассматривали преступле-

ние как аналог негативных природных процессов, стихийных бедствий, от которых следует оградить общество путём изоляции от него преступника; вульгарные материалисты искали причины преступного поведения в изначальной предрасположенности к нему конкретного человека, придя, таким образом, к теории «прирождённого преступника», а позже «опасного состояния» личности, которое также обуславливает необходимость применения мер «социальной защиты», в том числе, превентивных.

В диалектическом материализме, как известно, доминировала теория о том, что свобода воли является «осознанная необходимость», поведение людей является волевым и ответственным постольку, поскольку они осознают общественные закономерности, оказывающие на них влияние, и соразмеряют с ними свои поступки.

Диалектический материализм нашел свое проявление в двух разновидностях: механистическом и диалектическом детерминизме. Механистический детерминизм считает, что человек – слепая игрушка внешних обстоятельств, он подобен механизму, который лишь адекватно реагирует на внешние и внутренние раздражители. Поэтому каждый поступок человека, в том числе и преступление, является неминуемым, поскольку он уже определен всеми предыдущими событиями, имевшие место в жизни этого человека. В таком случае человек – раб обстоятельств, он лишен возможности свободного волеизъявления, а, следовательно, и свободного выбора своего поведения, которое уже предопределено. Поэтому проявление преступной воли в совершенном преступлении является лишь видимостью свободы, мнимая свобода, а если это так, то и невозможна негативная моральная оценка совершенного. Следовательно, обоснование уголовной ответственности в этом случае не столько в осуждении преступной воли, сколько в объективной вредности преступления для общества.

По мнению Спинозы человек никогда и ни в чем не бывает свободным, и его поступки всегда детерминированы внешними обстоятельствами[1].

Энгельс, как представитель диалектического материалистического детерминизма, признавая детерминирующую роль внешней среды, одновременно признавал и активную роль человеческого сознания, однако фактически, в конечном счете, отдавал предпочтение первому. Согласно диалектическому детерминизму, человек, очутившись перед выбором – совершить преступление или воздержаться от этого, зависит как от внешних обстоятельств, так и от собственного ума, совести, убеждений, склонностей, потребностей, интересов и т.п.[2] Здесь ни внешние обстоятельства, ни только внутреннее состояние лица не определяют в конечном итоге его поведение. Преступление, совершенное человеком, является причинно связанным как с его сознанием, так и с объективной действительностью. Внешние обстоятельства влияют на поведение лица, но

---

[1] Кечекьян С. Ф., Этическое миросозерцание Спинозы. – М., 1914; Мильнер Я., Бенедикт Спиноза. – М., 1940; Соколов В., Философия Спинозы и современность. – М.. 1964.

[2] Семенов Ю. Диалектический (прагмо-диалектический) материализм: его место в истории философской мысли и современное значение /научно-просветительский журнал «Скепсис» //Режим доступа: http://scepsis.net/library.

лишь переламываясь через ее внутренние психические установки, сознание. Именно ум, совесть, убеждение подсказывают человеку, как поступить ему в данной конкретной ситуации. Однако основание для этического и правового осуждения преступления и лица, которое его совершило, есть лишь в том случае, если это лицо имело объективную возможность избрать из имеющихся вариантов поведения (хотя бы из двух) непреступное средство достижения поставленной цели.

Нужно отметить, что в конкретных временно-пространственных границах и применительно к индивидуальному поведению никакие внешние условия, никакие дефекты социальной среды сами по себе, фатально не влекут противоправного деяния[1], социальные причины в каждом конкретном случае проявляются неодинаково. Правонарушение следует представлять не как механическое действие внешних условий и даже не как результат влияния этих условий через внутренние свойства личности, а как итог взаимодействия внешних и внутренних условий – социальной среды и личности[2].

Любое правонарушение, как и правомерное поведение, является актом внешне-объективированного характера, выражает отношение субъекта к реальной действительности, к другим людям или организациям. Нельзя считать правонарушением (преступлением) сами по себе мысли человека или его помыслы, пока они не нашли свою объективацию в поведении, в деянии человека.

Только проанализировав поведение субъекта, можно составить более или менее точное мнение о его мыслях и чувствах, дать им определенную оценку. К. Маркс писал, что нет иного мерила намерений лица, помимо содержания и формы его действий, что, помимо своих поступков, человек не существует для закона, а попытки реакционных властей ввести наказания за образ мыслей есть не что иное, как позитивно, законодательно санкционированный произвол[3]. В иной связи, В.И. Ленин также подчеркивал, что о реальных мыслях и чувствах личностей можно судить только по одному признаку – по действиям этих личностей[4].

Правонарушение – это определенное деяние, акт поведения находившегося под контролем воли и разума субъекта[5]. Деяние охватывает как активное действие, так и бездействие. В любом случае речь идет о волевом поведении как действии в «специфически человеческом смысле этого слова»[6].

Таким образом, наличие относительной свободы выбора поступка (степень свободы) и является обоснованием уголовной ответственности конкретного лица за избранный им преступный вариант поведения. В таком случае уголовная ответственность способна выступать средством воздействия на сознание и волю

---

[1] Кудрявцев В.Н. Причинность и криминологии. – М., 1968. – С. 74; Его же: Социально-психологические аспекты антиобщественного поведения. //Вопросы философии, 1974. – № 1.
[2] Долгова А. И. Криминологическое значение изучения личности преступника. //Советское государство и право. – 1973. – № 6. – С. 91.
[3] Маркс К. и Энгельс Ф. Соч., т. 1. – С. 120-122, 14.
[4] Ленин В.И. Полн. собр. соч., т. 1. – С. 423, 424.
[5] Иоффе О.С., Шаргородский М.Д. Вопросы теории права. – М., 1960. – С. 330.
[6] Рубинштейн С.Л. Основы общей психологии. – М., 1940. – С. 456.

людей и тем самым детерминировать их поведение в будущем. Следовательно, если человек сознательно избирает преступный вариант поведения, имея возможность сделать иначе, то это и обосновывает возможность и необходимость со стороны государства применить к нему меру принуждения, наказание.

Фактически все приведенные нами рассуждения сводятся к проблеме свободы человека. Свободен ли человек в любой момент принять решение в пользу добра, или он не обладает этой свободой выбора, поскольку детерминирован внешними и внутренними силами? И, несмотря на убедительные доводы многих из этих теорий и на множество книг, написанных об этом, дискуссия еще далека от завершения и проблема свободы воли, да еще и в совокупности с проблемой судьбы человека требует своего последующего разрешения.

Здесь уместно привести высказывание Уильяма Джеймса, который отмечал, что «широко распространено мнение, что дискуссия о свободе воли уже давно обессилела и увяла и тот, кто одержал в ней верх, может привести в споре лишь избитые аргументы, которые всем хорошо известны. Но это глубокое заблуждение. Я не знаю другой темы, которая была бы менее банальна и дала бы увлеченному человеку лучший шанс сделать новые открытия – возможно, не для того, чтобы навязать решение или вынудить прийти ко всеобщему согласию, но с тем чтобы поделиться с нами более глубоким пониманием того, о чем, собственно, идет речь в споре между двумя сторонами и что в действительности содержат идеи о судьбе и свободе воли»[1].

Думается, что более правильным методологическим подходом при рассмотрении проблемы свободы воли являются положения экзистенциальной психологии, и, прежде всего, высказывания одной из ключевых фигур экзистенциальной психологии Ролло Мэя, разработавшего новую концепцию человека. Экзистенциальная психология в разных интерпретациях придерживается точки зрения, согласно которой люди несут значительную долю ответственности за то, какие они есть[2].

Человек, с точки зрения Мэя, живет настоящим, для него актуально в первую очередь то, что происходит *здесь* и *сейчас*. В этой единственной подлинной реальности человек формирует себя сам и ответствен за то, кем он в конечном счете становится. Определяя понятие свободы, Мэй говорил, что «свобода личности – в ее способности знать о своей предопределенности». Слово «предопределенность» в этой фразе означает то, что в своих более поздних работах Мэй называл судьбой (destiny). В этом случае свобода рождается из осознания неизбежности своей судьбы: понимания того, что смерть возможна в любой момент, что мы рождены мужчинами или женщинами, что у нас есть какие-

---

[1] Джеймс У. Воля к вере («Воля к вере и другие очерки популярной философии»; «Прагматизм: новое название для некоторых старых методов мышления: Популярные лекции по философии»; «Речи и статьи») / Сост. Л.В. Блинников, А.П. Поляков. – М.: Республика, 1997. – 431 с.

[2] Мэй Р. Открытие Бытия. – М.: Институт Общегуманитарных Исследований, 2004. – 224 с.; Мэй Ролло. Любовь и воля. – М., Винтаж, 2007. – 288 с.; Мэй Р. Мужество творить. – М.: Институт общегуманитарных исследований, 2012. – 160 с.

то характерные для нас слабости, что, опираясь на впечатления раннего детства, мы склонны вести себя определенным образом в будущем, и т.д.

Свобода – это готовность к переменам, пусть даже конкретный характер этих перемен и остается непредсказуемым. Свобода «предполагает умение всегда держать в голове несколько различных возможностей, даже если в данный момент нам не совсем понятно, как именно нам следует действовать». Это обстоятельство часто ведет к увеличению тревоги, но это нормальная тревога, которую здоровые люди встречают с готовностью и которая вполне поддается управлению.

Мэй различал два вида свободы – свободу действия и свободу бытия. Первую он называл *экзистенциальной свободой*, вторую – *сущностной свободой*. Мэй настаивал на том, что *экзистенциальную свободу* (*existential freedom*) не следует путать с экзистенциальной философией или с экзистенциальной психологией. Это свобода делать что-либо – свобода действия. *Экзистенциальная свобода* – есть свобода действовать согласно собственному выбору.

Между тем свобода действия еще не обеспечивает свободу бытия. Иногда кажется, что в действительности *экзистенциальная свобода* даже затрудняет достижение *сущностной свободы* (*essential freedom*). Мэй приводил несколько случаев, когда заключенные тюрем и узники концентрационных лагерей с энтузиазмом говорили о своей «внутренней свободе». Возможно, одиночное заключение или другое ограничение свободы действия помогает человеку более ясно представить свою судьбу и развить в себе свободу бытия. В этой связи Мэй задается следующим вопросом: «Только ли тогда мы можем получить сущностную свободу, когда наше каждодневное существование встречает препятствия?».

Сам он отвечал на этот вопрос отрицательно. Не обязательно быть заключенным в тюрьму, чтобы достичь сущностной свободы, то есть свободы бытия. Судьба сама по себе – наша внутренняя тюрьма, и осознание этого факта подвигает нас думать больше о свободе бытия, а не о свободе действия. «Разве судьба, которая есть основа нашей жизни, не держит нас в заключении под надзором одиночества, суровости, а подчас и жестокости окружающего мира, и разве это не вынуждает нас стараться заглянуть за пределы обыденности? Разве неизбежность смерти... не концентрационный лагерь для всех нас? Разве тот факт, что жизнь – это одновременно и радость, и тяжелое обязательство, не толкает нас к размышлению о более глубокой стороне бытия?».

Мэй определял судьбу (destiny) как «структуру из ограничений и способностей, которые представляют собой „данные“ нашей жизни». Судьба – это «строение Вселенной, проявляющее себя в строении каждого из нас». Окончательная судьба всего живого есть смерть, но при более детальном рассмотрении наша судьба включает в себя и другие биологические свойства, такие, как уровень интеллекта, пол, физическая сила и размеры нашего тела, генетическая предрасположенность к тем или иным болезням и т. д. Различные психологические и культурные факторы также вносят свой вклад в формирование нашей судьбы.

«Судьба – это наш «концентрационный лагерь», который, тем не менее, определяет нашу сущностную свободу.» Судьба – это то, к чему мы движемся,

наша единственная конечная станция, наша цель. Это отнюдь не означает тотальную предопределенность и обреченность. В границах, определенных судьбой, мы имеем право на выбор, и эта свобода позволяет нам при необходимости противостоять своей судьбе и изменять ее. В то же время невозможно изменить все, чего бы мы ни захотели. Мы не можем достичь успеха в любой работе, победить любую болезнь, построить отношения с любым человеком в точном соответствии со своими представлениями. Жизнь всегда вносит свои коррективы. «С судьбой нельзя не считаться, мы не можем просто стереть ее или заменить чем-то другим. Но мы можем выбирать, как нам отвечать нашей судьбе, используя дарованные нам способности».

Мэй полагал, что понятия судьбы и свободы, так же как и любви-ненависти, жизни-смерти, являются не взаимоисключающими, а дополняющими друг друга, существующими в неразрывной связи как одно из отражений величайшего парадокса, которым является человеческая жизнь. «Парадокс заключается в том, что свобода обязана своей жизнеспособностью судьбе, судьба же обязана свободе своей значительностью».

Свобода и судьба слиты, таким образом, воедино, одна не может существовать без другой. Свобода без судьбы – это распущенность и вседозволенность. Как это ни странно, на первый взгляд, вседозволенность, ведущая к анархии, в конце концов, влечет за собой полное уничтожение свободы. Таким образом, без судьбы не бывает свободы, точно так же, как судьба без свободы теряет всякое значение.

Свобода и судьба порождают друг друга. Бросая вызов судьбе, мы обретаем свободу. Стремясь к свободе, мы выбираем свой путь, который, так или иначе, проходит через пространство, ограниченное нашей судьбой.

В реальной действительности каждый человек при совершении любого своего проступка, в том числе и преступления, обязательно проявляет свободу воли, но в том «коридоре», в тех границах и пределах, которые определила ему судьба.

В теории уголовного права предлагается рассматривать уголовную ответственность в двух аспектах: в позитивном и в негативном. Позитивная (перспективная) уголовная ответственность рассматривается как отсутствие нарушений запретов, установленных уголовным законом. Позитивная уголовная ответственность понимается как «обязанность соблюдать требования уголовного закона», «правовые требования», «выполнение должного», «социальный правовой долг». Правовым последствием данного вида ответственности является положительная уголовно-правовая оценка поведения лица со стороны государства, в том числе поощрение его действий. По мнению сторонников теории позитивной ответственности, она проявляется, например, в том, что исключается уголовная ответственность за преступление, которое лицо не совершало; в освобождении от ответственности лица, добровольно отказавшегося от совершения преступления и т.д.

Негативная (ретроспективная) уголовная ответственность связана с совершением лицом преступления, предусмотренного уголовным законом и заключается в применяемых государством мер принуждения.

Деление уголовной ответственности на негативную и позитивную не является общепринятым в науке уголовного права. Отмечается, что позитивная уголовная ответственность не имеет большого правового значения, поскольку «перенесение понятия ответственности в область должного, толкуемого не как объективная реальность, а как определённый психологический процесс, лишает её правового содержания». И в этом смысле позитивная уголовная ответственность скорее является институтом морали, чем права.

Отсюда именно негативная уголовная ответственность имеет наибольшее теоретическое и практическое значение; в большинстве работ институт уголовной ответственности рассматривается именно в этом аспекте.

Для раскрытия сущности основания уголовной ответственности многие ученые обращаются к понятию состава преступления, причем делается это поразному.

Одни рассматривают основанием уголовной ответственности наличие состава преступления, что, на наш взгляд, является неверным утверждением, поскольку общественно опасное и противоправное деяние (преступление) подменяется весьма абстрактным виртуальным понятием состава преступления. Общее понятие состава преступления является средством познания конкретных составов преступлений и позволяет подвергать научному анализу их признаки, классифицировать эти признаки и содержание конкретных составов преступлений. В теории уголовного права общий состав используется как эталон, основа для правильного определения в каждом конкретном случае наличия или отсутствия в действиях лица того или иного состава преступления. Таким образом, общий состав преступления в науке уголовного права выступает в качестве своеобразного теоретического постулата для правильной квалификации совершенного деяния.

Не соглашаясь с такой трактовкой основания уголовной ответственности, следует подчеркнуть, что реально существующее в действительности совершенное преступление фактически подменяется понятием состава преступления. Это чисто научный термин и его можно использовать в научных дискуссиях, а в не в законодательных дефинициях. Более того, многие ученые отвергают полезность и необходимость вообще использования такого термина как состав преступления, боясь, по-видимому, того, что к виртуальному понятию человек часто привыкает и в один момент психологически может его принять за сущее.

В действующем уголовном законодательстве многих западных стран понятие состава преступления отсутствует, оно не нужно, вносит путаницу при соотношении понятия преступления и состава преступления.

Некоторые ученые считают, что единственным основанием уголовной ответственности является установление в действиях лица определенного состава преступления. Здесь стараются как-то приблизить реальность к раскрытию сущности понятия состава преступления. Однако исходным моментом для квалификации деяния является совершенное преступление и сравнение его с тем, как оно описано в законе. Ведь совершенное деяние всегда конкретно, реально, истинно. Если мы говорим о конкретном составе совершенного преступления, тем самым суживаем возможности его квалификации, отсекаем возможные ва-

риации, которые могут и не охватываться установленным в законе составом преступления. Здесь уместно вспомнить о методологическом принципе, получивший название по имени английского монаха, философа Уильяма Оккама «Бритва (лезвие) Оккама»[1], который, как представляется, следует использовать в наших рассуждениях. В упрощенном виде он гласит: «Не следует множить сущее без необходимости» (либо «Не следует привлекать новые сущности без самой крайней на то необходимости»). Альберт Эйнштейн переформулировал принцип «Бритвы Оккама» таким образом: «Всё следует упрощать до тех пор, пока это возможно, но не более того».

Более правильной, на наш взгляд, является позиция авторов, считающих, что единственным основанием уголовной ответственности является деяние (действие или бездействие) общественно опасное, виновное и противоправное, т. е. преступление, признаки которого нашли отражение в конкретной статье Особенной части УК[2]. Преимущество такого понимания оснований уголовной ответственности заключается в том, что здесь подчеркивается одновременность возникновения уголовной ответственности с моментом, фактом совершения лицом указанного в законе конкретного деяния. А состав преступления, разработанный наукой уголовного права, в последующем для правоохранительных органов выступает уже в качестве образца, эталона уголовно-правовой оценки (квалификации) преступления и лица, его совершившего.

Исходя из данных рассуждений, считаю, следует изменить законодательное определение понятия основания уголовной ответственности, изложенное в ч. 1 ст. 2 УК Украины, и представить эту часть статьи в такой редакции: ***«1. Основанием уголовной ответственности является совершение лицом деяния (действия или бездействия) общественно опасного, виновного и противоправного, т. е. преступления, признаки которого предусмотрены в конкретной статье Особенной части Кодекса».***

---

[1] Ockham, Ockam, Occam; ок. 1285-1349.

[2] Уголовное право Украины. Общая часть: учебное пособие для обучающихся на русском языке /Под ред. В.М. Трубникова, Я.А. Лантинова [В.М. Трубников, М.В. Даньшин, Д.С. Слинько, А.Н. Храмцов и др.]. – Х.: Харьков юридический. – 2012. – 344 с.

Туранин В.Ю.

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИНТЕРНЕТ-РЕСУРСОВ В ПРОЦЕССЕ ОСУЩЕСТВЛЕНИЯ МОНИТОРИНГА РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА[1]

Аннотация. В данной статье анализируется вопрос об осуществлении мониторинга российского законодательства с использованием Интернет-ресурсов.

Ключевые слова: мониторинг российского законодательства, интернет-ресурсы.

Abstract. This paper analyzes the implementation of the monitoring of the Russian legislation, using Internet resources.

Key words: monitoring of the Russian legislation, internet resources.

Мониторинг законодательства и правоприменительной практики в настоящий момент воспринимается как один из основных инструментов обеспечения ответственного принятия государственных решений. Помимо активного обсуждения данной проблематики в научном юридическом сообществе[2], в 2011 году был принят Указ Президента Российской Федерации «О мониторинге правоприменения в Российской Федерации»[3]. В соответствии с данным указом, федеральным органам исполнительной власти и региональным властям поручено осуществлять мониторинг правоприменения.

Основными целями проведения мониторинга являются:

– ликвидация противоречий между нормативно-правовыми актами;

– устранение коррупциогенных факторов;

– совершенствование правовой системы.

Координация проводимого мониторинга в соответствии с Указом Президента Российской Федерации «О мониторинге правоприменения в Российской Федерации» возложена на Министерство юстиции Российской Федерации. В развитие данного указа была утверждена соответствующая методика осуществления мониторинга правоприменения в Российской Федерации[4].

Как отмечается в одном из ежегодных докладов Совета Федерации Российской Федерации, посвященном состоянию отечественного законодательст-

---

[1] Статья подготовлена в рамках Государственного задания Министерства образования и науки Российской Федерации подведомственным вузам на выполнение НИОКР: проект № *6.2866*.2011.

[2] См.: Правовой мониторинг: научно-практ. пособие / Под ред. Ю.А.Тихомирова, Д.Б.Горохова. – М., 2009; Правовой мониторинг: актуальные проблемы теории и практики. Монография / Под ред. Н.Н.Черногора. – М., 2010; Арзамасов Ю.Г., Наконечный Я.Е. Мониторинг в правотворчестве: теория и методология. – М., 2009; Арзамасов Ю.Г., Наконечный Я.Е. Концепция мониторинга нормативно-правовых актов. – М, 2011; Жужгов И.В. Мониторинг правового пространства Российской Федерации. Дисс... канд. юрид. наук. – Ставрополь, 2006; Невеселов А.А. Правовой мониторинг и государственная политика. дис... канд. юрид. наук. – М., 2009.

[3] Указ Президента Российской Федерации от 20.05.2011 г. № 657 «О мониторинге правоприменения в Российской Федерации» // Российская газета. Федеральный выпуск № 5486. 25 мая 2011 г.

[4] Постановление Правительства РФ от 19.08.2011 г. № 694 «Об утверждении методики осуществления мониторинга правоприменения в Российской Федерации» // Собрание законодательства РФ, 29.08.2011, № 35, ст. 5081.

ва, «если мы не научимся, принимая законы, понимать, в какой мере в целом они полезны и исполняемы, если мы не приучим чиновника ориентироваться на данные мониторинга, в котором свою роль будут играть экспертные сообщества, институты гражданского общества, нам не удастся решить ни одной из поставленных задач»[1].

Следует обратить внимание на то, что в отличие от мониторинга правоприменения, официальных установок на проведение мониторинга российского законодательства в настоящее время не существует. При этом такой мониторинг проводится весьма активно и самыми различными субъектами. Помимо Министерства юстиции Российской Федерации, для которого эта деятельность является объективно необходимой, мониторинг российского законодательства осуществляется и подразделениями различных государственных органов, научных и учебных заведений: Центром мониторинга законодательства и правоприменительной практики (Центр мониторинга права) при Совете Федерации Федерального Собрания Российской Федерации, отделом мониторинга законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, центром мониторинга государственного управления и права Российской академии государственной службы при Президенте Российской Федерации и др.

Отметим, что *мониторинг – это постоянная и систематическая деятельность, связанная со сбором и анализом информации о каком-то конкретном объекте. Он основан на наблюдении за развитием исследуемого объекта с целью выявления его признаков, формулировании оценки его развития и воздействия на определенные общественные отношения. В этой связи*, мониторинг не может быть неким статичным явлением, его основной признак – это ***динамика***, позволяющая оценивать объект в соответствии с четкими горизонтами времени. С нашей точки зрения, в условиях развития современного мира необходимую эффективность мониторингу придает его «привязка» к коммуникативному пространству Интернета.

В настоящее время мониторинг законодательства в Интернет-пространстве проводится многими субъектами российского права, имеющими определенные коммуникативные ресурсы. В результате проведенного выборочного анализа различных сайтов исследуемой тематики, мы пришли к выводу о том, что теоретически можно выделить два вида мониторинга российского законодательства, основанного на использовании Интернет-ресурсов:

– корпоративный;

– ведомственный.

Корпоративный мониторинг осуществляют определенные юридические лица, для которых эта деятельность является важной и необходимой по своей сути. Он может проводиться как для реализации коммерческой цели, когда результат мониторинга – это определенный интеллектуальный продукт, который может быть реализован, так и для внутрикорпоративного использования.

---

[1] Постановление Совета Федерации Федерального Собрания РФ от 8 февраля 2006 г. № 36-СФ «О докладе Совета Федерации Федерального Собрания Российской Федерации 2005 года «О состоянии законодательства в Российской Федерации» // Собрание законодательства Российской Федерации. 2006. № 7. Ст. 746.

Примером первой ситуации может являться мониторинг федерального и регионального законодательства, проводимый компанией «Гарант». На сайте http://www.garant.ru/hotlaw/federal/ существуют специальные рубрики «Федеральные горячие документы» и «Региональные горячие документы». В них представлены новые документы с краткими комментариями к ним (обзорами), подготовленными специалистами компании «Гарант», они публикуются ежедневно и в режиме реального времени. Кроме этого, на данном сайте представлена Энциклопедия мониторинга, предназначенная для изучения изменений в интересующей отрасли права за определенный период времени.

Примером второй ситуации может являться мониторинг, который проводится некоторыми крупными юридическими фирмами. Например, корпорация Tenzor Consulting Group уже на протяжении многих лет осуществляет подобный мониторинг, а его результаты представлены на сайте http://www.tencon.ru/monitoring.

Существует и ведомственный мониторинг российского законодательства. Примером здесь может являться соответствующая деятельность МЧС России: http://www.mchs.gov.ru/law/law_monitoring.

Мониторинг российского законодательства, проводимый с использованием Интернет-ресурсов, характеризуется перманентной динамикой. Полагаем, что это вряд ли может быть оспорено. Каждый может узнать его результаты в режиме реального времени. В этой связи, обладает ли необходимой динамикой мониторинг, который осуществляется Министерством юстиции Российской Федерации, Центром мониторинга права при Совете Федерации, и другими субъектами, которые упоминались выше, при отсутствии связи с Интернетом? Это вопрос спорный. С одной стороны, мы можем, к примеру, изучить доклад Совета Федерации, посвященный состоянию российского законодательства, в котором использованы результаты проведенного мониторинга, и сделать необходимые (по большей части, теоретические) выводы. Но, с другой стороны, насколько это актуально для практикующего юриста, которому нужно знать ситуацию ежедневно, что называется, «здесь и сейчас»?

В этой связи, наша точка зрения заключается в том, что мониторинг российского законодательства все-таки должен осуществляться на современной платформе, с использованием Интернет-ресурсов, что придает ему максимальную эффективность. И если в этом заинтересованы корпорации, отдельные ведомства, то почему здесь не может быть общегосударственного интереса? Полагаем, что необходимо создание крупного портала, посвященного мониторингу российского законодательства, модераторами которого могли бы выступить обе палаты Федерального Собрания Российской Федерации и региональные органы законодательной власти. Вполне возможно законодательное закрепление данной концепции. Кроме этого, с нашей точки зрения, целесообразна трансляция идеи мониторинга с привлечением Интернет-ресурсов и на муниципальный уровень, в целях создания портала муниципальных правовых актов. Модераторами здесь могут быть муниципальные представительные органы власти.

Тычинин С.В.

ДОСТУП К ИНФОМАЦИИ О ДЕЯТЕЛЬНОСТИ СУДОВ В СЕТИ «ИНТЕРНЕТ» И ТАЙНА ЧАСТНОЙ ЖИЗНИ

Аннотация. Рассмотрены основные нормативные акты в области права на доступ к информации о деятельности судов, дана критическая оценка некоторым правовым нормам, допускающим возможность широкого доступа к судебным актам посредством сети «Интернет».

Ключевые слова: тайна, частная жизнь, суд, «Интернет».

Abstract. The basic regulations on the right to access to information about the courts, made a critical evaluation of some legal norms, allowing broad access to judicial decisions through the «Internet».

Key words: secret, private life, the court, the «Internet».

Федеральный закон от 22 декабря 2009 года «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» (в ред. от 18.07.2011)[1] (далее – Закон) закрепляет комплекс норм, регулирующих отношения, связанные с обеспечением доступа пользователей к информации о деятельности судов.

Кроме названного закона к числу источников правового регулирования данных отношений отнесены Конституция РФ и другие федеральные конституционные законы, федеральные законы, устанавливающие порядок судопроизводства, полномочия и порядок деятельности судов, Судебного департамента, органов Судебного департамента, органов судейского сообщества, другими федеральными законами, а в отношении конституционных (уставных) судов субъектов Российской Федерации и мировых судей – также законодательством субъектов Российской Федерации, регламентами судов и (или) иными актами, регулирующими вопросы внутренней деятельности судов, актами органов судейского сообщества. Таким образом, компетенцией в определения порядка в сфере обеспечения доступа пользователей к информации о деятельности судов обладает значительное количество субъектов, что требует соблюдения принципов единообразия в установлении соответствующих правил.

Здесь следует подчеркнуть, что нормами международного договора могут предусматриваться иные правила в этой сфере (п.2 ст.3 Закона). В целом же, право на доступ к информации о деятельности публичных органов соответствует большинству основополагающих международных актов.

В числе способов, предоставляющих доступ к информации, назван такой способ, как размещение информации о деятельности судов в сети «Интернет» (п.3 ст. 6 Закона). Специальные вопросы доступа к информации о деятельности судов посредством ее размещения в сети Интернет урегулированы в Положении по созданию и сопровождению официальных интернет-сайтов судов; Регламенте размещения информации о деятельности судов общей юрисдикции, органов судейского сообщества, системы Судебного департамента при Верховном

[1] Собрание законодательства РФ. 2008. № 52 (ч. 1). Ст. 6217; 2011. № 30 (ч. 1). Ст. 4588.

Суде Российской Федерации в сети Интернет; Регламенте организации размещения сведений о находящихся в суде делах и текстов судебных актов в информационно-телекоммуникационной сети Интернет на официальном сайте суда общей юрисдикции[1].

Закон не дает перечня видов информации, которую вправе предоставлять компетентные органы, а вводит запрет на предоставления двух видов: 1) информации, которая отнесена в установленном федеральным законом порядке к сведениям, составляющим государственную тайну; 2) иную охраняемую законом тайну. При этом закон не уточняет, что понимать под «иной охраняемой законом тайной». Можно предположить, что речь идет о сведениях, касающихся частной жизни, коммерческой, нотариальной, адвокатской и др. тайны. В п. 8 ст. ст. 9 Закона прямо предусмотрен запрет на получение информации о частной жизни физического лица, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Важно так же учитывать, что в ст. 4 Закона, наряду с другими принципами, закреплен принцип соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права организаций на защиту их деловой репутации; соблюдение прав и законных интересов участников судебного процесса при предоставлении информации о деятельности судов.

П.п. 2, 3 ст. 8. Закона предусматривает, что граждане имеют право на получение от компетентных органов и их должностных лиц информации, непосредственно затрагивающей его права и свободы. Организация вправе получать информацию, непосредственно касающейся ее прав и обязанностей, либо информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности. Таким образом Закон недвусмысленно ограничивает неограниченный доступ для получения сведений о частных правах других гражданах и организаций, участвовавших в юрисдикционной деятельности суда.

К информации, которая может предоставляться без каких-либо ограничений, относится информация о нормативных актах, затрагивающих права, свободы и обязанности человека и гражданина, а также устанавливающих правовое положение организаций и полномочия государственных органов, органов местного самоуправления; информации о состоянии окружающей среды; информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну); 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; иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

---

[1] СПС Консультант плюс.

Сами же государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности.

Полный перечень сведений, которые составляют информацию о деятельности судов и подлежат обязательному размещению в сети «Интернет», приведен в статье 14 Закона об обеспечении доступа к информации.

В ст. 15 Закона определяются особенности размещения в сети «Интернет» текстов судебных актов.

Во-первых, из числа судебных актов, подлежащих опубликованию, исключены приговоры, не вступившие в законную силу. Отдельные акты, вполне оправданно, не подлежат размещению в сети «Интернет» тексты судебных актов, вынесенных по делам, затрагивающим безопасность государства; возникающим из семейно-правовых отношений и др.

Во-вторых, судебные акты (после вступления в силу и приговоры) подлежат опубликованию в сети «Интернет» в полном объеме.

В-третьих, при размещении в сети «Интернет» текстов судебных актов, вынесенных судами общей юрисдикции, в целях обеспечения безопасности участников судебного процесса из указанных актов исключаются персональные данные, кроме фамилий и инициалов истца, ответчика, других участников процесса.

Таким образом, фамилии и инициалы граждан в судебных актах сохраняются, следовательно, доступ к содержанию акта и его участниках, сути спора открыт неограниченному кругу лиц. С таким подходом законодателя сложно согласиться. Например, в условиях небольшого населенного пункта сохранение инициалов, а иногда и просто сути дела, дает ясную картину об обстоятельствах того иного юридического спора и его участниках. Вряд ли участники процесса заинтересованы в оглашении подробностей результата спора для широкого круга общественности. Обладание информацией о чужом споре в ряде случаев делает уязвимой право на тайну частной жизни. Стороны могли уже давно помириться, судимость была погашена, а решения и приговоры напоминают о былых юридических конфликтах. К сожалению, законодательство этот фактор не учитывает.

В п. 4 ст. 27 Постановления Пленума ВАС РФ от 8 декабря 2012 года №61 «Об обеспечении гласности в арбитражном процессе» судебные акты, принятые по делам, при рассмотрении которых исследовались сведения, составляющие коммерческую или иную охраняемую законом тайну, также не подлежат размещению в сети «Интернет»[1]. В данном случае речь идет о коммерческой и иной тайне. Представляется, что уже само размещение текста судебного акта, которое потенциально предназначено для всеобщего доступа неограниченному кругу лиц, может затрагивать частные интересы граждан и организаций и при этом не нарушать коммерческую тайну. Например, гражданина могут не взять на работу, так как посчитают сутяжником. Сведения о резуль-

[1] Вестник ВАС РФ. 2012. №12.

тате спора могут быть использованы контрагентами проигравшего ответчика в своих интересах.

Представляется, что обеспечение свободного доступа к итоговым судебным актам, выносимым по делам мировых судей, уголовным и гражданским делам, подсудным судам общей юрисдикции субъектов РФ, окружным арбитражным судам и их нижестоящим судам, могут осуществляться только с согласия истца и ответчика в гражданском процессе, обвиняемого и потерпевшего в уголовном процессе. Доступ к базе данных любых итоговых судебных актов может быть расширен для научных целей, необходимости обобщения практики по отдельным категориям дел. Возможно так же разрешить доступ к данным по отдельным ситуациям, когда имеется тесная взаимосвязь рассматриваемого дела с судебными актами по другим делам.

Что же касается оперативного ознакомления с материалами дела, например, с промежуточными актами через «Интернет», то здесь необходимо разработать особый алгоритм взаимоотношений лишь для участников конкретного процесса и по конкретному делу. Например, в США функционирует система общественного доступа к судебным электронным документам ПАСЕР (Public Access to Court Electronic Records (PACER).Для получения информации из системы ПАСЕР пользователь должен зарегистрироваться и получить персональное имя пользователя и пароль[1]. В результате обеспечивается хотя бы минимальный контроль за порядком пользования информацией с судебными актами.

Специальным исследованием Фонда свободной информации 126 сайтов судов общей юрисдикции[2] выявлены другие проблемные вопросы, возникающие в связи с публикацией судебных актов на сайтах: размещение значительно меньшего количества судебных актов, чем предписано законодательством; невыполнение сроков публикации судебных актов; необоснованное и чрезмерное удаление сведений из судебных актов; наличие технических сложностей, связанных с реализацией доступа к судебным актам (неудобная система организации поиска по базе данных судебных актов; отсутствие постоянного и беспрепятственного доступа к разделу «Судебные акты» в связи с нестабильностью работы сервера, на котором размещаются судебные акты.

Таким образом, вопросы доступа к актам правосудия через сеть «Интернет» требуют дальнейшего правового, организационного и технического совершенствования.

---

[1] См.: http://ncpi.gov.by.blog.tut.by/2012/02/17/razvitie-pravovoy-informatizatsii-za-rubezhom-elektronnoe-opublikovanie-sudebnyih-aktov/

[2] http://www.svobodainfo.org/ru/node/2346

Федорященко А.С.
Шафорост Т.Л.

НАДО ЛИ ПРЕДОСТАВЛЯТЬ ПРАВОВУЮ ЗАЩИТУ ОТ ИНФОРМАЦИИ, РАЗМЕЩЕННОЙ В БЛОГЕ ИЛИ НА ФОРУМЕ?

Аннотация. Данная статья посвящена решению одной из актуальных правовых проблем современного Интернет-сообщества: правовому статусу сведений, размещенных на таких специфических ресурсах сети как форумы, блоги, доски объявлений, чаты и т.п.

Ключевые слова: Интернет, форум, блог, недостоверная информация, честь, достоинство, деловая репутация.

Abstract. This article deals with the solution of one of the most actual legal problems of the modern Internet community: the legal status of the information posted on such specific network resources like forums, blogs, message boards, chat rooms, etc.

Key words: The Internet, forum, a blog, unreliable information, honor, dignity, business reputation.

Развитие информационных технологий, вовлечение средств сети Интернет в повседневную жизнь приводят к возникновению новых, ранее неизвестных правовой действительности способов распространение информации. Все уже давно привыкли к тому, что в Интернете сведения распространяются мгновенно, и их адресатами выступает все большая аудитория. Практически все традиционные средства массовой информации (теле– и радиоканалы, журналы, газеты) имеют свои сайты. Кроме того существует огромное количество собственно Интернет-СМИ, освещающих новости и события. К названным СМИ в полной мере применятся законодательство о средствах массовой информации, в том числе и нормы, касающиеся защиты прав и интересов лиц от распространения недостоверной информации, затрагивающей их честь, достоинство и деловую репутацию. Но Интернет предлагает не только сайты, зарегистрированные в качестве СМИ. Широкую популярность получили такие элементы сети, как форумы, блоги, доски объявлений, чаты и т.д., не имеющие статуса СМИ. Какой правовой статус имеет информация, размещенная на таких ресурсах? Какие правовые нормы применять в случае распространения недостоверной информации, скажем в блоге или на форуме? В конце концов, кого считать ответственным за распространение этой ложной информации? Современное российское законодательство не дает четких ответов на данные вопросы. Анализ правоприменительной деятельности показывает, что арбитражная практика в этой области неоднозначна, суды вынуждены выносить решения, основываясь на собственном мнении, которое зачастую у разных судов отличается кардинально.

При исследовании правового режима информации, размещенной в блогах или на форумах, в первую очередь следует определиться, можно ли относить ее к сведениями, которые могут быть опровергнуты, или она относится к оценочным суждениям, мнениям, убеждениям. А они, как известно, не являются предметом судебной защиты. Постановление Пленума Верховного Суда РФ «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» указывает, что в соответствии со

ст. 10 Конвенции о защите прав человека и основных свобод и ст. 29 Конституции Российской Федерации, гарантирующими каждому право на свободу мысли и слова, а также на свободу массовой информации, позицией Европейского Суда по правам человека при рассмотрении дел о защите чести, достоинства и деловой репутации судам следует различать имеющие место утверждения о фактах, соответствие действительности которых можно проверить, и оценочные суждения, мнения, убеждения, которые не являются предметом судебной защиты в порядке ст. 152 Гражданского кодекса Российской Федерации, поскольку, являясь выражением субъективного мнения и взглядов ответчика, не могут быть проверены на предмет соответствия их действительности[1].

Анализ научной литературы и арбитражной практики показывает, что существуют прямо противоположные мнения по данному вопросу.

Одни суды указывают, что согласно определению разговорника (авторы Д. Завалишин, Е. Завалишина, Е. Компановская) форум – это инструмент для общения на сайте, то есть представляет собой форму общения в виде сообщений конкретных лиц, которые высказывают собственные мнения и оценки относительно темы, заданной этими же лицами; сообщения на форумах и комментарии к статьям публикуются авторами в ходе широкого обсуждения – дискуссии, а в соответствии с позицией Европейского суда по правам человека в ходе публичных дискуссий допускаются несдержанные высказывания. Поддерживая свою позицию, суды указывают, что частное мнение автора, выраженное на форуме или в комментарии к статье, опубликованной в Интернете, может быть оспорено в порядке полемики, то есть ответа, реплики или комментария, которые истец может свободно и самостоятельно опубликовать на том же форуме[2].

Другие считают, что «...возможность опровержения сведений в порядке, предусмотренном положениями ст. 152 ГК РФ, поставлена в зависимость от содержания этих сведений, а не от формы или способа их изложения. Таким образом, в сообщениях лиц, которые размещаются на форуме, также могут содержаться утверждения порочащего характера, которые могут быть проверены на предмет их соответствия действительности»[3]. С данной позицией арбитражного суда согласна и Е.И. Сизова, которая тем не менее считает, что в данном случае необходимо разделить бремя ответственности между автором комментария и администратором сайта: на первого возлагать обязанность возмещения морального вреда, на второго – обязанность удаления порочащих сведений с сайта[4].

---

[1] Постановление Пленума Верховного Суда РФ от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Российская газета от 15 марта 2005 г.

[2] Постановление Седьмого арбитражного апелляционного суда от 22.12.2009 по делу № А45-15768/2009 // СПС «КонсультантПлюс».

[3] Постановление ФАС Уральского округа от 12.10.2009 № Ф09-7703/09-С6 по делу № А60-33583/2008-С7 // СПС «КонсультантПлюс».

[4] Сизова Е.И. Некоторые аспекты дел о защите деловой репутации, затронутой недостоверными порочащими сведениями, распространенными в сети Интернет // Арбитражные споры. 2010. № 4. С. 149.

Что касается зарубежного опыта, приведем здесь резюме, которое сделал Н.А. Дмитрик по результатам исследования американского подхода к рассматриваемой проблеме: «... как минимум в случае с оскорбительными или клеветническими высказываниями... нет вопроса о привлечении провайдеров к ответственности за контент третьих лиц»[1]. В ФРГ деятельность информационных посредников (хостинг-провайдеров) также защищается. Рассматриваемые способы коммуникаций наделяются особой правовой защитой, поскольку они создают «рынок мнений» (marketplace of opinions) в демократическом обществе, и потому каждому гарантируется возможность свободно формировать мнение[2].

Представляется, что истина как обычно где-то посередине.

Прежде всего, при разрешении вопроса защиты деловой репутации от недостоверных сведений, размещенных на форуме или в блоге, следует соблюсти тщательный баланс между свободой слова и правом на деловую репутацию.

Думается, что нельзя однозначно согласиться с указанной несколько выше позицией, что при решении вопроса о правовом статусе сообщений форума (или блога) следует принимать во внимание только понятие «форум» как дискуссии (блог также предполагает возможность публичной полемики). Наличие такого формата ресурса, который предполагает дискуссию или даже наличие непосредственно дискуссии, не устраняет того факта, что в рамках обсуждения возможно высказывание, которое не отражает личное мнение автора сообщения, а выдается им за достоверную информацию.

Кроме того, ставить возможность судебной защиты деловой репутации от наличия возможности самозащиты в корне неверно. Мы не можем сказать лицу, чье право нарушено (тем более юридическому лицу): «Это дискуссия, защищайся сам».

Поэтому в принципе, можно констатировать, что при разрешении вопроса о защите деловой репутации от недостоверной информации, размещенной на ресурсах форумов, блогов, чатов и т.д., значение имеет не формат ресурса, а словесная, текстуальная форма подачи информации. В одном случае, это может быть личное мнение автора сообщения, в другом порочащие сведения, которые подлежат опровержению.

Что же касается вопроса определения лица, обязанного понести ответственность за распространение недостоверных сведений (в процессуальном аспекте – надлежащего ответчика), то и здесь нет единства мнений.

Когда речь идет об оскорбительных, уничижительных или ненормативных высказываниях, посягающих на честь и достоинство, то администратор домена имеет реальную возможность их оценить и воспрепятствовать их публикации или удалить их. Но при опорочении деловой репутации сведения всего лишь не соответствуют действительности (они вполне могут быть корректны по форме) и оценить их достоверность администратором нереально. В отношение Интернет-СМИ Постановление Пленума ВС РФ указало: «Если на сайте в

---

[1] Дмитрик Н.А. Осуществление субъективных гражданских прав с использованием сети Интернет. М.: Волтерс Клувер, 2006. С.171.

[2] Там же.

сети Интернет, зарегистрированном в качестве средства массовой информации, комментарии читателей размещаются без предварительного редактирования (например, на форуме читателей материалов такого сайта), то в отношении содержания этих комментариев следует применять правила, установленные в части 2 статьи 24 и пункте 5 части 1 статьи 57 Закона Российской Федерации «О средствах массовой информации» для авторских произведений, идущих в эфир без предварительной записи»[1]. Правда вышеуказанная ст. 24 утратила силу, но п. 5 ч. 1 ст. 57 Закона «О средствах массовой информации»[2] продолжает действовать, и в соответствии с ним администратор домена не должен нести ответственность за сообщения форумов, блогов, чатов и т.д. Остается лишь дождаться распространения указанных норм и на сайты, которые не зарегистрированы в качестве средств массовой информации.

[1] Постановление Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации» // Российская газета от 18 июня 2010 г.

[2] Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» // Российская газета от 08 февраля 1992 г.

Чалых И.С.

К ВОПРОСУ ОБ ОПТИМИЗАЦИИ ОБЕСПЕЧЕНИЯ ПРАВА ЛИЧНОСТИ НА ДОСТУП К ЭКОЛОГИЧЕСКОЙ ИНФОРМАЦИИ[1]

Аннотация. В статье проанализирована нормативная правовая основа обеспечения конституционного права личности на доступ к экологической информации в современной России, выявлены законодательные пробелы определения и гарантирования данного института, рассмотрены доктринальные предпосылки их преодоления; уделено особое внимание вопросу реализации права личности на доступ к экологической информации посредством информационно-коммуникационных технологий, включая ресурсы сети «Интернет», в части государственно-программного подхода к информатизации деятельности органов государственной власти Российской Федерации.

Ключевые слова: право на доступ к информации, экологическая информация, право на обращение, обеспечение, конституционно-правовое регулирование, информационная система, электронный ресурс, оптимизация.

Abstract. In the article the legal and regulatory framework within which the constitutional right of individuals to have access to environmental information in today's Russia, identified legal gaps and ensure the definition of the institution, considered the doctrinal background of overcoming them, paid special attention to the implementation of the individual's right to access to environmental information through information and communication technologies, including those of the «Internet», in terms of public-program approach to information of public authorities of the Russian Federation.

Key words: right of access to information, environmental information, the right to appeal, the provision constitutionally legal regulation, information system, electronic resource optimization.

Современные тенденции развития информационных технологий и обусловленных ими общественных отношений актуализируют вопросы обеспечения права личности на информацию в государстве. При этом информация, выступая предметом правового регулирования, обретает не только статус объекта соответствующих правоотношений, но и необходимым условием жизнедеятельности. И здесь особое значение приобретают предоставляемые государством возможности доступа личности к информации и гарантии их осуществления.

Так, право граждан на доступ к информации и участие в принятии на ее основе решений закреплено в Конституции Российской Федерации[2] (ст.ст. 3, 29, 31-33, 42 и др.). Оно вытекает из естественных прав каждого человека на жизнь и свободу, а его осуществление предполагает, в том числе, возможность личности участвовать в решении вопросов государственного управления. Для этого должна наличествовать возможность получить исчерпывающую инфор-

[1] Данная работа выполнена в рамках государственного задания; регистрационный номер 6.2962.2011.

[2] Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок от 30 декабря 2008 г.) // Российская газета. 1993, 25 декабря; 2009, 21 января.

мацию по интересующим вопросам. А государство, претендующее на статус правового, обязано обеспечить эти важнейшие условия[1].

Подчеркнем, что роль информации постоянно возрастает и в экологической сфере. Информационный фактор, усиливающийся в условиях глобализации, приводит к активному развитию эколого-информационных общественных отношений, которые возникают по поводу экологической информации и в связи с ней[2]. Такая тенденция представляется вполне закономерной, несмотря на снижение активности в данной сфере в сравнение с концом XX века: специфика становления современного российского государства обусловила смещение акцента в правовом регулировании с экологического на экономический, а в процессе его развития усугубившиеся экологические проблемы заставили обратить на себя пристальное внимание и со стороны государства, и со стороны гражданского общества. В результате в современный период комплекс экологических прав, включая право на доступ к экологической информации, закрепленный в ст. 42 Конституции России, из декларации превратился в реальную конституционную основу и актуального доктринального осмысления, и адекватной правотворческой и правоприменительной практики.

Так, действующее российское законодательство определяет ряд правовых средств и методов, направленных на обеспечение права доступа к экологической информации. Данному вопросу посвящены как общие, так и специальные правовые нормы и институты. При этом правовую основу такого обеспечения, наряду с положениями указанной ст. 42, составляют нормы российской Конституции, закрепляющие: обязанность органов государственной власти и местного самоуправления, их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, за исключением случаев, предусмотренных законом (ч. 2 ст. 24); право каждого свободно искать и получать информацию любым законным способом (ч. 4 ст. 29); право граждан Российской Федерации обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления (ст. 33); гарантии государственной защиты прав и свобод человека и гражданина (ч. 1 ст. 45), включая право на самозащиту (ч. 2 ст. 45), гарантии судебной защиты соответствующих прав и свобод (ч. 1 ст. 46), право на обжалование действий и решений компетентных органов, общественных организацией и их должностных лиц в судебном порядке (ч. 2 ст. 46) и др. Указанные и иные конституционные нормы, как представляется, определяют вариацию юридических возможностей лица в части обеспечения его права на доступ к экологической информации, а также направления их дальнейшего правового регулирования.

---

[1] См.: Шадрина О.В. Физические лица как субъекты права доступа к экологической информации по законодательству Российской Федерации // Административное и муниципальное право. 2012. № 1.

[2] См.: Выпханова Г.В. Правовая категория «экологическая информация»: дискуссионные вопросы // Экологическое право. 2008. № 3.

Подчеркнем, что законодательные основы обеспечения доступа лица к любой информации закрепляют положения Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации»[1]. В частности, согласно нормам указанной статьи: расширен перечень субъектов доступа к информации – «граждане (физические лица)», а также определено, что таковые «вправе осуществлять поиск и получение любой информации в любых формах и из любых источников» при условии соблюдения требований российского законодательства, включая возможность получения информации, непосредственно затрагивающей их права и свободы, от государственных органов, органов местного самоуправления и их должностных лиц (ч.ч. 1, 2); установлено, что не может быть ограничен доступ к информации о состоянии окружающей среды (ч. 4); определено, что указанные компетентные органы обязаны в установленных законом пределах обеспечить доступ к информации о своей деятельности, в том числе, с использованием информационно-телекоммуникационных сетей (сети «Интернет» и пр.), а лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения (ч. 5); закреплено, что «решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд» (ч. 6). Представляется, отмеченные положения составляют, в том числе, структуру механизма обеспечения доступа заинтересованного лица к экологической информации.

Подтверждает данный вывод и содержание ряда статей общего и специального экологического законодательства. Так, право граждан на достоверную информацию о состоянии окружающей среды закреплено в ст. 11 Федерального закона Российской Федерации «Об охране окружающей среды»[2]. Согласно ее положениям граждане имеют право направлять обращения в органы государственной власти Российской Федерации и ее субъектов, органы местного самоуправления, иные организации и должностным лицам о получении своевременной, полной и достоверной информации о состоянии окружающей среды в местах своего проживания, мерах по ее охране. А, к примеру, ст. 29 Федерального закона Российской Федерации «Об охране атмосферного воздуха»[3] прямо предусматривает право на получение информации о состоянии атмосферного воздуха, его загрязнении, а также об источниках его загрязнения и вредного физического воздействия на него. С этим правом корреспондируют нормы, обязы-

---

[1] Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с посл. изм. от 28 июля 2012 г.) // Российская газета. 2006, 29 июля; www.consultant.ru

[2] Федеральный закон Российской Федерации от 10 января 2002 г. № 7-ФЗ «Об охране окружающей среды» (с посл. изм. от 25 июня 2012 г.) // СЗ РФ. 2002. № 2. Ст. 133; www.consultant.ru

[3] Федеральный закон Российской Федерации от 4 мая 1999 г. № 96-ФЗ «Об охране атмосферного воздуха» (с посл. изм. от 25 июня 2012 г.) // Российская газета. 1999, 13 мая; www.consultant.ru

вающие органы государственной власти и органы местного самоуправления предоставлять такую информацию, принимать другие меры по формированию информационных ресурсов, обеспечению к ним доступа и др.

Помимо указанного, действующее российское законодательство устанавливает и юридическую ответственность за нарушение права на доступ к экологической информации со стороны уполномоченных органов, организацией и их должностных лиц. В частности, следует отметить ст. 8.5. Кодекса Российской Федерации об административных правонарушениях[1], устанавливающую административную ответственность за сокрытие, умышленное искажение или несвоевременное сообщение полной и достоверной информации о состоянии окружающей природной среды и природных ресурсов, об источниках загрязнения окружающей природной среды и природных ресурсов или иного вредного воздействия на окружающую природную среду и природные ресурсы, о радиационной обстановке, а равно искажение сведений о состоянии земель, водных объектов и других объектов окружающей природной среды лицами, обязанными сообщать такую информацию. В свою очередь Уголовный кодекс Российской Федерации[2] в ст. 237 содержит состав преступления, связанного с сокрытием информации об обстоятельствах, создающих опасность для жизни и здоровья людей либо для окружающей среды, совершенные лицом, обязанным обеспечивать население и органы, уполномоченные на принятие мер по устранению такой опасности, указанной информацией.

Вышеизложенное свидетельствует о том, что вопросу обеспечения права доступа к экологической информации законодателем уделяется достаточное внимание. Официально соответствующие способы и средства обеспечения закрепляются как в общих, так и специальных правовых источниках. При этом можно сделать вывод, что наиболее распространенным и применяемым в современной России выступает институт обращений в компетентные органы публичной власти.

Однако, представленные и иные результаты их анализа позволяют выявить и ряд демонстративных проблем в данной сфере. Во-первых, до сих пор четко законодательно не определено само понятие экологической информации, что затрудняет предметно-содержательную интерпретацию права на доступ к ней. Здесь следует поддержать позицию ряда авторов, согласно которой для определения понятия «экологическая информация» необходимо выделить ее существенные признаки, которые позволят дифференцировать ее среди других видов информации. К таковым предлагается отнести ключевые признаки относимости, значимости и достоверности, что не исключает расширения данного перечня характеристик[3]. Представляется, данный вопрос требует официального

---

[1] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с посл. изм. от 17 января 2013 г.) // Российская газета. 2001, 31 декабря; www.consultant.ru

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с посл. изм. от 30 декабря 2012 г.) // СЗ РФ. 1996. № 25. Ст. 2954; www.consultant.ru

[3] См.: Шадрина О.В. Физические лица как субъекты права доступа к экологической информации по законодательству Российской Федерации // Административное и муниципальное право. 2012. № 1.

разрешения посредством внесения дополнений в общее экологическое законодательство (к примеру, Федеральный закон Российской Федерации «Об охране окружающей среды»).

Во-вторых, как отмечается в литературе, экологическая информация является ключевым составляющим элементом эколого-информационных правоотношений с участием физических лиц, включая граждан Российской Федерации, иностранцев и лиц без гражданства[1]. Основу таких правоотношений составляет Конституция Российской Федерации, в соответствии с которой право на достоверную информацию о состоянии окружающей среды отнесено к числу основных прав человека и гражданина (ст. 42) и принадлежит каждому (лицу). Однако официально субъекты, обладающие правом на доступ к экологической информации, в различных законодательных источниках обозначены не идентично – каждый человек, физическое лицо, гражданин, гражданин Российской Федерации. При этом, если использовать правило приоритета специальной нормы права, то круг субъектов реализации указанного права значительно сужается. Представляется, в данной связи логичнее ориентироваться на общие нормы, закрепленные, в частности, в «рамочном» Федеральном законе Российской Федерации «Об информации, информационных технологиях и о защите информации», но с учетом ограничений, предусмотренных иными федеральными законами.

В-третьих, основной задачей нормативного правового регулирования эколого-информационных отношений является установление правового механизма реализации права на доступ к экологической информации. При этом на законодательном уровне ни содержательно, ни критериально не определено, какие именно компетентные органы выступают адресатом обязанности обеспечения права доступа к экологической информации, кроме факта их отнесения к категории государственных, муниципальных или иных. Здесь, что логично, если речь идет об организациях, не обладающих властными полномочиями, вектор реализации права на доступ к экологической информации определяется в конкретной правовой ситуации. То есть, субъект данного права в большинстве случаев предполагает, какое предприятие или общественная организация выступят адресатом его реализации. Однако в аспекте идентификации компетентного органа публичной власти ситуация гораздо сложнее. В частности, дополнительно следует обратить внимание на подзаконное регулирование организационных вопросов, связанных с распределением предметов ведения и компетенции, разобраться в сложноорганизованной бюрократической системе таких органов и пр. Все это порождает проблему неопределенности для лица, заинтересованного в получении значимой для него экологической информации, в аспекте выбора адресата его правопритязания. В результате субъект-правообладатель либо получает несвоевременную или неактуальную информацию, либо вообще отказывается от реализации своего права да доступ к ней, что есть проявление эколого-правового нигилизма. В данной связи считаем обоснованным предложить упрощенный (для субъекта-правообладателя) механизм реализации права личности на доступ к экологической информации.

---

[1] См.: Мисник Г.А. Право на доступ к экологической информации // Журнал российского права. 2007. № 2.

Наиболее оптимальным здесь видится обращение к возможностям, предоставляемым современными информационно-коммуникационными технологиями и системами, в первую очередь, к ресурсам сети «Интернет». Рассмотрим перспективы их применения для обеспечения права доступа к экологической информации на примере такой фокусной группы, как федеральные органы исполнительной власти. Представляется, именно данная группа компетентных органов должна демонстрировать инновационные формы и методы своей деятельности, использовать современные инструменты, в первую очередь основанные на применении информационно-коммуникационных технологий, при осуществлении взаимодействия с другими органами власти, гражданами и организациями[1], на что в перспективе должны ориентироваться и иные компетентные органы в сфере публичной власти. Подтверждением тому служат задачи, поставленные в рамках государственной программы «Электронная Россия»[2], а наиболее применимым, как с технологических, так и с юридических позиций, в контексте заявленного направления исследования выступает ресурс «Электронное Правительство». На основе указанного ресурса предлагается разработать и внедрить государственную информационную систему «Экологическая информация», причем гиперссылка для доступа к ней, как представляется, и должна быть размещена на официальном сайте Правительства Российской Федерации.

В аспекте правового обеспечения заявленного способа реализации права на доступ к экологической информации отметим следующее. Так, следует согласиться, что юридические механизмы предоставления и распространения информации являются преимущественно административно-правовыми. Причем однозначно к категории административно-правовых можно отнести группу норм Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации», определяющих статус, порядок создания и функционирования государственных информационных систем (ст. 14). А создание таких систем и есть реализация внутриорганизационных отношений всех субъектов, осуществляющих государственно-властные функции[3].

Далее, согласно нормам той же ст. 14 для любой информационной системы, в том числе и государственной, одной из основ для создания является порядок наполнения ее информационными ресурсами. В соответствии с указанными нормами государственные информационные ресурсы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления. В данной связи порядок, объем и сроки предоставления необходимой (в том числе, экологической) информации должны быть урегулированы нормами административного

---

[1] См.: Устинович Е.С. Информационная деятельность федеральных органов исполнительной власти как специальный объект правового регулирования // Юридический мир. 2009. № 4.

[2] Постановление Правительства Российской Федерации от 28 января 2002 г. № 65 «О федеральной целевой программе «Электронная Россия (2002-2010 годы)» (с посл. изм. от 9 июня 2010 г.) // СЗ РФ. 2002. № 5. Ст. 531; www.consultant.ru

[3] См.: Рыжов Р.С. Правовое регулирование отношений, связанных с информационными технологиями и защитой информации // Административное и муниципальное право. 2011. № 9.

права. Представляется, субъектом правотворчества здесь должно выступить Правительство Российской Федерации, а необходимые нормативные правовые положения должны быть отражены в его постановлении «О создании и функционировании государственной информационной системы «Экологическая информация».

В технологическом аспекте предлагаемая система призвана решать двуединую задачу. С одной стороны, в рамках данной системы предлагается сформировать «навигационную» подсистему, позволяющую обычному пользователю максимально точно определить адресата обращения (компетентный орган, должностное лицо) для получения интересующей его экологической информации. Ориентиром здесь должен выступать комплекс предметно-объектных критериев, относимых к содержанию конкретной юридической ситуации (например, «экология строительства», «экология землепользования», «экология территории» и др.). С другой стороны, наряду с выбором адресата, в указанной системе должен быть предусмотрен механизм безконтактного к нему обращения для непосредственного получения экологической информации. Здесь технологической основой может выступить интернет-служба «электронная почта». Представляется, данный ресурс имеется в распоряжении всех федеральных органов исполнительной власти и их должностных лиц, а его технические характеристики позволяют фиксировать такие реквизиты и обеспечительные элементы, которые характерны для непосредственных (устных и письменных) обращений лиц в компетентные органы власти: дата и время получения обращения, должность получателя обращения, иные его персональные данные и др., а также использовать альтернативные им средства, например, электронную цифровую подпись. Помимо указанного, с применением возможностей электронной почты значительно увеличивается оперативность рассмотрения обращения, установления «обратной связи» с его адресантом, а также переадресации (при необходимости) такого обращения по подведомственности с учетом визирования, постановки резолюции и обязательного уведомления адресанта о переадресации. Ввиду того, что служба электронной почты фиксирует дату, время и данные переадресации, представляется технически и юридически возможным привлечение к ответственности должностного лица или компетентного органа за нарушение права на доступ к информации, включая экологическую, на основании данных такой «переписки», облеченных в документированную форму.

В заключение отметим, что обозначенный способ оптимизации имеющихся способов и средств обеспечения права личности на доступ к экологической информации являет собой структуру идеи автора, однако для ее развития и перспективности применения на практике требуется более детальное научное осмысление с привлечением данных иных отраслей знания, в том числе, технического профиля.

Шумилин С.Ф.

ИСПОЛЬЗОВАНИЕ СИСТЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ В РОССИЙСКОМ УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ГЕНЕЗИС И ПЕРСПЕКТИВЫ

Аннотация. В статье рассматриваются вопросы генезиса использования систем видеоконференц-связи в российском уголовном судопроизводстве и перспективы расширения сферы её использования, обусловленные международно-правовыми обязательствами Российской Федерации.

Ключевые слова: уголовное судопроизводство, видеоконференц-связь, генезис, международно-правовые договоры РФ, перспективы использования.

Abstract. The article examines the genesis of videoconferencing systems in the Russian criminal proceedings and the prospects of expanding the scope of its use due to international obligations of the Russian Federation.

Key words: criminal justice, video conferencing, genesis, international treaties of the Russian Federation, prospects.

Истории российского уголовного судопроизводства известно немало случаев, когда применение научно-технических средств, являясь средством достижения целей уголовно-процессуальной деятельности следователей, следователей и судей, детерминирует совершенствование уголовно-процессуального законодательства. Одним из таких случаев как раз и является использование систем видеоконференц-связи при рассмотрении судами уголовных дел и вопросов, возникающих в стадии исполнения приговора.

Как известно, термин «системы видеоконференц-связи» впервые появился в ч.3 ст.376 Уголовно-процессуального кодекса Российской Федерации 2001 года (далее – УПК РФ), однако использование систем видеоконференц-связи началось ещё в 1999 году. Причиной послужила проблема обеспечения участия осуждённых, содержащихся под стражей, в заседаниях судов кассационной инстанции. В соответствии с ч.2 ст.335 действовавшего в то время УПК РСФСР 1960 года решение об участии осуждённых, содержащихся под стражей, в заседаниях судов кассационной инстанции принимал суд. При этом суды нередко отказывали в удовлетворении ходатайств осуждённых, содержащихся под стражей, о допуске к участию в рассмотрении уголовных дел в кассационном порядке. В частности, как писала в 2000 году группа авторов, в том числе и председатель Челябинского областного суда Ф. Вяткин, «за несколько лет до 1999 года мы не можем привести ни одного случая доставки подсудимых[1] на заседания судебной коллегии по уголовным делам»[2].

В конечном итоге это стало предметом рассмотрения в Конституционном Суде РФ, по результатам которого было признано не соответствующим Конституции РФ закреплённое в ч.2 ст.335 УПК РСФСР положение, согласно кото-

[1] Очевидно, в данном случае допущена ошибка, и речь должна идти об осуждённых, содержащихся под стражей.

[2] Вяткин Ф., Зильберман С., Зайцев С. Видеоконференцсвязь при рассмотрении кассационных жалоб // Российская юстиция. 2000. №6. С.11.

рому вопрос об участии осуждённого в заседании суда, рассматривающего дело в кассационном порядке, разрешается этим судом, «в той мере, в какой оно позволяет суду кассационной инстанции в случае, если он отклоняет ходатайство осуждённого, содержащегося под стражей, о рассмотрении дела с его участием, принимать окончательное решение по делу, не предоставив такому осуждённому возможности ознакомиться с материалами судебного заседания и изложить свою позицию по рассмотренным судом вопросам»[1].

Выход из создавшегося положения был найден – использовать при рассмотрении уголовных дел судами кассационной инстанции систем видеоконференц-связи. Разработка и реализация проекта использования систем видеоконференц-связи в ходе рассмотрения уголовных дел в кассационном порядке осуществлялась в Челябинском областном суде. Первым результатом проведённой работы, и как утверждают М.А. Сильнов и А.С. Герман, первым не только в истории российского уголовного судопроизводства, но и в мировой практике[2], было заседание судебной коллегии по уголовным делам Челябинского областного суда, которое состоялось 18 ноября 1999 года.

Пилотный проект по внедрению технологии видеоконференцсвязи при рассмотрении уголовных дел в кассационном порядке осуществлялся также в Верховном Суде РФ, Хабаровском краевом суде, Московском городском суде и др. Опыт использования систем видеоконференц-связи в названных и других судах России, нашёл своё отражение в постановлении Совета Судей РФ от 16.11.2001 № 65 «Об информатизации и автоматизации судов». В названном постановлении региональным судам рекомендовалось использовать накопленный опыт использования систем видеоконференц-связи и руководствоваться при оснащении судов такими системами едиными техническими требованиями к аппаратно-программным комплексам видеоконференц-связи для дистанционного проведения кассационных судебных заседаний[3].

Правовая основа для использования систем видеоконференц-связи в российском уголовном судопроизводстве начала формироваться с принятием и введением в действие УПК РФ. В первоначальной редакции УПК РФ использование систем видеоконференц-связи предусматривалось лишь в суде кассационной инстанции: в ч.3 ст.376 УПК РФ, регламентирующей порядок назначения судебного заседания в суде кассационной инстанции, была закреплена норма, согласно которой «осуждённый, содержащийся под стражей и заявивший о своём желании присутствовать при рассмотрении жалобы или представления на приговор, вправе участвовать в судебном заседании непосредственно либо изложить свою позицию путём использования систем видеоконференц-связи».

---

[1] По делу о проверке конституционности части второй статьи 335 Уголовно-процессуального кодекса РСФСР в связи с жалобой гражданина М.А. Баронина: Постановление Конституционного Суда РФ от 10.12.1998 №27-П // Собрание законодательства РФ. 1998. №51. Ст.6341.

[2] Сильном М.А., Герман А.С. Практика применения видеоконференц-связи в уголовном процессе // Уголовный процесс. 2012. №9. С.57.

[3] Российская юстиция. 2002. №3.

По мере накопления практики использования систем видеоконференц-связи в УПК был внесён ряд изменений и дополнений.

Так, Федеральным законом от 29.11.2010 №323-ФЗ были внесены следующие изменения и дополнения:

– закреплённое в ч.3 ст.376 УПК положение было дополнено указанием на лицо, в отношении которого велось или ведётся производство о применении принудительной меры медицинского характера, в предмет рассмотрения суда кассационной инстанции было включено наряду с приговором постановление;

– часть вторая статьи 407 УПК была дополнена нормой, предусматривающей использование систем видеоконференц-связи при рассмотрении уголовных дел судом надзорной инстанции[1].

С 1 января 2013 г. указанные выше нормы утратили силу в связи с вступлением в силу Федерального закона от 29 декабря 2010 г. №433-ФЗ, согласно которому использование систем видеоконференц-связи предусматривается при рассмотрении апелляционных и кассационных жалоб и представлений (ч.2 ст.389[12] ч.2 ст.401[13] УПК РФ)[2].

Федеральным законом от 20 марта 2011 г. №40-ФЗ статья 240 УПК РФ была дополнена частью четвертой, согласно которой «Свидетель и потерпевший могут быть допрошены судом путём использования систем видеоконференц-связи» (ч.4) и, соответственно, УПК дополнен статьей 278[1], устанавливающей особенности допроса свидетеля путём использования систем видеоконференц-связи. Этим же федеральным законом статья 399 УПК РФ дополнена положением, согласно которому с использованием систем видеоконференц-связи могут проводиться судебные заседания по рассмотрению вопросов, возникающих в стадии исполнения приговора[3].

Приведенный генезис использования видеоконференц-связи в уголовном судопроизводстве, разумеется, не мог остаться незамеченным в юридической науке, что подтверждается высказанными в литературе, с одной стороны, критическими замечаниями по поводу возможности использования систем видеоконференцсвязи, а с другой, предложениями относительно расширения сферы её применения[4].

---

[1] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 29.11.2010 №323-ФЗ // Собрание законодательства РФ. 2010. №49. Ст.6419.

[2] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации: Федеральный закон от 29.12.2010 №433-ФЗ // Собрание законодательства РФ. 2011. №1. Ст.45.

[3] О внесении изменений в статью 399 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 20.03.2011 №40-ФЗ // Собрание законодательства РФ. 2011. №13. Ст.1687.

[4] Волеводз А.Г. Правовое регулирование новых направлений международного сотрудничества в сфере уголовного процесса. М.: Юрлитинформ, 2002. С.390-428; Терехин В.А., Федюнин А.Е. Видеоконференцсвязь в современном российском судопроизводстве // Российская юстиция. 2006. №1. С.22-24; Соколов Ю.Н. Информационные технологии в кассационном порядке рассмотрения уголовных дел // Российский судья. 2008. №8. С.22-23; Архипова Е.А. Применение видеоконференцсвязи в уголовном судопроизводстве России и

Объем и спектр высказанных суждений даёт основание для вывода о том, что проблемы использования систем видеоконференцсвязи в уголовном судопроизводстве нуждаются в самостоятельном исследовании, которое не может быть осуществлено в рамках настоящей статьи. Вместе с тем, представляется уместным высказать некоторые соображения относительно перспективы дальнейшего использования систем видеоконференц-связи в уголовном судопроизводстве. Прежде всего, это относится к вопросу использования систем видеоконференц-связи в досудебном производстве и в рамках международного сотрудничества в сфере уголовного судопроизводства.

На наш взгляд, актуальность этого вопроса обусловлена тем, что Россия является участницей ряда международных соглашений, исполнение которых предполагает расширение сферы использования видеоконференц-связи, как в национальном уголовном судопроизводстве, так и в сфере оказания международно-правовой помощи по уголовным делам.

Прежде всего, следует отметить, что Россия является одной из договаривающихся сторон в Рекомендациях группы старших экспертов «восьмёрки» от 12 апреля 1996 года. В п.15 данного международно-правового документа сформулировано положение, согласно которому в целях эффективной борьбы с международной организованной преступностью «государства должны предусмотреть возможность принятия соответствующих мер по обеспечению защиты свидетелей в ходе расследования уголовных дел» и «должны включать такие методы, как дача показаний по техническим каналам связи или ограничение разглашения сведений об адресе и установочных данных свидетелей». Здесь же рекомендуется «изучить возможность применения современных технологий, таких как видеосвязь для преодоления имеющихся в настоящее время трудностей с получением показаний от свидетелей, находящихся за пределами государств, проводящих расследование»[1]. До настоящего времени в России выполнена лишь одна рекомендация – об ограничении разглашения сведений (ч.3 ст.11, ч.6 ст.166, ч.8 ст.193, п.4 ч.2 ст.241 и ч.5 ст.278 УПК РФ). Вопрос о реализации остальной части приведённой рекомендации остаётся открытым.

Определённые обязательства в части использования систем видеоконференцсвязи вытекают из п.17 Приложения к Рекомендации № R (2005) Комитета

зарубежных стран // Вестник Академии Генеральной прокуратуры Российской Федерации. 2011. №5 (25). С.45-49; Иванов В.В. Использование систем видеоконференцсвязи в современном уголовном процессе // Уголовное судопроизводство. 2011. №3. С.25-27; Желтобрюхов С.П. Допрос свидетеля (потерпевшего) путём использования систем видеоконференц-связи // Российская юстиция. 2011. №8. С.43-44; Сумин С.А. Применение систем видеоконференц-связи при допросе защищаемых территориально удалённых лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности // Вестник Воронежского института МВД России. 2011. №3. С.68-74; Шиплюк В.А. Использование видеоконференцсвязи при осуществлении правовой помощи по уголовным делам // КриминалистЪ. 2012. №1 (10). С.56-60; и др.

[1] СПС «КонсультантПлюс: Международные правовые акты».

Министров Совета Европы[1], в котором сформулировано следующее положение: «при обеспечении сторонам адекватных возможностей оспаривать показания, данные свидетелем/лицом, сотрудничающим с правосудием, необходимо рассмотреть следующие, inter alia, меры, направленные на предотвращение идентификации свидетеля ... использование видеоконференций». Согласно п.32 указанного Приложения в сфере международного сотрудничества предлагается рассмотреть «более широкое и эффективное использование современных средств телекоммуникации, например, видеосвязи, и повышение их безопасности, при соблюдении прав сторон»[2].

Из положения, закреплённого в п.17 Приложения вытекает вопрос о разграничении свидетелей и лиц, сотрудничающих с правосудием, и таким образом, назревает решение проблемы допроса последних как в досудебном производстве, так и судебных стадиях уголовного судопроизводства.

Возможность проведения слушания с помощью средств видеосвязи, если личное присутствие соответствующего лица на территории запрашивающего государства невозможно или нежелательно, предусматривается Конвенций против транснациональной организованной преступности (ст.18)[3], Конвенцией Организации Объединенных Наций против коррупции (п.18 ст.46)[4].

Особо следует отметить закреплённое в Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, заключённой в г. Кишинёве 7 октября 2002 года положение, в соответствии с которым «договаривающиеся стороны оказывают взаимную правовую помощь путём ... *предъявления для опознания, в том числе с использованием видеосвязи* (выделено мною – С.Ш.), видеозаписи и иных технических средств» (ст.6)[5]. Конвенция не вступила в силу для Россией на 07.12.2012, однако это не дезавуирует необходимость проведения работы по приведению российского уголовно-процессуального законодательства в соответствии с вышеназванным и другими закреплёнными в ней положениями.

---

[1] Россия вступила в Совет Европы 28 февраля 1996 года. См.: Федеральный закон от 23.02.1996 №19-ФЗ «О присоединении Российской Федерации к Уставу Совета Европы» // Собрание законодательства РФ. 1996. №9. Ст.774.

[2] Рекомендация № R (2005) Комитета Министров Совета Европы государствам-членам о защите свидетелей и лиц, сотрудничающих с правосудием (20 апреля 2005 года) // СПС «КонсультантПлюс».

[3] Конвенция против транснациональной организованной преступности (Принята в г. Нью-Йорке 15.11.2000). Конвенция вступила в силу для России 25.06.2004 // Собрание законодательства РФ. 2004. №40. Ст.3882.

[4] Конвенция Организации Объединённых Наций против коррупции (Принята в г. Нью-Йорке 31.10.2003). Ратифицирована 08.03.2006 // Собрание законодательства РФ. 2006. №26. Ст.2780; №12. Ст.1231.

[5] Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. №2 (41). С.82-130.

СВЕДЕНИЯ ОБ АВТОРАХ

Авдеева Галина Константиновна – кандидат юридических наук, старший научный сотрудник, доцент Национального университета «Юридическая академия Украины имени Ярослава Мудрого»

Авершин Станислав Олегович – студент III курса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Андреев Юрий Николаевич – доктор юридических наук, проф. Центрального (г. Воронеж) филиала Российской академии правосудия судья, Воронежский областной суд

Архипцев Иванович Николай – кандидат юридических наук, доцент кафедры уголовного права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Бакирова Елена Юрьевна – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Батова Ольга Владимировна – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Белецкая Анастасия Анатольевна – ассистент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Белоус Василий Васильевич – кандидат юридических наук, доцент кафедры криминалистики Национального университета «Юридическая академия Украины имени Ярослава Мудрого»

Белоус Ольга Петровна – соискатель Научно-исследовательского института изучения проблем преступности Национальной академии правовых наук Украины имени академика В.В.Сташиса

Винокуров Эдуард Александрович – кандидат юридических наук, старший преподаватель кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Давидова Юлия Анатольевна – магистрант кафедры гражданского права и процесса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Демко Ольга Сергеевна – кандидат социологических наук, старший преподаватель кафедры уголовного права и процесса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Долженко Наталья Игоревна – кандидат юридических наук, доцент кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Дрога Андрей Анатольевич – преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородский юридический институт МВД России

Жилина Наталья Юрьевна – кандидат юридических наук, доцент кафедры уголовного права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Евтушенко Иван Владимирович – аспирант Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Звертаева Юлия Юрьевна – Белгородская областная Дума, начальник отдела юридической экспертизы правового управления аппарата Белгородской областной Думы

Зюлин Михаил Алексеевич – судья Белгородского областного суда; аспирант кафедры конституционного и муниципального права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Ищенко Евгений Петрович – заведующий кафедрой криминалистики Московской государственной юридической академии имени О.Е. Кутафина, доктор юридических наук, профессор.

Карачевцева Ольга Сергеевна – аспирантка Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Каторгина Наталья Петровна – ассистент кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Кислицина Ирина Николаевна – старший преподаватель кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Ковылов Владимирович Андрей – аспирант Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Комаров Игорь Михайлович – доктор юридических наук, профессор, заведующий кафедрой судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Косолапова Наталья Александровна – аспирантка Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Костин Алексей Александрович – кандидат экономических наук, доцент Белгородского университета кооперации, экономики и права

Костина Ольга Владимировна – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Коцюмбас Сергей Михайлович – судья Белгородского областного суда, старший преподаватель кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Куксин Иван Николаевич – заслуженный юрист РФ, доктор юридических наук, профессор кафедры теории и истории государства и права Государственного бюджетного образовательного учреждения высшего профессионального образования «Московского городского педагогического университета»

Лагуточкин Андрей Владимирович – кандидат юридических наук, старший преподаватель кафедры оперативно-разыскной деятельности БелЮИ России

Левченко Вячеслав Евгеньевич – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Лиликова Оксана Сергеевна – кандидат юридических наук, доцент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Ляхова Анжелика Ивановна – кандидат юридических наук, старший преподаватель кафедры уголовного права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Мамин Андрей Сергеевич – кандидат юридических наук, доцент кафедры административного и международного права юридического института НИУ «БелГУ»

Москаленко Станислав Александрович – аспирант кафедры конституционного и муниципального права Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»).

Митякина Надежда Михайловна – кандидат юридических наук, доцент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Мишакин Александр Васильевич – магистрант Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Насонова Валентина Афанасьевна – кандидат физико-математических наук, доцент кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права

Никонова Людмила Ивановна – кандидат юридических наук, доцент кафедры теории и истории государства и права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Новикова Алевтина Евгеньевна – кандидат юридических наук, доцент кафедры конституционного и муниципального права Юридического института НИУ «БелГУ»

Остапюк Владимир Григорьевич – кандидат юридических наук, заведующий кафедрой административного и международного права юридического института НИУ «БелГУ»

Олейник Николай Николаевич – доктор исторических наук, профессор Белгородского государственного исследовательского университета (НИУ «БелГУ»)

Олейник Александр Николаевич – кандидат юридических наук, доцент Харьковского национальногопедагогического университета имени Г.С. Сковороды

Петрова Наталья Александровна – аспирантка Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Пожарова Любовь Анатольевна – аспирантка кафедры теории и истории государства и права Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Пономаренко Оксана Михайловна – кандидат юридических наук, доцент, докторант кафедры гражданско-правовых дисциплин, хозяйственного и трудового права Харьковского национального педагогического университета имени Г.С. Сковороды

Пономаренко Юрий Анатольевич – кандидат юридических наук, доцент кафедры уголовного права Национального университета «Юридическая академия Украины имени Ярослава Мудрого»

Прокопенко Алексей Николаевич – начальник кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат технических наук, доцент, Белгородский юридический институт МВД России

Прохорова Мария Владимировна – студентка V курса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Родионова Марина Юрьевна – студентка V курса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Свинарь Андрей Любомирович – студент IV курса Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Семенов Роман Исрафилович – ассистент кафедры конституционного и муниципального права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Синенко Владимир Сергеевич – кандидат юридических наук, доцент, заведующий кафедрой трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Скворцова Татьяна Вячеславовна – ассистент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Степанюк Андрей Вячеславович – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Степанюк Оксана Сергеевна – кандидат юридических наук, доцент, зав. кафедры уголовного права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Табунщиков Андрей Тихонович – кандидат юридических наук, доцент кафедры гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Тонков Евгений Евгеньевич – доктор юридических наук, профессор, директор Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Трубников Василий Михайлович – профессор, доктор юридических наук, зав. кафедрой уголовно-правовых наук юридического факультета Харьковского национального университета имени В.Н. Каразина

Туранин Владислав Юрьевич – кандидат юридических наук, доцент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Тычинин Сергей Владимирович – доктор юридических наук, профессор, заведующий кафедрой гражданского права и процесса Белгородского государственного национального исследовательского университета (НИУ «БелГУ»).

Федорященко Алексей Сергеевич – кандидат юридических наук, доцент кафедры трудового и предпринимательского права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Чалых Ирина Сергеевна – кандидат юридических наук, старший преподаватель кафедры конституционного и муниципального права Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Шапошник Елена Ивановна – кандидат биологических наук, старший преподаватель кафедры судебной экспертизы и криминалистики Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Шафорост Татьяна Леонидовна – магистрант Юридического института Белгородского государственного национального исследовательского университета (НИУ «БелГУ»)

Шумилин Сергей Федорович – доктор юридических наук, доцент профессор кафедры уголовного права и процесса НИУ «БелГУ»

Научное издание

ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-РЕСУРСОВ И ПРАВОВОГО РАЗРЕШЕНИЯ КОНФЛИКТОВ С УЧАСТИЕМ СУБЪЕКТОВ ИНТЕРНЕТ-СООБЩЕСТВА

Материалы международной научно-практической конференции, посвященной 20-летию Юридического института НИУ «БелГУ» в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апреля 2013 г.

В авторской редакции
Компьютерная верстка *Н.А. Гапоненко*

Подписано в печать 16.04.2013. Формат 60×84/16.
Гарнитура Times, Georgia. Усл. п. л. 16,04. Тираж 80 экз. Заказ 158.
Оригинал-макет подготовлен и тиражирован в ИД «Белгород» НИУ «БелГУ»
308015, г. Белгород, ул. Победы, 85