ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(10) / 2013

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Свидетельство **ПИ № ФС77-44941** от 05.05.2011

Издатель: ООО «Южно-Уральский юридический вестник»

Адрес редакции: Россия, 454080, г. Челябинск, пр. Ленина, д. 76.

Тел./факс: (351) 267-90-65, 267-97-01.

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: urvest@mail.ru**

ПОДГОТОВКА СПЕЦИАЛИСТОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОТЗЫВЫ

ПРАКТИЧЕСКИЙ АСПЕКТ

SPECIALIST TRAINING IN THE FIELD OF INFORMATION SECURITY

TECHNICAL INFORMATION SECURITY

LEGAL REGULATION OF INFORMATION SECURITY

REVIEWS

THE PRACTICAL ASPECT

УДК 004.056 + 378.016 : 004.056
ББК Х 401.114 + Ч 448.44

Ю. В. Гараева

КОГНИТИВНЫЙ КОМПОНЕНТ ИНФОРМАЦИОННОЙ КОМПЕТЕНЦИИ БУДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ

Статья посвящена актуальным сегодня вопросам подготовки специалистов в сфере информационной безопасности. В статье на основе анализа литературы о развитии информационной компетенции будущего инженера в вузе, а также выявленной специфики информационной составляющей профессиональной деятельности специалиста по защите информации, обоснован когнитивный компонент его информационной компетенции. Установлено, что данный компонент занимает ключевое место в общей структуре информационной компетенции. Сформулировано определение когнитивно-информационной компетенции специалиста по защите информации. Под ней автор понимает его способность как отправителя и получателя информации осуществлять когнитивные операции информационной деятельности (объективизацию знания, субъективизацию информации и проецирование субъективированной информации на конкретные ситуации) с информационными объектами защиты и субъектами информационных отношений с целью реализации его профессиональных информационных потребностей, направленных на защищенное развитие этих объектов и субъектов. В работе ставится проблема развития когнитивно-информационной компетенции специалиста по защите информации в вузе в условиях перехода на уровневую систему образования.

Ключевые слова: *информационная компетенция, защита информации, когнитивный компонент, специалист.*

Y. V. Garaeva

COGNITIVE COMPONENT OF INFORMATION COMPETENCIES FUTURE INFORMATION SECURITY SPECIALIST

The article is devoted today to training specialists in the field of information security. On the basis of analysis of the literature on the development of information competence future engineer at the university , as well as identifying the specifics of the information component of the professional activities for the protection of information , justified the cognitive component of its

information competence. Found that this component is a key element in the overall information competence . The definition of cognitive information competence of information security specialists . Under it, the author understands his ability as a sender and receiver of information to carry out cognitive operations information activities (objectification of knowledge, information and subjeprojection of the subjective information on the specific situation) to protect the information objects and subjects of information relations in order to implement its professional information needs, aimed at the development of a secure these objects and subjects. The paper poses the problem of the development of cognitive information competence of information security specialists at the university in the transition to tiered system of education.

Keywords: *informational competence, data protection, cognitive component specialist.*

Ускоренные темпы научно-технического и информационного развития России требуют от вузов решения проблемы подготовки технических специалистов, способных решать профессиональные задачи, которые становятся информационно-насыщенными, а потому требуют от специалиста высокого уровня информационной компетенции. Особые требования предъявляются к специалисту по защите информации, призванному решать на практике специфические информоемкие проблемы.

Информационная компетенция будущего инженера, к каковым относится и специалист по защите информации, не раз становилась объектом педагогических исследований. Так, М. Ю. Валеев определяет профессиональную информационную компетентность, в состав которой входит умение программировать на языках высокого уровня, как центральный системообразующий фактор в организации всего учебного процесса[4]. С. В. Савельева уточняет сущность понятия «информационная компетентность будущих инженеров» посредством включения личностного (направленность на развитие личностного качества) и информационного (инженерная деятельность как информационный процесс) аспектов, обосновывает структуру информационной компетентности будущих инженеров как совокупность взаимосвязанных компонентов: мотивационного, операционального, результативно-рефлексивного. На основе системного, информационного, компетентностного и деятельностного подходов ученым разработана модель формирования информационной компетентности будущих инженеров в вузе, учитывающая функции и особенности инженерной деятельности, включающей взаимосвязанные блоки: целевой, содержательный, функционально-организационный, оценочный[9]. По мнению М. И. Глотовой, информационная компетентность будущего инженера является интегративным качеством личности, которое трактуется ею как готовность студента к активному использованию профессионально-ориентированных информационных технологий в измерениях информационного производственного процесса будущей сферы деятельности (создания стоимости, создания отношений, принятия решений) и смежных областей. Структурно она рассматривается как синтез когнитивного, технологического и ценностного компонентов[5]. Е. В. Панюкова считает, что информационная профессиональная компетентность – это интегральное свойство личности, характеризующее его стремление и готовность реализовать свой потенциал (знания, умения, опыт, личностные качества) в области информационных технологий для успешной творческой профессиональной деятельности, иметь устойчивую мотивацию к самообразованию в области информационных технологий, а также готовность к осознанию социальной значимости и личной ответственности за результаты своей информационной деятельности. Для каждого из блоков определены признаки, позволяющие формировать и диагностировать ИК[8].

К сожалению, названные определения информационной компетенции не отражают специфики информационной деятельности будущего инженера. Такую попытку делает Е. А. Крайнова, выявившая особенности профессиональной деятельности инженеров-механиков в области информационных технологий, заключающиеся в автоматизированной обработке данных, автоматизации управления производством, предприятием, автоматизированном проектировании, моделировании, разработке оптимальных технологий изготовления деталей машин, использовании информационных технологий для рас-

четов параметров технологических процессов. Однако в структуре информационной компетенции эти особенности никак не отражены[7].

А. В. Тараканов определяет тенденции в развитии инженерной деятельности в условиях информационного общества, которые должны быть приняты во внимание при определении содержания образования инженера в области информационных технологий: резкое усложнение социотехнических и системотехнических задач; гуманитаризация инженерной деятельности; широкое использование ИКТ в инженерной практике; востребованность инженера, способного к непрерывному профессиональному самообразованию. Учитывая эти особенности, он конкретизирует понятие «информационная культура инженера» как неразрывное единство таких компонентов, как: когнитивный, функциональный, коммуникативный, ценностно-рефлексивный, этический, психологический, эмоционально-эстетический[10].

Заслуживает также внимания обоснованный С. В. Савельевой комплекс педагогических условий, основывающийся на специфических структурных компонентах информационного процесса в инженерной деятельности и включающий: а) построение учебного материала на основе интеграции звуковой, текстовой, графической и видеоинформации; б) применение алгоритмических конструктов, активизирующих самостоятельную учебно-познавательную деятельность; в) усиление информационно-профессиональной подготовки будущих инженеров включением в образовательный процесс профессионально ориентированных задач[9]. Полагаем, что интеграция звуковой, текстовой, графической и видеоинформации, а также активное использование алгоритмических конструктов присутствуют в деятельности специалиста по защите информации, как и в деятельности любого инженера. Однако понятие его информационной компетенции имеет особенности.

В процессе нашего исследования воспользуемся определением информационной компетенции специалиста, обоснованным Л. В. Астаховой: «это способность специалиста осуществлять познавательные и коммуникационные операции информационной деятельности с целью реализации его общих и профессиональных информационных потребностей не только как отправителя информации (сообщение другим субъектам о познанном и пережитом; управление поведением других субъектов), но и как ее получателя (получение новых знаний, эмоциональных импульсов, советов или указаний; управление собственным поведением в процессе управления другими субъектами)[2].

Не умаляя коммуникативного компонента в информационной компетенции специалиста по защите информации, остановим наше внимание на ее когнитивном компоненте. Это обусловлено тем, что познание и анализ информации – это сущностная общепрофессиональная компетенция специалиста по защите информации. Без нее невозможно организовать и управлять системой защиты информации на объекте. Аналитическая работа является неотъемлемой составной частью всей работы специалиста по защите информации по предупреждению утечки защищаемой информации. С целью детального и всестороннего исследования особенностей, условий и обстоятельств прохождения, обращения, использования и надежности обеспечения сохранности всех видов защищаемой информации, а также выявления и устранения всех возможностей ее утечки специалист по защите информации проводит различные виды аналитических исследований: связанные с составлением и уточнением перечня сведений, подлежащих защите; в целях принятия решения о необходимости разработки и внедрения дополнительных режимных мероприятий перед началом новых работ или в связи с изменением оперативной обстановки; исследования фактической эффективности и надежности мер по защите сведений, отнесенных к тому или иному виду тайн, при проведении конкретных работ со сведениями, составляющими тот или иной вид тайны, по конкретной теме НИОКР, проблеме, заказу, конкретному проекту и т. п.; исследования тех сторон деятельности предприятия, которые имеют существенное значение для обеспеченности сохранности защищаемых сведений (анализ открытых публикаций, транспортировки спецпродукции, приема командированных лиц, осуществления международных связей и т. д.)[6].

Аналитической работой по выявлению и предупреждению возможной утечки охраняемой в интересах государства информации начали заниматься еще в Советском Союзе в первой половине 60-х годов. С начала 90-х годов, т. е. с периода вступления России в ры-

ночную экономику, в конкурентную среду, информационно-аналитические подразделения стали создаваться на частных предприятиях. Информационно-аналитическое обеспечение безопасности организации предназначено для выявления угроз и минимизации рисков. Экономическое благополучие предприятия во многом обеспечивается хорошо организованной системой сбора деловой информации, ее своевременной обработкой и распределением. Мы согласны с учеными в том, что просчеты в деятельности организаций часто связаны не с отсутствием информации, необходимой для принятия решений, а с тем, что она была неверно интерпретирована и не доведена вовремя до сведения соответствующих лиц[6]. Это подчеркивает приоритетность когнитивного компонента в информационной компетенции специалиста по защите информации. На увеличение когнитивной составляющей в деятельности специалиста по защите информации указывалось также в контексте усиления опасности угроз информационно-психологической безопасности[1], в связи с реализацией его управленческих функций[3] и др.

Сущность понятия информационной компетенции на основе когнитивного подхода с использованием философской концепции соотношения информации и знания и концепции ситуационного подхода также обосновала Л. В. Астахова. По ее мнению, «информационная компетенция специалиста с точки зрения когнитивного подхода – это его способность осуществлять непрерывный процесс объективизации знания, субъективизации информации, а также проецирования субъективированной информации на личные обстоятельства в рамках различных профессиональных ситуаций с целью адаптации к ним»[2].

Познание информации, извлечение и интерпретация смыслов первичных и вторичных информационных сообщений о защищаемой информации и ее носителях, об угрозах их безопасности; анализ и структурирование этих смыслов, принятие решений об их адекватном использовании для защиты объектов; мониторинг информации о состоянии защищенности объектов согласно требованиям технической документации – вот те когнитивные операции, которые специалист по защите информации осуществляет на всех этапах жизненного цикла своей деятельности.

Особенности информационно-когнитивной деятельности специалиста по защите информации заключены в следующем:

• информация выступает для него не только средством, но и объектом и предметом деятельности;

• информационные потребности этого специалиста связаны не только с защитой информации, но и с защитой пользователей этой информации;

• он связан в своей деятельности с большими объемами генерируемой первичной информации;

• ключевым видом информации для него является техническая информация и т. д.

Взяв за основу трактовку понятий информационной компетенции специалиста и информационной компетенции специалиста с позиций когнитивного подхода[2], а также особенности информационного содержания деятельности специалиста по защите информации, сформулируем определение его информационно-когнитивной компетенции. Информационно-когнитивная профессиональная компетенция специалиста по защите информации – это его способность как отправителя и получателя информации осуществлять когнитивные операции информационной деятельности (объективизацию знания, субъективизацию информации и проецирование субъективированной информации на конкретные ситуации) с информационными объектами защиты и субъектами информационных отношений с целью реализации его профессиональных информационных потребностей, направленных на защищенное развитие этих объектов и субъектов.

Развитие информационной компетенции будущих специалистов по защите информации в вузе в обозначенных в определении границах будет способствовать повышению качества их подготовки в условиях перехода на уровневую систему образования, а также стремительного информационного развития общества и усиления опасности информационных угроз.

Литература

[1] Астахова Л. В. Информационно-психологическая безопасность в регионе: культурологический аспект // Вестн. УрФО. Безопасность в информационной сфере. 2011. № 2. С. 40–47.

[2] Астахова Л. В. Понятие информационной компетенции: когнитивный подход // Вестн. ЮУрГУ. Сер. Образование. Педагогические науки. 2013. Т. 5. № 4. С. 10–16.

[3] Астахова Л. В. Развитие управленческой компетенции будущего специалиста по защите информации в вузе // Современные проблемы науки и образования. 2012. № 6. С. 330.

[4] Валеев М. Ю. Проектирование системы непрерывной информационной подготовки инженеров для наукоемких производств на примере специальности «Автоматизированные системы обработки информации и управления»: дис… канд. пед. наук. Казань, 2002. 173 с.

[5] Глотова М. И. Самостоятельная работа будущих инженеров как фактор развития информационной компетентности : дис…канд. пед наук. Оренбург, 2007. 259 с.

[6] Информационная безопасность региона: традиции и инновации : монография / под науч. ред. Л. В. Астаховой. Челябинск, 2009. С. 199–205.

[7] Крайнова Е. А. Профессиональная подготовка будущих инженеров-механиков в области информационных технологий : дис… канд. пед. наук. Нижний Новгород, 2007. 206 с.

[8] Панюкова Е. В. Проектирование содержания и технологии формирования информационной компетентности студентов инженерного профиля на примере специальности 150201 «Машины и технология обработки металлов давлением» : дис… канд. пед. наук. Тольятти, 2006. 204 с.

[9] Савельева С. В. Формирование информационной компетентности будущих инженеров в вузе: дис… канд. пед. наук. Челябинск, 2010. 187 с.

[10] Тараканов А. В. Развитие содержания профессиональной подготовки инженера в области информационных технологий : дисс… канд. пед. наук. М., 2007. 144 с.

References

[1] Astahova L.V. Informacionno-psihologicheskaja bezopasnost' v regione: kul'turologicheskij aspekt [Information and psychological security in regions: Cultural aspect] // Vestnik UrFO. Bezopasnost' v informacionnoj sfere [Bulletin of the Ural Federal Region. Information Security]. 2011. No. 2. p. 40-47.

[2] Astahova L. V. Ponjatie informacionnoj kompetencii: kognitivnyj podhod [The notion of the information competency: Cognitive approach] // Vestn. JuUrGU. Ser. Obrazovanie. Pedagogicheskie nauki [Bulletin of the South Ural State University. Series 'Education. Pedagogical Sciences]. 2013. V. 5. No. 4. p. 10-16.

[3] Astahova L.V. Razvitie upravlencheskoj kompetencii budushhego specialista po zashhite informacii v vuze [Development of administrative competency of the suture specialist in the field of information security] // Sovremennye problemy nauki i obrazovanija [Modern problems of science and education]. 2012. No. 6. p. 330.

[4] Valeev M.Ju. Proektirovanie sistemy nepreryvnoj informacionnoj podgotovki inzhenerov dlja naukoemkih proizvodstv na primere special'nosti «Avtomatizirovannye sistemy obrabotki informacii i upravlenija»: diss… kand. ped. nauk [Projecting of the system of continuous information training of engineers for science-intensive plants and factories on the example of the field of study 'Automated systems of data processing and control: Thesis of Cand. Sc. Pedagogics]. Kazan, 2002. 173 p.

[5] Glotova M.I. Samostojatel'naja rabota budushhih inzhenerov kak faktor razvitija informacionnoj kompetentnosti: diss…kand. ped nauk [Independent work of the future engineers as a factor of development of information competency: Thesis of Cand. Sc. Pedagogics]. Orenburg, 2007. 259 p.

[6] Informacionnaja bezopasnost' regiona: tradicii i innovacii : monografija [Information security of regions: Traditions and innovations: Monograph]; pod nauch. red. L.V. Astahovoj. Chelyabinsk, 2009. p.199-205.

[7] Krajnova E.A. Professional'naja podgotovka budushhih inzhenerov-mehanikov v oblasti informacionnyh tehnologij: diss…kand. ped. nauk [Professional training of future engineers and mechanics in the field of information technologies: Thesis of Cand. Sc. Pedagogics]. Nizhnij Novgorod, 2007. 206 p.

[8] Panjukova E.V. Proektirovanie soderzhanija i tehnologii formirovanija informacionnoj kompetentnosti studentov inzhenernogo profilja na primere special'nosti 150201 «Mashiny i tehnologija obrabotki metallov davleniem» : diss…kand. ped. nauk [Projecting of the subject matter and technologies of formation of information competency of the students-engineers on the example of the field of study 150201 'Machines and technologies of pressure metal treatment': Thesis of Cand. Sc. Pedagogics]. Toliatti, 2006. 204 p.

[9] Savel'eva S.V. Formirovanie informacionnoj kompetentnosti budushhih inzhenerov v vuze: diss…kand. ped. nauk [Formation of informational competency of future engineers in higher educational institutions: Thesis of Cand. Sc. Pedagogics]. Cheljabinsk, 2010. 187 p.

[10] Tarakanov A.V. Razvitie soderzhanija professional'noj podgotovki inzhenera v oblasti informacionnyh tehnologij: diss… kand. ped. nauk [Development of the subject matter of professional training of engineers in the field of information technologies: Thesis of Cand. Sc. Pedagogics]. Moscow, 2007. 144 p.

Гараева Юлия Владимировна, аспирант кафедры «Безопасность информационных систем» ЮУрГУ. E-mail: garaevajv@gmail.com.

Garaeva Julia, graduate student «Security of Information Systems» SUSU. E-mail: garaevajv@gmail.com.

УДК 002 : 004.056.57 + 004.056.57
ББК Х 401.114

В. П. Гуляев

РАСЧЕТ МИНИМАЛЬНОГО УРОВНЯ МАСКИРОВКИ ШУМОВЫМ СИГНАЛОМ КОНФИДЕНЦИАЛЬНОЙ РЕЧЕВОЙ ИНФОРМАЦИИ

Статья посвящена актуальным сегодня вопросам технической защиты информации ограниченного доступа, в том числе конфиденциальной речевой информации. В статье рассматривается алгоритм для определения минимального уровня маскирующего шума, обеспечивающего необходимую защищенность помещений, в которых циркулирует конфиденциальная речевая информация, от средств технической разведки. Автором определяются условия, при которых акустический (вибрационный) канал утечки речевой информации считается защищенным от перехвата средствами технической разведки.

Ключевые слова: *акустический, вибрационный, коэффициент звукопроводности (вибропроводности), звукоизоляция (виброизоляция), уровень сигнала.*

V. P. Gulyaev

CALCULATION OF THE MINIMUM LEVEL OF MASKING NOISE SIGNAL OF VOICE INFORMATION CONFIDENTIAL

The article is devoted today technical protection of information with limited access, including voice information confidential. Describes an algorithm to determine the minimum level of masking noise to ensure the necessary protection of the premises in which the information circulates confidential speech from technical intelligence. The author defines the conditions under which an acoustic (vibrating) channel leakage of audio information is considered protected from interception by means of technical intelligence.

Keywords: *acoustic, vibration, zvukoprovodnosti (vibroprovodnosti), sound (vibration isolation), signal level.*

Оценка возможности перехвата конфиденциальной речевой информации, циркулирующей в защищаемых помещениях, средствами технической разведки по акустическому и вибрационному техническим каналам утечки осуществляется по методике, разработанной и утвержденной Федеральной службой технического и экспертного контроля (ФСТЭК) России («Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам». Утверждена Первым заместителем Председателя Гостехкомиссии (ФСТЭК) России 8 ноября 2001 г.).

Данная методика основана на проведении измерений коэффициентов звукоизоляции Q_i (коэффициентов акусто-виброизоляции G_i) в октавных полосах со среднегеометрическими значениями частот 250, 500, 1000, 2000, 4000 Гц (i – соответствующий номер октавной полосы). Измеренные значения Q_i (G_i) сравнивают с нормированными значениями Q_iH (G_iH). Если хотя бы одно из значений Q_i (G_i) будет меньше соответствующих нормированных значений, то данное разведнаправление считается опасным и необходимо проводить мероприятия по предотвращению возможности перехвата речевой информации технической разведкой. Наиболее оперативным и экономичным способом решения этой задачи является активная маскировка речевого сигнала низкочастотным отрезком белого шума. В методике указывается на возможность предотвращения перехвата речевой информации средствами технической разведки путем маскировки речевых сигналов, выходящих за границы контролируемой зоны, специально сформированным шумом. Однако не приводится алгоритм определения минимальнонеобходимого уровня интенсивности маскирующего шума.

Для определения минимально необходимого уровня интенсивности маскирующего шума рассмотрим структуру рис. 1, отображающую акустический (вибрационный) канал утечки речевой информации.

По методике [1] процедуры измерений и оценок по акустическому и вибрационному каналам утечки речевой информации одинаковы, поэтому ниже рассмотрен только акустический канал безотносительно к октавным полосам.

1. Маскирующий шум отсутствует ($M = 0$) и на выходе схемы рис. 1 действует аддитивная смесь выходного сигнала X с внешним (фоновым) шумом N – $Y = \sqrt{X^2 + N^2}$. Измерению шумомером подлежат логарифмические уровни:

• тестового сигнала $L_{Si} = 20\lg\frac{S}{P_0}$, где $P_0 = 2 \cdot 10^{-5}$ $Па$ – порог слышимости по акустическому давлению;

• аддитивной смеси выходного сигнала с внешним (фоновым) шумом $L_{Yi} = 20\lg\frac{Y_i}{P_0}$;

• внешнего шума $L_{Ni} = 20\lg\frac{N_i}{P_0}$, $i = \overline{1,5}$.

По результатам измерений определяют выходной сигнал X_i и его логарифмический уровень L_{Xi}:

$$X_i = \sqrt{Y_i^2 - N_i^2} = S_i \cdot K\ (f_i). \qquad (1)$$

$$L_{Xi} = 20\lg\frac{X_i}{P_0}. \qquad (2)$$

По полученным данным находят фактические октавные коэффициенты звукоизоляции

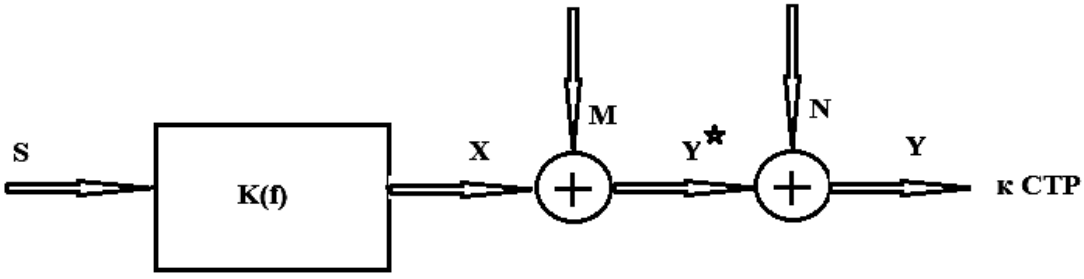


Рис. 1. Структурная схема перехвата сигнала СТР по акустическому (вибрационному) каналу:

S – тестовый акустический (вибрационный) сигнал; *Y** – аддитивная смесь выходного сигнала *X* с маскирующим шумом *M*; *Y* – аддитивная смесь выходного сигнала *X* с маскирующим шумом *M* и внешним шумом *N*; *K(f)* – коэффициент звукопроводности (акустовибропроводности) преграды в зависимости от частоты *f* тестового сигнала; *СТР* – средство технической разведки.

(виброизоляции) и сравнивают их с соответствующими нормированными коэффициентами по следующей процедуре:

$$\left\{Q_i\left(G_i\right) = L_{Si} - L_{Xi}\left(V_{Xi}\right)\right\}_{i=\overline{1,5}}, \qquad (3)$$

где V_{Xi} – логарифмический уровень вибрационного сигнала X_i.

Если хотя бы одно из $Q_i\left(G_i\right)$ будет меньше соответствующих $Q_{iн}\left(G_{iн}\right)$, то исследуемый канал требует проведения защитных мероприятий. Как указывалось выше, наиболее оперативным и экономичным способом решения этой задачи является активная маскировка речевого сигнала низкочастотным отрезком белого шума.

2. Рассмотрим случай, когда требования защищенности помещения не выполняются, то есть

$$Q_{iн}\left(G_{iн}\right) - Q_i\left(G_i\right) = \Delta Q_i\left(\Delta G_i\right), \qquad (4)$$

где $\Delta Q_i\left(\Delta G_i\right)$ – дефицит звукоизоляции (виброизоляции) в i - той октавной полосе частот. Задача активной маскировки заключается в задании такого минимального уровня маскирующего сигнала L_{Mi}, при котором $\Delta Q_i\left(\Delta G_i\right) \le 0$, $Q_i\left(G_i\right) \ge Q_{iн}\left(G_{iн}\right)$. Физически это можно достичь только архитектурно-строительными мерами, поэтому введем понятие «эквивалентного» коэффициента звукоизоляции (виброизоляции):

$$Q_{i\ экв}\left(G_{i\ экв}\right) = Q_{iн}\left(G_{iн}\right) = Q_i\left(G_i\right) + \Delta Q_i\left(\Delta G_i\right). \qquad (5)$$

Для выполнения условия (5) сформируем в разведопасном направлении активную шумовую помеху M. Такая помеха отличается от внешнего фонового шума относительной стабильностью интенсивности ее формирования на протяжении всего времени жизненного цикла речевого сигнала, что позволяет ввести понятие «эквивалентного» коэффициента звукоизоляции (виброизоляции). При $M \ne 0$ запишем кинематический параметр «эквивалентного» коэффициента звукоизоляции (виброизоляции) в виде:

$$q_{i\ экв} = 10^{0{,}05 \cdot Q_{i\ экв}(G_{i\ экв})} = \frac{S_i}{X_i \cdot \sqrt{1 + \frac{M_i^2}{X_i^2}}} = \frac{q_i}{\sqrt{1 + \frac{M_i^2}{X_i^2}}}, \qquad (6)$$

где

$$q_i = 10^{0{,}05 \cdot Q_i(G_i)}. \qquad (7)$$

Из выражений (4) – (7) кинематический параметр маскирующей помехи имеет вид:

$$M_i = X_i \cdot \sqrt{\frac{1}{10^{0{,}1 \cdot \Delta Q_i(\Delta G_i)}} - 1},$$

или минимально необходимый уровень интенсивности маскирующей помехи определится выражением

$$L_{M\,i}(V_{M\,i}) = 10 \cdot \lg\left[10^{0{,}1 \cdot L_{Yi}(V_{Yi})} - 10^{0{,}1 \cdot L_{Ni}(V_{Ni})}\right] + 20 \cdot \lg\left[\frac{1 - 10^{0{,}1 \cdot \Delta Q_i(\Delta G_i)}}{10^{0{,}1 \cdot \Delta Q_i(\Delta G_i)}}\right]. \qquad (8)$$

Настройка генератора маскирующей акустической (вибрационной) помехи осуществляется так, чтобы выполнялось неравенство

$$L_{M\,i\,ИЗМ}(V_{M\,i\,ИЗМ}) \ge L_{M\,i}(V_{M\,i}). \qquad (9)$$

При выполнении условия (9) акустический (вибрационный) канал утечки речевой информации считается защищенным от перехвата средствами технической разведки.

Гуляев Владимир Павлович, кандидат технических наук, доцент кафедры ТОР ИРИТ-РТФ ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина». E-mail: gulyaev-vp@ya.ru

Vladimir Pavlovich Gulyaev, Cand. Sc. Engineering, Associated professor of the Institute of Radioelectronics and Information Technologies of Ural Federal University named after the first President of Russia B. N. Yeltsin. E-mail: gulyaev-vp@ya.ru

УДК 659.1 : 004.056 + 343.534 : 004.056
ББК Х 401.114 : Ч 600.6

И. Ю. Ковалева

ПРЕДОТВРАЩЕНИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАСЕЛЕНИЯ В ОБЛАСТИ РЕКЛАМЫ

В статье рассмотрены вопросы законодательного регулирования и выявления скрытого психологического воздействия на подсознание потребителей рекламного продукта. Применяемые в рекламных кампаниях способы передачи информации могут представлять угрозу для информационной безопасности населения в тех случаях, когда они направлены на оказание воздействия на подсознание человека. Исследованы проблемы доступности использования методов эриксоновского гипноза при создании рекламного продукта на примере конкретных психологических шаблонов и возможности их выявления посредством психологических экспертиз.

Ключевые слова: *рекламный продукт, недопустимая реклама, эриксоновский гипноз, информационная безопасность, скрытое внушение.*

I. Yu. Kovalyova

INFORMATION SECURITY THREAT PREVENTION POPULATION IN ADVERTISING

In the article the questions of legislation and identify latent psychological effects of subliminal advertising consumer product are investigated. Used in advertising campaigns means of information transfer may pose a threat to public security in cases where they are aimed at influencing the subconscious. The problems of easily using methods of Erickson hypnosis in creating a promotional product are investigated in the context of using some specific psychological patterns and the possibility of detecting them by means of psychological examinations.

Keywords: *promotional product, Illegal advertising, Erickson hypnosis, information security, covert suggestion.*

В настоящее время человек подвержен воздействию огромного количества информации, в том числе рекламного характера, что актуализирует проблему выявления угрозы информационной безопасности населения при проведении рекламных кампаний.

В соответствии с положениями ч. 9 статьи 5 Федерального закона от 13 марта 2006 г. №38-ФЗ «О рекламе» не допускается использование в радио-, теле-, видео-, аудио- и кинопродукции или в другой продукции и распространение скрытой рекламы, то есть рекламы, которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами[1].

Аналогичное требование установлено в абз. 2 статьи 4 Закона РФ от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», которым предусмотрено, что запрещается использование в радио-, теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок и иных технических приемов и способов распространения информации, воздействующей на подсознание людей и (или) оказывающих вредное влияние на их здоровье[2].

Тем не менее, запрет на использование механизмов скрытого внушения, предусмотренный положениями Закона РФ № 2124-1 «О средствах массовой информации», существенно уже, нежели регламентированный Федеральным законом от 13 марта 2006 г. № 38-ФЗ «О рекламе», поскольку необходимо доказать наличие вредного влияния на здоровье людей, что представляется в большинстве случаев довольно затруднительным. Для признания же рекламы недопустимой достаточно лишь установить фактические обстоятельства, подтверждающие наличие неосознаваемого воздействия на сознание. Перечень механизмов и инструментов такого воздействия в законе не поименован, за исключением подпороговой стимуляции, которая технически может осуществляться посредством аудио- либо видеозаписи.

Умолчание законодателя относительно иных способов воздействия на подсознание потребителя рекламной продукции представляется более чем оправданным ввиду того, что технический прогресс современного общества не всегда позволяет оперативно выявить новые технологии, используемые для внушения.

Остается открытым вопрос положения психологических методик прямого и непрямого внушения в рамках легальных инструментов рекламы. Как определить черту, за которой использование техники нейролингвистического программирования переходит в рамки эриксоновского гипноза, задающего программы действий на уровне подсознания, избегая критическую оценку со стороны сознания? Допустим ли эриксоновский гипноз в сфере рекламы как способ более эффективного донесения информации до потребителей рекламного продукта или является злоупотреблением, создающим угрозу для информационной безопасности населения?

Исходя из буквального толкования положения ч. 9 статьи 5 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе», недопустимой является такая реклама, которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание. Иными словами, которая снимает блокировки сознательного и обращается к бессознательному человека – подсознанию.

Имеется разнообразная судебная практика, касающаяся обжалования решений Федеральной антимонопольной службы по признанию рекламы недопустимой и привлечению лиц к ответственности в соответствии со статьей 14.3 Кодекса об административных правонарушениях РФ. Большая часть разбирательств связана с использованием схожих графических изображений, формирующих скрытые ассоциативные связи у человека, что вызывает у потребителя интерес к продукту, а не к непосредственно представленному объекту рекламы (См.: Постановление Федерального арбитражного суда Центрального округа от 7 февраля 2006 г. № А36-2385/2005[3]). В случаях, когда элементы изобразительного и графического оформления наружной рекламы совпадают с аналогичными элементами этикетки продукта, суды признают факт правонарушения состоявшимся (См.: Постановление Федерального арбитражного суда Северо-Западного округа от 3 августа 2005 г. № А05-1789/05-22[4]).

Данный механизм, в психологии называемый «якорением», является далеко не единственным способом обращения к подсознанию человека и входит в сложную многоуровневую систему скрытого, или эриксоновского, гипноза.

Эриксоновский гипноз базируется на введении человека в трансовое состояние, по своим признакам отличное от понимания транса в контексте классического гипноза. Как отмечает сам основатель указанного направления психотерапевтической работы Милтон Эриксон: «Транс – это особое состояние, которое интенсифицирует терапевтические взаимоотношения и сосредотачивает человека на нескольких аспектах внутренней реальности. Гипнотическое внушение – это и есть процесс вызывания и утилизации собственных психических процессов человека такими способами, которые лежат за пределами досягаемости его собственного, обычного, произвольного и волевого контроля»[5].

Раскрывая метод воздействия, М. Эриксон также выделяет существенные преимущества такого рода внушений при использовании в повседневной действительности: «Обычные, повседневные, негипнотические внушения принимаются потому, что мы оценили их с помощью своих обычных сознательных установок и нашли, что они являются приемлемым руководством для нашего поведения, и мы выполняем их добровольно. Гипнотическое внушение отличается тем, что человек с удивлением обнаруживает, что опыт и поведение изменилось, казалось бы, автономным образом; опыт, похоже, находится вне нашего обычного контроля и самоуправления. Об успешном опыте гипноза можно говорить, когда транс меняет привычные установки и модели функционирования так, чтобы тщательно сформулированные гипнотические внушения могли вызывать и утилизировать другие паттерны ассоциаций и другие потенциалы пациента для достижения определенных целей»[6].

Сложность выявления механизма эриксоновского гипноза заключается в том, что для его включения достаточно подачи информации, построенной определенным образом, причем методы довольно разнообразны и на первый взгляд могут не выделяться из общего аудиолибо видеоматериала. В литературе, посвященной психотерапии с использованием скрытого гипноза, отмечается, что «гипнотические формы есть приемы коммуникации, которые облегчают вызывание и использование собственных ассоциаций человека, его возможностей и естественных механизмов психики такими способами, которые человеком обычно переживаются как непроизвольные».[7] Таким образом, лицо не осознает, что на него оказывается воздействие, не оценивает получаемую информацию как директивную, хотя она может являться таковой.

Производитель рекламного продукта, в особенности транслируемого на телевидении, имеет широкие возможности по включению в него элементов гипнотического внушения. Первым шагом формирования внушения является присоединение к потребителю рекламного продукта в его восприятии мира и поведении в нем. Обширные социологические и маркетинговые исследования, открытые для свободного доступа, позволяют определить психологический портрет потенциального покупателя продвигаемого продукта – его ценностные ориентиры и узкие метапрограммы, что снижает сопротивляемость потребителя к предоставляемой информации на базовом уровне.

Работа с подсознанием начинается с момента вербального присоединения и ведения объекта, иными словами, включения его в процесс скрытого гипноза. Методы включения могут быть самыми разнообразными, наиболее простой и распространенный – метод инертного согласия – начало повествования, основанного на принципе последовательного соглашения, т. е. постановка последовательных положительных утверждений (ответ «да») с малым промежутком во времени, иными словами, произнося раз за разом утверждения, с которыми человек не имеет оснований не соглашаться, производитель рекламного продукта имеет возможность присоединять к такой последовательности утверждения, согласие с которыми при других условиях было бы менее вероятным[8].

По схожему принципу построен шаблон наведения гипнотического транса, называемого «5-4-3-2-1», предусматривающего специальную систему вербальной подачи информации с использованием обращения к трем репрезентативным системам: создание иллюзии того, что человек видит, слышит и чувствует. Общее описание шаблона сводится к тому, что презентация информации ведется по спирали следующим образом: дается четыре фразы, описывающих, что человек видит, касательно положительных свойств продвигаемого продукта, после чего вставляется прямое внушение, затем четыре фразы, описывающих, что человек слышит, затем прямое внушение, после этого четыре фразы, описывающих ощущения человека, и опять прямое внушение. Это первый круг подачи информации. Всего кругов пять, с каждым последующим одна из фраз, относящихся к ощущениям объекта, заменяется на фразу с прямым внушением, таким образом, чтобы на последнем круге не оставалось никакой информации, кроме директивной команды.

Использование данного метода эффективно ввиду того, что, во-первых, осуществляется сенсорная перегрузка, во-вторых, включается механизм обращения потребителя к внутренним ассоциациям и переживаниям. Шаблон может быть использован при посроении истории, презентующей продукт, в этом случае повышается запоминаемость материала. Как отмечает Джеффри К. Зейг, «структура человеческой памяти такова, что смысл рассказанной истории западает в память скорее, чем простая констатация той же самой мысли»[9]. Использование данного шаблона является классическим методом эриксоновского гипноза, оно не очень удобно для рекламных роликов, транслируемых по телевидению ввиду ограничения эфирного времени, отведенного под рекламу (не более 15% в течение эфирного часа в соответствии с ч. 3 ст. 14 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе»).

Существуют иные, более доступные для производителя рекламы механизмы наведения транса в рамках ограниченного по времени аудио- либо видеоролика. Одним из них является сенсорная перегрузка. Как отмечает И. Н. Мелихов, «эта методика быстрого наведения транса связана с тем, что каждый человек может усваивать поступающую информацию с определенной скоростью, может сознательно удержать в кратковременной памяти определенный объем информации. Если эту скорость превысить, то сознание не успевает обработать новые сведения, и они идут в подсознание, т. к. только в трансе мозг способен усваивать без ограничений любой объем информации. Таким образом, можно быстро навести трансовое состояние и выйти на контакт с подсознанием. Человек способен сознательно держать в поле своего внимания совсем немного мыслей: около семи «кусков» информации в одно время. Речь человек может полностью понимать лишь при скорости, не превышающей 2,5 слова в секунду. Фраза, произносимая без паузы дольше 5–6 секунд, перестает осознаваться. Все, выходящее за эти пределы, сознанием рассматривается как «масса», относится к перегрузке и обрабатывается бессознательно. Всякий раз, когда сознательная обработка перегружается, есть возможность передать информацию прямо в подсознание, и человек будет реагировать на эту информацию»[10].

Другим легко доступным для рекламы способом погружения человека в гипнотическое состояние является техника разрыва шаблона ввви-

ду отсутствия необходимости предварительной подстройки и синхронизации бессознательных процессов гипнооператора и объекта. Суть состоит в том, чтобы сознательно не строить никаких естественных осмысленных переходов, а, наоборот, вызвать у человека состояние замешательства или потрясения, после чего выдать прямую информацию-внушение. По данным И. Н. Мелихова, «в состоянии недоумения психика человека готова воспринять любую подсказку, как выйти из тупика. Таким образом, человек находится в этот момент в естественном расслабленном трансе. После разрыва шаблона в течение 2–4 секунд человек слышит и понимает значение слов, но не может выстроить логическое внутреннее понимание услышанного. Именно в эти 2–4 секунды есть возможность давать директивы, которые он внутренне ощутит как первое легко понимаемое сообщение, предлагаемое ему, за которое можно «зацепиться», не обдумывая суть предложения»[11].

Методы введения человека в состояние пониженной критичности предоставленного материала разнообразны, к ним, в частности, относится использование историй с описанием состояния, называемого «даунтайм», контингентные внушения, техника вставленных маркированных сообщений и др.

Переданная посредством указанных методик информация, по нашему мнению, содержит признаки недопустимой рекламы, определенные в законе, поскольку оказывает неосознаваемое воздействие. Судебная практика пришла к единообразному толкованию вышеназванного положения, в соответствии с которым воздействие представляется противоправным, если препятствует осознанию данного вида вмешательства и влияет на свободу выбора потребителя, содержит какие-либо скрытые побуждения, воздействующие на бессознательный уровень восприятия (См.: Постановление Федерального арбитражного суда Северо-Западного округа от 30 августа 2010 г. № Ф07-7831/2010[12]).

Исходя из этого, представляется целесообразным поднять вопрос об обеспечении информационной безопасности населения и ведении контроля за рекламой на основании использования достижений психологии. В целях определения наличия в рекламе механизмов внушения, действующих на подсознание человека, могут быть использованы заключения психологических экспертиз.

Как отмечается на сайте Российского федерального центра судебной экспертизы при Министерстве юстиции Российской Федерации, проблема исследования психологического воздействия возникает перед судебной экспертизой в том числе и при определении влияния информационных технологий. В частности, может быть произведена психолингвистическая экспертиза, которая хоть и не является в настоящее время полноценным родом экспертиз, но может быть учтена уполномоченными органами при принятии решений[13].

Таким образом, представляется целесообразным при осуществлении проверки допустимости рекламы уполномоченными органами не ограничивать внимание только на исследовании внешнего сходства графических изображений, влекущих возникновение подсознательных ассоциативных связей у потребителя, но также исследовать вопрос наличия либо отсутствия в рекламной информации скрытых психологических внушений.

Литература

[1] О рекламе: федеральный закон от 13 марта 2006 г. № 38-ФЗ // Собр. законодательства Рос. Федерации. – 2006. - № 12. – ст. 1232.

[2] О средствах массовой информации: закон РФ от 27 декабря 1991 г. № 2124-1 // Российская газета. – 8 февраля. – 1992. – № 32.

[3] Постановление Федерального арбитражного суда Центрального округа от 7 февраля 2006 г. № А36-2385/2005 // Официальный сайт Федерального арбитражного суда Центрального округа. URL: http://fasco.arbitr.ru/ (дата обращения 17.09.2013).

[4] Постановление Федерального арбитражного суда Северо-Западного округа от 3 августа 2005 г. № А05-1789/05-22 // Официальный сайт Арбитражного суда Северо-Западного округа. URL: http://fasszo.arbitr.ru/ (дата обращения 17.09.2013).

[5] Эриксон М., Росси Р., Росси Ш. Гипнотические реальности: наведение клинического гипноза и формы косвенного внушения. – М.: Независимая фирма «Класс», 1999. – С. 36.

[6] Эриксон М., Росси Р., Росси Ш. Гипнотические реальности: наведение клинического гипноза и формы косвенного внушения. – М.: Независимая фирма «Класс», 1999. – С. 37.

[7] Эриксон М., Росси Р., Росси Ш. Гипнотические реальности: наведение клинического гипноза и формы косвенного внушения. – М.: Независимая фирма «Класс», 1999. – С. 38.

[8] Смирнов А. Методические материалы к семинару по эриксоновскому гипнозу // Библиотека. URL: http://www.koob.ru (дата обращения 17.09.2013).

[9] Джеффри К. З. Семинар с доктором медицины Милтоном Г. Эриксоном. – М.: Независимая фирма «Класс», 2003. – С. 14.

[10] Мелихов И. Н. Скрытый гипноз. Практическое руководство. – Волгоград: Перемена, 2003. – С. 131.

[11] Мелихов И. Н. Скрытый гипноз. Практическое руководство. – Волгоград: Перемена, 2003. – С. 124.

[12] Постановление Федерального арбитражного суда Северо-Западного округа от 30 августа 2010 г. № Ф07-7831/2010 по делу № А52-6308/2009 // Официальный сайт Арбитражного суда Северо-Западного округа. URL: http://fasszo.arbitr.ru/ (дата обращения 17.09.2013).

[13] Психологическая экспертиза // Официальный сайт Российского федерального центра судебного экспертизы при Министерстве юстиции Российской Федерации. URL: http://www.sudexpert.ru/possib/psych.php (дата обращения 18.09.2013).

References

[1] O reklame: federal'nyi zakon ot 13 marta 2006 g. № 38-FZ [On advertising: Federal law as of March 13, 2006 No.38-FZ]// Sobr. zakonodatel'stva Ros. Federatsii [Official Gazette of the Russian Federation]. – 2006. – No.12. – Art. 1232.

[2] O sredstvakh massovoi informatsii: zakon RF ot 27 dekabrya 1991 g. № 2124-1 [On mass media: Federal law as of December 27, 1991 No.2124-1]// Rossiiskaya gazeta [Russian post]. – February 8. – 1992. – No. 32.

[3] Postanovlenie Federal'nogo arbitrazhnogo suda Tsentral'nogo okruga ot 7 fevralya 2006 g. № A36-2385/2005 [Decree of the Federal Arbitrate Court of the Central District as of February 7, 2006 No. A36-2385/2005]// Ofitsial'nyi sait Federal'nogo arbitrazhnogo suda Tsentral'nogo okruga [Official website of the Federal Arbitrate Court of the Central District]. URL: http://fasco.arbitr.ru/ (date of compellation 17.09.2013).

[4] Postanovlenie Federal'nogo arbitrazhnogo suda Severo-Zapadnogo okruga ot 3 avgusta 2005 g. № A05-1789/05-22 [Decree of the Federal Arbitrate Court of the North-West District as of August 3, 2005 No. A05-1789/05-22]// Ofitsial'nyi sait arbitrazhnogo suda Severo-Zapadnogo okruga [Official website of the Federal Arbitrate Court of the North-West District]. URL: http://fasszo.arbitr.ru/ (date of compellation 17.09.2013).

[5] Erikson M., Rossi R., Rossi Sh. Gipnoticheskie real'nosti: navedenie klinicheskogo gipnoza i formy kosvennogo vnusheniya [Hypnotic realities: Targeting clinical hypnosis and forms of concealed suggestion]. – Moscow: Nezavisimaya firma «Klass», 1999. – p. 36.

[6] Erikson M., Rossi R., Rossi Sh. Gipnoticheskie real'nosti: navedenie klinicheskogo gipnoza i formy kosvennogo vnusheniya [Hypnotic realities: Targeting clinical hypnosis and forms of concealed suggestion]. – Moscow: Nezavisimaya firma «Klass», 1999. – p. 37.

[7] Erikson M., Rossi R., Rossi Sh. Gipnoticheskie real'nosti: navedenie klinicheskogo gipnoza i formy kosvennogo vnusheniya [Hypnotic realities: Targeting clinical hypnosis and forms of concealed suggestion]. – Moscow: Nezavisimaya firma «Klass», 1999. – p. 38.

[8] Smirnov A. Metodicheskie materialy k seminaru po Eriksonovskomu gipnozu [Educational materials to the seminar on Erikson hypnosis]// Biblioteka. URL: http://www.koob.ru (date of compellation 17.09.2013).

[9] Dzheffri K.Z. Seminar s doktorom meditsiny Miltonom G. Eriksonom [Seminar with Dr.Milton and G.Erikson]. – Moscow: Nezavisimaya firma «Klass», 2003. – S. 14.

[10] Melikhov I.N. Skrytyi gipnoz. Prakticheskoe rukovodstvo [Concealed hypnosis. Practical guidance]. – Volgograd: Peremena, 2003. – p. 131.

[11] Melikhov I.N. Skrytyi gipnoz. Prakticheskoe rukovodstvo [Concealed hypnosis. Practical guidance]. – Volgograd: Peremena, 2003. – p. 124.

[12] Postanovlenie Federal'nogo arbitrazhnogo suda Severo-Zapadnogo okruga ot 30 avgusta 2010 g. № F07-7831/2010 po delu N A52-6308/2009 [Decree of the Federal Arbitrate Court of the North-West District as of August 30, 2010 No. F07-7831/2010 on the case No. A52-6308/2009]// Ofitsial'nyi sait arbitrazhnogo suda Severo-Zapadnogo okruga [Official website of the Federal Arbitrate Court of the North-West District]. URL: http://fasszo.arbitr.ru/ (date of compillation 17.09.2013).

[13] Psikhologicheskaya ekspertiza [Psychological expertise]// Ofitsial'nyi sait Rossiiskogo federal'nogo tsentra sudebnogo ekspertizy pri Ministerstve yustitsii Rossiiskoi Federatsii [Official website of the Russian Federal Center of forensic expertise at the Ministry of Justice of the Russian Federation]. URL: http://www.sudexpert.ru/possib/psych.php (date of compellation 18.09.2013).

Ковалева Изольда Юрьевна, юрисконсульт ООО «Комплексная консалтинговая компания». E-mail: isolde_kov@mail.ru.

Kovaleva Isolde Y., counsel Ltd. «Comprehensive consulting company». E-mail: isolde_kov@mail.ru.

УДК 342.9.07:002.6 + 34.03 :[002:004.056]
ББК Х 401.132 + Х 401.114:Х 401.132

Ю. В. Пономарева

АКТУАЛЬНЫЕ ВОПРОСЫ СЛУЖЕБНОЙ ТАЙНЫ

В статье анализируются актуальные вопросы защиты служебной тайны. Открытость и ограничение доступа к информации является одной из центральных проблем правового регулирования. В настоящее время институт служебной тайны практически не урегулирован законодательно, есть большие проблемы в регулировании служебной тайны в различных государственных органах. Многие нормативные акты находятся в противоречии друг с другом. Вопрос регулирования использования служебной тайны можно рассматривать как с точки зрения ограничения бесконтрольного «засекречивания» информации, так и с точки зрения избежания ситуации манипулирования информацией или её «утечки».

Ключевые слова: *информации ограниченного доступа, служебная тайна, конфиденциальность, тайна.*

Y. V. Ponomareva

CURRENT ISSUES OF OFFICIAL SECRETS

The article analyzes the current issues of protection of official secrecy. Openness and limited access to information is one of the central problems of legal regulation. Currently, the institute of official secrecy practically settled law, there are big problems in the regulation of official secrecy by various governmental bodies. Many regulations are in conflict with each other. The regulation of the use of official secrecy can be seen both in terms of limiting the uncontrolled "classification" of information, and from the point of view of the situation to avoid the manipulation of information or "leaks".

Keywords: *confidential and restricted information; official secrecy, confidentiality, secrecy.*

Одним из ключевых принципов построения мирового пространства сегодня выступает принцип информационной открытости. Основным принципом функционирования государственных органов в нашей стране также является информационная открытость и «прозрачность» деятельности. Однако всегда была, есть и будет информация, доступ к которой имеют лишь немногие, сохранность которой обеспечивается государством. Необходимость такого ограничения может быть продиктована интересами безопасности, стратегическими интересами государства. Однако одной из основных задач, которую необходимо решать в ходе осуществления государственного управления, является задача обеспечения баланса между стратегическими интересами государства и требованием информационной открытости.

Отнесение той или иной информации к разряду тайны, ограниченного доступа обусловлено несколькими факторами: особым содержанием самой информации, закрытость которой обеспечивает безопасность личности, государства и общества в целом; характером тех общественных отношений, в которые интегрирована

та или иная информация и которые охраняются законом.

В настоящее время законодательством предусмотрены ограничения к следующим категориям информации ограниченного доступа: персональные данные; семейная и личная тайны; профессиональная тайна (врачебная, адвокатская, тайна исповеди и др.); государственная тайна; коммерческая тайна (секреты производства); кредитные истории; инсайдерская информация; служебная тайна.

Каждая категория информации имеет собственную подробную законодательную регламентацию. Такое тщательное регулирование неслучайно. С одной стороны, оно служит целям эффективной защиты информации, а с другой стороны, призвано не допустить злоупотребление правом на ограничение доступа к информации.

Среди информации ограниченного доступа важное место занимает служебная тайна, обладающая самостоятельными юридически значимыми характеристиками и имеющая важное значение в деятельности государственно-властных структур.

Институт служебной тайны практически не урегулирован законодательно, есть большие проблемы в регулировании служебной тайны в различных государственных органах. Многие нормативные акты находятся в противоречии друг с другом. Вопрос осуществления управления в государственных органах и регулирование использования служебной тайны можно рассматривать как с точки зрения ограничения бесконтрольного «засекречивания» информации, так и с точки зрения избежания ситуации манипулирования информацией или её «утечки». Кроме того, бесконтрольное ограничение доступа к информации является весьма серьезным коррупциогенным фактором. Регулирование служебной тайны должно повысить прозрачность деятельности государственных органов и должностных лиц.

Одним из наиболее показательных примеров из международной практики, касающейся разглашения информации о деятельности государственных органов, является так называемое дело Сноудена, когда была разглашена информация, статус которой по законодательству США аналогичен статусу служебной тайны по законодательству России. Именно для того, чтобы не допустить возникновения подобных неоднозначных и скандальных ситуаций, необходимо разработать механизм детальной регламентации с возникновением и работой с информацией ограниченного доступа в государственных учреждениях. Защита такой информации является важным фактором эффективности государственного управления.

В юридической литературе проблемы служебной тайны как правового института рассматриваются в основном в сравнительном аспекте с другими правовыми институтами информации конфиденциального характера. К сожалению, масштабного, полного исследования правового института служебной тайны в юридической литературе нет. Диссертации, в которых раскрывается правовая сущность служебной тайны, обычно рассматривают этот институт применительно к отраслевой специфике этого института, либо применительно к вопросам ответственности за разглашение такой тайны.

Федеральный закон «Об информации, информационных технологиях и о защите информации» подразделяет информацию в зависимости от категории доступа к ней на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). А. В. Минбалеев отмечает, что «данный классификационный критерий является ключевым в механизме правового регулирования информационных отношений. Именно на основе закрепления права каждого на информацию и возможных его ограничениях в государстве устанавливаются различные правовые режимы доступности информации»[1].

Вопрос нормативно-правового обеспечения режима информации ограниченного доступа является в настоящее время одним из актуальных. Активно идет разработка и усовершенствование законодательства в сфере государственной, коммерческой, профессиональной, семейной и иных видов тайн. Одним из наименее урегулированных институтов в области информации ограниченного доступа является институт служебной тайны.

В настоящее время в научной юридической литературе наблюдается плюрализм мнений в отношении сущности правовой природы института служебной тайны. Связано такое многообразие точек зрения, прежде всего, с историей регулирования института служебной тайны. Как отмечает Т. М. Занина, «свое наиболее четкое оформление институт служебной тайны получил в юридической конструкции, предложенной Инструкцией по обеспечению режима секретности в министерствах и ведомствах СССР, утвержденной постановлением Совета Министров СССР от 12.05.87 № 556-126, которой вводилось интегрированное понятие государственных секретов, которые по степени важности подразделялись на государственную и служебную тайны. Данная конструкция полностью отражала систему воззрений того периода на роль и место служебной тайны в функционировании механизма государства. К сожалению, принятие Закона о государственной тайне, привнеся массу позитивных моментов, повлекло за собой одно существенное негативное последствие – отнесение в соответствии с указанным

Законом грифа «секретно» для обозначения исключительно сведений, составляющих государственную тайну, де-факто ликвидировало служебную тайну как институт и заодно создало серьезную правовую неопределенность в вопросе квалификации ранее обозначенных им сведений»[2]. Кроме того, в 1994 году был принят Гражданский кодекс Российской Федерации, в ст. 139 которого было предусмотрено следующее положение: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами». То есть фактически предусматривалось регулирование служебной тайны по аналогии с коммерческой, при этом служебной тайне приписывались свойства «действительной или потенциальной коммерческой ценности», что фактически подрывало всю научную доктрину в области конфиденциальной информации как таковой. Несмотря на то что через 12 лет статья утратила силу, разрешения вопросов, касающихся института служебной тайны в законодательстве так и не появилось.

В частности, возникает вопрос, кто является субъектом отношений по охране служебной тайны? Многие исследователи сходятся во мнении, что субъектом служебной тайны являются государственные/муниципальные служащие[3], они мотивируют свою точку зрения тем, что в указе используется понятие «служебные сведения», а также тем, что доступ к сведениям ограничивается органами государственной власти. Однако с этой точкой зрения можно поспорить: во-первых, использование понятие «служебные» ещё не является однозначным доказательством того, что указанная информация используется только в пределах государственной службы. Так, к примеру, в Гражданском кодексе Российской Федерации существует институт служебного произведения, отраслевая принадлежность которого определена как гражданско-правовая, причем данный институт никак не связывают с государственной службой.

Есть точка зрения, согласно которой правовой режим служебной и коммерческой тайны одинаков, а одно и то же лицо без всяких ограничений может быть обладателем и той, и другой тайны[4]. Кроме того, как отмечают В. А. Дозорцев, Э. П. Гаврилов и некоторые другие ученые, служебная тайна есть информация, которая стала доступна (известна) гражданину при исполнении им своих трудовых (служебных) обязанностей. При этом не имеет значения, работает такой гражданин в государственной (муниципальной) или частной организации, заключен ли трудовой договор с юридическим лицом или индивидуальным предпринимателем. Попытки ограничить понятие служебной тайны рамками отношений, возникающих в государственных организациях, не находят законодательного подтверждения и неверны по сути, а потому могут только нанести ущерб общему правовому регулированию[5]. Существует также иная точка зрения, согласно которой служебная тайна фактически рассматривается как одна из разновидностей профессиональной тайны[6].

В свою очередь, существует точка зрения, согласно которой использование понятия «служебная тайна» в корне неверно, более корректным будет использование понятия «трудовая тайна». По мнению автора этой точки зрения, данный термин будет полно отражать сущность служебной тайны и основания ее возникновения[7].

По мнению И. Ю. Павлова, «наличие дополнительной самостоятельной разновидности информации о деятельности государственных органов и органов местного самоуправления, относящейся к категории ограниченного доступа, представляется чрезмерным, поскольку характеристика объекта, который охраняется в режиме «служебной тайны» в его сегодняшнем понимании, эквивалентна характеристике объекта, охраняющегося в режиме «государственной тайны»[8]. Вместе с тем, автор этой точки зрения приходит к выводу, что целесообразно рассматривать служебную тайну как «чужую» тайну, а именно конфиденциальную информацию, ставшую известной государственным органам, должностным лицам при оказании ими государственных полномочий. И при таком подходе, с точки зрения И. Ю. Павлова, не возникнет потребности в принятии закона «о служебной тайне». Достаточно распространенная точка зрения, однако возникает в этой связи вопрос о том, как же быть с «внутренней информацией» государственных органов? В случае принятия такой концепции сложится такая ситуация, когда вся внутренняя информация будет беспрепятственно распространяться, что, на наш взгляд, не есть выражением взвешенного подхода к информационной безопасности. Схожую классификацию можно найти в работе Т. М. Заниной[9], которая предлагает относить к категории служебной тайны следующую информацию:

• конфиденциальные сведения в области военного управления (военная тайна);

• сведения, охватываемые понятием «тайна связи» (в той мере, в которой операторами выступают органы государственной власти и подведомственные им организации, учреждения);

• информация, образующаяся на стадии предварительного расследования;

• банковская тайна (которая обеспечивается органами государственной власти и ЦБ РФ);

• конфиденциальная информация, хранящаяся о гражданах в органах государственной власти и местного самоуправления.

В отличие от позиции И. Ю. Павлова, в данном подходе предлагается принятие отдельного федерального закона «О служебной тайне», который бы детально регулировал отношения в сфере охраны служебной тайны. Однако вряд ли можно сказать, что эта точка зрения лишена недостатков, так как фактически автор перечислил некоторые виды тайн, которые становятся известны государственным органам и должностным лицам, при этом абсолютно неясно, по каким причинам не включены в перечень иные виды тайн, такие, как коммерческая тайна.

Существует также одна точка зрения, которая кардинально отличается от всех предыдущих. Согласно этой точке зрения, категорию «служебная тайна» в настоящее время государственные органы не могут использовать вообще, так как использование такой категории тайны не урегулировано федеральным законодательством[10]. Очень интересная позиция, не лишенная здравого смысла. По сути, действительно, мы не можем использовать правовые категории, даже правовые институты, коим является институт служебной тайны, которые в законодательстве никак не раскрыты, правовое регулирование которых фактически отсутствует. Тем более это является институтом публичного, а не частного права, где господствует позиция «всё, что не разрешено, запрещено». Кроме того, в законодательстве даже нет единства терминологии: в различных нормативных актах используются понятия «служебная тайна», «информация для служебного пользования», «служебная информация», «внутренняя информация государственных органов». Как же в этом случае можно вообще говорить об использовании института «служебной тайны»?

Безусловно, и эта точка зрения не является бесспорной, однако проблема заключается отнюдь не в достаточной аргументированности точек зрения, а в отсутствии должного правового регулирования института служебной тайны на законодательном уровне.

Кроме того, вопросы возникают относительно ограничения доступа к информации органами государственной власти. Насколько правомерно такое ограничение доступа к информации, особенно если рассматривать этот вопрос в свете принципа открытости и доступности информации о деятельности государственных органов и органов местного самоуправления?[11]

Надо отметить, что такое разночтение, как в теории, так и в практике неслучайно. Даже на уровне федеральных законов, указов Президента Российской Федерации, Постановлений Правительства Российской Федерации, приказов министерств нет единообразного понимания того, что же есть служебная тайна, служебная информация и на каком основании может ограничиваться доступ к ней.

При рассмотрении понятия служебной тайны чаще всего возникают следующие вопросы:

1. Каково соотношение понятий «служебная тайна», «служебная информация», «коммерческая тайна», «государственная тайна», «профессиональная тайна», «информация ограниченного доступа», гриф «для служебного пользования», «внутренняя информация государственных органов» и других?

2. Кто является субъектом в отношениях по охране служебной тайны?

3. Что является объектом отношений по охране служебной тайны?

4. Каково содержание отношений по охране служебной тайны (каков порядок ограничения доступа, принципы и основания наложения подобных ограничений к допуску, порядок допуска к такой информации)?

5. Какая наступает ответственность за разглашение служебной тайны?

На наш взгляд, ответы на все эти вопросы должны содержаться в федеральном законе (законах), так как в Федеральном законе «Об информации, информационных технологиях и защите информации» предусмотрено требование, согласно которому ограничение доступа к информации устанавливается только федеральным законодательством, к которому, в свою очередь, данный закон относит исключительно федеральные законы.

В законодательстве понятие служебной тайны активно используется, но четкого закрепления данного понятия в нормативных актах нет. По большому счету, режим «служебной тайны» регулируется двумя подзаконными актами: Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» и Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».

Относительно возможности применения постановления и указа Президента Российской Федерации существуют обоснованные сомнения: в Федеральном законе «Об информации, информационных технологиях и защите информации» предусмотрено требование, согласно которому ограничение доступа к информации

устанавливается только федеральным законодательством[12]. В связи с чем возникают объективные сомнения в правомерности установления регулирования служебной тайны Указом Президента Российской Федерации и Постановлением Правительства Российской Федерации.

В настоящее время регулирование такой категории, как «служебная тайна», происходит исключительно на подзаконном уровне, что противоречит как требованию Федерального закона «Об информации, информационных технологиях и защите информации», так и требованиям Конституции Российской Федерации; кроме того, такое регулирование является недопустимым, также существует мнение, что если регулирование ограничения информации осуществляется не федеральным законом, как того требует законодательство, то исполнение таких требований не является обязательным. На наш взгляд, это излишне категоричная точка зрения, однако и в ней есть доля правды. Следует также подчеркнуть, что при отсутствии федерального закона ответы на поставленные выше вопросы найти крайне сложно в связи с несистематезированностью требований подзаконных актов, а также их противоречивостью.

Существует интересное решение по этому вопросу, которое было вынесено Верховным Судом Российской Федерации ещё в 2005 году: И. Ю. Павлов обратился в Верховный Суд Российской Федерации с заявлением о признании недействующими норм Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти (утвержденного постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233), ссылаясь на то, что они нарушают предусмотренное статьей 29 Конституции Российской Федерации право заявителя свободно искать и получать информацию.

В заявлении указано, что в силу ст. 10 Федерального закона «Об информации, информатизации и защите информации» государственные информационные ресурсы являются открытыми и общедоступными. <...> Таким образом, критерии идентификации конкретной информации для отнесения ее к категории ограниченного доступа должны быть определены специальным федеральным законом. Вместе с тем в Российской Федерации не принимался федеральный закон, ограничивающий доступ к несекретной служебной информации. По мнению заявителя, оспариваемые предписания Положения противоречат статьям 10 и 12 Федерального закона «Об информации, информатизации и защите информации», статьям 4, 40 и 47 Закона Российской Федерации «О средствах массовой информации». С указанными доводами суд не согласился, в удовлетворении заявленных требованиях отказал. Суд мотивировал своё решение тем, что в силу пункта 5 ст. 10 Закона отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 данного Федерального закона (информация о гражданах).

Использование в приведенной норме закона двух терминов, а именно «законодательство Российской Федерации» и «федеральный закон», свидетельствует о том, что отнесение информации к конфиденциальной в случаях, не подпадающих под действие ст. 11 Закона, может осуществляться в порядке, установленном не только федеральными законами, но и указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

Любопытно отметить, что в ранее действовавшем законе до 2006 года действительно использовалась такая формулировка. И в тот момент суд совершенно справедливо, исходя из анализа норм закона, пришел к такому выводу. Однако в действующем законе такая формулировка заменена на более конкретную: «Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение»[13]. Исходя из новой формулировки, решение Верховного Суда могло бы звучать совершенно иначе... Именно поэтому необходимо урегулировать отношения в области служебной тайны нормами федерального закона, а не законодательства.

Как было сказано ранее, понятие служебной тайны активно используется, но четкого закрепления данного понятия в нормативных актах нет. Существует лишь определение, закрепленное в Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Оно звучит следующим образом: служебная тайна – это служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами. Кроме указанного понятия в законах и подзаконных актах используется такое понятие, как «служебная информация ограниченного доступа». Это понятие определяют как «несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью»[14]. При сопоставлении этих двух понятий возникает вопрос об их соотношении: являются ли они тождественными? Указанные формулировки хоть и схожи, однако имеют различия: в

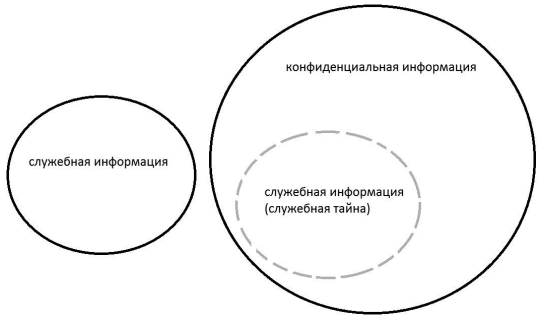
первом случае служебная тайна – это сведения, доступ к которым ограничен, во втором случае – это несекретная информация с ограничением на распространение. Возникает вопрос: что такое секретная информация, а что такое тайна? И может ли быть тайна несекретной информацией? Если исходить из общелексического толкования, то можно сказать, что слова «секрет» и «тайна» являются синонимичными по смыслу[15]. Если же исходить из контекстного толкования, то можно предположить, что такое разночтение в понятиях вызвано лишь недостатком юридической техники. Вероятнее всего, имелся в виду тот факт, что указанная информация ограниченного доступа не является государственной тайной (проведена аналогия с секретными сведениями, защита которых предусмотрена Федеральным законом «О государственной тайне»).

Итак, мы полагаем, что понятия «служебная тайна» и «служебная информация ограниченного доступа» являются тождественными.

Кроме того, в законодательстве достаточно часто упоминается такая категория информации, как «служебная информация», статус которой является также достаточно неоднозначной: так, в одном из Постановлений Правительства Российской Федерации[16] используется такой термин, как «служебная информация». Примечательно, что этот термин во всех формулировках логически обособлен от других видов конфиденциальной информации. В постановлении используется формулировка «служебная и конфиденциальная информация», то есть законодатель фактически разграничил служебную и конфиденциальную информацию. Интересно также то, что в постановлении дается определение «служебной информации» – «любая не являющаяся общедоступной и не подлежащая разглашению информация, находящаяся в распоряжении должностных лиц и сотрудников организации в силу их служебных обязанностей, распространение которой может повлиять на рыночную стоимость активов, в которые размещаются средства пенсионных накоплений».

В связи с чем возникают вопросы относительно того, на каком основании происходит ограничение доступа к данной категории информации, если эта информация не является конфиденциальной? И вообще чем отличается конфиденциальная информация от информации, не подлежащей разглашению?

В указанном постановлении также дается определение понятию «конфиденциальная информация»: «конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации». Напомним, что перечень «конфиденциальной информации» предусмотрен Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера»[17]. В этот перечень включены также служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна). Вот здесь и возникает логическое кольцо: служебная информация не тождественна конфиденциальной информации, в состав которой, в свою очередь, входит служебная информация. Соотношение понятий можно изобразить так:



В этом случае получается, что в постановлении отграничено понятие «служебная информация» от понятия «конфиденциальная информация», при этом неясно, на каком основании, т. к. служебная информация включается в категорию «конфиденциальная информация». В связи с этим можно сделать следующий вывод: либо налицо непроработанность с точки зрения юридической техники, либо в данном контексте разделяются понятия «служебная тайна» и «служебная информация». Во втором случае абсолютно неясно, на каком основании разграничиваются эти два понятия. Так как если не отождествлять служебную информацию со служебной тайной, то малейшие основания для ограничения доступа к такой информации просто отсутствуют. Можно предположить, что режим такой информации в контексте рассматриваемого постановления аналогичен режиму инсайдерской информации.

В других же правовых актах, использующих понятие «служебная информация», такая категория информации характеризуется как чисто техническая, вспомогательная информация, указывающая на «адрес» места хранения тех или иных сведений. Так, например, такое понимание данной категории информации встречается в Указаниях Центробанка Российской Федерации[18].

Такое разночтение в понятиях «служебная информация» и «служебная тайна» далеко не редкость. На наш взгляд, понятие «служебная информация» значительно шире по своей сути, чем понятие «служебная тайна» либо «служебная информация ограниченного доступа», она охватывает большой объем информации, образующийся в результате деятельности. И доступ к

ней не может быть ограничен в произвольном порядке.

Таким образом, на наш взгляд, необходимо унифицировать понятийно-категориальный аппарат, используемый в законодательстве относительно ограничения доступа к служебной информации, используя применительно к такой категории информации ограниченного доступа термин «служебная тайна», «информация (сведения) составляющие служебную тайну». Так как именно этот правовой институт законодатель выделяет в законе «Об информации, информационных технологиях и о защите информации».

Вопрос о субъектах правоотношений по охране служебной тайны до конца не решен в законодательстве. Так, в Указе Президента Российской Федерации речь идет о таком субъекте, как государственные органы. В Постановлении Правительства Российской Федерации № 1233 также речь идет о таком субъекте как государственные органы, но такой вывод можно сделать только исходя из контекстной трактовки определения «служебной тайны», которое дается в этом постановлении. Надо отметить, что недостаток самого определения заключается в том, что в качестве субъекта отношений по охране служебной тайны называется организация, а не государственный орган.

Следует учесть, что данное понимание субъектов по охране служебной тайны является доминирующим в законодательстве и в различных ведомственных актах, однако не единственным. Так, Федеральный закон «О страховании вкладов физических лиц в банках Российской Федерации» содержит положение, согласно которому «Агентство вправе получать информацию, составляющую служебную, коммерческую и банковскую тайну банка, в отношении которого наступил страховой случай». Это значит, что служебная тайна может существовать не только у государственного органа, но и у коммерческого банка. Кроме того, аналогичная позиция существует в Федеральном законе «О рекламе»[20]. В ст. 34 указанного закона содержится положение о том, что «Юридические лица, индивидуальные предприниматели обязаны представлять в антимонопольный орган (его должностным лицам) по его мотивированному требованию в установленный срок необходимые документы, материалы, объяснения, информацию в письменной и (или) устной форме (в том числе информацию, составляющую коммерческую, служебную и иную охраняемую законом тайну)». Опять в данном случае очевидно, что законодатель допускает возможность наличия служебной тайны у юридических лиц.

На наш взгляд, такое противоречивое понимание категории «служебная тайна» в законодательстве связано с позицией, ранее закреплявшейся в ст. 139 ГК РФ. Указанная статья утратила силу с 1 января 2008 года, а законодательство не было надлежащим образом унифицировано. Данная статья содержала следующее определение: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности». То есть ранее критерием отнесения информации к категории «служебная тайна» была ее действительная или потенциальная коммерческая ценность. Из-за этого и сложилось мнение о том, что служебная тайна может быть также в негосударственных организациях. Однако законодатель исключил данную формулировку из Гражданского кодекса, при этом не внес изменения в соответствующие нормативные акты. На данный момент, по нашему мнению, субъектами отношений по обороту и охране сведений, составляющих служебную тайну, являются государственные органы и должностные лица, и нет оснований полагать, что субъектами охраны служебной тайны являются негосударственные организации.

Что касается объектов служебной тайны (т. е. непосредственно той информации, которая является служебной тайной), то здесь достаточно сложно говорить объективно. Как справедливо отмечает И. А. Павлов, проблемой служебной тайны, как и государственной, является то, что перечень сведений, которые относятся к категории «служебная тайна», устанавливается внутренними актами либо ведомственными актами, которые, в свою очередь, также не подлежат разглашению. Фактически получается замкнутый круг: в нормативном акте предусмотрено, что доступ может ограничиваться теми сведениями, перечень которых предусмотрен нормативным актом, в свою очередь акт, в котором предусмотрен такой перечень сведений, сам является служебной информацией ограниченного доступа. И поэтому проверить законность либо незаконность отнесения той или иной информации к служебной тайне не представляется возможным. Так, к примеру, перечень сведений ограниченного доступа в МЧС России утвержден приказом МЧС России от 10.03.2006 № 144ДСП «Об утверждении Перечня сведений, составляющих служебную информацию ограниченного распространения, Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий». При этом открытый доступ к данному документу отсутствует, что прямо нарушает положение ст. 9 ФЗ «Об информации, информационных технологиях и о защите информации».

Таким образом, разработка вопроса категории сведений, которые могут относиться к служебной тайне, носит больше теоретический характер.

В основу же практических исследований мы взяли нормативные акты, открытый доступ к которым представляется возможным.

Сразу стоит отметить, что при поиске различных актов в сети Интернет доступно большое количество актов, принятых государственными органами Украины. Анализ законодательства Украины показал, что там доступность таких перечней гораздо выше.

Проанализируем несколько перечней сведений, доступ к которым удалось получить[21]. В основном доступны перечни администраций муниципальных районов, администраций областей. В первых категориях перечней под служебной информацией понимаются сведения об информационно-аналитической системе, аналитические прогнозы, заключения, вследствие разглашения которых возможно нарушение конституционных прав и свобод человека и гражданина, наступление негативных последствий в государстве и районе, создание препятствий в работе райсовета и его исполнительного аппарата, Сведения о технических возможностях программного обеспечения, компьютерной техники, которые используются, служебная корреспонденция, сведения об экономическом положении крупнейших предприятий, о научно-технических разработках, сведения о структуре, составе, объеме автопарка, маршруте передвижения главного должностного лица области, Сведения о местах хранения вооружений, Сведения о предстоящих международных визитах, содержании экономических договоренностей, программах пребывания, также персональные данные, сведения, составляющие тайну судопроизводства[22], Сведения, связанные с профессиональной деятельностью (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений).

Таким образом, мы можем сделать вывод, что в нормативных актах к служебной информации ограниченного доступа относят либо внутреннюю информацию государственных органов или органов местного самоуправления, касающуюся экономической обстановки, важных научных разработок, внутренней корреспонденции, либо так называемую «чужую тайну» – информацию, ставшую известной государственным органам, органам местного самоуправления и относящуюся к категории конфиденциальной (персональные данные, профессиональная тайна, тайна следствия и т. д.).

Следует отметить, что в некоторых перечнях есть такая категория информации, как «разные сведения». К ним по непонятным причинам были отнесены сведения о происшествиях, могущие вызвать панику, межнациональные конфликты до официального завершения расследования, сведения о наличии радиоактивных веществ[23]. Такое ограничение к доступу информации просто недопустимо, так как напрямую противоречит положению ФЗ «Об информации, информационных технологиях и о защите информации». На наш взгляд, необходимо сделать перечень таких сведений открытым, так как даже в открытых перечнях можно обнаружить нарушения законодательства.

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» регламентирует порядок работы со служебной информацией ограниченного распространения: на документах проставляется пометка «для служебного пользования», а также регистрируется количество копий таких документов. В постановлении дан перечень информации, доступ (распространение) которой не может быть ограничен. Но из Положения не ясен ни критерий отнесения информации к категории «Информация ограниченного распространения», ни основания такого отнесения. Следует отметить всё же, что в одном из перечней сведений, относящихся к служебной информации ограниченного распространения, содержатся интересные критерии для отнесения сведений к указанной категории:

• «служебная информация должна создаваться на средства районного бюджета или пребывать во владении, пользовании или распоряжении районного совета;

• использоваться с целью обеспечения национальных интересов государства и интересов территориальной громады района; не относиться к государственной тайне.

В случае разглашения такой информации возможно:

• нарушение конституционных прав и свобод человека и гражданина;

• наступление негативных последствий во внутриполитической, внешнеполитической, экономической, социальной, гуманитарной, научно-технологической, экологической, информационной сферах и в сферах государственной безопасности и безопасности государственной границы;

• нанесение ущерба интересам территориальной громады района;

• создание препятствий в работе районного совета и его исполнительного аппарата». (Распоряжение председателя Нижнегорского районного совета №12 от 20 июня 2011 года «Перечень сведений, составляющих служебную

информацию в Нижнегорском районном совете и его исполнительном аппарате»).

Выделение данных критериев отнесения информации к информации ограниченного доступа, на наш взгляд, достаточно полно отражает основные требования, которые должны предъявляться к информации, относящейся к служебной тайне. Безусловно, и эти критерии небезупречны. Так, к примеру, вопросы возникают относительно критерия возможных негативных последствий. На наш взгляд, эта группа критериев носит весьма оценочный характер, что может привести к злоупотреблениям при ограничении доступа к сведениям.

Однако необходимо закрепить определенные критерии, по которым информация может быть отнесена к категории «служебная тайна» либо по аналогии с законом «О государственной тайне» установить определенные категории сведений, которые могут быть отнесены к служебной тайне. Как было сказано, это те сведения, ставшие известными государственным органам в ходе реализации властных полномочий и доступ к которым ограничен законом (конфиденциальная информация), а также сведения, относящиеся к информации внутреннего пользования, круг которой должен быть установлен федеральным законом.

Основываясь на Постановлении Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии», были приняты ряд других подзаконных актов, устанавливающих правила работы со служебной информацией ограниченного доступа[24].

В указанных нормативных актах также регламентируется порядок обращения с документами, содержащими такую информацию. Стоит отметить, что все эти документы являются однотипными. Различаются по содержанию в основном кругом должностных лиц, которые уполномочены относить служебную информацию к разряду ограниченного распространения. Кроме того, в некоторых инструкциях содержится положение, согласно которому учет документов с пометкой «ДСП» ведется совместно с другими несекретными документами, что по сути своей лишает смысла ограничение доступа к служебной тайне. Стоит, однако, отметить Приказ Министерства юстиции Российской Федерации (Минюст России) от 7 октября 2010 г. № 250, в котором достаточно детально рассмотрен порядок обращения с документами, обозначенными грифом «ДСП».

Для обозначения ограничения распространения информации инструкции предлагают использовать пометку «для служебного пользования». Однако существует вопрос, может ли эта пометка использоваться не только в государственных, но и в коммерческих организациях? В настоящее время достаточно много публикаций посвящено указанной проблеме. И на этот вопрос нет единой точки зрения. Фактически закон не запрещает использовать пометку «для служебного пользования» коммерческим организациям.

При анализе многочисленных инструкций и разъяснений обнаружился интересный документ, в котором даются инструкции[25] по общему порядку обращения с документами и другими материальными носителями информации (далее – документами), содержащими служебную информацию ограниченного распространения в организациях, учреждениях, предприятиях и т. д. То есть фактически это означает, что охрана и ограничение доступа к служебной информации применяется и в негосударственных организациях, учреждениях, предприятиях. Такое положение, в свою очередь, полностью не соответствует иным подзаконным актам. Такая проблема возникла именно из-за отсутствия четко сформулированной позиции относительно служебной тайны/служебной информации ограниченного доступа в законодательстве. Причем на него периодически встречаются ссылки в других инструкциях, хотя надо отметить, что даже реквизитов у этого документа как таковых нет. Известен только год и орган, его принявший. На наш взгляд, использование такого документа крайне нежелательно.

Любопытным является и тот факт, что обозначенные приказы министерств и служб были приняты в период с 2009 по 2011 год. На наш взгляд, это связано с тем, что на рассмотрении в Государственной Думе в то время находился проект Федерального закона «О служебной тайне», принятия которого ждали многие. Однако последнее событие к тому времени было датировано 2007 годом, законопроект был отправлен «в долгий ящик», но, так как отношения в сфере служебной тайны должны были регулироваться, органы исполнительной власти приняли вышеназванные инструкции. В дальнейшем законопроект был отклонен.

Ещё одним важным аспектом защиты информации является ответственность за её разглашение. Как отмечают исследователи, вопрос ответственности за разглашение информации в настоящее время в основном ограничивается лишь дисциплинарной[26].

Существует административная ответственность за разглашение информации с ограниченным доступом. Штраф за такое правонарушение для граждан составляет от пятисот до тысячи рублей, для должностных лиц – от четырех до пяти тысяч рублей[27].

Уголовной ответственности за разглашение служебной тайны не предусмотрено. На наш взгляд, такая ответственность (дисциплинарная и административная) не может обеспечивать в полной мере надежную защиту служебной тайны. Тем более что служебная тайна иногда становится предметом незаконного оборота. Нередко, как отметил Генеральный прокурор Российской Федерации Ю. В. Чайка, «государственные служащие "торгуют" вверенной им информацией, оказывают подконтрольным структурам содействие в получении незаконных льгот и привилегий»[28].

На наш взгляд, было бы целесообразно ввести административную ответственность в виде дисквалификации на определенный срок. При таком виде ответственности должностное лицо лишается доступа к объекту незаконных посягательств.

В некоторых исследованиях отмечалась необходимость введения уголовной ответственности за разглашение служебной тайны. Так, А. А. Дворников предлагал ввести следующие статьи в Уголовный кодекс Российской Федерации: «Статья 293.1 Разглашение либо блокирование служебной тайны. Разглашение служебной тайны, то есть умышленное деяние, направленное на сообщение информации, составляющей служебную тайну, постороннему лицу либо ее блокирование, совершенное государственным либо муниципальным служащим, а равно иным лицом, обладающим допуском к служебной тайне, если это повлекло наступление тяжких последствий».

Дополнить главу 30 УК РФ статьей 293.2, предусматривающей ответственность за неосторожное обращение с носителем служебной тайны при наличии тяжких последствий: «Статья 293.2 Нарушение правил обращения с носителем служебной тайны. Нарушение лицом, имеющим допуск к служебной тайне, установленных правил обращения с носителем служебной тайны, если это повлекло по неосторожности наступление тяжких последствий»[29].

Другой исследователь предлагает ввести в уголовный кодекс следующие нормы: «Включить в главу 32 УК РФ «Преступления против порядка управления» самостоятельную статью 320.1 «Собирание, разглашение или использование сведений, образующих служебную тайну, а равно нарушение установленных правил обращения с документами, содержащими служебную тайну» с диспозицией следующего содержания:

«1. Собирание сведений, образующих служебную тайну, в целях незаконного их разглашения либо незаконного использования, совершенное путем похищения документов, подкупа или угроз, а равно иным незаконным способом, наказывается …

2. Незаконные разглашение или использование сведений, образующих служебную тайну, если это повлекло по неосторожности наступление тяжких последствий, наказывается …

3. Нарушение установленных правил обращения с документами, содержащими служебную тайну, а равно их утрату, если это повлекло по неосторожности наступление тяжких последствий, наказывается...

Примечание:

1. Если деяния, предусмотренные ст. 320-1 УК РФ, причинили вред интересам исключительно коммерческой организации, не являющейся государственным или муниципальным предприятием, уголовное преследование осуществляется по заявлению этой организации или с ее согласия.

2. Если деяния, предусмотренные ст. 320-1 УК РФ, причинили вред интересам других организаций, а также интересам граждан, общества или государства, уголовное преследование осуществляется на общих основаниях»[30].

На наш взгляд, введение уголовной ответственности за разглашение служебной тайны излишне, так как это не будет отвечать самому смыслу правового института «служебная тайна». Однако ужесточение административной ответственности путем введения дисквалификации как меры ответственности за разглашение служебной тайны, на наш взгляд, является уместным.

В нашем государстве назрела острая необходимость в детальном регулировании института служебной тайны на уровне федерального закона. До сих пор, несмотря на то, что ст. 139 ГК РФ уже утратила силу, во многие законы не были внесены соответствующие изменения. Это порождает, в свою очередь, немало путаницы в правоприменительной практике. Кроме того, не определены базовые принципы, которые должны быть положены в основу охраны служебной тайны и в основу принятия решений об отнесении той или иной информации к категории служебной тайны.

Основываясь на проведенном исследовании, можно сделать следующие выводы:

1. Понятие «служебная тайна» является ключевым при регулировании порядка обращения со служебной информацией ограниченного доступа. Необходима унификация понятийно-категориального аппарата, что позволит избежать разночтений как в теории, так и в практике, кроме того, позволит унифицировать механизм охраны и оборота такой информации.

2. Субъектами отношений в сфере оборота и охраны являются государственные органы и должностные лица, на которые, в свою очередь, возложена обязанность по охране служебной

тайне, также даны полномочия по отнесению тех или иных сведений к служебной тайны. Однако стоит заметить, что регламентацию отношений по порядку оборота и охраны служебной тайны необходимо установить в федеральном законе, который должен стать базовым при регулировании данных отношений.

3. Объектами служебной тайны являются сведения, которые составляют так называемую «чужую» тайну – сведения конфиденциального характера, ставшие известными органам государственной власти и должностным лицам в связи с выполнением ими возложенных государственных полномочий, а также сведения, являющиеся внутренней информацией государственных органов и органов местного самоуправления, к которым относятся прежде всего внутренние информационно-аналитические системы и служебная корреспонденция, а также сведения о некоторых стратегически важных предприятиях.

4. В законодательстве крайне не урегулированы основные вопросы, касающиеся отношений в сфере служебной тайны, а именно: нет конкретных критериев, на основе которых информация может быть отнесена к категории «служебной тайны». В настоящее время существует только один общий критерий «служебная необходимость», который является оценочным и размытым, не позволяющим адекватно оценить законность отнесения той или иной информации к служебной тайне. Также не ясен порядок ее оборота и хранения. Нет установленных законом требований к порядку ее оборота, порядку хранения, как нет и требований к сроку неразглашения служебной тайны после прекращения трудовых отношений.

5. Установлена малоэффективная административная ответственность за разглашение служебной тайны. Дисциплинарная ответственность, в свою очередь, также не в силах обеспечить безопасность сведений, составляющих служебную тайну. На наш взгляд, необходимо усиление административной ответственности в части введения такой меры ответственности за разглашение информации, как дисквалификация должностного лица.

На наш взгляд, назрела острая необходимость в регулировании служебной тайны на уровне федерального закона, который разрешил бы многие противоречия, встречающиеся на практике, а также упорядочил бы деятельность государственных органов по «тотальному засекречиванию» информации и злоупотреблению таким правом. Кроме того, это повысит эффективность государственного управления, повысит информационную открытость власти и, как следствие, доверие граждан.

Литература

[1] Минбалеев А. В. Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества. Дис. … докт. юрид. наук. Челябинск, 2012. С. 79.

[2] Занина Т. М. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев // Вестник Воронежского института МВД России. 2008. № 1. С. 31.

[3] Яковец Е. Н., Смирнова И. Н. Нормативное регулирование оборота сведений, составляющих служебную тайну // Электронный ресурс, 2009.

[4] Жилинский С. Э. Предпринимательское право (правовая основа предпринимательской деятельности) // М.: НОРМА, 2001. 672.

[5] Гаврилов Э. П. К вопросу об охране коммерческой, служебной и личной тайны. Гражданско-правовые аспекты // Хозяйство и право. 2003. № 5. С. 27

[6] Салихов И. И. Информация с ограниченным доступом как объект гражданских правоотношений. Автореф. дис. … канд.юрид.наук. Казань, 2004. С. 12–13

[7] Мирских И. Ю. Коммерческая тайна как вид конфиденциальной информации: Трудоправовой и цивилистический аспекты : дис. ... канд. юрид. наук. Пермь, 2005. С. 51.

[8] Павлов И. Ю. Современные проблемы правового регулирования государственной и служебной тайны в России : автореф. дис. … канд. юрид. наук. М., 2012.

[9] Занина Т. М. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев... С. 33.

[10] Такая точка зрения высказывается на сайте фонда свободы информации. Согласно высказанной точки зрения, использование такой категории для ограничения доступа к информации является незаконным в существующей правовой обстановке и прямо нарушает право граждан на доступ к информации [электронный ресурс]. http://www.svobodainfo.org/ru/node/146

[11] Ст. 4 ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02.2009 г. № 8-ФЗ // СПС «КонсультантПлюс».

[12] Ст. 9 ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».

[13] П. 4. ст. 9 ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

[14] П.1.2. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» // СПС «КонсультантПлюс».

[15] Секрет – то, что держится в тайне, скрывается от других. См.: Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Ин-т рус. яз. им. В. В. Виноградова. 4-е изд., доп. М.: Азбуковник, 1999. 944 с.

[16] Постановление Правительства РФ от 12.12.2004 № 770 «Об утверждении типового Кодекса профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с формированием и инвестированием средств пенсионных накоплений, и Правил согласования Кодексов профессиональной этики управляющих компаний, специализированного депозитария, брокеров, осуществляющих деятельность, связанную с формированием и инвестированием средств пенсионных накоплений, с Федеральной службой по финансовым рынкам» // СПС «КонсультантПлюс».

[17] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // СПС «КонсультантПлюс».

[18] См. напр., Указание Банка России от 26.11.2004 № 1519-У «О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом и от проведения операции с денежными средствами или иным имуществом» // СПС «КонсультантПлюс»; Указание Банка России от 26.11.2004 № 1519-У «О порядке представления кредитными организациями в уполномоченный орган сведений о случаях отказа от заключения договора банковского счета (вклада) с физическим или юридическим лицом и от проведения операции с денежными средствами или иным имуществом» // СПС «КонсультантПлюс».

[19] См. ст. 31 Федерального закона от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации» // СПС «КонсультантПлюс».

[20] Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» // СПС «КонсультантПлюс».

[21] Сразу оговоримся, что проверить, являются ли эти документы действующими, не представляется возможным в силу их особого характера.

[22] Указ Губернатора Архангельской области от 25.08.2011 № 125-у «Об организации работы со служебной информацией ограниченного доступа в исполнительных органах государственной власти Архангельской области» // СПС «КонсультантПлюс»; распоряжение председателя Нижнегорского районного совета №12 от 20 июня 2011 года «Перечень сведений, составляющих служебную информацию, в Нижнегорском районном совете и его исполнительном аппарате» // СПС «КонсультантПлюс».

[23] Постановление администрации Кировской области от 18.06.1997 № 183 «Об утверждении временного перечня сведений, составляющих служебную информацию ограниченного распространения» (ред. от 08.10.1997) // СПС «КонсультантПлюс».

[24] См. инструкцию о порядке обращения со служебной информацией ограниченного распространения в Ространснадзоре, утвержденную приказом Ространснадзора от 22 декабря 2011 г. № АК-1235фс // СПС «КонсультантПлюс»; инструкцию о порядке обращения со служебной информацией ограниченного распространения в Минобрнауки России, утвержденную приказом Минобрнауки России от 30 декабря 2010 г. № 2233 // СПС «КонсультантПлюс»; Порядок обращения со служебной информацией ограниченного распространения в Росавиации и организациях, подведомственных Росавиации, утвержденный приказом Росавиации от 11 августа 2010 г. № 299 // СПС «КонсультантПлюс»; инструкцию о порядке обращения со служебной информацией ограниченного распространения в ФМБА России, утвержденную приказом ФМБА от 21 января 2009 г. № 20 // СПС «КонсультантПлюс»; Приказ Министерства юстиции Российской Федерации (Минюст России) от 7 октября 2010 г. № 250 «Об упорядочении обращения со служебной информацией ограниченного распространения в Минюсте России и его территориальных органах»// СПС «КонсультантПлюс».

[25] Инструкция о порядке обращения с документированной служебной информацией ограниченного распространения в организациях, учреждениях, предприятиях и т. д. Москва: Главгосэкспертиза России, 2000.

[26] Занина Т. М. Особенности защиты служебной тайны / Т. М. Занина, П. Н. Кораблев... С. 34.

[27] Ст.13.14 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

[28] Щит и меч. 2006 –23 нояб. (№ 44 (1060)) – С. 2

[29] Дворников А. А. Уголовно-правовая охрана государственной и служебной тайны в органах внутренних дел автореф. дис. ... к. ю. н. Тюмень, 2007. 22 с.

[30] Щадрин С. Ф. Уголовно-правовая охрана служебной тайны : автореферат дис. … канд. юрид. наук. Ростов-н/Д, 2002.

References

[1] Minbaleev A.V. Teoreticheskie osnovaniya pravovogo regulirovaniya massovykh kommunikatsii v usloviyakh razvitiya informatsionnogo obshchestva [Theoretical foundations of legal regulation of mass communications in conditions of the development of information society]. Chelyabinsk, 2012. p. 79.

[2] Zanina T.M. Osobennosti zashchity sluzhebnoi tainy [Peculiarities of judicial secrecy]// Vestnik Voronezhskogo instituta MVD Rossii. 2008. No. 1. p. 31.

[3] Yakovets E.N., Smirnova I.N. Normativnoe regulirovanie oborota svedenii, sostavlyayushchikh sluzhebnuyu tainu [Legal regulation of circulation of information which comprises official secrecy]// Electronic resource, 2009.

[4] Zhilinskii S. E. Predprinimatel'skoe pravo (pravovaya osnova predprinimatel'skoi deyatel'nosti) [Entrepreneurial law]// Moscow: Izdatel'stvo NORMA, 2001. 672 p.

[5] Gavrilov E.P. K voprosu ob okhrane kommercheskoi, sluzhebnoi i lichnoi tainy. Grazhdansko-pravovye aspekty [To the question of protection of commercial, official, and personal secrets]// Khozyaistvo i pravo. 2003. No. 5. p. 27

[6] Salikhov I.I. Informatsiya s ogranichennym dostupom kak ob»ekt grazhdanskikh pravootnoshenii [Information with restricted access as an object of civil law relations]. Kazan, 2004. p. 12-13

[7] Mirskikh I. Yu. Kommercheskaya taina kak vid konfidentsial'noi informatsii: Trudopravovoi i tsivilisticheskii aspekty [Commercial secret as a type of confidential information: Labour, legal, and civil aspects]. Perm, 2005. p. 51.

[8] Pavlov I. Yu. Sovremennye problemy pravovogo regulirovaniya gosudarstvennoi i sluzhebnoi tainy v Rossii [Modern problems of legal regulation of state and official secrets in Russia]. Moscow, 2012.

[9] Zanina T.M. Osobennosti zashchity sluzhebnoi tainy [Peculiar features of official secret]. p. 33

[10] Such point of view is expressed on the website of the fund of information freedom. According to this point of view the use of such category for restriction of the access is illegal in current legal surroundings and violates the rights of the citizens for the access to the information [Electronic resource]. http://www.svobodainfo.org/ru/node/146

[11] Art. 4, Federal Law «On provision of the access to the information on the activities of local government bodies» as of 09.02.2009 No. 8-FZ // SPS «Konsul'tantPlyus».

[12] Art. 9, Federal law «On information, information technologies and information security» as of July 27, 2006 No. 149-FZ // SPS «Konsul'tantPlyus».

[13] Provision 4, Art. 9, Federal Law as of 27.07.2006 No. 149-FZ «On information, information technologies and information security» // SPS «Konsul'tantPlyus».

[14] Provisions.1.2. Resolution of the Russian Federation as of November 3, 1994 No. 1233 «On confirmation of Provision on access to official information of restricted circulation in federal bodies of executive power and appointed administration bodies in charge of control of the use of nuclear energy» // SPS «Konsul'tantPlyus».

[15] A secret is what is held confidential and hidden from others. Ozhegov S. I., Shvedova N. Yu. Tolkovyi slovar' russkogo yazyka: 80 000 slov i frazeologicheskikh vyrazhenii [Russian thesaurus: 80 000 words and phraseological units]/ Rossiiskaya akademiya nauk. Institut russkogo yazyka im. V. V. Vinogradova. 4-e izd., dopolnennoe [Russian Academy of Science. V.V. Vinogradov Institute of the Russian Language. 4th revised edition]. Moscow: Azbukovnik, 1999. 944 p.

[16] Resolution of the Government of the Russian Federation as of 12.12.2004 No. 770 «On the establishment of a standard code of professional ethics of management companies, specialized depositary, brokers conducting activities connected with formation and investment of pension assets, as well as standard conformance rules for codes of professional ethics of management companies, specialized depositary, brokers conducting activities connected with formation and investment of pension assets and Federal Service for Financial Markets » // SPS «Konsul'tantPlyus».

[17] Presidential decree of the Russian Federation as of 06.03.1997 No. 188 «On the establishment of a list of information of confidential nature» // SPS «Konsul'tantPlyus».

[18] Instruction of the Bank of Russia as of 26.11.2004 No. 1519-U «On procedures for provision of information on refusals to conclude the agreement on opening a bank account with an individual person or legal body, as well as on refusals to conduct operations with monetary funds or other properties» // SPS

«Konsul'tantPlyus»; Instruction of the Bank of Russia as of 26.11.2004 No. 1519-U «On procedures for provision of information on refusals to conclude the agreement on opening a bank account with an individual person or legal body, as well as on refusals to conduct operations with monetary funds or other properties» // SPS «Konsul'tantPlyus».

[19] Art. 31 of the Federal Law as of 23.12.2003 No. 177-FZ «On insurance of bank deposits of physical persons in Russian Federation» // SPS «Konsul'tantPlyus».

[20] Federal law as of 13.03.2006 No. 38-FZ «On advertising» // SPS «Konsul'tantPlyus».

[21] We specify in advance that it is impossible to check whether the documents are valid or not under their specific features.

[22] Decree of the Governor of Arkhangelsk Region as of 25.08.2011 No. 125-u «On operations with official information of restricted access in executive bodies of the state government of Arkhangelsk Region» // SPS «Konsul'tantPlyus»; Decree of the chairman of Nizhnegorskii District Soviet No. 12 as of June 20, 2011 «Official information in Nizhnegorskii District Soviet and its authorities» // SPS «Konsul'tantPlyus».

[23] Resolution of the administration of Kirov Region as of 18.06.1997 No. 183 «On establishment of temporary list of official information of restricted access» (edited 08.10.1997) // SPS «Konsul'tantPlyus».

[24] Instruction on access to official information of restricted distribution in Rostransnadzor established by the Order of Rostransnadzor as of December 22, 2011 No. AK-1235fs // SPS «Konsul'tantPlyus»; Instruction on access to official information of restricted distribution in Ministry of Education and Science established by the Order of Ministry of Education and Science as of December 30, 2010 No. 2233 // SPS «Konsul'tantPlyus»; Procedures of accessing official information of restricted distribution in Rosaviatsia and organizations subordinate to it established by the Order of Rosaviatsia as of August 11, 2010 No. 299 // SPS «Konsul'tantPlyus»; Instruction on access to official information of restricted distribution in Federal Medical and Biological Agency established by the Order of Federal Medical and Biological Agency of Russia as of January 21, 2009 No. 20 // SPS «Konsul'tantPlyus»; Order of the Ministry of Justice of the Russian Federation as of October 7, 2010 No. 250 , Moscow «On regulation of the official information handling procedures in the Ministry of Justice of the Russian Federation and its territorial bodies»// SPS «Konsul'tantPlyus».

[25] Instruction on official information handling procedures in organizations, institutiona, enterprises, etc. Moscow, 2000, Glavgosekspertiza Rossii.

[26] Zanina T.M. Osobennosti zashchity sluzhebnoi tainy [Peculiarities of protection of official secrets]/ T.M. Zanina, P.N. Korablev. p. 34.

[27] Art.13.14 of the Administrative Offences Code as of December 30, 2001 No. 195-FZ

[28] Shchit i mech [Dome and dart]. November 23, 2006 (No. 44 (1060)) – p. 2

[29] Dvornikov A.A. Ugolovno-pravovaya okhrana gosudarstvennoi i sluzhebnoi tainy v organakh vnutrennikh del [Criminal and legal protection of state and official secrets in bodies of internal affairs]. Tyumen, 2007. 22 p.

[30] Shchadrin S.F. Ugolovno-pravovaya okhrana sluzhebnoi tainy [Criminal and legal protection of official secrets]. Rostov-on-Don, 2002.

Пономарева Юлия Владимировна, аспирант кафедры конституционного и административного права ЮУрГУ. E-mail: julia.ponomareva17@mail.ru.

Ponomareva Julia, postgraduate Department of Constitutional and Administrative Law SUSU. E-mail: julia.ponomareva17@mail.ru

УДК 349.2:[002:004] + 34.03:[002:004.056]
ББК Х 405.11 + Х 401.114:Х 405.11

У. М. Станскова

ЛОКАЛЬНОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ТРУДОВЫХ ОТНОШЕНИЯХ

В статье рассматриваются вопросы, связанные с принятием работодателем локальных нормативных актов, регулирующих права и обязанности работников по обеспечению конфиденциальности. Определены требования законодательства к содержанию локальных нормативных актов в данной сфере. Устанавливаются способы их принятия, исследуются проблемы, связанные с ознакомлением работников с локальными нормативными актами, обеспечивающими режим конфиденциальности. Предлагается конкретизировать порядок регламентации мер по защите персональных данных, принимаемых совместно работниками, работодателями и их представителями.

Ключевые слова: *конфиденциальность, информация ограниченного доступа, трудовые отношения, локальные нормативные акты работодателя, коммерческая тайна, персональные данные.*

U. M. Stanskova

LOCAL REGULATION OF INFORMATION WITH RESTRICTED ACCESS IN LABOR RELATIONS

The article discusses issues related to the adoption of the employer of local regulations governing the rights and obligations of employees to ensure confidentiality. Defined legal requirements to the content of local normative acts in this area. Established ways of their decision, explores the problems associated with familiarization employeeswith local normative acts ensuring confidentiality. It is proposed to specify the procedure for regulation measures to protect personal data, taken together workers, employers and their representatives.

Keywords: *confidentiality, restricted access information, labor relations, local normative acts of the employer, trade secrets, personal data.*

Локальные нормативные акты являются эффективным инструментом, средством установления субъективных прав, обязанностей, льгот, запретов, поощрений и наказаний, связанных с информацией ограниченного доступа (далее – ИОД) в трудовых правоотношениях. Однако законодатель не всегда регламентирует вид, содержание и порядок принятия локальных нормативных актов в данной сфере, в то время как именно посредством принятия локальных нормативных актов регламентируются практически все меры в составе режима ИОД.

В Трудовом кодексе Российской Федерации (далее – ТК РФ) данные локальные нормативные акты не обозначены в качестве обяза-

тельных, поэтому их принятие зависит от усмотрения обладателя ИОД.

В то же время указание на существование локальных нормативных актов по защите ИОД содержит: 1) абз. 4 ст. 88 ТК РФ – работодатель должен осуществлять передачу персональных данных работника в соответствии с локальным нормативным актом; 2) п. 2 части первой ст. 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»[1] – оператор обязан издавать локальные акты по вопросам обработки персональных данных и локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и устранение последствий таких нарушений. Названные требования свидетельствуют о необходимости принятия локальных нормативных актов в отношении персональных данных. При осуществлении работодателем передачи персональных данных обязательно наличие локального акта об их передаче. Соответственно, должны быть приняты локальные нормативные акты, регламентирующие передачу персональных данных, их обработку работодателем, а также регламентирующие предотвращение и выявление нарушений законодательства. Возможно закрепление названных требований в едином локальном нормативном акте.

В некоторых случаях требуется: 1) принять ряд документов (типовое обязательство, типовая форма согласия), утвердить должностную инструкцию ответственного за организацию обработки персональных данных (Постановление Правительства РФ от 21.03.2012 г. № 211[2]); 2) ознакомить работников с документами, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области (п. 8 ст. 86 Трудового кодекса РФ[3]); 3) разработать и утвердить порядок доступа к инсайдерской информации (ст. 11 Федерального закона от 27.07.2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»[4]); 4) установить порядок обращения с коммерческой тайной и контроля его соблюдения, ознакомить работников под расписку с установленным режимом коммерческой тайны (ст. 10 Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»[5]). Такого рода требования могут быть реализованы работодателем только с помощью системы локальных нормативных актов, а термин «документы» может подразумевать и локальные нормативные акты.

Акты, которые не поименованы в ТК РФ и других нормативных актах, могут быть приняты для эффективного управления, для реализации правомочий работодателя, повышения гарантий прав работников. В них могут быть определены условия, порядок доступа, конфиденциального делопроизводства, обучения работе с ИОД, дополнительные выплаты, порядок осуществления контроля соблюдения режима ИОД и учета лиц, получающих доступ, закреплен перечень сведений и т. д.

Разработка перечня сведений является обязательным этапом для некоторых видов ИОД, в частности, для коммерческой тайны. Такой перечень может закрепляться в локальном нормативном акте. Анализ нормативных правовых актов позволяет выделить способы определения таких перечней: 1) закрепление перечня в нормативном порядке для государственной тайны или казуистическое перечисление в федеральных законах состава профессиональных и некоторых служебных тайн; 2) смешанный порядок закрепления: например, состав инсайдерской информации определяется нормативным правовым актом и перечнем, утвержденным самим инсайдером (ст. 3 Закона об инсайдерской информации).

Представляется спорным рассмотрение перечня сведений, составляющих коммерческую (служебную) тайну, в качестве приложения к трудовому договору[6]. В случае принятия перечня как локального нормативного акта он имеет иную природу, отличную от приложения к трудовому договору. Согласно ст. 57 ТК РФ приложения и отдельные письменные соглашения к трудовому договору составляют неотъемлемую часть трудового договора, а, следовательно, являются индивидуальными актами. Локальные нормативные акты в отличие от индивидуальных договоров распространяют свое действие на неопределенный круг лиц и принимаются работодателем в пределах его компетенции. Профессор А. М. Куренной указывает на недопустимость включения в трудовой договор конкретных пунктов из положений о тайне в связи с необходимостью выдачи экземпляра трудового договора на руки работнику[7]. Ска-

занное подтверждает недопустимость закрепления перечня как условия трудового договора.

Отсутствуют нормативные требования относительно локального регулирования профессиональной, служебной тайны и другой ИОД, не отнесенной к охраняемой законом тайне, хотя требования Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»[8] об обязательном принятии мер по защите информации и обеспечении ее конфиденциальности являются общими для любых видов ИОД. Не предусмотрено закрепления перечня сведений других видов ИОД, поэтому их состав также может быть определен в локальном порядке. Если состав ИОД не установлен нормативно, то отсутствие локально закрепленных перечней нарушает весь механизм ИОД: не определены сведения, составляющие ИОД, не введены ограничения на их распространение, следовательно, нет режима, нет ответственности. Поэтому если работодатель желает установить режим ИОД, то ему необходимо определить и закрепить перечень соответствующих сведений (кроме профессиональной и государственной тайны). Возможность самостоятельного определения перечня иных видов ИОД в локальном порядке обеспечивает интересы работодателя. В локальных нормативных актах по охране ИОД работодатель вправе в пределах действующих норм уточнять и конкретизировать их применительно к требованиям своей производственной среды. Возникает вопрос о возможности закрепления в таких актах процедуры определения пригодности работника для работ с ИОД. По этому вопросу мы солидарны с Е. А. Ершовой в том, что самостоятельное восполнение работодателем пробелов в трудовом праве в случаях, не предусмотренных законодателем, может иметь место только с целью принятия работодателем актов, улучшающих права работников[9]. Работодатель не должен выходить за рамки запрета ухудшения положения работника. Локальное нормотворчество, будучи делегированным, допускается только в пределах, установленных законодательством, и имеет своей целью его конкретизацию[10].

В связи с отсутствием требования о способе принятия рассматриваемых локальных нормативных актов они принимаются самим работодателем, если иной порядок не закреплен в коллективном договоре, соглашении. В связи с чем интерес представляет требование п. 10 ст. 86 ТК РФ о совместной выработке мер по защите персональных данных работников работодателями, работниками и их представителями. Названное требование направлено на соблюдение прав и законных интересов работников – субъектов персональных данных. Однако данная норма не может быть рассмотрена как обязанность работодателя принять локальные нормативные акты о персональных данных совместно или с учетом мнения с представителями работников. Профессоры А. М. Лушников и М. В. Лушникова указывают, что принять такой локальный нормативный акт лучше с учетом мнения выборного органа первичной профсоюзной организации о защите персональных данных работника[11]. Но при отсутствии соответствующего нормативного требования учет мнения остается правом работодателя. Соответственно, норма п.10 ст. 86 ТК РФ может быть обеспечена требованием о принятии локального нормативного акта о персональных данных работников с учетом мнения их представительного органа только в случае установления такой обязанности в ТК РФ. Вместе с этим, принятие локального акта не исчерпывает все возможные меры охраны персональных данных. Поэтому п. 10 ст. 86 ТК РФ может быть дополнен следующим уточнением: работодатели, работники и их представители совместно вырабатывают меры охраны персональных данных работников, предусмотренные коллективным договором, соглашением. В отношении локальных нормативных актов по вопросам защиты ИОД может быть сохранена возможность их единоличного принятия.

Работодатель – физическое лицо, не являющийся индивидуальным предпринимателем, лишен права принимать локальные нормативные акты. Требование об обеспечении конфиденциальности сведений о частной жизни работодателя, его личных и семейных тайн, персональных данных могут быть включены в трудовые договоры с работниками в качестве условия, существенного для сторон (ч. 2 ст. 303 ТК РФ). В сфере применения труда данным работодателем наличие коммерческой тайны маловероятно. Однако при ее наличии должны быть сделаны исключения из перечня мер по установлению режима коммерческой тайны (ст. 10, 11 Закона о коммерческой тайне), обусловленные особенностя-

ми правового статуса данного работодателя. Поэтому для таких работодателей режим ИОД предполагает закрепление ограничительных условий в трудовом договоре, определение в нем сведений, не подлежащих разглашению, ознакомление работника с мерами ответственности и создание условий для обеспечения конфиденциальности.

Одним из обязательных действий работодателя является ознакомление с локальными нормативными актами работников до подписания трудового договора (ч. 3 ст. 68 ТК РФ). Однако данное требование может повлечь ознакомление с ИОД лиц, которые в данный момент времени не являются работниками и могут не вступить в трудовые отношения, ознакомившись с ИОД. Выход видится в ознакомлении таких лиц только с документами, не содержащими ИОД, ознакомление с другими документами (например, перечнем) может происходить только после подписания трудового договора или после истечения испытательного срока.

Достаточно спорной представляется формулировка, предусмотренная в п. 6 части первой ст. 18. 1 Закона о персональных данных. В ней указывается на ознакомление работников оператора с локальными нормативными актами по вопросам обработки персональных данных и (или) обучение указанных работников. Использование разделительного союза «или» предполагает вместо ознакомления работников с локальными актами проведение обучения работников. Однако замена одной процедуры другой недопустима, так как работники не обязаны соблюдать локальные нормативные акты, с которыми они не ознакомлены под роспись. Поэтому возможно только сочетание ознакомления с обучением и использование соединительного союза «и». Более того, обучение работников работе с информацией ограниченного доступа должно закрепляться в качестве обязательной меры, направленной на обеспечение режима конфиденциальности. ТК РФ предусматривает требования по обеспечению работнику условий для соблюдения работниками дисциплины труда, по созданию надлежащих условий для хранения имущества (ст. 189, 239 ТК РФ).Соблюдение требований локальных нормативных актов в отношении персональных данных и других видов ИОД также должно обеспечиваться созданием работнику необходимых условий для соблюдения режима, в том числе, посредством обучения работника работе с ИОД. Обучение в данной ситуации преследует цель – обеспечить знание работниками своих обязанностей и нормативных требований в отношении ИОД, и, в конечном счете,направлено на защиту ИОД от противоправных посягательств и предотвращение нарушений установленного режима. Перечисленные действия создают правовые условия для обеспечения сочетания интересов личности и общества, а также направлены на воспитание работника. Поэтому в локальных нормативных актах может быть регламентирован порядок обучения работников в отношении ИОД.

В Законе РФ от 21.07.1993 г. № 5485-1 «О государственной тайне»[12] отсутствует обязанность ознакомить работника с перечнем сведений, составляющих государственную тайну. Необходимость такого требования вытекает из аналогичных правил в составе режима коммерческой тайны, а также требования ТК РФ об ознакомлении работника со всеми локальными актами, имеющими отношение к его трудовой функции. Для соблюдения своих обязанностей в отношении государственной тайны знание, о каких сведениях идет речь, является обязательным. Поэтому следует закрепить обязанность ознакомить с перечнем сведений, составляющих государственную тайну.

Не исключена регламентация режима ИОД в коллективном договоре, соглашении, которые могут содержать взаимные информационные обязательства сторон, а также реализовать требования п. 10 ст. 86 ТК РФ.

Таким образом, принятие локальных нормативных актов, регламентирующих права и обязанности в отношении информации ограниченного доступа, осуществляется работодателем самостоятельно, без участия представительного органа работников. Их принятие следует рассматривать как отправную точку в установлении режима конфиденциальности. При этом следует конкретизировать порядок регламентации мер по защите персональных данных, принимаемых совместно работниками, работодателями и их представителями, а также внести изменения и дополнения в федеральные законы, регламентирующие обеспечение защиты информации ограниченного доступа.

Литература

[1] Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451 (далее – Закон о персональных данных).

[2] Постановление Правительства РФ от 21.03.2012 г. № 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» // Собрание законодательства РФ. 2012. № 14. Ст. 1626.

[3] Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ // Собрание законодательства РФ. 2002. № 1 (ч.1). Ст. 3 (далее – ТК РФ).

[4] Российская газета. 2010. № 168. 30 июля (далее – Закон об инсайдерской информации).

[5] Собрание законодательства РФ. 2004. № 32. Ст. 3283 (далее – Закон о коммерческой тайне).

[6] См.: Бондаренко Э. Н. Трудовой договор как основание возникновения правоотношения. СПб.: Юридический центр Пресс, 2004. С. 46.

[7] См.: Куренной А. М. Трудовой мастер-класс… // Трудовое право. 2011. № 4. С. 14.

[8] Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[9] Ершова Е. А. Нормативные правовые акты работодателя, содержащие нормы трудового права // Трудовое право. 2009. № 1. С. 65.

[10] Драчук М. А. О роли, видах, содержании и сущности локальных нормативных актов в структуре юридического механизма управления работниками // Российский ежегодник трудового права. 2008. № 4. С. 85.

[11] Лушников А. М., Лушникова М. В. Курс трудового права. Т. 1. М., 2009. С. 867.

[12] Собрание законодательства РФ. 1997. № 41. Ст. 8220–8235.

References

[1] Sobranie zakonodatel'stva RF. 2006. No. 31 (Part 1). Art. 3451. (hereafter – Law on personal data).

[2] Resolution of the Government of the Russian Federation as of 21.03. 2012 No. 211 'On the establishment of measures aimed at ensuring performance of duties provided by the Federal Law 'On personal data' and statutory acts by state or municipal bodies'// Sobranie zakonodatel'stva RF. 2012. No. 14. Art. 1626.

[3] Labour Code of the Russian Federation as of 30.12.2001 No. 197-FZ // Sobranie zakonodatel'stva RF. 2002. No. 1 (Part1). Art. 3 (hereafter – LC RF).

[4] Rossiiskaya gazeta. 2010. No. 168. July 30. (hereafter – Law on insider information)

[5] Sobranie zakonodatel'stva RF. 2004. № 32. St. 3283. (dalee – Zakon o kommercheskoi taine)

[6] Bondarenko E.N. Trudovoi dogovor kak osnovanie vozniknoveniya pravootnosheniya [Employment agreement as a basis for legal relations]. SPb.: Izdatel'stvo «Yuridicheskii tsentr Press», 2004. p. 46.

[7] Kurennoi A.M. Trudovoi master-klass [Labour master class]// Trudovoe pravo. 2011. No. 4. p. 14.

[8] Sobranie zakonodatel'stva RF. 2006. No.31 (Part 1). Art. 3448.

[9] Ershova E.A. Normativnye pravovye akty rabotodatelya, soderzhashchie normy trudovogo prava [Statutory acts of an employer encompassing labour legal provisions]// Trudovoe pravo. 2009. No. 1. p.65.

[10] Drachuk M.A. O roli, vidakh, soderzhanii i sushchnosti lokal'nykh normativnykh aktov v strukture yuridicheskogo mekhanizma upravleniya rabotnikami [On the role, types, purview, and essence of local statutory acts in the structure of legal mechanism of personnel management]// Rossiiskii ezhegodnik trudovogo prava. 2008. No. 4. p.85.

[11] Lushnikov A.M., Lushnikova M.V. Kurs trudovogo prava [Course of labour law]. V. 1. Moscow, 2009. p. 867.

[12] Sobranie zakonodatel'stva RF. 1997. No. 41. Art. 8220-8235.

Станскова Ульяна Михайловна, старший преподаватель кафедры Трудового и социального права Южно-Уральского государственного университета. E-mail: uljana-st@yandex.ru

Uliana Mikhailovna Stanskova, senior lecturer and teacher of the Department of Labour and Social Law of South Ural State University. E-mail: uljana-st@yandex.ru

УДК 002:004.056.57 + 34.03:002.6
ББК Х 401.114

В. С. Ханова

АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОЙ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ В РОССИИ

В статье автором рассматриваются актуальные вопросы защиты коммерческой тайны. Делается вывод, что меры по защите коммерческой тайны, установленные Федеральным законом «О коммерческой тайне», в совокупности применяются крайне редко, а значит ставится под сомнение охраноспособность соответствующей информации. Данная неопределенность служит интересам лиц, неправомерно завладевших конфиденциальной информацией и использующих ее. Поэтому целесообразно внести изменения в законодтаельство, исключающие возможность требовать от участников гражданского оборота принятия всех без исключения мер, которые перечислены в Федеральном законе «О коммерческой тайне».

Ключевые слова: *информация ограниченного доступа, коммерческая тайна, секреты производства, защита.*

V. S. Khanova

TOPICAL ISSUES OF LEGAL PROTECTION OF TRADE SECRETS IN RUSSIA

In this article the author discusses current issues of commercial confidentiality. It is concluded that the protection of trade secrets, established by the Federal Law "On Commercial Secrets" in the aggregate are used very rarely, and therefore questioned patentability relevant information. This uncertainty is in the interest of persons wrongfully themselves the owners of confidential information and using it . Therefore it is expedient to amend the law to exclude the possibility of demand from participants in civil adoption of all measures , without exception , are listed in the Federal Law "On Commercial Secrets".

Keywords: *restricted access information , trade secrets , trade secrets , protection.*

Закрепление в Конституции Российской Федерации гарантий, обеспечивающих реализацию прав и свобод личности, и последующее развитие соответствующих конституционных положений в федеральном и региональном отраслевом законодательстве положили начало новому этапу развития правового государства в России.

Интенсивное развитие гражданско-правовых институтов частной собственности и нематериальных благ обусловили необходимость должного нормативно-правового регулирования таких гражданско-правовых институтов, как коммерческая, профессиональная, служебная, банковская тайна, тайна связи, защита персональных данных и ряда дру-

гих сведений ограниченного распространения.

Применение ряда норм о коммерческой тайне на практике сегодня вызывает ряд вопросов и сложностей. Рассмотрим некоторые из них.

В соответствии со ст. 126 Федерального закона от 26 октября 2002 г. № 127-ФЗ «О несостоятельности (банкротстве)»[1] (далее – Закон) при открытии конкурсного производства наступают определенные правовые последствия, при одном из которых сведения о финансовом состоянии должника уже не относятся к категории сведений, носящих конфиденциальный характер либо являющихся коммерческой тайной.

В действующем законодательстве России отсутствует единое понятие конфиденциальной информации, равно как и четкое определение ее структурного состава, что вызывает трудности в правоприменительной практике. Следует отметить и проблему, связанную с употреблением Законом термина «коммерческая тайна» – на наш взгляд, не слишком удачным – из его формулировки может возникнуть ощущение о прекращении режима коммерческой тайны с момента открытия конкурсного производства.

В соответствии с п. 2 ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в зависимости от категории доступа информация подразделяется на общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (так называемая информация ограниченного доступа).

Специального закона, который устанавливал бы подобного рода ограничения, не существует, а нормы, регулирующие ограничения в отношении отдельных категорий сведений, включены в различные федеральные законы и даже подзаконные нормативные правовые акты, и естественно, не все из них касаются в содержательном плане финансового состояния субъектов права. Именно поэтому применение нормы ст. 126 Закона на практике и вызывает известные затруднения.

Таким образом, вопрос о сведениях, носящих конфиденциальный характер и перестающих быть таковыми с открытием конкурсного производства, нуждается в уточнении.

На наш взгляд, наиболее близкой по характеру сведений, относимых к конфиденциальным, будет в данном случае выступать информация, находящаяся в режиме:

1) налоговой тайны (ст. 102 Налогового кодекса РФ[2]);

2) аудиторской тайны (ст. 9 Федерального закона от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности»)[3];

3) банковской тайны (ст. 26 Федерального закона 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»)[4];

4) тайны страхования (ст. 946 Гражданского кодекса РФ).

Подобная позиция находит свое выражение в арбитражной практике (Постановление ФАС Дальневосточного округа от 10 декабря 2010 г. № Ф03-8647/2010[5]).

Следует заметить, что порядок отнесения информации к конфиденциальной и виды конфиденциальной информации установлены также Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»[6] (далее – Указ), однако ни один из составов этих сведений (персональные данные, тайна следствия и судопроизводства, служебная тайна, профессиональная тайна, коммерческая тайна, сведения о сущности некоторых объектов промышленной собственности), за исключением сведений, находящихся в режиме коммерческой тайны, не подпадает под критерий сведений финансового характера и не представляет интереса в контексте рассматриваемой проблемы.

Таким образом, коммерческая тайна является одним из видов конфиденциальной информации. Указ определяет ее как «сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами». Данное определение имеет отсылочный характер. Центральное место среди правовых источников, определяющих статус коммерческой тайны, занимает Гражданский кодекс РФ. В соответствии со ст. 139 ГК РФ информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности[7].

Следует заметить, что в Федеральном законе от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» используется несколько иной подход – законодатель разделяет понятия «коммерческая тайна» и «информация, составляющая коммерческую тайну».

Так, в соответствии с п. 1 ст. 3 данного закона коммерческая тайна представляет собой режим конфиденциальной информации, позволяющий ее обладателю при соответствующих или возможных обстоятельствах увеличить доходы, избежать неоправданных

расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

При этом информацией, составляющей коммерческую тайну (секретом производства), признаются сведения любого характера (производственные, технические, экономические, организационные и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. В свою очередь, под режимом коммерческой тайны понимаются введенные правообладателем меры по охране конфиденциальности такой информации.

Представляется, что разделение понятий «коммерческая тайна» и «информация, составляющая коммерческую тайну» носит искусственный характер и не может считаться полезным с точки зрения практического применения. Кроме того, подобный подход противоречит ст. 139 ГК РФ. В юридической литературе по данному вопросу в подавляющем большинстве случаев используется именно термин «коммерческая тайна», иными словами, эти два термина используются не иначе как синонимы[8].

Итак, коммерческая тайна в гражданско-правовом смысле – это информация, имеющая реальную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и принятии обладателем мер к охране ее конфиденциальности.

Подобная информация является охраноспособной с точки зрения гражданского права, объем ее охраны определяется законом или договором. Открытие конкурсного производства на режим такой информации не влияет и в случае ее разглашения обязанность возместить убытки ложится на лиц, незаконными методами получивших информацию, работников, нарушивших соответствующие запреты трудового договора (контракта), контрагентов, сделавших это вопреки гражданско-правовому договору.

После открытия же конкурсного производства перестают относиться к числу конфиденциальных исключительно сведения, касающиеся финансового состояния должника, и таким образом, исключительно только такие сведения утрачивают режим коммерческой тайны. Примечательно, что Федеральный закон от 8 января 1998 г. № 6-ФЗ «О несостоятельности (банкротстве)» предусматривал, что именно на этапе конкурсного производства осуществляется первая публикация, из которой можно сделать вывод об испытываемых должником финансовых сложностях (ранее любая информация о конкурсе не подлежала разглашению). В соответствии же с Федеральным законом от 26 октября 2002 г. № 127-ФЗ «О несостоятельности (банкротстве)» публикуются все сообщения о конкурсном процессе в отношении должника.

При определении сведений, находящихся в режиме коммерческой тайны и касающихся финансового состояния должника, следует ориентироваться на локальный их перечень, который, как правило, содержится в положениях по защите сведений конфиденциального характера, утверждаемых руководителем организации-должника.

Однако на практике зачастую такой перечень отсутствует либо является «юридически примитивным», так как отличается «последовательной» неполнотой. На наш взгляд, ввиду изложенного следует согласиться с мнением В. И. Кайнова о целесообразности закрепления в законе примерного перечня сведений, относящихся к коммерческой тайне, которые с открытием конкурсного производства перестают быть таковыми[9].

В хозяйственной деятельности практически любого субъекта предпринимательских отношений существует необходимость сохранить определенного рода информацию в тайне. Поэтому адекватное регулирование общественных отношений в данной сфере является крайне важным. Через несколько лет после принятия Федерального закона от 29 июля 2004 г. «О коммерческой тайне» (далее — Закон о коммерческой тайне) вступила в силу четвертая часть ГК РФ, где вопросам информации, составляющей коммерческую тайну (ноу-хау, или секрету производства), посвящена отдельная глава 75. Однако, к сожалению, действующее законодательство, регулирующее отношения, связанные с ноу-хау, больше вызывает вопросы, чем дает ответы. Неудивительно, что и арбитражную практику в этой сфере сложно назвать сложившейся.

Между тем проблемы ноу-хау остались практически без внимания как в Постановлении Пленумов Верховного Суда и Высшего Арбитражного Суда РФ № 5/29 от 26 марта 2009 г.[10], так и в Концепции развития гражданского законодательства об интеллектуальной собственности[11]. Однако многие вопросы требуют самого пристального рассмотрения. Остановимся на перечисленных в законе

признаках информации, составляющей коммерческую тайну.

Основной признак данной информации, упоминаемый в законе, — ее неизвестность третьим лицам. Он тесно связан с другим — отсутствием свободного доступа к сведениям на законном основании. Действительно, если сведения общедоступны, нередко они являются и общеизвестными. В европейском законодательстве и международных договорах эти два признака вместе определяются как секретность сведений.

Ст. 39 Соглашения по торговым аспектам прав интеллектуальной собственности от 1995 г. (далее – ТРИПС) определяет, что секретной признается такая информация, которая в целом или в точной форме и совокупности составляющих ее частей не является известной вообще или легкодоступной для лиц, принадлежащих к кругам, которые обычно имеют отношение к данному виду информации.

Аналогичное определение содержится в Регламенте № 772/2004[12], принятом Европейской комиссией (далее — регламент Европейской комиссии), в ст. 1 которого под секретностью информации, составляющей ноу-хау, понимается ее необщеизвестность и отсутствие легкого доступа.

Как следует из положений, содержащихся в ТРИПС, группа лиц, которым информация не должна быть известной, ограничена кругом специалистов в определенной области. Подобный подход представляется оправданным, поскольку общеизвестность важна именно среди тех, кто использует данные сведения, и нет необходимости доказывать, что последние не являются общеизвестными для других специалистов. Аналогичный подход имеет смысл применять и при толковании российского закона, даже без прямого указания в нем на определенный круг лиц.

В то же время предоставление конфиденциальной информации ограниченному кругу лиц, например уполномоченным государственным органам в случаях, предусмотренных законодательством, или своим работникам, само по себе не превращает ее в общеизвестную.

Рассматриваемые определения говорят не только об известности, но и о доступности указанной информации. Иногда данные понятия отождествляются. Так, при пересмотре дела суд отметил следующее: «при рассмотрении дела в суде первой инстанции ответчиком были предоставлены доказательства того, что идея ... была известна до подписания Соглашения. Данное утверждение подтверждается положениями опубликованного патента из краткого описания к запатентованному изобретению»[13]. Однако следует признать: тот факт, что информация является общедоступной, еще не свидетельствует о том, что она общеизвестна. В то же время любые общеизвестные сведения признаются законодателем общедоступными. Так, согласно ст. 7 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Другой вопрос, который возникает при анализе российского законодательства, связан с понятием «свободный доступ» к информации, определением границ этой «свободы» и того, в чем конкретно она должна заключаться.

Необходимо обратить внимание на отсутствие в российском законодательстве прямого указания на то, что свободный доступ имеет место только в том случае, если он является «легким». В связи с этим может создаться впечатление, что если теоретически информацию получить можно, например, путем анализа продукции ее обладателя, то свободный доступ к ней есть и она не может считаться составляющей коммерческую тайну.

Несомненно, критерий отсутствия именно «легкого» доступа должен применяться и при толковании российского закона. Так, например, если информацию можно найти в опубликованных материалах, доступных в национальных библиотеках страны, где обладатель хочет получить охрану, или в сети Интернет, то, несомненно, легкий доступ к ней есть. Однако едва ли можно говорить о нем, например, для российского специалиста, если сведения опубликованы в зарубежных изданиях, которые недоступны в России.

Еще более интересной является ситуация, когда информацию получить можно, но для этого продукция конкурента, пусть даже свободно обращающаяся на рынке, требует лабораторных исследований, которые теоретически могут быть проведены. Представляется, что такие сведения нельзя считать находящимися в свободном доступе, прежде всего потому, что он не является «легким».

Как справедливо отмечается в литературе со ссылкой на практику американских судов, не может признаваться общеизвестной та информация, которая хотя потенциально и может быть раскрыта специалистом в данной сфере деятельности, но фактически требует долговременных, сложных или дорогостоящих исследований, которые по своему характеру могут быть приравнены к самостоятельному и независимому созданию секрета производства[14].

Если лицо действительно получило информацию, проведя независимые самостоятельные исследования, то подобные действия следует считать законными. Так, согласно п. 2 ст. 1466 ГК РФ, лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.

Однако даже в случае, если другое лицо провело самостоятельное исследование и получило информацию, это не означает, что она стала общедоступной. Это лишь свидетельствует о том, что еще одно лицо получило указанные сведения на законном основании, т. е. в данном случае не нужно смешивать понятия «свободный доступ» и «доступ на законном основании». При наличии доступа на законном основании, который приобрело конкретное лицо, свободного доступа к информации третьих лиц может и не быть.

Таким образом, как следует из вышеизложенного, неизвестность и необщедоступность информации, составляющей коммерческую тайну (ноу-хау), всегда имеют относительный характер, поскольку указанные сведения не являются абсолютно неизвестными и недоступными всем третьим лицам[15].

Более того, если речь идет о некой совокупности информации, то необщеизвестность и необщедоступность должны касаться не каждого ее элемента в отдельности (которые могут и отвечать данным признакам), а всей информации в целом или в определенном сочетании ее компонентов.

Также возникает вопрос о том, кто должен доказывать наличие или отсутствие указанных признаков в случае спора о нарушении прав на ноу-хау: обладатель информации или предполагаемый нарушитель. Более правильным представляется второй вариант, исходя из того, что «отрицательные» факты не подлежат доказыванию[16]. Было бы странным требовать от каждого обладателя информации, который пытается защитить свои права, проводить исследование, подтверждая, что она не является общеизвестной и общедоступной. С учетом сложности и высокой стоимости проведения подобного исследования защита прав обладателей конфиденциальной информации может быть поставлена под сомнение[17].

Данный признак предполагает, что сведения имеют ценность не только для их обладателя, но и для третьих лиц, например для конкурентов предпринимателя, а первому дают конкурентные преимущества, т. е., по сути, эта информация может быть товаром, является оборотоспособной. Справедливо отмечается, что если участие объекта в экономическом обороте возможно, коммерческая ценность, пусть даже потенциальная, существует[18]. При этом необходимо отметить, что информация должна иметь ее именно в силу неизвестности третьим лицам. Это означает, что коммерческую ценность данные сведения имеют до тех пор, пока они отвечают первому признаку — неизвестности третьим лицам и необщедоступности.

Но как же установить коммерческую ценность сведений? Доказательством ее могут быть различные обстоятельства. Так, например, убедительным будет то, что данная информация передавалась контрагенту по гражданско-правовому договору за плату, например по лицензионному договору о передаче ноу-хау. Коммерческую ценность подтверждает и то, что организация на протяжении многих лет вкладывает значительные финансовые ресурсы в совершенствование той или иной разработки и успешно продвигает на рынке товар, созданный с ее использованием.

Если же данные сведения никого, кроме правообладателя, с коммерческой точки зрения не интересуют, хотя он и желает сохранить их в тайне, то они, по смыслу закона, не могут быть отнесены к информации, составляющей коммерческую тайну. Однако это не означает, что лицо не вправе для подобных сведений установить в своей организации режим, аналогичный режиму коммерческой тайны, и также запретить работникам по трудовым и контрагентам по гражданско-правовым договорам разглашать их. Представляется, что для совершения подобных действий нет никаких юридических препятствий. Несоблюдение условий трудового или гражданско-правового договоров повлечет вытекающую из них ответственность.

В связи с вышеизложенным возникает вопрос о том, кто должен доказывать коммерческую ценность, если сведения, в отношении которых установлен режим коммерческой тайны, незаконно получены и используются третьим лицом. Представляется, что в данном случае из самого факта использования данной информации третьим лицом в предпринимательских целях должен следовать вывод о ее коммерческой ценности. Это будет особенно важно в таких встречающихся на практике ситуациях, когда лицо незаконно получило сведения, использует их в своей предпринимательской деятельности, но при этом заявляет об отсутствии их коммерческой ценности.

Порядок установления режима коммерческой тайны регулируется ст. 10 Закона о

коммерческой тайне. Она содержит положение о том, что названный режим считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в первой части настоящей статьи.

Создается впечатление, что необходимо принять все меры, предусмотренные п. 1 ст. 10. Именно такого мнения придерживаются некоторые авторы[19]. Так же нередко толкуются данные положения закона в арбитражной практике. Например, арбитражный суд указал, что «режим коммерческой тайны считается установленным только после принятия всех вышеперечисленных мер (п.2 ст. 10 Закона о коммерческой тайне)»[20]. Однако если проанализировать их, подобный вывод можно поставить под сомнение.

Так, например, довольно странно считать, что режим коммерческой тайны не установлен, если на материальные носители не нанесен гриф «Коммерческая тайна» с указанием обладателя информации, а все остальные требования соблюдены. Еще более парадоксальная ситуация возникает, если гриф нанесен, но содержит надпись не «Коммерческая тайна», а, например, «Секретно» или «Конфиденциально» и не указан обладатель информации или его адрес.

Между тем некоторыми судами названное положение толкуется именно как предписание о необходимости соблюдения данной меры. Так, ФАС Волго-Вятского округа отметил: «...вывод о непринятии ОАО "Уралвагонзавод" всех необходимых мер для охраны конфиденциальной информации является правомерным. Нанесение на материальные носители... грифа "Коммерческая тайна" с указанием обладателя этой информации является одной из таких мер. Доказательств нанесения соответствующей информации на чертежи боковой рамы истец не представил, а потому в удовлетворении соответствующего требования истца отказано обоснованно»[21].

Аналогичный вопрос возникает, если в организации отсутствует какой-либо специальный учет лиц, получивших доступ к информации. Во-первых, не исключено, что в силу характера работы его имеют все сотрудники небольшой организации, занимающиеся определенного вида деятельностью. Поэтому неясно, зачем вести их учет. Во-вторых, если информация была передана контрагенту по гражданско-правовому договору, в который включена его обязанность сохранять ее в тайне, возникает вопрос, почему режим коммерческой тайны следует считать неустановленным только потому, что нет специального учета подобных контрагентов.

Неправильным было бы считать режим коммерческой тайны неустановленным и в случае, если в организации отсутствует специальный контроль над соблюдением порядка обращения с ней. Представляется, что он может осуществляться в рамках общего контроля руководства за соблюдением правил работы в организации и выполнением условий трудовых договоров работниками.

Верным представляется следующий вывод: для того чтобы режим коммерческой тайны считался установленным, необходимо соблюдение не всех мер, перечисленных в п. 1 ст. 10, а тех, которые «разумно достаточны» для сохранения конфиденциальности информации, как требуется п. 5 ст. 10. Так, по мнению Э. П. Гаврилова, если приняты не все предусмотренные законом меры, то «коммерческая тайна как объект не исчезает, она продолжает существовать и на нее должны распространяться нормы Закона»[22]. А суть этих мер, носящих рекомендательный характер, заключается в оповещении любого лица, которое «приближается» к чужой коммерческой тайне, о том, что эта информация является конфиденциальной, и в предоставлении ее обладателю возможности доказать, что нарушитель должен был осознавать незаконность своих действий[23].

Подобное толкование вполне согласовалось бы со ст. 39 ТРИПС, в которой прямо говорится, что информация должна быть объектом «надлежащих в данных обстоятельствах шагов, направленных на сохранение ее секретности». Действительно, комплекс мер, которые необходимо предпринять для сохранения секретности сведений, может различаться в зависимости от обстоятельств: особенностей конкретного юридического лица, информации и др. И только в результате их оценки можно сделать вывод о том, являются ли данные меры достаточными для обеспечения конфиденциальности информации.

Однако вывод о том, что все вышеуказанные меры соблюдать необязательно, делается далеко не всегда, поскольку если рассматривать п. 1 ст. 10 в отрыве от ее п. 5, то можно прийти к выводу о том, что должны быть приняты все меры, перечисленные в п. 1. В то же время соблюдение всех требований, перечисленных в нем, крайне обременительно для участников гражданского оборота. Это приводит к тому, что все эти меры в совокупности применяются крайне редко, а значит, ставится под сомнение охраноспособность соответствующей информации.

Между тем данная неопределенность служит интересам лиц, неправомерно завладевших конфиденциальной информацией и использующих ее. В качестве аргумента они выдвигают несоблюдение режима коммерче-

ской тайны, а значит, и отсутствие самого объекта охраны. Поэтому во избежание возможности двоякого толкования данного положения закона целесообразно внести изменения в указанную статью, исключающие возможность требовать от участников гражданского оборота принятия всех без исключения мер, которые перечислены в п. 1 ст. 10 Закона о коммерческой тайне.

В целом, все вышеизложенные проблемы, связанные с неопределенностью толкования понятия ноу-хау, успешно используются недобросовестными участниками гражданского оборота, которые ссылаются на то, что информация не обладает всеми признаками, необходимыми для того, чтобы считать ее охраноспособной. Нет ноу-хау – нет и его неправомерного использования.

Помимо положений ГК РФ, предусматривающих ответственность за нарушение права на ноу-хау, существует ряд норм закона, направленных на защиту не только частных, но и публичных интересов в данной области. Так, Федеральный закон от 26 июля 2006 г. «О защите конкуренции» рассматривает незаконное получение, использование, разглашение информации, составляющей коммерческую тайну, как акт недобросовестной конкуренции. Ст. 183 УК РФ предусматривает уголовную ответственность за незаконные получение и разглашение сведений, составляющих коммерческую тайну. Однако все эти нормы остаются нежизненными до тех пор, пока нет ясного и адекватного определения информации, составляющей коммерческую тайну (ноу-хау), и отдельных ее признаков с учетом европейских тенденций регулирования аналогичных отношений или, по крайней мере, разумного толкования существующего определения.

Литература

[1] Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» // СЗ РФ. 2002. № 43. Ст. 4190.

[2] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // СЗ РФ.1998. № 31. Ст. 3824.

[3] Федеральный закон от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2009. № 1. Ст. 15.

[4] Федеральный закон от 02.12.1990 № 395-1 (ред. от 30.09.2013) «О банках и банковской деятельности» // СЗ РФ. 1996. № 6. Ст. 492.

[5] Постановление ФАС Дальневосточного округа от 10.12.2010 № Ф03-8647/2010 по делу № А59-3990/2009. Исходя из смысла положений ФЗ «О несостоятельности (банкротстве)» и ФЗ «О несостоятельности (банкротстве) кредитных организаций» с момента открытия в отношении банка-должника конкурсного производства не только сведения о финансовом состоянии должника прекращают относиться к категории сведений, носящих конфиденциальный характер либо являющихся коммерческой тайной, но и сведения, составляющие банковскую тайну. // [Электронный документ]// Режим доступа: http://base.coNºsultaNºt.ru

[6] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127; Бетров Д. М. Коммерческая тайна и секрет производства. Новые аспекты законодательства // Вестник УрФО. Безопасность в информационной сфере. 2011. № 2. С. 12–16.

[7] Дерюга Н. Н. Коммерческая тайна как фактор сохранения бизнеса // Безопасность бизнеса. 2012. № 4. С. 29–31.

[8] См.: Бандурина О. С. Коммерческая тайна в информационный век // Патентное дело. 2011. № 10. С. 3-5; Шостак И. Коммерческая тайна и договорные правоотношения // Интеллектуальная собственность. Промышленная собственность. 2013. № 11. С. 38–45; Нюлланс Е. С., Перевалов В. А. Охрана и защита информации, составляющей коммерческую тайну // Закон. 2013. № 6. С. 48–55.

[9] См.: Кайнов В. И., Кайнова Ю. В. Субъекты, имеющие право на получение сведений, составляющих банковскую тайну // Юридический мир. 2008. № 2. С. 56–57.

[10] Постановление Пленума Верховного Суда РФ № 5, Пленума ВАС РФ № 29 от 26.03.2009 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» // Вестник ВАС РФ. 2009. № 6.

[11] Концепция развития гражданского законодательства об интеллектуальной собственности. [Электронный документ] // Режим доступа: http://www.privlaw.ru/coNºcep_iNºtel.rtf

[12] Commission Regulation (EC) № 772/2004 of 27 April 2004 on the application of Article 81(3) of the Treaty to categories of technology transfer agreements. [Электронный документ]// Режим доступа: http://eur-lex.europa.eu/

[13] Постановление тринадцатого апелляционного суда от 11.12.2008 г. по делу № А56-47340/2007. Требование о взыскании убытков, причиненных разглашением информации о технологических решениях и идеях, переданной по соглашению о конфиденциальности, подлежит отклонению, если не представляется возможным установить характер, объем и содержание переданных материалов. [Электронный документ] // Режим доступа: http://base.consultant.ru

[14] См.: Шишмарева Е. В. Признак коммерческой тайны – неизвестность информации третьим лицам//Безопасность бизнеса. 2005. № 1

[15] Комментарий к части четвертой Гражданского кодекса Российской Федерации / Гаврилов Э. П., Еременко В.И.. М., 2009. С. 770

[16] См., напр.: Комментарий к Гражданскому кодексу Российской Федерации, части второй, постатейный / Под ред. С. П. Гришаева, А. М. Эрделевского. М., 2007; Гордон В. М. Устав гражданского судопроизводства с комментариями. СПб., 1914. С. 368; Юдельсон К. С. Проблема доказывания в советском гражданском процессе. М., 1951. С. 281–284.

[17] См.: Балакин Д. Каким быть новому законодательству РФ о ноу-хау?// Промышленная собственность. 2003. № 2. С. 9

[18] Дозорцев В. А. Понятие секрета промысла («ноу-хау»)//Вестник Высшего Арбитражного Суда РФ. 2001. № 7

[19] См., напр.: Ефимцева Т. Некоторые аспекты правового регулирования секретов производства// Право и экономика. 2008. № 4. С. 55; Погуляев В. В. Постатейный комментарий к Федеральному закону «О коммерческой тайне». М., 2005

[20] Постановление Тринадцатого апелляционного суда от 27.02.2007 г. по делу № А56-39537/2006, Постановление ФАС Волго-Вятского округа от 04.06.2008 г. по делу № А79-2693/2007.

[21] Постановление ФАС Волго-Вятского округа от 04.06.2008 г. по делу № А79-2693/2007.

[22] Гаврилов Э. П. Вопросы правовой охраны коммерческой тайны // Хозяйство и право. 2004. № 11.

[23] Гаврилов Э. П. О коммерческой тайне. Подготовлен для системы КонсультантПлюс, 2005. [Электронный документ] // Режим доступа: http://base.consultant.ru/

References

[1] Federal law as of 26.10.2002 No. 127-FZ «On insolvency (bankruptcy)» // SZ RF. 2002. No.43. Art. 4190.

[2] Tax Code of the Russian Federation (Part 1) as of 31.07.1998 No. 146-FZ // SZ RF.1998. No. 31. Art. 3824.

[3] Federal Law as of 30.12.2008 No. 307-FZ «On auditing activities» // SZ RF. 2009. No. 1. Art. 15.

[4] Federal law as of 02.12.1990 No. 395-1 (edited 30.09.2013) «On forms and banking activities» // SZ RF. 1996. No. 6. Art. 492.

[5] Resolution of the Federal Antimonopoly Service of Far Eastern District as of 10.12.2010 No. F03-8647/2010 on the case No. A59-3990/2009. On the assumption of the meaning of the provisions of the Federal Law «On insolvency (bankruptcy)» and Federal Law «On insolvency (bankruptcy) of banking institutions» starting from the moment when the bankruptcy proceedings have been opened against the bankrupted institution confidential information and banking secrets are not considered confidential or banking secrets anymore.// [Electronic document]// http://base.coNºsultaNºt.ru

[6] Presidential Decree of the Russian Federation as of 06.03.1997 No. 188 «On the establishment of information classified as confidential» // SZ RF. 1997. No. 10. Art. 1127; Betrov D.M. Kommercheskaya taina i sekret proizvodstva. novye aspekty zakonodatel'stva [Commercial secrets and the secret of production. New aspects of legislation]// Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. 2011. No.2. p. 12-16.

[7] Deryuga N.N. Kommercheskaya taina kak faktor sokhraneniya biznesa.[Commercial secret as a factor of business security]// Bezopasnost' biznesa. 2012. No. 4. p. 29-31

[8] Bandurina O.S. Kommercheskaya taina v informatsionnyi vek [Commercial secrets in the age of information]// Patentnoe delo. 2011. No. 10. p. 3-5; Shostak I. Kommercheskaya taina i dogovornye pravootnosheniya [Commercial secrets and contractual relationships]// Intellektual'naya sobstvennost'. Promyshlennaya sobstvennost'. 2013. No. 11. p. 38-45; Nyullans E.S., Perevalov V.A. Okhrana i zashchita informatsii, sostavlyayushchei kommercheskuyu tainu [Commercial information security]// Zakon. 2013. No. 6. p. 48-55.

[9] Kainov V.I., Kainova Yu.V. Sub»ekty, imeyushchie pravo na poluchenie svedenii, sostavlyayushchikh bankovskuyu tainu [Persons who have right for access to banking secret information]// Yuridicheskii mir. 2008. No. 2. p. 56-57

[10] Resolution of the Plenum of the Supreme Court of the Russian Federation No. 5, of the Plenum of the

Supreme Court of the Russian Federation No. 29 as of 26.03.2009 «On certain questions in connection with introduction of Part 4 of the Civil Code of the Russian Federation» // Vestnik VAS RF. 2009. No. 6.

[11] Concept of the development of the civil legislation on intellectual property [Electronic resource] // http://www.privlaw.ru/coNºcep_iNºtel.rtf

[12] CommissioNº RegulatioNº (EC) Nº 772/2004 of 27 April 2004 oNº the applicatioNº of Article 81(3) of the Treaty to categories of techNºology traNºsfer agreemeNºts. [Electronic document]// http://eur-lex.europa.eu/

[13] Resolution of the 13th Appeal Court as of 11.12.2008 on the case No. A56-47340/2007. Claim to recover damages caused by the disclosure of information on technological solutions and ideas given on conditions of a confidentiality agreement must be rejected if it is not possible to establish the nature, scope and content of the materials [Electronic resource] // http://base.coNºsultaNºt.ru

[14] Shishmareva E. V. Priznak kommercheskoi tainy – neizvestnost' informatsii tret'im litsam [Attribute of commercial secrets – the information is unknown to third parties]//Bezopasnost' biznesa. 2005. No. 1

[15] Commentaries to Part 4 of the Civil Code of the Russian Federation/ Gavrilov E. P., Eremenko V.I.. Moscow, 2009. p 770

[16] Commentaries to Part 2 of the Civil Code of the Russian Federation // Under the editorship of S.P. Grishaeva, A.M. Erdelevskogo. Moscow, 2007; Gordon V. M. Ustav grazhdanskogo sudoproizvodstva s kommentariyami [Regulation of civil legal proceedings with commentaries]. SPb., 1914. p. 368; Yudel'son K. S. Problema dokazyvaniya v sovetskom grazhdanskom protsesse [Proof in soviet civil proceedings]. Moscow, 1951. p. 281-284

[17] Balakin D. Kakim byt' novomu zakonodatel'stvu RF o nou-khau? [What will the new legislation on know-how in Russia be?]// Promyshlennaya sobstvennost'. 2003. No. 2. p. 9

[18] Dozortsev V. A. Ponyatie sekreta promysla («nou-khau») [The notion of trade secret]//Vestnik Vysshego Arbitrazhnogo Suda RF. 2001. No. 7

[19] Efimtseva T. Nekotorye aspekty pravovogo regulirovaniya sekretov proizvodstva [Certain aspects of legal regulation of production sectors]//Pravo i ekonomika. 2008. No. 4. p. 55.; Pogulyaev V. V. Postateinyi kommentarii k Federal'nomu zakonu «O kommercheskoi taine» [Article-by-article commentaries to the Federal law 'On commercial secret']. Moscow, 2005

[20] Resolution of the 13th Appeal Court as of 27.02.2007 g. on the case № A56-39537/2006, Resolution of the Federal Commercial Court of Volgo-Vyatskii District as of 04.06.2008 on the case No. A79-2693/2007

[21] Resolution of the Federal Commercial Court of Volgo-Vyatskii District as of 04.06.2008 on the case No. A79-2693/2007

[22] Gavrilov E. P. Voprosy pravovoi okhrany kommercheskoi tainy [Questions of legal protection of commercial secret]// Khozyaistvo i pravo. 2004. № 11.

[23] Gavrilov E. P. O kommercheskoi taine [On commercial secret]. Podgotovlen dlya sistemy Konsul'tantPlyus, 2005. [Electronic resource] // http://base.coNºsultaNºt.ru/

Ханова Вероника Сергеевна, студент магистратуры кафедры предпринимательского и коммерческого права ЮУрГУ. E-mail: shelen89@mail.ru.

Khanova Veronica, graduate student of the department of business and commercial law SUSU. E-mail: shelen89@mail.ru.

УДК 351.713 + 34.03 : 336.22 + 34 : 002.6
ББК Х 402.23 : Х 401.114 + Х 401.114 : Х 402.23

И. А. Белишко

ПРАВОВОЙ РЕЖИМ НАЛОГОВОЙ ТАЙНЫ

В статье автором рассматриваются актуальные вопросы защиты налоговой тайны. Налоговая тайна рассматривается автором как комплексный правовой институт, поскольку регулируется нормами различных отраслей права: административным, финансовым, информационным, гражданским. Правовое значение налоговой тайны состоит в том, что она обеспечивает защиту прав и законных интересов налогоплательщиков в отношении информации, отнесенной законодательством к налоговой тайне. Автором предлагается авторское определение налоговой тайны как информации, признаваемой федеральным законом необщедоступной в целях защиты прав и законных интересов в сфере налогообложения, соответствующей установленным законом условиям охраноспособности.

Ключевые слова: *информация ограниченного доступа, налоговая тайна, правовой режим, защита.*

I. A. Belishko

LEGAL REGIME OF TAX SECRETS

In this article the author discusses current issues of tax secrecy protection. Tax secrecy is considered by the author as a complex legal institution, as regulated by the various branches of law: administrative, financial, information, civil. The legal significance of tax secrecy is that it protects the rights and legitimate interests of taxpayers in respect of information classified as secret to tax legislation. The author proposes the author's definition of tax secrecy as information Nonpublic recognized by federal law to protect the rights and legitimate interests in the field of taxation, the relevant statutory conditions of patentability.

Keywords: *restricted access information, tax secrecy, secret legal regime of protection.*

В современных условиях развития экономики особую актуальность приобретают вопросы, связанные с обеспечением финансовой безопасности государства в целом и его налоговой сферы, в частности. Сохранность налоговой тайны имеет особое значение для эффективного функционирования социально-экономического механизма страны. Практически каждый дееспособный гражданин является налогоплательщиком, поэтому одной из приоритетных задач государства в этой области становится обеспечение правовой безопасности субъектов, участвующих в финансовых отношениях. Вопросы защиты конфиденциальных сведений тесно взаимосвязаны с институтом налоговой тайны, что также подтверждает его значимость. Появление в российском законодательстве положений о налоговой тайне следует признать значительным шагом вперед в совершенствовании финансово-правовой защиты прав и законных интересов граждан.

Законодательное закрепление понятия «тайна» представляется крайне важным, в том числе на конституционном уровне, поскольку «тайна» с правовой точки зрения это специальный правовой режим как доступа и хранения, так и использования определенной

совокупности конфиденциальной информации, за нарушение которого должна быть предусмотрена юридическая ответственность. Налоговозначимая информация – это особый тип информации, предназначенный непосредственно для целей налогообложения, поэтому информация, которой располагают налоговые органы, является не только экономической информацией, но и содержит персональные данные налогоплательщиков, налоговых агентов и лиц, сопутствующих уплате налогов, которые подпадают под режим защиты Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В этой связи вывод о том, что при определенных обстоятельствах одна и та же экономическая информация может одновременно подпадать под юрисдикцию нескольких правовых режимов защиты, представляется наиболее соответствующим положениям российского законодательства. Так, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные ресурсы разделены по категориям доступа на общедоступные и ресурсы с ограниченным доступом, а по условиям ее правового режима – на информацию, отнесенную к государственной тайне, и конфиденциальную. Легальное определение понятия «налоговая тайна» дано в п. 1 ст. 102 Налогового кодекса РФ (далее – НК РФ), согласно которому: «Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений, исчерпывающий перечень которых законодатель закрепил в этой же статье».

Налоговая тайна по своей сути есть информация, причем информация с ограниченным доступом. Иными словами, на данные виды информации распространяются все признаки правового режима информации с ограниченным доступом. Понятие налоговой тайны содержится в п. 1 ст. 104 Налогового кодекса. Кроме этого, с 1 января 2013 г. п. 1 ст. 106 НК РФ был дополнен подпунктом 6 следующего содержания: 6) предоставляемых в Государственную информационную систему о государственных и муниципальных платежах, предусмотренную Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

В научной литературе часто подчеркивается, что относительно информации, составляющей налоговую тайну, могут складываться различные правоотношения, связанные со сбором, получением, хранением, распространением, защитой такой информации, а также ответственностью за неправомерное ее разглашение и использование. Что касается института налоговой тайны, то его определяют как комплексный, включающий в себя нормы не только налогового, но и информационного, административного, уголовного и других отраслей права.

Правовой режим охраны налоговой тайны можно охарактеризовать прежде всего ограниченным и четко регламентированным порядком доступа к ней. Таким образом, под налоговой тайной понимается информация, признаваемая федеральным законом необщедоступной в целях защиты прав и законных интересов в сфере налогообложения, соответствующая установленным законом условиям охраноспособности.

Степень доверия между гражданином и государством, способствующая правильному исчислению и уплате налогов, в определенной мере зависит от того, каким образом государство в дальнейшем распорядится сведениями, полученными в связи с осуществлением налогообложения.

Отсюда возникает (либо должна возникнуть) система правового регулирования обеспечения сохранности полученной информации от противоправного распространения с указанием точного числа государственных субъектов, которые вправе использовать ее в своей деятельности, а также пределов такого использования.

Данная система в настоящий период сконцентрирована в основном в нормах, объединенных в ст. 102 НК РФ, получившей название «Налоговая тайна».

Объем сведений, относимых к налоговой тайне, определен законодателем методом исключения.

Исходя из приведенных в ст. 102 НК РФ положений, можно сделать следующие выводы:

1. Объем сведений, относимых к налоговой тайне, изначально не является точно определенным, что порождает множественность подходов к толкованию его содержания.

2. Законодатель конкретизировал ряд субъектов, имеющих право на получение такого рода информации, в единственном числе, а ряд – во множественном. Это означает, что в системе «обладатель информации – получатель информации» некоторых субъектов можно конкретизировать (налоговый орган и

орган государственного внебюджетного фонда – по территориальности нахождения налогоплательщика, таможенный орган – по существу сделки или виду транспорта, перевозившего товар), а ряд субъектов (органы внутренних дел, а с 15 января 2011 года также следственные органы) являются неопределенными, поэтому требуется специальный порядок для их конкретизации.

Данный перечень не является исчерпывающим. Так, в частности, в письме Федеральной налоговой службы от 11.06.2009 № МН-22-6/469 «О предоставлении информации»[1] указывается буквально следующее: «Хотя согласно части 2 статьи 102 Налогового кодекса Российской Федерации сведения о наименовании банков и иных кредитных организаций с указанием расчетных счетов должника, запрашиваемые судебными приставами-исполнителями и взыскателями, отнесены к конфиденциальной информации, они должны им предоставляться с учетом правовой позиции, изложенной в Постановлении Конституционного Суда Российской Федерации от 14.05.2003 № 8-П[2].

Суть ее в том, что судебный пристав-исполнитель вправе получать в банках, иных кредитных организациях необходимые сведения о вкладах физических лиц в размере и пределах, которые определены судом и необходимы для исполнения исполнительного документа».

Отсюда следует, что и органы юстиции в лице судебных приставов-исполнителей являются получателями данной информации. Правда, последние – только по конкретным делам.

Поскольку субъектов-получателей неопределенно много и они имеют различную ведомственную принадлежность, необходим акт правительственного уровня, который конкретизировал бы общую норму (ч. 3 ст. 102 НК РФ), согласно которой поступившие в налоговые органы, органы внутренних дел, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа. Такого акта до сего времени нет, хотя данная норма действует с 1998 года.

Обозначенная неопределенность неизбежно приводит к злоупотреблениям со стороны отдельных должностных лиц, утечке информации, наносящей ущерб налогоплательщикам, и в целом свидетельствует о том, что государство пока не проявляет должной заботы об обеспечении информационной безопасности лиц, у которых оно в административном порядке истребует значительные объемы частной информации.

Кроме того, следует отметить, что в этом году принят закон «О противодействии незаконным финансовым операциям»[3], который частично используется и должен вступить в силу в полном объеме 1 июля 2014 года.

Самое обсуждаемое положение документа касается открытия для налоговых служб доступа к информации о счетах физических лиц. С середины следующего года банки должны будут передавать в налоговую службу данные об открытии и закрытии всех счетов граждан.

Также по запросу налоговики смогут получать выписки о движении средств, сведения о суммах вкладов. Правда, возможен столь подробный запрос только в том случае, если в отношении отдельно взятого гражданина осуществляется проверка.

При этом следует отметить, что сегодня налоговики получают информацию только по счетам и вкладам юридических лиц и индивидуальных предпринимателей.

Изменения коснутся и правоохранительных органов: в рамках расследования тяжких и особо тяжких преступлений органы оперативно-разыскной службы смогут запрашивать у банков информацию о счетах компаний и граждан. Для такого запроса понадобится санкция суда. Сейчас эта информация предоставляется только органам следствия при расследовании конкретного уголовного дела. Таким образом, полномочия и налоговиков, и правоохранительных органов расширяются.

Следует отметить, что банкиры выступали против такого расширения. «Еще в процессе рассмотрения законопроекта мы выступали против этой нормы, поскольку она расширяет пределы понятия «банковская тайна», фактически размывает его, – рассказывает ведущий специалист правового департамента Ассоциации российских банков Вероника Кинсбурская[4]. – Несмотря на наличие в документе положения, что информация может быть запрошена только по решению суда, все это может впоследствии отпугнуть клиентов банков. Учитывая наши реалии (например, случаи коррупции), граждане могут начать бояться открывать новые вклады и вести счета».

Что касается банков, в целом они не против уточнения порядка запроса информации со стороны госорганов. Банкиры в связи с этим вспоминают поправки в ФЗ «О банках и

банковской деятельности», давшие органам внутренних дел право получать в кредитных организациях справки по операциям и счетам юридических лиц и индивидуальных предпринимателей. Тогда банковское сообщество ожидало волну «пустых» запросов в свой адрес со ссылкой на необходимость выявления налоговых преступлений. Однако, к всеобщему удивлению, такой волны не последовало.

«В целом список лиц, обладающих правом доступа к банковской тайне, периодически расширяется,– говорит начальник юридической службы КБ «Московское ипотечное агентство» Максим Князев.– Но ни одно из таких изменений, на мой взгляд, не создало для банковской системы России серьезных проблем, связанных с нежеланием клиентов продолжать работать в предлагаемом правовом поле. Поэтому изменения в части доступа к банковской тайне налоговых органов не будут особым образом отмечены со стороны клиентов кредитных организаций. Законопослушным гражданам, не имеющим долгов перед государством и не скрывающим свои доходы от налогов, бояться рассматриваемой законодательной инициативы не стоит»[5].

Если изменение доступа к банковской тайне кредитные организации в общем встретили спокойно и с пониманием, то предполагаемое начало реализации новшеств (с 1 июля 2014 года) вызывает у них вопросы. Дело в том, что банки пока не успевают нужным образом доработать информационные технологии. Президент Национального платежного совета Андрей Емелин уже подготовил соответствующее письмо председателю Центробанка Эльвире Набиуллиной, где банковское сообщество просит отложить начало применения ФЗ «О противодействии незаконным финансовым операциям» до 1 января 2015 года. По словам Емелина, кредитным организациям необходимо время на коррекцию существующих правил внутреннего контроля, разработку дополнительных локальных документов.

Также необходимо привести автоматизированные системы контроля в согласие с новыми требованиями. Банки, да и сами налоговые органы вскоре столкнутся с серьезной организационной проблемой. Открытие счетов физических лиц – это потоковый продукт, основанный на публичных отношениях. Теоретически банки могут автоматизировать у себя эти процессы. Но вот что будет с самой ФНС, когда к ней попадет весь тот безумный поток информации об открытых физическими лицами счетах, пока не ясно[6].

Как бы то ни было, принятие ФЗ «О противодействии незаконным финансовым операциям» – событие в русле мировых тенденций. «Мы движемся по западному пути,– говорит генеральный директор Центра антикоррупционных исследований и инициатив «Трансперенси Интернешнл – Россия» Елена Панфилова.– Так как мы остаемся членами «восьмерки» и «двадцатки», то раз за разом подписываем все новые международные документы. Если мы хотим хоть как-то навести порядок с выведением средств из незаконной налоговой оптимизации, нам придется жить по новым правилам. Если же мы из этой системы выпадем, то неизбежно понесем глобальные экономические потери».

Как отмечают эксперты, новый закон принят, чтобы прежде всего привести российское законодательства в соответствие с требованиями ФАТФ – межправительственной организации, созданной для борьбы с отмыванием денег[7]. Если в России не будут появляться подобные законы, ее внесут в черный список стран, которые с отмыванием не борются, что может повлечь серьезные санкции, вплоть до приостановки всех зарубежных финансовых операций.

Во всем мире тайна банковских вкладов все в большей степени становится условной. Так, Швейцария уже предоставила США полную информацию по нескольким тысячам американских вкладчиков в банках страны.

Впервые система, защищавшая тайну банковских сбережений, пошатнулась в 2009 году, когда швейцарский банк UBS раскрыл американским властям данные по 4500 клиентам – гражданам США. После чего ему пришлось выплатить $780 млн штрафа, а подозрительные вкладчики были вынуждены забрать из него деньги.

Немного позднее, в 2011 году, банк Credit Suisse также согласился предоставить США информацию о своих клиентах, подозреваемых в уклонении от уплаты налогов. В 2012 году брешь в банковской тайне страны пробил документ под неофициальным названием «закон Дювалье», который позволил замораживать активы членов правительств иностранных государств[8].

Наконец, летом 2013 года правительство Швейцарии официально разрешило нескольким банкам сотрудничать с американскими властями. Согласно новой схеме раскрытия банковской тайны, властям США будут предоставляться детали счетов американских

вкладчиков. Речь идет прежде всего о клиентах, уклоняющихся от уплаты налогов. Вслед за США желание получать аналогичную информацию о своих гражданах изъявили Великобритания, Франция и Германия.

Евросоюз в целом движется в том же направлении. Так, Европейская комиссия готовит глобальный документ, который позволит создать единую базу данных компаний и частных вкладчиков, что даст возможность государственным чиновникам следить в том числе за деятельностью инвестиционных фондов.

На данный момент активно поддерживают отказ от соблюдения банковской тайны власти Германии, Франции, Великобритании, Италии и Испании. Постепенно меняют свою позицию Австрия и Люксембург, которые раньше блокировали введение новых правил. Власти Люксембурга, например, со следующего года намерены предоставлять информацию о счетах иностранных компаний, а не только частных лиц. Вместе с тем строгую банковскую тайну все еще сохраняют Гибралтар, Монако, Андорра и Лихтенштейн.

О перспективах разработки европейского закона, предусматривающего обмен информацией по поводу счетов налогоплательщиков – резидентов стран ЕС в банках разных юрисдикций, говорится в совместном обзоре НП «Национальный платежный совет» и ЗАО КПМГ «Новости FATCA» от 31 октября 2013 года[9]. В обзоре приводятся слова главы рабочей группы Европейского комитета банковской индустрии (EBIC) Рене Вэка о том, что Европейский парламент «будет готов» объявить стандарты обмена информацией в рамках этого закона уже в начале 2014 года. Об этом господин Вэк сообщил на проходящей в Италии конференции НП «Национальный платежный совет». Как следует из пересказа его выступления, на первом этапе к закону присоединятся 28 государств ЕС, а впоследствии также страны с льготным режимом налогообложения, в частности, Каймановы острова и остров Мэн. Россия сможет присоединиться к европейскому аналогу FATCA с 2015 года, следует из обзора.

FATCA – важнейший закон США по борьбе с уклонением собственными гражданами от налогов.

В отличие от Европы, где идут серьезные дебаты о банковской тайне, в США эти вопросы давно решены. Формально закон о тайне вкладов существует там с 1970 года, однако информацию он практически не защищает. Банки обязаны предоставлять властям данные, которые могут быть необходимы в рамках расследования уголовных дел и при решении вопросов, связанных с налогами.

Кроме того, данные о подозрительных денежных переводах сразу же поступают в центральный электронный архив, к которому имеют доступ ЦРУ, ФБР, налоговое ведомство, Агентство по борьбе с наркотиками. Клиентам банков о передаче в соответствующие службы такой информации при этом не сообщается.

FATCA с 1 января 2013 года требует от американских компаний и физических лиц сообщать в Налоговую службу США сведения о собственных зарубежных активах, банковских счетах и движениях средств по ним (более $50 тыс.). А с 2014 года поступления в США средств из-за пределов страны, не идентифицированные по правилам FATCA, будут облагаться 30-процентным сбором. FATCA имеет международное расширение: страны, готовые присоединиться к акту, могут или позволить своим банкам сообщать налоговикам США сведения об американских резидентах, или обмениваться этой информацией с американской налоговой службой через собственные налоговые органы[10].

Россия пока склоняется ко второму варианту, поскольку первый сопряжен с нарушением кредитными организациями банковской тайны. Но окончательное решение вопроса пока нигде не зафиксировано.

Между тем к иностранным банкам, обслуживающим американских налогоплательщиков и не выполняющих требования FATCA, уже с 1 июля 2014 года будут применены жесткие санкции. Они не смогут открывать и работать по счетам в американских банках и вести расчеты в американских долларах. О санкциях за невыполнение европейского аналога FATCA упоминается в обзоре – «полный запрет на осуществление деятельности для банков стран, которые не будут выполнять требования».

Видимо, в данном случае речь идет о разрыве корреспондентских отношений, приостановлении операций и расчетов, что сулит потери уже не клиентам таких банков, а самим банкам, которые лишатся возможности проводить операции с зарубежными контрагентами.

Обнародование таких деталей серьезно обеспокоило российских банкиров. Ведь до сих пор идея создания европейского аналога FATCA обсуждалась лишь в общем приближении: ни о санкциях, ни о конкретных сроках речи не было. Сама идея появилась в конце

прошлого года, когда страны Евросоюза начали присоединяться к американскому закону. Тема создания европейского аналога FATCA упоминалась в ходе переговоров в рамках G20, однако никакой конкретики в стандартах передачи информации пока не обнародовалось.

Оценить риски в случае реализации идеи европейских стран банкиры в связи с отдаленностью этой перспективы не берутся. Но если будет реализована и эта мера, России впору писать свой собственный FATCA и требовать от других стран присоединяться к нему. «Под перекрестный огонь мы все равно попадем, а отток капитала, в частности, в виде неуплаченных налогов, в нашей стране весьма велик», – иронизирует глава службы финмониторинга банка из топ-10[11].

Следует отметить, что вышеприведенные заявления не убедили экспертов в том, что идея европейского FATCA все-таки будет реализована. «Некоторые эксперты считают, что это виртуальный контраргумент ЕС, призванный оказать ответное давление на США и, возможно, отсрочить полномасштабное внедрение FATCA». «Пока не заработал американский закон и, более того, не все межправительственные соглашения подписаны, рано говорить о применении его аналогов», – считает и Дмитрий Чистов. Идея США может быть подхвачена другими юрисдикциями, если FATCA докажет свою эффективность в борьбе с уклонением от уплаты налогов, соглашается Максим Кандыба[12].

Однако в целом сегодня Россия делает решительные шаги на пути к отказу от банковской тайны, что соответствует мировой практике.

«Законопослушным клиентам, которые не попадают под меры специального регулирования, новый закон не принесет никаких дополнительных трудностей. Документ вводится для повышения прозрачности и чтобы раскрывать движение незаконных активов. Беда наша заключается лишь в том, что в силу коррупционных тенденций даже такие правильные решения могут оказаться болезненными для обычных людей», – говорит Елена Панфилова[13].

Осложняется ситуация техническими проблемами, которые не позволяют банкам качественно и вовремя перестроиться согласно принятым Думой положениям. Если сроки вступления в силу ФЗ «О противодействии незаконным финансовым операциям» не будут отодвинуты на 2015 год, банки ожидает череда сбоев в работе. С другой стороны, Россия в случае отсрочки может не вписаться в имидж страны, которая отвечает требованиям, предъявляемым международным сообществом.

Итак, в рамках реализации положений Основных направлений налоговой политики Российской Федерации на 2014 год и на плановый период 2015 и 2016 годов летом этого года был принят Федеральный закон от 28.06.2013 № 134-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям», который значительно расширяет полномочия налоговых органов по истребованию информации.

Теперь «справки о наличии счетов, вкладов (депозитов) и (или) об остатках денежных средств на счетах, вкладах (депозитах), выписки по операциям на счетах, по вкладам (депозитам) физических лиц, не являющихся индивидуальными предпринимателями, в банке, справки об остатках электронных денежных средств и о переводах электронных денежных средств могут быть запрошены налоговыми органами при наличии согласия руководителя вышестоящего налогового органа или руководителя (заместителя руководителя) федерального органа исполнительной власти, уполномоченного по контролю и надзору в области налогов и сборов, в случаях проведения налоговых проверок в отношении этих лиц либо истребования у них документов (информации) в соответствии с пунктом 1 статьи 93.1 НК РФ».

При этом банки обязаны сообщать в налоговый орган по месту своего нахождения не только сведения, указанные в п. 1 ст. 86 НК РФ, но и сведения о счетах и вкладах физических лиц. Указанным Законом было также изменено понятие счета для целей налогообложения (ст. 11 НК РФ). Под счетом понимаются счета организаций и индивидуальных предпринимателей, нотариусов, занимающихся частной практикой, адвокатов, учредивших адвокатские кабинеты, и все счета, открытые на основании договора банковского счета (изменение вступает в силу 01.01.2014).

Также изменения были внесены в Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Ст. 8 указанного Закона в новой редакции выглядит следующим образом: «При наличии достаточных оснований, свидетельствующих о том, что операция, сделка связаны с легализацией (от-

мыванием) доходов, полученных преступным путем, или с финансированием терроризма, уполномоченный орган направляет соответствующие информацию и материалы в правоохранительные или налоговые органы в соответствии с их компетенцией». Данная формулировка этой нормы предоставляет налоговым органам еще один источник информации о налогоплательщике.

Вернемся к действующим на данный момент редакциям ст. 86 и 93.1 НК РФ, которые также предоставляют широкие полномочия налоговым органам в отношении доступа к информации, подпадающей под режим банковской тайны. Причем эти полномочия проистекают не столько из прямого указания на них в статьях НК РФ, сколько из расширительного толкования этих норм налоговыми органами и Минфином.

Почти все примеры такого «выгодного» толкования ст. 86 и 93.1 НК РФ можно разделить на те, которые расширяют круг субъектов, имеющих право запрашивать информацию, и те, что расширяют перечень запрашиваемой информации (то есть объектов запроса). Примером первого типа толкования может служить разъяснение Минфина: «Положениями статьи 86 Кодекса не установлено обязательное направление запросов в банк с целью получения указанной в пункте 2 данной статьи информации по счетам налогоплательщиков только тем налоговым органом, которым в отношении этих налогоплательщиков проводятся мероприятия налогового контроля».

Другой пример: информация по ст. 86 НК РФ может быть запрошена любым налоговым органом, который проводит контрольные мероприятия, в том числе и в случае, когда указанная организация не состоит на учете в этом налоговом органе. Также Минфин «разрешает» налоговым органам «истребовать у банка в порядке, предусмотренном статьей 93.1 Кодекса, документы (информацию) о контрагенте проверяемого налогоплательщика и о контрагентах указанного контрагента, располагающих документами (информацией), касающимися деятельности проверяемого налогоплательщика (плательщика сбора, налогового агента)». Этот случай толкования можно отнести ко второму типу – ситуация, когда Минфин расширяет круг запрашиваемой информации.

Еще пример: Минфин в ответ на вопрос о законности истребования у контрагента проверяемого налогоплательщика информации о персональных данных сотрудников контрагента дает следующий ответ: «Статья 93.1 Кодекса не содержит конкретный перечень истребуемых налоговыми органами документов, содержащих информацию, касающуюся деятельности проверяемого налогоплательщика. Полагаем, что к таким документам относятся любые документы, содержащие информацию, касающуюся деятельности проверяемого налогоплательщика (плательщика сбора, налогового агента)».

Таким образом, налоговые органы находятся в очень выгодном положении, используя не только статьи НК РФ, но и письма Минфина, расширяющие их полномочия по истребованию информации, являющейся банковской тайной. К тому же подход Минфина поддерживается КС РФ. В одном из своих Определений по делу об оспаривании нормы Закона «О налоговых органах Российской Федерации», содержавшей (на данный момент оспариваемая норма отменена) открытый перечень информации, которая могла быть истребована налоговым органом у банка, КС РФ объяснил, что подход расширительного толкования оправдан публичными интересами деятельности налоговых органов.

При этом КС РФ отметил, что «закрепление в законе отступлений от банковской тайны... не может быть произвольным; такие отступления... должны отвечать требованиям справедливости, быть адекватными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе частных и публичных прав и интересов граждан, не затрагивать существо соответствующих конституционных прав, то есть не ограничивать пределы и применение основного содержания закрепляющих эти права конституционных положений».

Из всего вышесказанного можно сделать вывод о том, что для налоговых органов как для органов власти, деятельность которых преследует соблюдение публичных интересов, понятие банковской тайны носит особое, отличное от общего понятия значение. Банковская тайна для налогового органа может быть преодолена с помощью тех полномочий, которыми он обладает в силу прямого указания закона, в частности НК РФ. Но, получив от банка информацию, налоговый орган, так же как и кредитная организация, обязан соблюдать особый режим использования данных. В отношении налогового органа эта обязанность будет носить название «налоговой тайны». Согласно ст. 102 НК РФ «налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел,

следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике». Налоговая тайна, так же как и банковская, является особым режимом доступа и использования информации.

Таким образом, налоговая тайна как бы защищает ту информацию, которая входит в банковскую тайну, но была передана кредитной организацией налоговому органу в установленном законом порядке. Хотя границы банковской тайны для налоговых органов постепенно размываются, этот институт продолжает работать и выполнять свою основную функцию – защищать информацию о клиенте от передачи третьим лицам в порядке, не предусмотренном законом.

Итак, налоговая тайна является комплексным правовым институтом, т. е. регулируется нормами различных отраслей права: административным, финансовым, информационным, гражданским. И данное обстоятельство находит свое отражение, в частности, еще и в том, что по своей правовой природе налоговая тайна является одновременно и тайной служебной. В силу того, что изначально налоговая тайна является по своей сути информацией (причем, самого разнообразного характера), она может соотноситься с такими видами конфиденциальной информации, как персональные данные, коммерческая тайна.

Правовое значение налоговой тайны состоит в том, что она обеспечивает защиту прав и законных интересов налогоплательщиков в отношении информации, отнесенной законодательством к налоговой тайне, в этой связи законодательное закрепление самого понятия «тайна» позволит не только распространить свою защиту на информацию, независимо от того, на каком материальном носителе она задокументирована и на счет какой информационной системы (ресурса) относится, но также подчеркнет публичный характер тайны и особый статус ее конфидентов.

Литература

[1] Письмо ФНС РФ от 11.06.2009 № МН-22-6/469@ «О предоставлении информации». [Электронный документ] // Режим доступа: http: //base.consultant.ru

[2] Постановление Конституционного Суда РФ от 14.05.2003 № 8-П «По делу о проверке конституционности пункта 2 статьи 14 Федерального закона "О судебных приставах" в связи с запросом Лангепасского городского суда Ханты-Мансийского автономного округа» // СЗ РФ. 2003. № 21. Ст. 2058.

[3] Федеральный закон от 28.06.2013 № 134-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям» // СЗ РФ. 2013. № 26. Ст. 3207.

[4] Аликина Е. Не храните тайны в банках // Журнал «Коммерсантъ Деньги». 2013. № 34. С. 37.

[5] В России принят закон, по которому в следующем году банки обяжут передавать Федеральной налоговой службе информацию о движении средств физлиц. [Электронный документ] // Режим доступа: http: //kommersant-irk.com/ Дата обращения: 27.11.2013.

[6] Гузеев, Ю. Г. Принцип налоговой публичности: понятие, природа, перспективы введения в России // Финансовое право. 2013. № 9. С. 41–42.

[7] См.: Эдиев С. А. Вопросы обеспечения банковской тайны в налоговом контроле: законодательное обеспечение и проблемы судебной практики // Финансовое право. 2013. № 7. С. 45–48; Васильев И. В. Деофшоризация – Стратегия экономической репатриации инвестиционных потоков в Российскую Федерацию / И. В. Васильев, В. А. Карпов // Национальная безопасность / nota bene 2013. № 4. С. 629–635; Кастанова Е. Д. Проблемы правового регулирования обмена информацией в рамках соглашений об избежании двойного налогообложения, заключенных швейцарской конфедерацией // Право и управление. XXI век. 2012. № 1. С. 109–110.

[8] Кастанова Е. Д. Обмен налоговой информацией в рамках борьбы с уклонением от уплаты налогов в новом международном контексте // Актуальные проблемы российского права. 2013. № 10. С. 122–123.

[9] Золотарев Е. В. О противодействии легализации (отмыванию) преступных доходов в условиях автоматизации процессов контроля и экстерриториальных принципов FATCA // Налоговая политика и практика. 2013. № 9–1 (129). С. 7–10.

[10] Борисов О. И. FATCA: новый вызов для российской банковской системы // Банковское дело. 2013. № 1. С. 24–31.

[11] Курныкина О. В. FATCA: борьба с уклонением от налогов с позиции силы? // Банковское дело. 2013. № 7. С. 24–28.

[12] Старженецкая Л. Н. Борьба с уклонением от налогообложения через офшоры: новые модели международного обмена информацией // Налоговед. 2013. № 10. С. 72–81.

[13] Магомедов М. Ш. Удастся ли реализовать поддержанную на саммите G20 идею об автоматическом обмене налоговой информацией? // Евразийский юридический журнал. 2013. № 8 (63). С. 55–56.

References

[1] Pis'mo FNS RF ot 11.06.2009 № MN-22-6/469@ «O predostavlenii informacii» [Letter of the Federal Tax Service of the Russian Federation as of 11.06.2009 No. MN-22-6/469@ 'On information supply'] [Electronic resource] // Rezhim dostupa: http: //base.consultant.ru

[2] Postanovlenie Konstitucionnogo Suda RF ot 14.05.2003 № 8-P «Po delu o proverke konstitucionnosti punkta 2 stat'i 14 Federal'nogo zakona «O sudebnyh pristavah» v svjazi s zaprosom Langepasskogo gorodskogo suda Hanty-Mansijskogo avtonomnogo okruga» [Decision of the constitutional court of the Russian Federation as of 14.05.2003 No. 8-P 'On the case of checking of point 2, Article 14 of the Federal Law 'On court marshals' in connection with the enquiry of the Langepass City Court of the Khanty-Mansiisk Autonomous District'] // SZ RF [Official Gazette of the Russian Federation]. 2003. No. 21. Art. 2058.

[3] Federal'nyj zakon ot 28.06.2013 № 134-FZ «O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii v chasti protivodejstvija nezakonnym finansovym operacijam» [Federal Law as of 28.06.2013 No. 134-FZ 'On the amendments in certain statutory acts of the Russina Federation in the field of countermeasures against illegal financial business']// SZ RF [Offiial Gazette of the Russian Federation]. 2013. No. 26. Art. 3207.

[4] Alikina E. Ne hranite tajny v bankah [Do not keep your secrets in jars and pots]// Zhurnal «Kommersant# Den'gi»]. 2013. No. 34. p. 37.

[5] V Rossii prinjat zakon, po kotoromu v sledujushhem godu banki objazhut peredavat' Federal'noj nalogovoj sluzhbe informaciju o dvizhenii sredstv fizlic. [Russia has passed the law which implies that next year banks will have to send the Federal Tax Service the information on the flow of funds] [Electronic resource] // Rezhim dostupa: http: //kommersant-irk.com/ Data obrashhenija [Date of compellation]: 27.11.2013

[6] Guzeev, Ju.G. Princip nalogovoj publichnosti: ponjatie, priroda, perspektivy vvedenija v Rossii [The principle of tax publicity: the notion, nature, and perspectives of introduction in Russia] // Finansovoe pravo [Financial law]. 2013. No. 9. p. 41-42.

[7] Sm.: Jediev S.A. Voprosy obespechenija bankovskoj tajny v nalogovom kontrole: zakonodatel'noe obespechenie i problemy sudebnoj praktiki [Questions of ensuring bank secrecy in tax control: state ensuring and problems of judicial practice]// Finansovoe pravo [Financial Law]. 2013. No. 7. p. 45-48.; Vasil'ev I.V. Deofshorizacija – Strategija jekonomicheskoj repatriacii investicionnyh potokov v Rossijskuju Federaciju. [Starategy of economic repatriation of investment flows in the Russian Federation]/ I.V. Vasil'ev, V.A. Karpov. // Nacional'naja bezopasnost' [National security]/ nota bene 2013. No. 4. p. 629-635; Kastanova E.D. Problemy pravovogo regulirovanija obmena informaciej v ramkah soglashenij ob izbezhanii dvojnogo nalogooblozhenija, zakljuchennyh shvejcarskoj konfederaciej [Problems of legal regulation of information exchange within the framework of agreements on the avoidance of double taxation made by the Swiss confederation]// Pravo i upravlenie. XXI vek [Law and Administration. 21st century]. 2012. No. 1. p. 109-110.

[8] Kastanova E.D. Obmen nalogovoj informaciej v ramkah bor'by s ukloneniem ot uplaty nalogov v novom mezhdunarodnom kontekste [Tax information exchange within the framework of the fight against evasion of taxes in new international context]// Aktual'nye problemy rossijskogo prava [Topical issues of the Russian Law]. 2013. No.10. p. 122-123.

[9] Zolotarev E.V. O protivodejstvii legalizacii (otmyvaniju) prestupnyh dohodov v uslovijah avtomatizacii processov kontrolja i jeksterritorial'nyh principov FATCA [On countermeasures against legalization of criminal profit in the conditions of automatixation of control processes and exterritorial principles of FATCA]// Nalogovaja politika i praktika [Legal Policy and Practice]. 2013. No. 9-1 (129). p. 7-10

[10] Borisov O.I. FATCA: novyj vyzov dlja rossijskoj bankovskoj sistemy [FATCA: New challenge for Russian bank system]// Bankovskoe delo [Banking business]. 2013. No. 1. p. 24-31.

[11] Kurnykina O.V. FATCA: bor'ba s ukloneniem ot nalogov s pozicii sily? [FATCA: Anti-evasion measures from the viewpoint of force]// Bankovskoe delo [Banking business]. 2013. No. 7. p. 24-28.

[12] Starzheneckaja L.N. Bor'ba s ukloneniem ot nalogooblozhenija cherez offshory: novye modeli mezhdunarodnogo obmena informaciej [Anti-evasion through the off-shore: New models of international information exchange]// Nalogoved [Tax expert]. 2013. No. 10. p. 72-81.

[13] Magomedov M.Sh. Udastsja li realizovat' podderzhannuju na sammite G20 ideju ob avtomaticheskom obmene nalogovoj informaciej? [Will we succeed in the realization of the support the idea of automated tax information exchange on the summit G20]// Evrazijskij juridicheskij zhurnal [Eurasian legal journal]. 2013. No. 8 (63). p. 55-56.

Белишко Иван Андреевич, студент магистратуры кафедры предпринимательского и коммерческого права ЮУрГУ. E-mail: vev635@mail.ru.

Belishko Ivan Andreyevich, graduate student of the department of business and commercial law SUSU. E-mail: vev635@mail.ru.

УДК 347.19.03
ББК Х 404.013 + Х 404.021

А. В. Минбалеев

ОТЗЫВ НА АВТОРЕФЕРАТ ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ЮРИДИЧЕСКИХ НАУК О. Ш. АЮПОВА ПО ТЕМЕ «ЗАЩИТА ДЕЛОВОЙ РЕПУТАЦИИ ЮРИДИЧЕСКОГО ЛИЦА ОТ ДИФФАМАЦИИ В ГРАЖДАНСКОМ ПРАВЕ РОССИИ»

Отзыв подготовлен на автореферат диссертации на соискание ученой степени кандидата юридических наук по теме «Защита деловой репутации юридического лица от диффамации в гражданском праве России». Работа посвящена актуальной проблеме, разрабатываемой как в науке гражданского права, так и информационного права. В работе рассматриваются проблемы современных способов защиты деловой репутации юридических лиц при распространении информации, не соответствующей действительности.

Ключевые слова: *диффамация, защита, деловая репутация, отзыв, диссертация.*

A. V. Minbaleev

COMMENT ON ABSTRACT THESIS FOR THE SCIENTIFIC DEGREE IN LAW O. SH. AIUPOVA ON «PROTECTION OF GOODWILL ENTITY FROM DEFAMATION IN CIVIL LAW OF RUSSIA»

Review prepared on the dissertation for the degree of master of laws on «Protection of business reputation of the legal entity of the civil law of defamation in Russia." The paper is devoted

to the actual problem, as developed in the science of civil law and information law. The paper deals with the problems of modern methods of protection of business reputation of legal entities in disseminating information, untrue.

Keywords: *protection, defamation, business reputation, review, thesis.*

Современные социально-экономические преобразования, происходящие в настоящее время в нашей стране, привели к активному обмену информацией, в том числе о юридических лицах. Неудивительно, что достаточно существенная часть этой информации представляет собой диффамацию. В условиях развития информационного общества сегодня очень легко распространить неопределенному кругу лиц любые сведения через различные средства интернет-коммуникации. В этой связи вопросы диффамации и защиты от нее не перестают терять актуальности. Любая организация сегодня сталкивается с освещением тех или иных сторон ее деятельности сотрудниками, клиентами, партнерами, СМИ, общественностью. С развитием системы WEB 2.0 и ее совершенствования до современных 5.0 возможности создания любых интернет-источников, посвященных той или иной организации, а также построения на их базе архитектуры системы свободного открытого обсуждения ее деятельности становится доступной любому пользователю сети Интернет. За прошедшие годы новой истории России были приняты нормативные правовые акты, которые регулируют отношения, возникающие в связи с диффамацией. Появилась судебная практика, которая чрезвычайна неоднозначна и не всегда позволяет выработать единые представления о защите деловой репутации юридических лиц от диффамации. В связи с этим выбор темы исследования также представляется очень актуальным.

Несомненным и главным достоинством работы является системное, комплексное исследование вопросов защиты деловой репутации юридических лиц от диффамации в условиях обновленного российского законодательства. Автор исследует сущность диффамации, впервые в науке гражданского права детально рассматривает субъективное право юридического лица на деловую репутацию сквозь призму современных представлений о диффамации и особенностей ее реализации в сети Интернет.

В автореферате содержится ряд выводов, с которыми трудно не согласиться. В частности, автор в работе убедительно показывает, что не во всех случаях, когда происходит распространение оценочных сведений, мы можем говорить об освобождении от диффамации. Анализ ряда судебных решений и материалов, вышедших в средствах массовой информации, свидетельствует, что очень часто журналисты, иные специалисты в сфере массовых коммуникаций, используя те или иные приемы эмоциональной окраски текста, в том числе тропы, вводные слова и выражения, специально создают образ, который ассоциируется у аудитории как достоверный. В данном случае мы можем говорить о злоупотреблении правом, что должно учитываться судом и рассматриваться как диффамация (с. 8–9, 15–16 автореферата).

Автором верно обосновывается идея, что при определении объема информации, которая признана судом как диффамационная, которая должна быть удалена из сети Интернет, необходимо учитывать конституционное право на свободу слова и определять пределы удаления информации (С. 19 автореферата). Правда, из автореферата не следует, рассматривает ли автор другие основания для отказа судом в удовлетворении требований по удалению диффамационного материала из сети Интернет? Автором в автореферате не затрагивается вопрос возможностей такого отказа. К большому сожалению, ни ст. 152 Гражданского кодекса Российской Федерации, ни акты высших судебных инстанций, в которых отражается его позиция по диффамации, не содержат возможности отказа в удалении. Между тем такие основания имеются, например решение Европейского суда по правам человека по делу Вегржиновски и Смолчевски против Польши содержит в себе позицию, согласно которой материалы культурного и исторического значения не подлежат удалению из архивов интернет-СМИ.

Заслуживают внимание также и другие предложения, сделанные автором, которые, бесспорно, вносят вклад в теорию гражданского права, а также будут полезны правоприменителю при рассмотрении диффамационных споров.

В то же время представляется, что в работе содержатся отдельные положения, носящие дискуссионный характер.

1. Так, сложно однозначно согласиться с автором в критериях разграничения полной и усеченной диффамации (с. 15 автореферата). Автор указывает, что нельзя применять компенсацию морального вреда при усеченной диффамации, поскольку при ней не порочатся честь, достоинство и деловая репутация. Данный вывод может быть применим только в отношении юридических лиц, поскольку распространение недостоверной информации может затрагивать и другие нематериальные блага физических лиц. Также указывается, что бремя доказывания при усеченной диффамации лежит на истце. С этим сложно согласиться, полагаем, что истец должен доказывать только факт распространения сведений, а на ответчике лежит обязанность доказывания достоверности распространенных сведений.

2. При рассмотрении вопросов ответственности владельца сайта за диффамацию, осуществленную анонимными пользователями, автор достаточно подробно рассматривает возможности привлечения к ответственности провайдера и владельца сайта (с. 17–18 автореферата). При этом, однако, в работе не указываются положения о возможности такой ответственности, заложенные решением Европейского суда по правам человека по делу Делфи против Эстонии, в рамках которого владелец сайта был привлечен к ответственности за диффамацию, осуществленную анонимными пользователями.

Изложенные замечания, однако, не влияют на глубокую разработанность темы и высокий научный уровень диссертационного исследования. Оно представляет собой самостоятельный творческий труд по весьма актуальной для современного периода проблеме.

Содержание автореферата свидетельствует о том, что кандидатская диссертация Аюпова Олега Шамильевича по теме «Защита деловой репутации юридического лица от диффамации в гражданском праве России» соответствует предъявляемым к ней требованиям, а диссертант, без сомнения, заслуживает присуждения ему ученой степени кандидата юридических наук.

Минбалеев А. В., доцент кафедры предпринимательского и коммерческого права Южно-Уральского государственного университета, д.ю.н., доцент.

Minbaleev A. V., assistant professor of business and commercial law South-Ural State University, Doctor of Law, Associate Professor.

ЦЕНТР ПО ЭКСПОРТНОМУ КОНТРОЛЮ ЮУрГУ

В соответствии с решением Комиссии по экспортному контролю Российской Федерации Южно-Уральский госуниверситет получил Свидетельство о специальном разрешении № 027 на осуществление деятельности по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля.

В настоящее время ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ) располагает научно-педагогическим персоналом с высоким профессиональным и интеллектуальным уровнем, а также развитой лабораторной базой, это позволяет профессионально и качественно осуществлять деятельность по проведению независимой идентификационной экспертизы товаров и технологий, проводимой в целях экспортного контроля.

В соответствии с номенклатурой продукции, в отношении которой планируется осуществлять экспертизу, подобрано 107 экспертов, из них докторов наук 35, кандидатов наук 57 и 15 специалистов, не имеющих ученой степени. Все эксперты являются сотрудниками университета и способны квалифицированно и качественно провести экспертизу.

Если Вы являетесь поставщиками оборудования, машин, материалов, запасных частей и комплектующих для них, выпускаете сложную технику, научно-техническую продукцию и Вам приходится сталкиваться с терминами **«экспортный контроль»** и **«товары двойного назначения»**, то мы можем быть Вам полезны.

В соответствии с российским законодательством экспертизу товаров и технологий для целей экспортного контроля могут проводить только экспертные организации, получившие специальное разрешение Комиссии экспортного контроля Российской Федерации.

Центр по экспортному контролю ЮУрГУ осуществляет деятельность по проведению независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля в отношении **продукции по всей номенклатуре действующих контрольных списков, утвержденных указами Президента Российской Федерации.**

Директор Центра:
Анатолий Григорьевич Мещеряков.
Тел. (351) 267-95-49.

Заключения нашей экспертизы действуют на всей территории России и являются официальным документом, подтверждающим принадлежность или непринадлежность объекта экспертизы к продукции, включенной в списки контролируемых товаров и технологий.

Наши услуги:

1. Оформление заключений идентификационной экспертизы для целей экспортного контроля и таможенного оформления.
2. Консультация по экспортному контролю товаров (технологии).

Перечень документов, необходимых для проведения экспертизы:

1. Заявка.
2. Контракт (договор, соглашение).
3. Спецификация (перечень поставляемой продукции) и иные приложения.
4. Техническая документация (паспорта, сертификаты качества, руководства по эксплуатации, технические описания, этикетки и пр.).
5. Доверенность.

Наши координаты

Адрес: 454080, г. Челябинск, пр. им. В. И. Ленина, 85, корпус 3А, ауд. 502.
Телефон (351) 267-95-49
E-mail: exp-174@mail.ru
Транспорт (автобус, троллейбус, маршрутное такси): остановка «ЮУрГУ»

ФИРМЕННЫЙ БЛАНК ОРГАНИЗАЦИИ

Исх. № _____
от «___» _____ 201__ г.

Директору Центра по экспортному
контролю ГОУ ВПО «ЮУрГУ»
А. Г. Мещерякову
454080, пр. им. В. И. Ленина, 85,
корпус 3А, ауд. 502

ЗАЯВКА
на проведение работ

Прошу Вас провести независимую идентификационную экспертизу товаров (технологий) в целях экспортного контроля и таможенного оформления.

Грузоотправитель: _____
_____

Грузополучатель: _____
_____

Перечень поставляемой продукции:

№ п/п	Наименование продукции	Единица измерения	Количество	Код ТН ВЭД

Оплату работ по выставлении счета гарантирую.

Уполномоченный по техническим вопросам: _____
_____

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Полезная информация

1. Экспертиза проводится в течение 3-х рабочих дней. По просьбе заказчика экспертиза может быть проведена в более короткие сроки.

2. Стоимость проведения экспертизы зависит от:

- объема рассматриваемого материала, продукции, информации, представленных согласно заявке;
- количества наименований товаров;
- количества кодов ТН ВЭД;
- сроков исполнения заявки;
- степени секретности материала, представленного на экспертизу.

3. Готовое заключение выдается на бумажном носителе (по просьбе заказчика — в электронном варианте).

4. Договор на оказание услуг заключается каждый раз в соответствии с заявкой.

Федеральные органы исполнительной власти

ФСТЭК России: http://www.fstec.ru/

РЕГИОНАЛЬНЫЙ АТТЕСТАЦИОННЫЙ ЦЕНТР ЮУрГУ

«Региональный аттестационный центр» создан на основании решения Ученого совета Южно-Уральского государственного университета от 25.06.2007 г. № 10 по согласованию с Управлением ФСБ России по Челябинской области. Основными функциями «Регионального аттестационного центра» являются:

1) всестороннее обследование предприятий-заявителей на предмет их готовности к выполнению работ, связанных с использованием сведений, составляющих государственную тайну;

2) осуществление мероприятий по оказанию услуг в данной области;

3) повышение квалификации сотрудников режимно-секретных подразделений.

Решением Межведомственной комиссии по защите государственной тайны № 95 от 06 апреля 2005 года Южно-Уральский государственный университет включен в перечень учебных заведений, осуществляющих подготовку специалистов по вопросам защиты информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну» (в зачет государственной аттестации).

Категория слушателей: руководители организаций, заместители руководителей организации, ответственные за защиту сведений, составляющих государственную тайну.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации, которое дает право руководителям предприятий, учреждений, организаций на освобождение от государственной аттестации.

Форма обучения – очно-заочная (48 часов заочная, 24 часа – очная форма обучения).

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске, учебным пособием курса лекций.

Курсы повышения квалификации по программе «Защита информации, составляющей государственную тайну».

Категория слушателей: руководители и сотрудники структурных подразделений по защите государственной тайны.

По окончании обучения слушателям выдается удостоверение государственного образца о краткосрочном повышении квалификации.

Форма обучения – очная (72 часа). Обучение слушателей осуществляется с отрывом от производства – 2 недели.

Слушатели обеспечиваются раздаточным материалом, нормативными документами на компакт-диске.

Программа предусматривает изучение следующих дисциплин:

1) Правовое и нормативное обеспечение защиты государственной тайны;

2) Организация комплексной защиты информации в организациях;

3) Организация режима секретности в организации;

4) Организация защиты информации, обрабатываемой средствами вычислительной техники;

5) Организация защиты информации при осуществлении международного сотрудничества;

6) Допуск граждан к сведениям, составляющим государственную тайну;

7) Организация и ведение секретного делопроизводства;

8) Ответственность за нарушение законодательства РФ по защите государственной тайны. Порядок проведения служебного расследования по нарушениям.

«Региональный аттестационный центр» на договорной основе предоставляет предприятиям, учреждениям и организациям услуги в сфере защиты государственной тайны:

• оказание методической и консультационной помощи работникам режимно-секретных подразделений предприятий и организаций;

• специальное обслуживание предприятий, не имеющих в своей структуре режимно-секретных подразделений:

1) ведение допускной работы в соответствии с требованиями «Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне», утвержденной постановлением Правительства РФ от 06 февраля 2010 г. № 63;

2) выделение для проведения секретных работ помещений, соответствующих требованиям Инструкции по обеспечению режима секретности в Российской Федерации, утвержденной постановлением Правительства РФ от 05.01.2004 № 3-1 (далее – Инструкция № 3-1-04 г.);

3) выделение для хранения секретных документов помещений, соответствующих требованиям Инструкции № 3-1-04 г.;

4) организация и ведение секретного делопроизводства в соответствии с общими нормативными требованиями Инструкции № 3-1-04 г.;

5) обеспечение защиты государственной тайны при обработке и хранении секретной информации на средствах вычислительной техники и (или) в автоматизированных системах;

6) подготовка Заключения о фактической осведомленности работников в сведениях, составляющих государственную тайну;

7) разработка нормативно-методической документации по вопросам защиты государственной тайны;

8) профессиональная подготовка и обучение работников Заказчика, допущенных к работам с носителями секретной информации;

9) осуществление мероприятий по подготовке к проведению специальной экспертизы Заказчика на предмет получения и продления лицензии на право работ с использованием сведений, составляющих государственную тайну, а также к проведению государственной аттестации его руководителя, ответственного за защиту сведений, составляющих государственную тайну.

Контактные адреса и телефоны:

Юридический адрес: 454080, г. Челябинск, пр. им. В. И. Ленина, д. 76
Фактический адрес: г. Челябинск, пр. им. В. И. Ленина, д. 85, ауд. 512/3
Телефоны: (351) 267-91-55, 267-93-14, 267-92-85
E-mail: rac512@mail.ru

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ К ПУБЛИКАЦИИ В ЖУРНАЛЕ «ВЕСТНИК УрФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ».

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцом оформления рукописи, а также приложить к статье сведения о себе (см. Сведения об авторе).

Сведения об авторе

ФИО (полностью)	
Ученая степень	
Ученое звание	
Должность и место работы (полностью)	
Домашний адрес	
Контактные телефоны	
e-mail	
Тема статьи	
Являетесь ли аспирантом (если да, то указать дату приема в аспирантуру и научного руководителя)	

УДК
ББК

ОБРАЗЕЦ

А. А. Первый, Б. Б. Второй, В. В. Третий

НАЗВАНИЕ СТАТЬИ, ОТРАЖАЮЩЕЕ ЕЕ НАУЧНОЕ СОДЕРЖАНИЕ, ДЛИНОЙ НЕ БОЛЕЕ 12—15 СЛОВ

Аннотация набирается одним абзацем, отражает научное содержание статьи, содержит сведения о решаемой задаче, методах решения, результатах и выводах. Аннотация не содержит ссылок на рисунки, формулы, литературу и источники финансирования. Рекомендуемый объем аннотации — около 50 слов, максимальный — не более 500 знаков (включая пробелы).

Ключевые слова: список из нескольких ключевых слов или словосочетаний, которые характеризуют Вашу работу.

Рисунки

Вставляются в документ целиком (не ссылки). Рекомендуются черно-белые рисунки с разрешением от 300 до 600 dpi. Подрисуночная подпись формируется как надпись («Вставка», затем «Надпись», без линий и заливки). Надпись и рисунок затем группируются, и устанавливается режим обтекания объекта «вокруг рамки». Размер надписей на рисунках и размер подрисуночных подписей должен соответствовать шрифту Times New Roman, 8 pt, полужирный. Точка в конце подрисуночной подписи не ставится. На все рисунки в тексте должны быть ссылки.

Все разделительные линии, указатели, оси и линии на графиках и рисунках должны иметь толщину не менее 0,5 pt и черный цвет. Эти рекомендации касаются всех графических объектов и объясняются ограниченной разрешающей способностью печатного оборудования.

Формулы

Набираются со следующими установками: стиль математический (цифры, функции и текст — прямой шрифт, переменные — курсив), основной шрифт — Times New Roman 11 pt, показатели степени 71 % и 58 %. Выключенные формулы должны быть выровнены по центру. Формулы, на которые есть ссылка в тексте, необходимо пронумеровать (сплошная нумерация). Расшифровка обозначений, принятых в формуле, производится в порядке их использования в формуле. Использование букв кириллицы в формулах не рекомендуется.

Таблицы

Создавайте таблицы, используя возможности редактора MS Word или Excel. Над таблицей пишется слово «Таблица», Times New Roman, 10 pt, полужирный, затем пробел и ее номер, выравнивание по правому краю таблицы. Далее без абзацного отступа следует таблица. На все таблицы в тексте должны быть ссылки (например, табл. 1).

Примечания

Источники располагаются в порядке цитирования и оформляются по ГОСТ 7.05-2008.

Статья публикуется впервые
Подпись, дата

Структура статьи (суммарный объем статьи – не более 40 000 знаков):

1. УДК, ББК, название (не более 12–15 слов), список авторов.
2. Аннотация (не более 500 знаков, включая пробелы), список ключевых слов.
3. Основной текст работы.
4. Примечания

Объем статьи не должен превышать 40 тыс. знаков, включая пробелы, и не может быть меньше 5 страниц. Статья набирается в текстовом редакторе Microsoft Word в формате *.rtf шрифтом Times New Roman, размером 14 пунктов, в полуторном интервале. Отступ красной строки: в тексте — 10 мм, в затекстовых примечаниях (концевых сносках) отступы и выступы строк не ставятся. Точное количество знаков можно определить через меню текстового редактора Microsoft Word (Сервис — Статистика — Учитывать все сноски).

Параметры документа: верхнее и нижнее поле — 20 мм, правое — 15 мм, левое — 30 мм.

В начале статьи помещаются: инициалы и фамилия автора (авторов), название статьи, аннотация на русском языке объемом до 50 слов, ниже отдельной строкой — ключевые слова. Инициалы и фамилия автора (авторов), название статьи, аннотация и ключевые слова должны быть переведены на английский язык.

В случае непрямого цитирования источников и литературы в начале соответствующего примечания указывается «См.:».

Цитируемая литература дается не в виде подстрочных примечаний, а общим списком в конце статьи с указанием в тексте статьи ссылки порядковой надстрочной цифрой (Формат — Шрифт — Надстрочный) (например, [1]). Запятая, точка с запятой, двоеточие и точка ставятся после знака сноски, чтобы показать, что сноска относится к слову или группе слов, например: по иску собственника[1]. Вопросительный, восклицательный знак, многоточие и кавычки ставятся перед знаком сноски, чтобы показать, что сноска относится ко всему предложению, например: …все эти положения закреплены в Федеральном законе «О ветеранах»[1].

Литература дается в порядке упоминания в статье.

При подготовке рукописи автору рекомендуется использовать ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления» (Полный текст ГОСТ Р размещен на официальном сайте Федерального агентства по техническому регулированию и метрологии).

В конце статьи должна быть надпись *«Статья публикуется впервые»,* ставится дата и авторучкой подпись автора (авторов). При пересылке статьи электронной почтой подпись автора сканируется в черно-белом режиме, сохраняется в формате *.tif или *.jpg и вставляется в документ ниже затекстовых сносок.

Обязательно для заполнения: В конце статьи (в одном файле) на русском языке помещаются сведения об авторе (авторах) — ученая степень, ученое звание, должность, кафедра, вуз; рабочий адрес, электронный адрес и контактные телефоны.

В редакцию журнала статья передается качественно по электронной почте одним файлом (название файла — фамилия автора). Тема электронного письма: Информационная безопасность.

Порядок прохождения рукописи

1. Все поступившие работы регистрируются, авторам сообщается ориентировочный срок выхода журнала, в макет которого помещена работа.

2. Поступившая работа проверяется на соответствие всем формальным требованиям и при отсутствии замечаний, в случае необходимости, направляется на дополнительную экспертизу.

3. Для публикации работы необходима положительная рецензия специалиста из данной или смежной области. На основании рецензии принимается решение об опубликовании статьи (рецензия без замечаний) или о возврате автору на доработку, в этом случае рукопись может проходить экспертизу повторно. При получении второй отрицательной рецензии на работу редакция принимает решение об отказе в публикации.

Материалы к публикации отправлять по адресу
E-mail: urvest@mail.ru в редакцию журнала «Вестник УрФО».

Или по почте по адресу:
Россия, 454080, г. Челябинск, пр. им. В. И. Ленина, 76, ЮУрГУ, Издательский центр.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(10) / 2013

Подписано в печать 20.12.2013. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,60. Тираж 300 экз. Заказ 13/34.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.