ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 3(9) / 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**

В НОМЕРЕ

ORGANIZATIONAL AND TECHNICAL INFORMATION SECURITY

LEGAL REGULATION OF INFORMATION SECURITY

TOPICAL ISSUES OF CYBER SECURITY

REVIEWS

THE PRACTICAL ASPECT

УДК 342.7:004.056.5 + 37.014:004.056.5
ББК Х401.114 + Ч4:Х401.114

Астахова Л. В., Завадский А. О.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В статье рассматриваются проблемы информационной безопасности образовательных организаций. Авторы исследуют методы обеспечения информационной безопасности образовательных организаций. В качестве основной проблемы, поднимаемой в работе, является вопрос защиты персональных данных. Особенности защиты персональных данных в образовательных организациях обусловлены организационными, техническими, кадровыми и финансовыми аспектами деятельности последних. Авторами выявлены основные проблемы реализации Федерального закона «О персональных данных».

Ключевые слова: *персональные данные, информационная безопасность, образовательные организации, защита.*

Astakhova L. V., Zavadsky A. O.

PECULIARITIES OF THE PERSONAL DATA SECURITY IN AN EDUCATIONAL INSTITUTION

The article considers the topical issues of information security in educational institutions. The authors investigate the methods of security arrangements in educational institutions. The matter of personal data security is raised as a main issue of the article. The peculiarities of personal data security in educational institutions are determined by organizational, technical, personnel, and financial aspects of their activities. The authors also discover the chief problems of the realization of the Federal Law 'On Personal Data'.

Keywords: *personal data, information security, educational institutions, security.*

Проблема информационной безопасности образовательных организаций обусловлена противоречием между ускоряющимися темпами информатизации образования и виртуализации образовательной среды[1], требованиями действующего российского законодательства по защите электронных информационных ресурсов, с одной стороны, и

недостаточной готовностью к этой серьезной деятельности школ, колледжей, техникумов, вузов – с другой. Количество угроз информации растет с каждым днем, изменяются нормативно-правовая база и способы обработки информации. Согласно реалиям времени должны изменяться и методы обеспечения информационной безопасности образовательных организаций.

В проблеме обеспечения информационной безопасности любой организации четко выделяются технический, организационный и документационный аспекты. Технический аспект связан с выбором технологий защиты и программного обеспечения, организационный – с проведением мероприятий для реализации закона № 152-ФЗ «О персональных данных»[13], а документационный – с созданием локальных актов образовательного учреждения на основе действующих нормативно-правовых актов федерального уровня.

Специфика образовательной организации такова, что обработке подвергаются не только данные сотрудников и преподавателей, но и студентов, школьников (обучающихся) и их родителей или законных представителей. Соответственно, для выполнения требований законодательства необходима система получения согласия родителей или законных представителей на обработку персональных данных их самих и их детей (в случае, если обучающийся совершеннолетний, то он сам дает такое согласие).

Ситуация осложняется тем, что в отличие от Трудового кодекса РФ, полно и конкретно описывающего порядок обработки персональных данных работника работодателем, до недавно принятого ФЗ «Об образовании в Российской Федерации»[14] не было. Только в феврале 2011 года была принята поправка в закон, регламентирующая порядок получения образовательными учреждениями согласия субъектов персональных данных и некоторые вопросы их обработки, но касается она только тех, кто так или иначе связан с единым государственным экзаменом. Часть 5.1 статьи 15 «Общие требования к организации образовательного процесса» указанного закона определяет: «Органы и организации осуществляют передачу, обработку и предоставление полученных в связи с проведением единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего профессионального образования персональных данных обучающихся, участников единого государственного экзамена, лиц, привлекаемых к его проведению, а также лиц, поступающих в такие образовательные учреждения, в соответствии с требованиями законодательства Российской Федерации в области персональных данных без получения согласия этих лиц на обработку их персональных данных»[14]. А это значит, что в соответствии со 152-ФЗ образовательные учреждения должны каким-то образом получить согласие на обработку персональных данных субъектов, т. е. обучающихся или воспитанников. Поскольку значительная часть обучающихся не достигла совершеннолетия, получать согласие надо у их законных представителей.

Органы власти выдвигают требования о быстром и эффективном внедрении информационных технологий в работу образовательных учреждений. Выступая на выездном заседании Совета при Президенте по развитию информационного общества, Дмитрий Медведев отметил, что внедрение электронных образовательных ресурсов идет еще медленно, а электронный журнал оценок с организацией доступа к нему родителей через Интернет и в ряде случаев с их SMS-оповещением используется только в школах крупных городов[7]. Между тем, раздел «Квалификационные характеристики должностей работников образования» предусматривает такие должностные обязанности учителя, как осуществление контрольно-оценочной деятельности в образовательном процессе «с использованием современных способов оценивания в условиях информационно-коммуникационных технологий (ведение электронных форм документации, в том числе электронного журнала и дневников обучающихся)»[6].

Электронный журнал оценок в терминах закона – это информационная система персональных данных, которую надо защищать в соответствии с обязательными требованиями, установленными Правительством РФ. При передаче содержащихся в нём сведений по незащищенным интернет-каналам необходимо применять средства защиты информации, прошедшие процедуру оценки соответствия нормативным требованиям, результаты которой должны быть подвергнуты экспертизе в ФСБ России.

Главная проблема здесь – соответствие закону о персональных данных, соблюдение

конфиденциальности персональных данных при передаче её в сетях информационного обмена. Для решения этой проблемы необходимо определить, какая информация доступна учителю, родителям или ребенку. Для использования Интернета при передаче информации требуются определенные технические решения, над которыми работают Минкомсвязи и Рособрнадзор, однако о конкретных сроках говорить преждевременно.

В дополнение к электронным журналам Министерство образования и науки предложило внедрить еще и Паспорт здоровья школьника, который среди прочего предусматривает указание следующих сведений, в том числе отнесенных законом 152-ФЗ к категории специальных: ФИО, год рождения, образование, специальность, должность, рабочие, домашние и мобильные телефоны родителей, дедушек, бабушек, братьев и сестер; семейная обстановка (характеризующие ее параметры – благополучная; конфликтная; есть ли член семьи с ограниченными двигательными способностями; есть ли тяжелобольной в семье); ФИО заведующих детскими отделениями и врачей-терапевтов всех поликлиник, куда ребенок обращался, с указанием телефонов и адресов; перенесенные и хронические заболевания (очень конкретно), полученные черепно-мозговые травмы, сведения о госпитализациях, о травмах, группа крови и резус-фактор, санаторно-профилактическое лечение; формула полового развития ребенка; сведения о регулярности потребления тридцати трёх групп пищевых продуктов; сведения о курящих или бросивших курение членах семьи; карта индивидуального психологического развития школьника 1–4 классов.

Ситуация с выполнением в образовательных учреждениях требований ФЗ-152 существенно усложняется особенностями их функционирования. К таковым можно отнести следующие:

• отсутствие в бюджетах образовательных учреждений статей расходов на реализацию мер по организационной и технической защите персональных данных;

• специфика построения информационных систем образовательных учреждений, зачастую созданных с использованием «самописного» и свободного программного обеспечения;

• наличие в эксплуатации довольно большого количества компьютеров, часть которых будет требовать реализации регламентов по защите персональных данных;

• отсутствие штатных специалистов по информационной безопасности, а часто и по информационным технологиям;

• сложность разграничения отношений между образовательным учреждением, обучаемыми, их представителями и иными лицами (родителями, опекунами, работодателями, организациями, выделяющими гранты, и т. п.).

Наибольшие трудности возникают с технической стороны защиты персональных данных. В силу особенности организации учебного процесса, обработка персональных данных ведется на многих компьютерах, не всегда объединенных в локальную сеть. Возникает необходимость использования одной базы данных с организацией доступа по паролю, что влечет за собой изменение и расширение структуры локальной сети образовательного учреждения. Также необходимо определить возможные каналы утечки информации и возможные угрозы информационной системе, построить модель угроз нарушителя и на их основе строить модель защиты. Выполнить эту работу неспециалисту в области защиты информации практически невозможно, соответственно возникает проблема: либо обучаться самостоятельно, либо платить деньги за обучение сотрудника, либо полностью передать вопрос защиты персональных данных сторонней организации. Не стоит забывать, что еще один необходимый шаг в организации технической стороны защиты персональных данных – обязательная сертификация программного обеспечения для ИСПДн также требует немалых финансовых средств.

Выявленные проблемы могут быть решены следующим образом.

1. Недостаток финансовых средств на реализацию требований законодательства в сфере персональных данных.

Значительную часть стоимости внедрения защищенной ИСПДн составляет закупка и внедрение сертифицированных средств инженерно-технической защиты. Так, по мнению авторитетного аналитика в области персональных данных А. Лукацкого, стоимость аттестации ИСПДн в среднем составляет 6% от расходной части бюджета муниципального учреждения[9]. В то же время стоимость защиты напрямую зависит от класса, который был присвоен информационной системе. Ис-

ходя из этого, решение данной проблемы кроется в принятии мер по снижению классов информационных систем, если они высоки и требуют, по полученным оценкам, значительных затрат на обеспечение защиты.

Рособразование справедливо предлагает следующие способы понижения классов ИСПДн:

- обезличивание персональных данных;
- полное исключение из ИСПДн сведений, касающихся политических взглядов, состояния здоровья;
- сегментирование ИСПДн и классификацию сегментов как самостоятельных систем более низкого класса (такое часто возможно, но для этого потребуются межсетевые экраны);
- оптимизацию подключения к сетям связи общего пользования и сети Интернет (если не всей сети учреждения, то хотя бы того выделенного сегмента, где обрабатываются персональные данные);
- обеспечение обмена между ИСПДн с помощью сменных носителей (использовать так называемый «флоппинет»);
- создание ИСПДн на выделенных автоматизированных рабочих местах, куда полностью переносится обработка этой категории сведений из локальной сети[6].

Акцент делается на обезличивании как наиболее эффективном и дешевом способе снижения класса системы. Обрабатывающая обезличенные данные ИСПДн относится к уровню защищенности 4 и не требует принятия дорогостоящих мер по обеспечению конфиденциальности сведений. С этой целью агентство рекомендовало присвоить каждому субъекту внутренний идентификационный номер (условный код) на весь период обучения или работы и использовать его в информационных системах вместо ФИО.

2. Защита электронных журналов.

Согласно Распоряжению Правительства России от 25 апреля 2011 г. № 729-р «Об утверждении перечня услуг, оказываемых государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ), подлежащих включению в реестры государственных или муниципальных услуг и предоставляемых в электронной форме»[8], названные услуги должны быть включены в реестры государственных или муниципальных услуг и предоставляться в электронной форме.

В этом перечне предусмотрены следующие обязанности образовательных учреждений: предоставление информации в электронном виде о текущей успеваемости ученика, об образовательных программах и учебных планах, рабочих программах учебных курсов, предметах, дисциплинах, годовых календарных учебных графиках; ведение дневника и журнала успеваемости. Специфика таких видов услуг выражается в автоматизированной передаче персональных данных третьим лицам (представителям сервиса), их обработке за пределами школы.

Коммерческие организации предлагают различные on-line сервисы, работающие напрямую со школами и предлагающие на первых порах бесплатную для школы услугу по ведению электронных журналов и дневников, что затем, как правило, сменяется платным обслуживанием и нередко требует дополнительного оборудования. Однако такие сервисы зачастую не выполняют всех требований законодательства, не обеспечивают безопасность персональных данных при их трансграничной передаче и перекладывают всю ответственность на образовательное учреждение. Кроме того, для обработки и передачи ПД учеников зачастую используется «самописное» ПО, не прошедшее сертификацию ФСБ, что также влечет за собой негативные последствия.

Единые требования «Системы ведения журналов успеваемости учащихся в электронном виде в общеобразовательных учреждениях Российской Федерации» были разработаны Минобрнауки Российской Федерации и введены в действие с 1 июля 2011 года[4]. Документ устанавливает весьма высокие требования к функционированию электронного классного журнала (ЭКЖ), которые далеко не все программные продукты в состоянии обеспечить. Функциональность ЭКЖ должна обеспечить возможность полной замены традиционного классного журнала на бумажном носителе при учёте выполнения учебной программы (без анкетных, медицинских и других дополнительных данных, учёт которых можно вести другими средствами, в том числе электронными). ЭКЖ должен обеспечивать потребности школы при учёте реализации учебной программы, в том числе:

- в ведении необходимых структур учебного года;

• в отражении систем оценивания;

• в преобразовании результатов из одной системы оценивания в другую;

• в делении классов на группы по различным предметам;

• в формировании смешанных учебных групп;

• в совместимости с другими информационными системами, используемыми в школе.

Учитывая, что исполнять принятые нормативные акты должны все школы, переходить на электронное ведение классных журналов и дневников через какое-то время придётся всем школам. Для того чтобы не тратить лишние силы и средства, школам рекомендуется сразу внедрять программные продукты, в полной мере соответствующие Единым требованиям, утверждённым Минобрнауки России. Естественно, что такие программные продукты должны также соответствовать и требованиям защиты персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Поэтому в обязанности школы должна входить разработка необходимых инструкций пользователя и оператора ЭКЖ, разработка парольных политик, поддержание и контроль функционирования программной среды и т. д.

3. Отсутствие квалифицированных специалистов.

В большинстве штатных расписаний образовательных учреждений отсутствует «специалист по защите информации». Ответственными за обработку персональных данных в образовательных учреждениях чаще всего назначаются специалисты, не получившие необходимой квалификации, – системные администраторы, лица, ответственные за автоматизацию и информатизацию образовательного процесса.

Рособразование рекомендовало для ИСПДн классов К3 и К4 все работы выполнять своими силами, выбирая наименее затратное подходящее типовое техническое решение, а для защиты систем остальных классов привлекать специализированные организации, имеющие необходимые лицензии ФСБ России и ФСТЭК. При эксплуатации ИСПДн 3 и 4 уровня защищенности ответственным за обработку персональных данных необходимо пройти специализированные курсы, которые также проводят организации – лицензиаты ФСТЭК.

Поскольку доступ к электронным дневникам, кроме персонала образовательных учреждений, имеют также родители и учащиеся, остро стоит вопрос повышения культуры их информационной безопасности. А это значит, что требуется развитие управленческих компетенций специалистов по защите информации [3]. Если учесть неблагоприятное состояние культуры информационно-психологической безопасности в регионе в целом [2], то становится очевидным необходимость оперативного решения названной проблемы.

4. Обработка специальных категорий персональных данных обучающихся, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением следующих случаев:

• обучающийся (родитель) дал согласие в письменной форме на обработку своих персональных данных;

• персональные данные являются общедоступными;

• персональные данные относятся к состоянию здоровья обучающегося, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия обучающегося невозможно;

• обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью в соответствии с Договором между медицинским учреждением и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

• обработка персональных данных необходима в связи с осуществлением правосудия;

• обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

Очевидно, что для образовательных учреждений обеспечение соответствия законодательству является весьма непростой задачей. Но рекомендации Рособразования и имеющиеся на рынке сертифицированные ИБ-продукты дают возможность решить ее с разумными затратами, не прибегая к излишним дорогостоящим и сложным мерам.

Таким образом, особенности защиты персональных данных в образовательных учреждениях обусловлены организационными, техническими, кадровыми и финансовыми аспектами деятельности последних. Представленные в статье меры по решению выявленных специфических проблем защиты персональных данных в сфере образования связаны с реализацией мер по понижению классов ИСПДн и снижению требований к обеспечению их безопасности (с акцентом на обезличивание данных и реализацию организационных мер); актуализацией моделей угроз для ИСПДн различных классов (на основе максимальной типизации документов и требований); повышением уровня знаний сотрудников образовательного учреждения в вопросах обработки персональных данных, а также повышения культуры информационной безопасности учащихся и их родителей.

Литература

[1] Астахова, Л. В. Виртуальная образовательная среда: сущность понятия / Астахова Л. В., Запускалова Н. С. // Сибирский педагогический журнал. 2011. № 12. С. 63–68.

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

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

[4] Единые требования «Системы ведения журналов успеваемости учащихся в электронном виде в общеобразовательных учреждениях Российской Федерации» были разработаны Минобрнауки Российской Федерации и введены в действие с 1 июля 2011 г. [Электронный ресурс]. Режим доступа: http://www.apkit.ru/files/MON_treb_ej_v5-8.pdf. Загл. с экрана.

[5] Емельянников, М. Персональные данные в образовательных учреждениях: сложно, но возможно! [Электронный ресурс]. Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=132703. Загл. с экрана.

[6] Письмо Рособразования от 22.10.2009 № 17-187 «Об обеспечении защиты персональных данных» [Электронный ресурс]. Режим доступа: http://www.ed.gov.ru/normtv/oficdoc/pifao/11620. Загл. с экрана.

[7] Приказ Минздравсоцразвития РФ от 26.08.2010 № 761н «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих» [Электронный ресурс]. Режим доступа: http://www.rg.ru/2010/10/20/teacher-dok.html. Загл. с экрана.

[8] Распоряжение Правительства России от 25 апреля 2011 г. № 729-р «Об утверждении перечня услуг, оказываемых государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ), подлежащих включению в реестры государственных или муниципальных услуг и предоставляемых в электронной форме» [Электронный ресурс]. Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=113446. Загл. с экрана.

[9] Садердинов, А. А. Информационная безопасность предприятия /А. А. Садердинов, В. А. Трайнев, А. А. Федулов. М.: Дашков и Ко. 2006. 336 с.

[10] Скиба, В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба. СПб: Питер, 2008. 320 с.

[11] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.07.2011) [Электронный ресурс]. Режим доступа: http://www.rg.ru/2001/12/31/trud-dok.html. Загл. с экрана.

[12] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=144689. Загл. с экрана.

[13] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных» [Электронный ресурс]. Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=144649. Загл. с экрана.

[14] Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» [Электронный ресурс]. Режим доступа: http://www.rg.ru/2012/12/30/obrazovanie-dok.html. Загл. с экрана.

[15] Цена защиты// Ведомости. [07.07.2011] [Электронный ресурс]. Режим доступа: http://www.vedomosti.ru/newspaper/article/263553/cena_zaschity. Загл. с экрана.

[16] Электронные журналы и защита персональных данных [Электронный ресурс]. Режим доступа: http://mordovoobraz.68edu.ru/index.php. Загл. с экрана.

References

[1] Astahova, L.V. Virtual'naja obrazovatel'naja sreda: sushhnost' ponjatija [Virtual educational reality: Essence of the notion]/ Astahova L.V., Zapuskalova N.S. // Sibirskij pedagogicheskij zhurnal [Siberian pedagogical journal]. 2011. No. 12. p. 63-68.

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

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

[4] Edinye trebovanija «Sistemy vedenija zhurnalov uspevaemosti uchashhihsja v jelektronnom vide v obshheobrazovatel'nyh uchrezhdenijah Rossijskoj Federacii» byli razrabotany Minobrnauki Rossijskoj Federacii i vvedeny v dejstvie s 1 ijulja 2011 g. [Standard requirements of the system of keeping gradebooks in electronic form in educational institutions of the Russian Federation were developed by the Ministry of Education of the Russian Federation and implemented from July 1, 2011] [Electronic resource]. Rezhim dostupa: http://www.apkit.ru/files/MON_treb_ej_v5-8.pdf. Zagl. s jekrana.

[5] Emel'jannikov, M. Personal'nye dannye v obrazovatel'nyh uchrezhdenijah: slozhno, no vozmozhno! [Personal data in educational institutions: Difficult but possible!] [Electronic resource]. Rezhim dostupa: http://www.pcweek.ru/security/article/detail.php?ID=132703 . Zagl. s jekrana.

[6] Pis'mo Rosobrazovanija ot 22.10.2009 N 17-187 «Ob obespechenii zashhity personal'nyh dannyh» [Letter of the Federal Education Agency as of October 22, 2009 No. 17-187 'On ensuring of the protection of personal data] [Electronic resource]. Rezhim dostupa: http://www.ed.gov.ru/normtv/oficdoc/pifao/11620. Zagl. s jekrana.

[7] Prikaz Minzdravsocrazvitija RF ot 26.08.2010 № 761n «Ob utverzhdenii Edinogo kvalifikacionnogo spravochnika dolzhnostej rukovoditelej, specialistov i sluzhashhih» [Decree of the Ministry of Health and Social Development of the Russian Federation as of August 26, 2010 No. 761n 'On the establishment of the Unified Classifying Reference Book of Chief Managerial Positions, Specialists and Clerks'] [Electronic resource]. Rezhim dostupa: http://www.rg.ru/2010/10/20/teacher-dok.html. Zagl. s jekrana.

[8] Rasporjazhenie Pravitel'stva Rossii ot 25 aprelja 2011 g. № 729-r «Ob utverzhdenii perechnja uslug, okazyvaemyh gosudarstvennymi i municipal'nymi uchrezhdenijami i drugimi organizacijami, v kotoryh razmeshhaetsja gosudarstvennoe zadanie (zakaz) ili municipal'noe zadanie (zakaz), podlezhashhih vkljucheniju v reestry gosudarstvennyh ili municipal'nyh uslug i predostavljaemyh v jelektronnoj forme» [Decree of the Government of the Russian Federation as of April 25, 2011 No. 729-r 'On the establishment of the list of services rendered by state and municipal institutions and other organizations where the state or municipal order included in the state or municipal service register is placed'] [Electronic resource]. Rezhim dostupa: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=113446. Zagl. s jekrana.

[9] Saderdinov, A.A. Informacionnaja bezopasnost' predprijatija [Information security of an enterprise]/A. A. Saderdinov, V. A. Trajnev, A. A. Fedulov. Moscow: Dashkov i Ko. 2006. 336 p.

[10] Skiba, V.Ju. Kurbatov, V.A. Rukovodstvo po zashhite ot vnutrennih ugroz informacionnoj bezopasnosti [Guidance on internal threats defense of the information security]/ V.Ju. Skiba. St. Peterburg: Piter, 2008. 320 p.

[11] Trudovoj kodeks Rossijskoj Federacii ot 30.12.2001 № 197-FZ (red. ot 19.07.2011) [Labour Code of the Russian Federation as of December 30, 2001 No. 197-FZ (editorship as of July 19, 2011] [Electronic resource]. Rezhim dostupa: http://www.rg.ru/2001/12/31/trud-dok.html . Zagl. s jekrana.

[12] Federal'nyj zakon ot 27.07.2006 № 149-FZ (red. ot 06.04.2011, s izm. ot 21.07.2011) «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» [Federal Law as of July 27, 2006 No. 149-FZ (editorship as of April 06, 2011, amendments as of July 21, 2011) 'On information, information technologies and information security'] [Electronic resource]. Rezhim dostupa: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=144689. Zagl. s jekrana.

[13] Federal'nyj zakon ot 27.07.2006 № 152-FZ (red. ot 25.07.2011) «O personal'nyh dannyh» [Federal Law as of July 27, 2006 No. 152-FZ (editorship as of July 25, 2011) 'On personal data'] [Electronic resource]. Rezhim dostupa: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=144649. Zagl. s jekrana.

[14] Federal'nyj zakon Rossijskoj Federacii ot 29 dekabrja 2012 g. № 273-FZ «Ob obrazovanii v Rossijskoj Federacii» [Federal Law of the Russian Federation as of December 29, 2012 No.273-FZ 'On education in the Russian Federation'] [Electronic resource]. Rezhim dostupa: http://www.rg.ru/2012/12/30/obrazovanie-dok.html. Zagl. s jekrana.

[15] Cena zashhity [Price of protection] // Vedomosti. [07.07.2011] [Electronic resource Rezhim dostupa: http://www.vedomosti.ru/newspaper/article/263553/cena_zaschity. Zagl. s jekrana.

[16] Jelektronnye zhurnaly i zashhita personal'nyh dannyh [Electronic journals and protection of personal data] [Electronic resource]. Rezhim dostupa: http://mordovoobraz.68edu.ru/index.php. Zagl. s jekrana.

Астахова Людмила Викторовна, д. п. н., профессор, профессор ЮУрГУ.

Завадский Алексей Олегович, студент ЮУрГУ.

Liudmila Viktorovna Astakhova, PhD in Education, Professor, Professor of SUSU.

Aleksey Olegovich Zavadsky, student of SUSU.

УДК 004.056.5 + 004.7.056.5
ББК Х401.114

Косенко М. Ю.

СБОР ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

В работе рассматриваются основные фазы процесса проведения оценки безопасности компьютерных систем и сетей средствами моделирования атак злоумышленника. Предлагается модель распределенного сетевого сканирования, использующая в качестве платформы облачные технологии. Представленный метод повышает эффективность проведения тестирования на проникновение за счет сокращения времени, отводящегося на этап сбора информации.

Ключевые слова: *тестирование на проникновение, сканирование сети, облачные технологии.*

Kosenko M. U.

GATHERING INFORMATION DURING PENETRATION TESTING

The paper presents the main phases of process the evaluation security of computer systems and networks with simulation hackers attacks. Presents a model of distributed network scanning on cloud-based technologies. This method will increase the efficiency of penetration testing by reducing the time tailrace on information-gathering phase.

Keywords: *penetration testing, network scanning, cloud computing.*

1. Введение

В настоящее время при оценке безопасности компьютерных систем и сетей используются различные методы, один из которых – тестирование на проникновение. Тестирование на проникновение – это тестирование безопасности, в котором эксперты имитируют реальные атаки в попытке определить методы обхода функций безопасности приложения, системы или сети[1]. Тестирование часто включает в себя элементы реальных атак на системы, используя инструменты и методы, используемые злоумышленниками. Большинство тестов на проникновение включают в себя поиск комбинаций уязвимостей одной или нескольких систем, которые можно использовать, чтобы получить больший уровень доступа, чем может быть достигнуто с помощью одной уязвимости.

Тест на проникновение также может быть полезным для определения[2]:

• толерантности системы к шаблонам реальных атак;

• вероятного уровня сложности, при котором атакующий может успешно компрометировать систему;

• дополнительных контрмер, которые могли бы ослабить угрозы против системы;

• возможности защитников по обнаружению атак и реагированию соответствующим образом.

На рис. 1 представлены четыре фазы проведения тестирования на проникновение: планирование, сбор информации, атака, от-

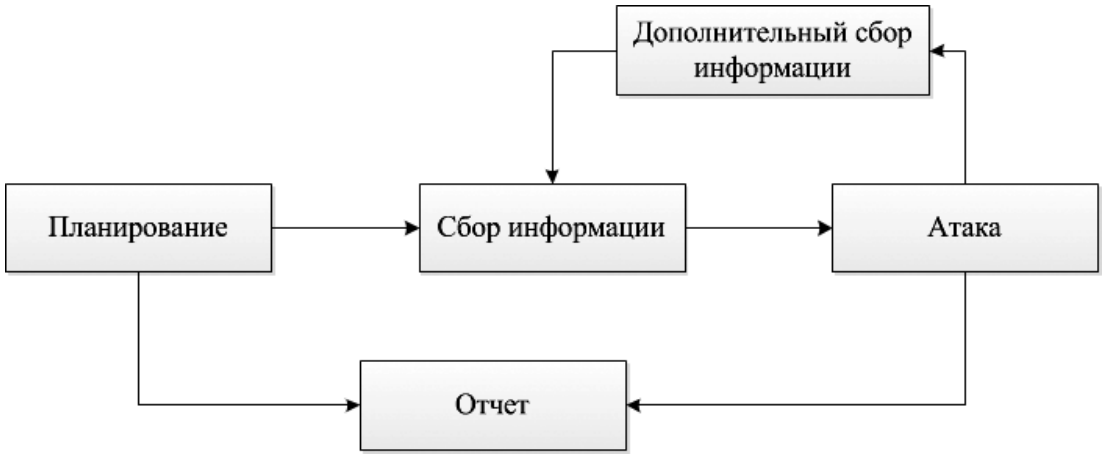

Рис. 1. Фазы проведения тестирования на проникновение.

чет. На этапе планирования определяются правила тестирования, документируется согласие руководства, устанавливаются цели. Данный этап определяет основу для проведения успешного теста на проникновение.

Фаза сбора информации состоит из двух частей. Первая часть является началом фактического тестирования и охватывает сбор общей информации о системе и сканирование. На этом этапе производятся обнаружение активных устройств в сети, открытых на них портов, и идентификация работающих служб. В дополнение могут использоваться другие методы сбора информации о целевой системе:

• Имена хостов и информация об IP-адресах может быть собрана различными методами, в том числе при опросе DNS, WHOIS запросах, прослушивании сети.

• Имена и контактная информация сотрудников может быть получена с помощью поиска на веб-сервере организации.

• Информацию о системе можно найти с помощью протокола NetBIOS или протокола информационной службы сети (Network Information Service, NIS).

• Информацию о приложениях и службах, такую, как номер версии, можно получить, используя метод «banner grabbing».

Вторая часть заключается в анализе уязвимостей и включает в себя автоматический поиск уязвимостей услуг, приложений и операционных систем отсканированных хостов, а также ручной поиск уязвимостей. Для выявления уязвимостей вручную эксперт может использовать свои собственные знания или общественные базы данных уязвимостей, таких как национальная база данных уязвимостей (National Vulnerability Database, NVD). Третий этап – основа теста на проникновение и включает в себя проведение атаки. Это процесс проверки ранее выявленных уязвимостей и попытка их эксплуатации. Фаза отчетности происходит одновременно с тремя другими фазами тестирования на проникновения. Отчет, как правило, разрабатывается для описания выявленных уязвимостей, представляет актуальные риски системы и дает указания о том, как смягчить обнаруженные слабые стороны.

Фаза атаки является основой любого теста на проникновение. Атака представляет процесс проверки выявленных уязвимостей путем их использования. Эта фаза включает в себя следующие шаги: получение доступа к системе, расширение привилегий, осмотр системы, установка в систему дополнительных инструментов.

Фаза отчетности происходит одновременно с тремя другими этапами. На этапе планирования разрабатывается и описывается план действий. На этапе сбора информации и атаки ведется журнал работы. По завершении теста на проникновение в отчет заносится описание выявленных уязвимостей и даются рекомендации по устранению обнаруженных недостатков.

Первая часть второй фазы проведения тестирования на проникновение, сканирование может занять большое количество времени, особенно если стоит задача просканировать большую сеть. Таким образом, при реализации этого этапа становится актуальной возможность параллельно распределить трафик к сканируемым хостам.

2. Модель распределенного сканирования сетей

Целью данной работы является разработка инструмента, позволяющего создавать и управлять множеством хостов, имеющих свой собственный канал для сканирования исследуемой сети.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Построить концептуальную модель распределенного сканирования сети.

2. Разработать алгоритм работы системы распределенного сканирования.

3. Проанализировать инструменты сканирования сети.

4. Разработать инструмент распределенного сканирования.

2.1. Описание модели

Сетевое сканирование является отправной точкой в тестировании на проникновение. Цель этого процесса состоит в определении числа достижимых систем для тестирования, их IP-адресов, открытых портов, идентификации работающих сервисов и операционных систем[3]. За последние пару десятков лет сканирование очень сильно развилось и было разработано множество методов его проведения[4]. Если рассматривать технологии сетевого сканирования с точки зрения многоуровневой модели TCP/IP, то существует достаточно много техник: сканирование на уровне 2, ICMP-сканирование, UDP-сканирование, TCP-сканирование (различные варианты SYN, ACK, FIN)[5]. Каждая из этих технологий наилучшим образом применима в различных ситуациях, связанных с настройкой сканируемых хостов.

Для размещения системы распределенного сканирования сети можно использовать облачную модель предоставления услуг – инфраструктура как услуга (Infrastructure as a Service, IaaS)[6]. Данная услуга позволяет за короткие сроки развернуть в сети множество подконтрольных виртуальных машин. Используя возможности, предоставляемые сервисом IaaS, можно обходить различные защитные средства, такие как Intrusion detection system (IDS, система обнаружения вторжений) или Intrusion prevention system (IPS, система предотвращения вторжений). Такая возможность появляется за счет того, что сканирование может происходить с десятка различных IP-адресов, выдерживая временные интервалы.

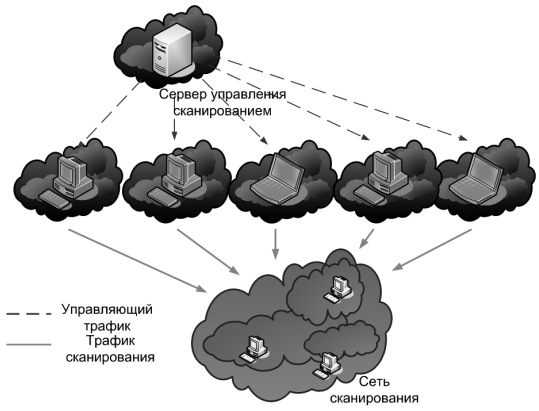

Рис. 2. Концептуальная модель распределенного сканирования с использованием облачных технологий

На рис. 2 представлена концептуальная модель распределенного сканирования. Компонентами этой модели являются:

• клиенты, осуществляющие сканирование (скан-бот). Виртуальные машины, выполняющие функцию сканирования. По окончании выполнения команды скан-бот передаёт результаты сканирования серверу управления;

• сервер управления сканированием. Виртуальная машина, выполняющая функцию управления скан-ботами. Скан-боты соединяются с сервером управления сканированием и получают команды для выполнения;

• цель сканирования. Компьютерная сеть, либо отдельные компьютеры, которые нужно просканировать.

2.2. Алгоритм системы распределенного сканирования

Создать систему распределенного сканирования можно, используя модель взаимодействия клиент/сервер[7]. В таком случае алгоритм работы системы распределенного сканирования будет следующим.

1. Сервер управления сканированием запускается и загружает задачи сканирования из заранее заполненного лицом, проводящим тестирование, файла. В данном файле приводится список всех задач, которые необходимо распределить по скан-ботам.

2. Скан-бот осуществляет подключение к серверу. При запуске скан-бота в качестве параметров передаются адрес и порт сервера управления сканированием.

3. При подключении нового скан-бота сервер выдает ему очередное задание, ожидающее выполнения.

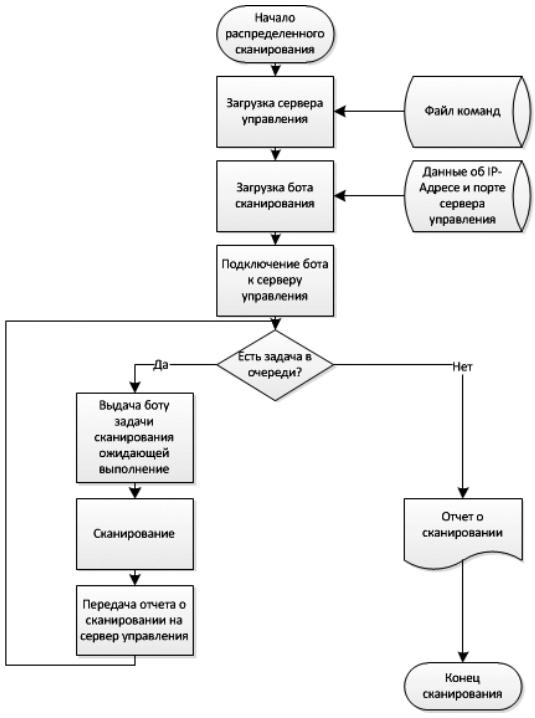

Рис. 3. Блок-схема алгоритма распределенного сканирования

4. Скан-бот выполняет задание. Результат передает серверу управления сканированием.

5. Сервер управления агрегирует полученную информацию сканирования в специальном каталоге. При наличии ожидающей выполнения задачи передает её освободившемуся скан-боту.

Блок-схема алгоритма работы системы распределенного сканирования приведена на рис. 3.

2.3. Реализация системы распределенного сканирования

В качестве облачного провайдера был выбран DigitalOcean, предоставляющий облачную модель инфраструктуры как услуги. С использованием сервиса DigitalOcean были созданы два образа виртуальной машины. Первый образ был подготовлен в качестве сервера управления сканированием. Второй образ включал все необходимые компоненты для осуществления сканирования. Сервис DigitalOcean позволяет быстрым образом запускать множество клонов созданной виртуальной машины.

Для сканирования использовался сетевой сканер Nmap. Nmap ("Network Mapper") – это программа с открытым исходным кодом для исследования сети и проверки безопасности[8]. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Данный сетевой сканер выбран потому, что обладает рядом преимуществ перед другими сканерами:

• Гибкость. Nmap включает в себя множество механизмов сканирования портов, обнаружение операционной системы, определение версий служб.

• Мощность. Nmap может быть использован для сканирования огромных сетей, состоящих из сотен тысяч машин.

• Кроссплатформенность. Большинство операционных систем поддерживают Nmap, включая Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, MacOS, NetBSD и др.

Серверное и клиентское программное обеспечение системы распределенного сканирования было реализовано с использованием языка программирования Python. Помимо основных задач, сервер, используя пакет python-digitalocean, обеспечивающий простой доступ к DigitalOcean API, имеет возможность запуска виртуальных машин скан-ботов в облачной инфраструктуре. Количество запускаемых виртуальных машин определяется согласно количеству задач в очереди сканирования.

3. Заключение

В рамках представленной работы были достигнуты следующие результаты:

• описана модель распределенного сканирования сети;

• разработан алгоритм работы системы распределенного сканирования;

• реализована система распределенного сканирования на базе облачных технологий.

Разработанная система повышает эффективность проведения теста на проникновение за счет сокращения времени, отводящегося на этап сбора информации.

Примечания

[1] Thomas Wilhelm. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab". Syngress, 2009.

[2] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. "Technical Guid to Information Security Testing and Assessment". NIST Special Publication 800–115.

[3] Pete Herzog. "Open-Source Security Testing Methodology Manual". ISECOM, 2006.

[4] M. Allman, V. Paxson, and J. Terrell. "A brief history of scanning". In IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, 2007, pp 77–82.

[5] Richard J Barnett, Barry Irwin. "Towards a Taxonomy of Network Scanning Techniques". In SAICSIT, 2008.

[6] Косенко М. Ю. Злонамеренное использование облачных технологий. Труды Первой Международной конференции «Информационные технологии и системы». 2012. с. 67–69.

[7] Douglas E. Comer, David L. Stevens. "Internetworking with TCP/IP. Vol III. Client-Server Programming and Applications Linux/POSIX Socket Version". Addison-Wesley, 2000.

[8] Gordon Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning". Nmap Project, 2009.

[9] James Messer. "Secrets of Network Cartography: A Comprehensive Guide to Nmap".

[10] Chris McNab. "Network Security Assessment". O'Reilly Media, Second Edition, 2007.

[11] "Penetration Testing: Procedures & Methodologies". EC-Council, 2010.

References

[1] Thomas Wilhelm. "Professional Penetration Testing: Creating and Operating a Formal Hacking Lab". Syngress, 2009.

[2] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh. "Technical Guid to Information Security Testing and Assessment". NIST Special Publication 800-115.

[3] Pete Herzog. "Open-Source Security Testing Methodology Manual". ISECOM, 2006.

[4] M. Allman, V. Paxson, and J. Terrell. "A brief history of scanning". In IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, 2007, pp 77-82.

[5] Richard J Barnett, Barry Irwin. "Towards a Taxonomy of Network Scanning Techniques". In SAICSIT, 2008.

[6] Kosenko M.Yu. Zlonamerennoe ispol'zovanie oblachnykh tekhnologii. Trudy pervoi mezhdunarodnoi konferentsii «Informatsionnye tekhnologii i sistemy» [Use of cloud technologies for malicious purposes. Materials of the international conference 'Information technologies and systems]. 2012. p.67-69.

[7] Douglas E. Comer, David L. Stevens. "Internetworking with TCP/IP. Vol III. Client-Server Programming and Applications Linux/POSIX Socket Version". Addison-Wesley, 2000).

[8] Gordon Lyon. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning". Nmap Project, 2009.

[9] James Messer. "Secrets of Network Cartography: A Comprehensive Guide to Nmap".

[10] Chris McNab. "Network Security Assessment". O'Reilly Media, Second Edition, 2007.

[11] "Penetration Testing: Procedures & Methodologies". EC-Council, 2010.

Косенко Максим Юрьевич, преподаватель института информационных технологий Челябинского государственного университета. г. Челябинск, ул. Братьев Кашириных, 129, к. 415. E-mail: kosenko@csu.ru

Maksim Yurievich Kosenko, lector and teacher of the Institute of Informational Technologies of Chelyabinsk State University. Office 415, Bratiev Kashyrinykh Str., Chelyabinsk. E-mail: kosenko@csu.ru

УДК 34.03:[002:004] + 349.22:[002:004]
ББК Х401.114 + Х 405.116:Х401.114

Офман Е. М.

СОКРЫТИЕ ИНФОРМАЦИИ РАБОТНИКОМ КАК ОДНА ИЗ ФОРМ ЗЛОУПОТРЕБЛЕНИЯ ПРАВОМ: НОВЫЕ ПОДХОДЫ И МЕХАНИЗМ ПРОТИВОДЕЙСТВИЯ

В статье рассмотрены случаи злоупотребления правом работником в форме сокрытия информации. На основе анализа судебной практики США и России выявлены специфические правовые последствия злоупотребления правом работником, сформулированы предложения о совершенствовании трудового законодательства; предложен механизм противодействия злоупотреблению правом в форме сокрытия информации со стороны работников.

Ключевые слова: *злоупотребление правом, сокрытие информации, защита информации в трудовых отношениях, работник.*

Ofman E. M.

WITHHOLDING OF INFORMATION BY THE EMPLOYEE AS A FORM OF ABUSE OF THE RIGHT: NEW APPROACHES AND MECHANISM OF RESISTANCE

In the article is considered the cases of abuse of the right of the worker in the form of information hiding. Based on the analysis of the judicial practice of the U.S. and Russia identified specific legal consequences of abuse of the right of the RA-ботником, proposals on improvement of labour legislation and proposed a mechanism of counteraction to the right in the form of withholding information from employees.

Keywords: *abuse of rights, withholding of information, data protection in the employment relationship, the employee.*

Информация в трудовом праве имеет определяющее значение на всех этапах регулирования трудовых и непосредственно связанных с ними отношений: начиная со стадии трудоустройства у данного работодателя и заканчивая разрешением трудовых споров. В зависимости от информированности работодателя о тех или иных юридически важных сведениях о работнике, первый (работодатель) принимает те или иные решения (например, о необходимости заключения трудового договора без установления работнику испытания [с беременными женщинами (ч. 4 ст. 70 Трудового кодекса Российской Федера-

ции[1])]; о сокращенном рабочем времени [работнику-инвалиду (ч. 1 ст. 92 Трудового кодекса Российской Федерации)]; о невозможности расторжения трудового договора по инициативе работодателя за невиновное поведение с одинокой матерью, воспитывающей ребенка-инвалида до восемнадцати лет или малолетнего ребенка в возрасте до четырнадцати лет, с другим лицом, воспитывающим указанных детей без матери, с родителем (законным представителем ребенка), являющимся единственным кормильцем ребенка-инвалида в возрасте до восемнадцати лет либо единственным кормильцем ребенка в возрасте до трех лет в семье, воспитывающим трех и более малолетних детей, если другой родитель (законный представитель) не состоит в трудовых отношениях (ч. 4 ст. 261 Трудового кодекса Российской Федерации); использование «донорских» дней в удобное для работника время без предварительного предупреждения об этом работодателя, в том числе для того, чтобы избежать увольнения за виновное поведение; о правомерности привлечения к дисциплинарной ответственности при отсутствии работника на работе в случае временной нетрудоспособности.

Несмотря на всю важность и значимость данных фактов, законодатель не установил в Трудовом кодексе Российской Федерации обязанность работников предоставлять указанную информацию работодателю, в связи с чем работник (либо претендент на работу) вправе предоставлять данные сведения по своему усмотрению и только в случаях, когда (по мнению работника) данные сведения необходимы в связи с трудовыми отношениями, что на практике порождает злоупотребление правом. Свобода работников в осуществлении своего права (право предоставлять информацию о себе, о членах семьи) является неограниченной, допускающей возможность воздерживаться от использования свого права в ущерб интересам работодателя и интересам других работников. Практика свидетельствует, что работники информируют работодателя о юридически значимых фактах только уже на стадии разрешения трудового спора, когда работодатель не может ничего изменить или исправить[2].

В современной судебной практике хрестоматийными стали формы злоупотребления правом работником, указанные в п. 27 постановления Пленума Верховного Суда Российской Федерации от 17 марта 2004 г. № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации»[3]: сокрытие информации временной нетрудоспособности на время увольнения работника с работы либо сокрытия того обстоятельства, что работник является членом профессионального союза или руководителем (его заместителем) выборного коллегиального органа первичной профсоюзной организации (не ниже цехового и приравненного к нему), не освобожденным от основной работы, когда решение вопроса об увольнении должно производиться с соблюдением процедуры учета мотивированного мнения выборного органа первичной профсоюзной организации либо соответственно с предварительного согласия вышестоящего выборного профсоюзного органа.

Между тем, можно отметить, что современное трудовое право развивается быстрее трудового законодательства и судебной практике известны иные, новые формы злоупотребления правом работниками и работодателями, по которым у судов не выработалась единая практика. Следует остановиться на этих новых формах злоупотреблений со стороны работников.

Чаще всего работники злоупотребляют правом в форме бездействия, как правило, скрывая от работодателя информацию, имеющую существенное значения для проведения кадровых процедур (увольнения – прежде всего):

1) сокрытие информации о прохождении дополнительного обучения по специальности, о присвоении работнику новой квалификации по имеющейся должности при проведении работодателем процедуры сокращения численности/штата работников[4];

2) сокрытие работником-отцом информации о составе семьи, а также того обстоятельства, что мать (супруга этого работника) в трудовых отношениях не состоит и занимается уходом за детьми[5];

3) сокрытие информации о реальном основании прекращения трудового договора с прежним работодателем при трудоустройстве у нового работодателя (если разрыв трудовой связи был связан с виновным основанием расторжения трудового договора)[6].

Какой механизм противодействия указанному поведению работников предлагает трудовое законодательство? К сожалению, Трудовой кодекс Российской Федерации не устанавливает правовых последствий в отно-

шении злоупотребившего правом работника. Единственным актом, указывающим на правовые последствия сокрытия работником от работодателя информации, является постановление Пленума Верховного Суда Российской Федерации от 17 марта 2004 г. № 2, в п. 27 которого указывается, что при установлении факта злоупотребления правом работником работнику суд может отказать в удовлетворении его иска о восстановлении на работе (изменив при этом по просьбе работника, уволенного в период временной нетрудоспособности, дату увольнения), поскольку в указанном случае работодатель не должен отвечать за неблагоприятные последствия, наступившие вследствие недобросовестных действий со стороны работника.

При этом нижестоящие суды выработали принцип, согласно которому именно работодатель должен доказать факт сокрытия от него работником информации при осуществлении тех или иных действий (в частности, при привлечении работника к дисциплинарной ответственности или при расторжении с ним трудового договора)[7]. Если работодатель докажет, что он запрашивал, а работник скрыл от него информацию, необходимую для принятия решения об увольнении, то увольнение будет признано законным[8].

В связи с этим возникают вопросы о достаточности выработанных судебной практикой правовых последствий в случае установления факта злоупотребления правом со стороны работников и об иных (не связанных с судебным порядком рассмотрения и разрешения споров) способах противодействия работодателем сокрытия работником информации, имеющей важное значение в области регулирования отношений в сфере труда. Для ответа на данные вопросы считаю необходимым обратиться к судебной практике США.

В практике США также распространено злоупотребление правом работником в форме сокрытия юридически значимых фактов как при приеме на работу, так и в процессе работы у работодателя[9]. Например, гражданин США Джошуа Флинт (Joshua Flint) при приеме на работу не поставил в известность работодателя о своей инвалидности (он использовал протез стопы). Проработав в издательстве газеты Houston Chronicle два года, при переходе на другую работу он обратился в дирекцию газеты с требованием выплатить компенсацию в связи с фактом инвалидности. Работодатель, не знавший ранее об этом, обратился в суд с вопросом об определении действий работника. Суд Хьюстона нашел в действиях Джошуа Флинта злоупотребление правом и отказал ему в выплате компенсации в связи с сокрытием факта инвалидности при приеме на работу.

Однако в судебной практике США имеются достаточно интересные формы злоупотребления правом работником. При этом обращает на себя внимание то, что в случае установления злоупотреблений со стороны работников суд встает на защиту прав и интересов работодателей. Кроме этого, интересны устанавливаемые судами США правовые последствия злоупотребления правом. Рассмотрим примеры.

В 2009 г. в Сиэтле, штат Вашингтон, у гражданина США Р. Вайклифа (R. Wyclef) при сдаче анализов при приеме на работу была выявлена ВИЧ-инфекция. Компания-работодатель, в которой работал Р. Вайклиф, обязалась за свой счет выплачивать ему ежемесячное пособие на дорогостоящее лечение, чтобы сохранить здоровье ценного сотрудника. В 2007 г. при очередном обследовании Р. Вайклиф получил отрицательный результат анализа на ВИЧ, впоследствии повторно подтвержденный. Однако он не счел нужным уведомить об этом работодателя и продолжал еще больше года получать деньги на лечение. Когда же был выявлен факт сокрытия работником информации о состоянии своего здоровья, работодатель обратился в суд с требованием определить действия своего работника и указать ответственность за них.

Законодательство США (в частности, Закон об американцах с ограниченной трудоспособностью) запрещает дискриминацию больных СПИДом. Кроме того, отдел Департамента труда по программам рассмотрения жалоб по федеральным контрактам требует лечения заболеваний типа СПИДа согласно Закону о профессиональной реабилитации[10]. Самым важным для большинства работодателей является то, что дискриминация людей, больных СПИДом, обычно считается незаконной[11].

В указанном случае суд Сиэтла обозначил действия Р. Вайклифа как злоупотребление правом и постановил вернуть компании-работодателю все денежные средства, полученные на лечение в период после снятия диагноза.

Действующее трудовое законодательство РФ устанавливает запреты на увольне-

ние с работы, на отказ в приеме на работу, а также ограничение иных прав и законных интересов ВИЧ-инфицированных на основании наличия у них ВИЧ-инфекции[12]. Поэтому работник вправе предоставлять данные сведения по своему усмотрению, и только в случаях, когда они необходимы в связи с трудовыми отношениями, что на практике может порождать злоупотребление правом. Работодатель, в свою очередь, не вправе требовать предоставления подобной информации от работника, даже если законом установлен запрет на выполнение данной работы ВИЧ-инфицированными. Данный факт может быть установлен только при прохождении обязательного медицинского обследования.

Еще один интересный случай злоупотребления правом со стороны работника произошел в Нью-Йорке в 2008 г. Работник сети женской парфюмерной продукции за несколько месяцев до приема на работу произвел операцию по смене пола. Устраиваясь на работу, он не уведомил об этом работодателя и был принят за женщину. Помимо консультирования клиентов и продажи товара работник занимался разгрузкой и складированием поступающей продукции. Работодатель, будучи уверенным, что на работу была взята именно женщина, ежемесячно выплачивал работнику денежную надбавку за выполнение такого мужского труда. Более того, в качестве дополнительного бонуса каждая женщина-работник данной компании в конце квартала получала бесплатную парфюмерию. Подобный бонус был получен и данным работником.

После некоторого времени у работодателя возникли подозрения по поводу половой принадлежности работника. В результате собеседования «работница» призналась, что «раньше она действительно была мужчиной». По просьбе работодателя был проведен ряд анализов (в том числе анализ гормонов), в итоге однозначно определивший пол работника как мужской.

Работодатель уволил работника и обратился в суд, который однозначно определил действия работника как злоупотребление правом, так как при устройстве на работу им не была предоставлена достоверная информация о своей половой принадлежности. Суд постановил работника вернуть работодателю деньги, полученные в качестве надбавки, а также вернуть сумму, эквивалентную стоимости всей полученной в качестве бонуса парфюмерии.

Анализируя приведенные примеры, можно сделать вывод, что сам факт злоупотребления правом со стороны работников в зарубежной практике является обоснованной причиной для расторжения с ними трудового договора по инициативе работодателя. Как указывает Н. Демидов, в отраслях трудового права Великобритании, США, Ирландии, Новой Зеландии правовые нормы о расторжении трудового договора за совершение проступка направлены, скорее, на защиту работодателя от недобросовестного работника, чем на разграничение их интересов. В Великобритании одним из грубых трудовых проступков, достаточных для расторжения трудового договора по инициативе работодателя, является злоупотребление доверием (п. 57 Процедурного кодекса № 1, изданного Консультативной службой примирения и арбитража)[13].

Кроме этого, обращают на себя внимание правовые последствия, применяемые в отношении злоупотребившего правом работником: суды обязали работников вернуть работодателю денежные средства, полученные на лечение в период после снятия диагноза, а также деньги, полученные в качестве надбавки и бонусов.

Подобного правового последствия трудовое законодательство и судебная практика России не знают. Представляется, что российскому законодателю было бы целесообразно перенять данный позитивный опыт США: закрепить в Трудовом кодексе Российской Федерации обязанность злоупотребившего правом работника возместить причиненный им работодателю прямой действительный ущерб, а также возможность освободить работодателя, добросовестно выполняющего свои трудовые обязанности, от несения неблагоприятных последствий, возникших в результате злоупотребления правом со стороны работника.

Российской практике известны случаи, когда работодатель применительно к злоупотребившему правом работнику может применить такое правовое последствие, как отказ в заключении трудового договора. Это происходит тогда, когда претендент на работу, скрыв информацию о наличии у него заболевания, препятствующего заключению трудового договора, пытается вступить в трудовое правоотношение с работодателем.

Приведем пример. На работу токарем обратился кандидат, при проведении медицинского осмотра которого выяснилось, что он страдает эпилепсией. Данный вид работы относится к числу тяжелых работ, при осуществлении которых согласно ст. 213 Трудового кодекса Российской Федерации работники должны пройти обязательное психиатрическое освидетельствование. В частности, Постановлением Совета Министров — Правительства РФ от 28 апреля 1993 г. № 377 «О реализации Закона РФ "О психиатрической помощи и гарантиях прав граждан при ее оказании"[14] установлены медицинские психиатрические противопоказания для осуществления отдельных видов профессиональной деятельности в условиях повышенной опасности. Согласно данному акту общими медицинскими психиатрическими противопоказаниями при работе на токарных станках являются хронические и затяжные психические расстройства с тяжелыми стойкими или часто обостряющимися болезненными проявлениями, в том числе и эпилепсия.

При устройстве на работу претендент скрыл от работодателя наличие у него данного заболевания. Сокрытие информации о состоянии здоровья является злоупотреблением правом, так как, реализуя свое право на заключение трудового договора, лицо выбрало недобросовестный способ его реализации, чем поставило работодателя в неблагоприятное положение: своевременное предоставление данной информации позволило бы работодателю избежать материальных издержек по проведению медицинского осмотра.

Между тем в некоторых случаях работодатель может быть лишен права расторгнуть трудовой договор по своей инициативе. Это происходит тогда, когда трудовым законодательством предоставляются гарантии определенным категориям работников. Например, данная ситуация возможна при заключении трудового договора или при его расторжении с беременной женщиной, когда она скрывает информацию о своей беременности (ст. 70, 261 Трудового кодекса Российской Федерации). Не предоставляя указанную информацию и злоупотребляя предоставленными трудовым законодательством возможностями, женщина фактически ограничивает право работодателя самостоятельно, под свою ответственность принимать необходимые кадровые решения: он, вступив в трудовые отношения с работницей, не может расторгнуть по своей инициативе трудовой договор даже в случае установления факта несоответствия работницы поручаемой ей работе или совершения дисциплинарного проступка, достаточного для увольнения (например, прогула)[15].

Еще один пример из судебной практики США. Судами штата Луизиана в конце августа – начале сентября 2005 г. после разрушительного урагана Катрина были вынесены постановления по ряду случаев, связанных со злоупотреблением правом работниками по «донорским» дням. Многие жители штата в то время сдавали кровь для пострадавших в результате разрушений. Некоторые из них не уведомили об этом своих работодателей и позже использовали так называемый «восстановительный день» по своему усмотрению. В результате на некоторых из них работодатели подали в суд, в том числе и за прогулы. В большинстве случаев суды становились на сторону работодателей и определяли такие действия работников-доноров именно как злоупотребление правом[16].

Судебная практика России по этому вопросу диаметрально противоположна. Суды, как привило, встают на сторону защиты прав и интересов работников. В частности, Постановление Пленума Верховного Суда РФ от 17 марта 2004 г. № 2 (подп. «д» п. 39) разъясняет, что не является прогулом использование работником дней отдыха в случае, когда работодатель вопреки закону отказал в их предоставлении и время использования работником таких дней не зависело от усмотрения работодателя (например, отказ работнику, являющемуся донором, в предоставлении в соответствии со ст. 186 Трудового кодекса Российской Федерации дня отдыха непосредственно после каждого дня сдачи крови и ее компонентов).

Статья 186 Трудового кодекса Российской Федерации устанавливает обязанности работодателя: освободить работника от работы в день сдачи крови и ее компонентов, а также в день связанного с этим медицинского обследования; предоставить дополнительный день отдыха работнику после каждого дня сдачи крови и ее компонентов; сохранить за работником его средний заработок за дни сдачи крови и ее компонентов. Одновременно с этим ст. 26 Федерального закона от 20 июля 2012 г. № 125-ФЗ «О донорстве крови и ее компонентов»[17] устанавливает обязанности

для работодателей по оказанию содействия субъектам обращения донорской крови и (или) ее компонентов в привлечении доноров к сдаче крови и (или) ее компонентов; по предоставлению работникам и военнослужащим, сдавшим кровь и (или) ее компоненты, гарантий и компенсаций, установленных законодательством Российской Федерации; по предоставлению безвозмездно необходимых помещений для донации.

Однако указанные акты не содержат обязанности работника информировать своего работодателя о том, что он собирается сдавать, сдает или уже сдал кровь и ее компоненты.

Вместе с тем, рассматривая приведенные выше ситуации, следует поставить вопрос о том, должен ли работник информировать работодателя о своем особом статусе. Трудовое законодательство не содержит обязанности работника предоставлять работодателю информацию подобного рода, кроме норм ст. 21 и 214 Трудового кодекса Российской Федерации, устанавливающих, что работник должен незамедлительно сообщить о возникновении ситуации, представляющей угрозу жизни и здоровью людей, сохранности имущества работодателя (в том числе имущества третьих лиц, находящегося у работодателя, если работодатель несет ответственность за сохранность этого имущества); сообщить о каждом несчастном случае на производстве, в том числе о проявлении признаков острого профессионального заболевания (отравления). Однако вряд ли информацию о смене пола, донорстве, инвалидности возможно отнести к ситуации, угрожающей жизни и здоровью людей или сохранности имущества.

По российскому законодательству любая информация, относящаяся к физическому лицу, составляет его персональные данные. Из смысла понятия «персональные данные работника», закрепленного в ст. 85 Трудового кодекса Российской Федерации, следует, что объем информации о работнике определяет работодатель. Вместе с тем законодатель установил границы, которые работодатель не вправе преступить при обработке и при получении информации от работника или о работнике. Во-первых, установлен перечень данных, обработка которых запрещена. Речь идет о специальных категориях персональных данных, к которым относятся сведения, касающиеся: расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состоянии здоровья, интимной жизни, судимости. Обработка перечисленных данных может осуществляться только в случаях, предусмотренных в законодательстве (ст. 10 Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). Во-вторых, ст. 88 Трудового кодекса Российской Федерации запрещает работодателю запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником своей трудовой функции. На практике работодатель может обосновать свое требование о предоставлении работником сведений о состоянии здоровья, связывая его с возможностью (невозможностью) выполнять работу по обусловленной трудовой функции. Однако такое требование идет вразрез с нормами законодательства о защите персональных данных. В связи с этим применение названного исключения возможно только в рамках ст. 69 и 214 Трудового кодекса Российской Федерации, предусматривающих случаи прохождения работником обязательного медицинского обследования.

Однако при прохождении такого обследования работодателю не должна быть предоставлена информация о конкретных заболеваниях работника, решается лишь вопрос о возможности выполнения работы или наличии противопоказаний для ее выполнения. В противном случае нарушается требование законодательства о сохранении врачебной тайны. Более того, следует отметить, что даже при оформлении листков нетрудоспособности сохраняется конфиденциальность диагноза.

Поэтому сообщение информации, составляющей персональные данные, является исключительно правом работника, в том числе и в тех случаях, когда имеются противопоказания для выполнения данной работы, и работник о них осведомлен на момент трудоустройства и в период осуществления трудовой функции. Чтобы исключить возможность злоупотребления правом, следует установить в Трудовом кодексе Российской Федерации следующее правило: если работник обладает специальным статусом, то для получения льгот и гарантий он сообщает данную информацию работодателю. Если работник не предоставляет работодателю сведения о своем особом статусе, то он считается отказавшимся от дополнительных гарантий и льгот; поведение работодателя должно регу-

лироваться не императивными, а диспозитивными нормами, т. е. должно быть поставлено в зависимость от возможности (невозможности) выполнения им своих обязанностей. Субъект не должен отказываться от своего права на тайну, поэтому при получении информации ограниченного доступа (персональных данных, личной и семейной тайны) требуется обеспечить в отношении таких сведений режим конфиденциальности. Обязанность по установлению такого режима в отношении информации о работнике, полученной в связи с трудовыми отношениями, возлагается на работодателя.

Помимо этого, представляется, что работодатель в некоторых случаях может самостоятельно бороться с непредоставлением недобросовестным работником необходимой информации для реализации гарантий, установленных трудовым законодательством, определив в локальных нормативных актах обязанность работников по своевременному информированию работодателя или его представителя о юридически значимых обстоятельствах, необходимых и достаточных для осуществления «хозяйской» власти.

Литература

[1] Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (ч. 1). Ст. 3.

[2] Определение Верховного Суда Российской Федерации от 13 января 2006 г. № 46-В05-44 // Справочная правовая система «КонсультантПлюс».

[3] Бюллетень Верховного Суда Российской Федерации. 2004. № 6.

[4] forum.yurclub.ru/lofiversion/index.php/t84631.html (дата обращения 17 октября 2013 г.).

[5] Постановление Конституционного Суда Российской Федерации от 15 декабря 2011 г. № 28-П «По делу о проверке конституционности части четвертой статьи 261 Трудового кодекса Российской Федерации в связи с жалобой гражданина А. Е. Остаева»// Собрание за-конодательства Российской Федерации. 2011. № 52. Ст. 7639.

[6] Материалы семинара Головиной С. Ю. «Модульный курс по Трудовому кодексу Российской Федерации. Модуль 2. «Кадровые процедуры. Оформление трудовых отношений». – Екатеринбург, 22 ноября 2011 г.

[7] Решение Ковдорского районного суда от 15.08.2011 по делу № 2-1046/2011// http://www.sudoved.ru/ru/docs/3282773 (дата обращения 11 декабря 2013 г.); Кассационное определение Томского областного суда от 08.02.2011 по делу № 33-272/2011 // http://www.sudoved.ru/ru/docs/1727191 (дата обращения 11 декабря 2013 г.).

[8] Решение Елецкого городского суда от 06.09.2011 // http://www.sudoved.ru/ru/docs/3642329(дата обращения 11 декабря 2013 г.); Кассационное определение Курского областного суда по делу № 33-57-2012// http://www.sudoved.ru/ru/docs/4982183 (дата обращения 11 декабря 2013 г.).

[9] В законодательстве США сформулирован принцип запрета злоупотребления правом, под которым понимается недобросовестное осуществление сторонами трудового договора субъективных прав, когда управомоченное лицо создает иллюзию законности собственного поведения, направленного на необоснованное получение имущественных, организационных и других выгод, связанное с обманом другой стороны трудового договора — работника или работодателя (Forced labor // www.law.cornell.edu/uscode/18/usc_sec_18_00001589----000-.html (дата обращения 11 декабря 2013 г.)

[10] Bureau of National Affairs. «Guidelines on AIDS» // Fair Employment Practices. 1989. March 30. P. 39.

[11] Десслер Г. Управление персоналом. М.: БИНОМ. Лаборатория знаний, 2004. С. 75.

[12] Федеральный закон от 30 марта 1995 г. № 38-ФЗ «О предупреждении распространения в Российской Федерации заболевания, вызываемого вирусом иммунодефицита человека (ВИЧ-инфекции)» // Собрание законодательства Российской Федерации. 1995. № 14. Ст. 1212.

[13] Демидов Н. Выбор работодателя: увольнять или нет? Применение п. 6 ст. 81 ТК РФ // Кадровик. Трудовое право для кадровика. 2008. № 9.

[14] Собрание актов Президента и Правительства Российской Федерации.1993. № 18.

[15] Определение Конституционного Суда Российской Федерации от 4 ноября 2004 г. № 343-О об отказе в принятии к рассмотрению запроса Советского районного суда г. Красноярска о проверке конституционности ч. 1 ст. 261 Трудового кодекса Российской Федерации // Собрание законодательства Российской Федерации. 2004. № 51. Ст. 5263.

[16] New Maplecroft report highlights poor labour standards in the Middle East // www.maplecroft.com/news/new_report_highlights_poor_labour_standards_in_middle_east_10.php (дата обращения 11 декабря 2013 г.).

[17] Собрание законодательства Российской Федерации. 2012. № 30. Ст. 4176.

[18] Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.

References

[1] Labour Code of the Russian Federation as of December 30, 2001 No. 197-FZ // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 2002. No.1 (Part 1). Art. 3.

[2] Decision of the Supreme Court of the Russian Federation as of January 13, 2006 No. 46-V05-44 // Spravochnaya pravovaya sistema «Konsul'tant Plyus».

[3] Bulletin of the Supreme Court of the Russian Federation. 2004. No. 6.

[4] forum.yurclub.ru/lofiversion/index.php/t84631.html (accessed October 17, 2013).

[5] Resolution of the Constitutional Court of the Russian Federation as of December 15, 2011 No. 28-P «On the case of testing the constitutionality of part 4 of the Article 261 of the La-bour Code of the Russian Federation in connection with the complaint of A.E.Ostaev'// So-branie zakonodatel'stva Rossiiskoi Federatsii. 2011. No. 52. Art. 7639.

[6] Materials of the seminar of S.Yu. Golovina 'Module course on the Labour Code of the Rus-sian Federation. Module 2. HR procedures. Labour relations'. - Yekaterinburg, November 22, 2011.

[7] Decision of Kovdorskii District Court as of 15.08.2011 on the case No. 2-1046/2011// http://www.sudoved.ru/ru/docs/3282773 (accessed December 11, 2013); Cassational ruling of Tomsk regional court as of 08.02.2011 on the case No. 33-272/2011 // http://www.sudoved.ru/ru/docs/1727191 (accessed December 11, 2013).

[8] Decision of Eletskii City Court as of 06.09.2011 // http://www.sudoved.ru/ru/docs/3642329 (accessed December 11, 2013); Cassational ruling of Kursk Regional Court on the case No. 33-57-2012// http://www.sudoved.ru/ru/docs/4982183 (accessed December 11, 2013).

[9] The legislation of the USA has formed the principle of prohibition against abuse of rights under which dishonest implementation of rights by the labour treaty parties is understood. It is described as a case when a holder of the right (an authorized person) create an illusion of legitimacy and justice of his/her own behavior aimed at ill-found gaining of proprietary, or-ganizational and other benefits connected with a fraud. (Forced labor // www.law.cornell.edu/uscode/18/usc_sec_18_00001589----000-.html (accessed December 11, 2013)

[10] Bureau of National Affairs. «Guidelines on AIDS» // Fair Employment Practices. 1989. March 30. P. 39.

[11] Dessler G. Upravlenie personalom [Personnel management]. Moscow: BINOM. Laborato-riya znanii, 2004. p. 75.

[12] Federal Law as of March 30, 1995 No. 38-FZ «On control of the spread of diseases caused by immunodeficiency virus in the Russian Federation»// Sobranie zakonodatel'stva Ros-siiskoi Federatsii. 1995. No.14. Art. 1212.

[13] Demidov N. Vybor rabotodatelya: uvol'nyat' ili net? Primenenie p. 6 st. 81 TK RF [Em-ployer's choice – to dismiss or not to dismiss? The application of provision 6, Art. 81 of the Labour Code of the Russian Federation]// Kadrovik. Trudovoe pravo dlya kadrovika. 2008. No. 9.

[14] Collected Acts of the President and the Government of the Russian Federation.1993. No. 18.

[15] Decision of the Constitutional Court of the Russian Federation as of November 4, 2004 No. 343-O on refusal to accept for consideration the request of Soviet district court of Kras-noyarsk on testing the constitutionality of part 1 of the Article 261 of the Labour Code of the Russian Federation // Sobranie zakonodatel'stva Rossiiskoi Federatsii.2004. No. 51. Art. 5263.

[16] New Maplecroft report highlights poor labour standards in the Middle East // www.maplecroft.com/news/new_report_highlights_poor_labour_standards_in_middle_east_10.php (accessed December 11, 2013).

[17] Sobranie zakonodatel'stva Rossiiskoi Federatsii. 2012. No. 30. Art. 4176.

[18] Sobranie zakonodatel'stva Rossiiskoi Federatsii. 2006. No. 31 (part. 1). Art. 3451.

Офман Елена Михайловна, кандидат юридических наук, доцент кафедры гражданского права Уральского филиала ФГБОУ ВПО «Российская академия правосудия» (г. Челябинск), 454084, Челябинская область, г. Челябинск, просп. Победы, д. 160. E-mail: elena-ofman@yandex.ru

Elena Mikhailovna Ofman, Cand. Sc. Law, associate professor of the Department of the Civil Law of the Ural Branch of the Federal State Budgetary Educational Institution of Higher Professional Education 'Russian Academy of Justice' (Chelyabinsk), 160, Pobedy Av., Chelyabinsk, 454084, Chelyabinsk Region. E-mail: elena-ofman@yandex.ru

УДК 342.7 + 002:004
ББК Х404.021 + Х404.022

Чеботарева А. А.

ПРАВО НА ЗАЩИТУ ЧЕСТИ, ДОСТОИНСТВА И ДЕЛОВОЙ РЕПУТАЦИИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

В статье рассматриваются актуальные сегодня проблемы реализации и защиты права на защиту чести, достоинства и деловой репутации в современных условиях. Автор подчеркивает важность решения вопроса охраны частной жизни гражданина, защиты чести, достоинства и деловой репутации в условиях формирования информационного общества. Акцентируется внимание на проблеме возможного ограничения права граждан на частную жизнь на современном этапе развития информационного общества России.

Ключевые слова: *информационное общество, электронное государство, права и свободы, защита чести, достоинства и деловой репутации, охрана частной жизни гражданина, ограничение права на частную жизнь.*

Tchebotareva A. A.

THE RIGHT FOR PROTECTION OF HONOUR, ADVANTAGE AND BUSINESS REPUTATION IN INFORMATION SOCIETY

The article discusses the current problems today realization and protection of the right to protection of honor, dignity and business reputation in modern conditions. The author emphasizes importance of the solution of a question of protection of private life of the citizen, protection of honor, advantage and business reputation in the conditions of formation of information society. The attention is focused on a problem of possible restriction of the right of citizens on private life at the present stage of development of information society of Russia.

Keywords: *information society, electronic state, rights and freedoms, protection of honor, advantage and business reputation, protection of private life of the citizen, restriction of the right on private life.*

Важным событием 2013 года стало внимание законодателя к сфере неприкосновенности частной жизни граждан: 1 октября вступил в силу Федеральный закон от 2 июля 2013 г. № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации»[1], новая статья которого – 152.2 ГК РФ – устанавливаетзапрет без согласия гражданина на сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о

месте его пребывания или жительства, о личной и семейной жизни.

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Право на неприкосновенность частной жизни имеет прямое отношение к понятию «информационная безопасность личности», которая, согласно положениям Доктрины информационной безопасности Российской Федерации, определяется как состояние защищенности ее интересов в информационной сфере.

Дела о защите чести, достоинства и деловой репутации граждан в нашем обществе имеют тенденцию к увеличению. Прежде всего, в последние годы новое звучание приобрела проблема интернет-диффамации, т. е. распространения в сети Интернет не соответствующих действительности сведений, порочащих чьи-либо честь, достоинство, репутацию, доброе имя.

Право на неприкосновенность частной жизни относится к числу основных прав человека и защищено Всеобщей декларацией прав человека и Конституцией Российской Федерации.

Соблюдение конституционных прав и свобод человека и гражданина – задача любого государства, позиционирующего себя в мировом сообществе как демократическое. Перечень и содержание основных прав и свобод человека закреплены во Всеобщей декларации прав человека, которую называют совестью мира, нравственным эталоном человечества. В этом историческом документе, как и в Уставе ООН, подтверждена истина: все люди рождаются свободными и равными в своем человеческом достоинстве и основных, естественных правах. Во всеобщей декларации утверждается право каждого человека на жизнь без нужды и страха за личную неприкосновенность, свободу слова и убеждений…[2]

С беспрецедентным распространением высоких технологий, а также с быстрым ростом распространения информации и создания информационного общества связано немало проблем. Единое мировое информационное пространство, создавая условия безграничной свободы и отсутствия должного правового регулирования, ставит под сомнение ряд закрепленных основным законом государства прав и свобод.

Право на свободу слова вкупе с правом на защиту чести, достоинства и деловой репутации граждан в условиях виртуальной реальности приобретают признаки явного дисбаланса.

Исторической вехой в решении вопроса защиты чести, достоинства и деловой репутации в случае распространения ложной или оскорбляющей информации в Интернете стало Постановление Конституционного Суда РФ от 9 июля 2013 года № 18-П[3]. Данным Постановлением некоторые положения ст. 152 Гражданского кодекса РФ признаны соответствующими требованиям Конституции, в частности, что сведения, порочащие честь и достоинство гражданина, опубликованные в сети Интернет на сайтах, не являющихся средствами массовой информации, нарушают конституционные права гражданина. Однако владелец данного сайта или лицо, отвечающее за его администрирование, не могут нести никакой ответственности за их публикацию.

В то же время, некоторые положения ст. 152 Гражданского кодекса РФ названным Постановлением КС РФ были признаны не соответствующими нормам Основного закона. Речь прежде всего о том, что статья не обязывает владельца или администратора такого интернет-ресурса удалять сведения, опубликованные третьими лицами и признанные по решению суда ложными или оскорбляющими честь и достоинство гражданина.

Информационное общество, то есть общество, в котором информационные процессы осуществляются главным образом на основе использования информационно-коммуникационных технологий, информационные ресурсы доступны всем слоям населения, при этом полноценно решена проблема признания, реализации и защиты прав и свобод субъектов информационных правоотношений, переживает сегодня один из самых активных этапов своего развития. В процессе формирования информационного общества вступившие в силу изменения Гражданского кодекса РФ – очередной значимый шаг.

Согласно п. 4 введенной в ГК РФ ст. 152.2 в случаях, когда информация о частной жизни гражданина, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении

дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно.

При этом нужно иметь в виду, что формулировка введенной в Гражданский кодекс РФ статьи 152.2 предполагает открытый характер списка информации, относящейся к понятию частной жизни. Таким образом, понятие частной жизни включает и образ мыслей, и политическое и социальное мировоззрение, увлечения, творчество, целый ряд профессиональных тайн (например, врачебная тайна, адвокатская тайна и т. д.), перечень иных сведений, которые, по мнению человека, должны остаться в тайне.

Фактически, именно гражданин решает, какие именно сведения относятся к его частной жизни и подлежат защите, что неизбежно вызовет увеличение судебных споров по этому вопросу. Конечно, суд может с ним не согласиться и отказаться относить какие-либо сведения к частной жизни.

Законодателем подчеркивается, что не являются неправомерными сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, а также в случаях, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле. И если с распространением информации по воле самого гражданина все понятно, то с вопросом, какие именно государственные, общественные или иные публичные интересы будут оправдывать вмешательство в частную жизнь гражданина, дело обстоит гораздо сложнее.

Помимо того, что гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно, закон не исключает и дополнительные гражданско-правовые способы защиты права на неприкосновенность частной жизни. К таковым закон относит возможность компенсации морального вреда и другие способы гражданских прав, предусмотренные ст. 12 ГК РФ.

В скором времени появится возможность проанализировать складывающуюся практику правоприменения новелл Гражданского кодекса в части охраны частной жизни гражданина, однако механизм реализации Федерального закона от 2 июля 2013 г. № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации» нельзя признать полностью понятным, как в части самого процесса удаления неправомерно распространенной ложной или оскорбляющей честь и достоинство гражданина информации, так и в части точного определения информации, относящейся к понятию частной жизни, а также в вопросе правомерности сбора, хранения, распространения и использования информации о частной жизни гражданина в государственных, общественных или иных публичных интересах. Последнее тем более актуально в условиях, когда в решении вопроса охраны частной жизни заинтересовано мировое сообщество. Так, сегодня мы наблюдаем, как Германией и Бразилией инициируется распространение на Интернет закрепленное в Международном пакте право на невмешательство в частную жизнь[4]. Эти страны, за лидерами которых шпионило Агентство национальной безопасности (АНБ) США, внесли на рассмотрение ООН проект резолюции против шпионажа.

Документ призывает все страны пересмотреть законодательство и методы, касающиеся сбора информации за границей. «Те права, которые люди имеют офлайн, должны быть защищены и в режиме онлайн, в первую очередь – право на частную сферу», – подчеркивается в тексте проекта резолюции. В проекте резолюции особенно актуализируется право каждого гражданина на частную жизнь, в том числе во время использования возможностей Интернета. В связи с этим авторы резолюции требуют пересмотреть методы сбора разведданных и ужесточить законодательство в данной сфере.

И вновь на повестке дня вопрос: право каждого гражданина на частную жизнь и воз-

можность ограничения этого права. В отношении судебной практики по вопросу применения норм вступившего в силу Федерального закона от 2 июля 2013 г. № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации» правоприменителю необходимо будет учитывать правовую позицию Конституционного Суда Российской Федерации, высказанную в Постановлении Конституционного Суда Российской Федерации от 30 октября 2003 г. № 15-П[5]:

а) ограничения конституционных прав должны быть необходимыми и соразмерными конституционно признаваемым целям таких ограничений;

б) при допустимости ограничения того или иного права в соответствии с конституционно одобряемыми целями государство, обеспечивая баланс конституционно защищаемых ценностей и интересов, должно использовать не чрезмерные, а только необходимые и строго обусловленные этими целями;

в) публичные интересы, перечисленные в ст. 55 (ч. 3) Конституции РФ, могут оправдать правовые ограничения прав и свобод, только если такие ограничения отвечают требованиям справедливости, являются адекватными, пропорциональными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе прав и законных интересов других лиц, не имеют обратной силы и не затрагивают само существо конституционного права с тем, чтобы исключить возможность несоразмерного ограничения прав и свобод человека и гражданина в конкретной правоприменительной ситуации.

Литература

[1] Федеральный закон от 2 июля 2013 г. № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации» // СЗ РФ. 08.07.2013. № 27. Ст. 3434.

[2] Саидов А. Х. Общепризнанные права человека. М.: МЗ ПРЕСС, 2004. С. 3.

[3] Постановление Конституционного Суда РФ от 09.07.2013 № 18-П «По делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации в связи с жалобой гражданина Е. В. Крылова» // Рос. газета. № 157. 19.07.2013.

[4] РИА-Новости [Электронный ресурс] // Режим доступа: http://ria.ru/world/20131030/973721054.htm (30.10.2013).

[5] Постановление Конституционного Суда РФ от 30.10.2003 № 15-П «По делу о проверке конституционности отдельных положений Федерального закона "Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации"» в связи с запросом группы депутатов Государственной Думы и жалобами граждан С. А. Бунтмана, К. А. Катаняна и К. С. Рожкова» // Рос. газета. № 221. 31.10.2003.

References

[1] Federal law as of July 2, 2013 No. 142-FZ «On amendments in Subsection 3, Section I, Part 1 of the Civil Code of the Russian Federation» // SZ RF. 08.07.2013. No. 27. Art. 3434.

[2] Saidov A.Kh. Obshchepriznannye prava cheloveka [Generally recognized human rights]. Moscow: MZ PRESS, 2004. p. 3.

[3] Resolution of the Constitutional Court of the Russian Federation as of 09.07.2013 No. 18-P «On the case of testing the constitutionality of the provisions of Sections 1, 5, and 6 of the Article152 of the Civil Code of the Russian Federation in connection with the complaint of E.V. Krylov» // Ros. gazeta. No. 157. 19.07.2013.

[4] Rianovosti [Electronic resource] // http://ria.ru/world/20131030/973721054.htm (30.10.2013).

[5] Resolution of the Constitutional Court of the Russian Federation as of 30.10.2003 No. 15-P « On the case of testing the constitutionality of certain provisions of the Federal law «On basic guarantees of electoral rights and the right to participate in the referendum of the citizens of the Russian Federation» in connection with an enquiry of a group of deputies of the State Dume and complaints of S.A. Buntman, K.A. Katanyan, and K.S. Rozhkov» // Ros. gazeta. No. 221. 31.10.2003.

Чеботарева Анна Александровна, кандидат юридических наук, доцент, доцент юридического института Московского государственного университета путей сообщения, докторант РПА Минюста России. E-mail: anna_galitskaya@mail.ru

Tchebotareva Anna, associate professor Moscow State University of Railway Engineering, candidate of jurisprudence, docent. 127994, Moscow, Obraztsova St., 9/9. E-mail: anna_galitskaya@mail.ru

УДК 34.03:004.056.5
ББК Х401.114 + Х401.011.1:Х401.114

Дубровин О. В.

К ВОПРОСУ ГОСУДАРСТВЕННОЙ КИБЕРБЕЗОПАСНОСТИ

В статье рассмотрены некоторые элементы кибербезопасности Соединенных Штатов Америки, организаций Североатлантического договора, основы стратегии кибербезопасности России, а так же предложения по защите информационного пространства Российской Федерации. Автор приходят к выводу о необходимости принятия и реализации стратегии кибербезопасности России в ряду первоочередных и стратегических вопросов Правительства Российской Федерации, а также необходимости объединения усилий государств в разработке и принятии международных конвенций по вопросам кибербезопасности.

Ключевые слова: *кибербезопасность, государственная кибербезопасность, стратегия кибербезопасности России.*

Dubrovin O. V.

TO THE QUESTION OF THE STATE CYBER SECURITY

The article considers certain aspects of cyber security of the United States of America, organizations of the North American Treaty, fundamental strategies of cyber security in Russia, as well as the proposals on the information security in the Russian Federation. The author concludes the necessity of the realization of the strategy of cyber security in Russia as a top priority issue for the Government of the Russian Federation, as well as the necessity of the integrating efforts in the development of international conventions on the questions of cyber security.

Keywords: *cyber security, state cyber security, strategy of cyber security in Russia.*

Развитие информационных и телекоммуникационных технологий, расширение и доступность интернет-пространства, его использование гражданами, бизнесом, органами государственной и муниципальной власти – эти и многие другие факторы заставляют задуматься о кибербезопасности как об одной из ключевых составляющих национального суверенитета Российской Федерации.

Частные компании и государственные учреждения, некоммерческие организации и политические партии, города-государства и ведущие страны мира, все сталкиваются с реальными проявлениями угроз кибербезопасности, беспрецедентными по своему масштабу, разнообразию и сложности.

В Интернете не проведены границы государств, куда можно было бы выставить в охранение караулы, в связи с этим остается открытым вопрос поиска и привлечения к ответственности лиц, нарушающих законы с применением интернет-пространства, информационных и телекоммуникационных технологий.

Следует согласиться с мнением Бирюковой Т. А., Беляковой Е. Г., Копьева А. В., Морозова С. Ю., Хлистун Ю. В., Юдиной А. Б., которые считают,

что при создании и использовании российских сегментов систем глобальной подвижной персональной спутниковой связи должны приниматься исчерпывающие меры по обеспечению информационной безопасности, исключающие ухудшение качественных характеристик функционирования российского сегмента, неконтролируемое его использование и блокирование его работы по конъюнктурным или политическим мотивам, что может приводить к нанесению ущерба пользователям и владельцу российского сегмента и интересам национальной безопасности и суверенитету РФ[1].

При этом требования по обеспечению одного из важнейших элементов информационной безопасности – российских сегментов указанных систем – установлены в 1999г.[2]

Представляется необходимым рассмотреть мировой опыт решения данной проблемы.

Одним из лидеров в области обеспечения информационной безопасности и контроля над глобальной сетью Интернет 26 мая 2010 года была опубликована «Стратегия национальной безопасности Соединенных Штатов»[3].

Согласно указанному документу спектр военных угроз остается широким, включая угрозы в космосе и в киберпространстве, таким же широким является спектр потенциальных противников, от целых государств до негосударственных организаций.

Угрозами для внутренней безопасности названы широкомасштабные кибератаки. При этом в Стратегии национальной безопасности Соединенных Штатов отмечено, что особую важность имеет защищенность киберпространства, поскольку от этого зависит и гражданский (личностная безопасность, экономика, торговля, инфраструктура жизнеобеспечения), и военный сектор[4].

Следует отметить, что Соединенные Штаты Америки стремятся завоевать главенствующее положение в мире, особое внимание уделяют глобальному информационному пространству, создавая военное киберкомандование.

В американской трактовке контроль над киберпространством означает защиту собственных информационных систем и хранящейся в них информации, а также способность вести наступательные кибернетические операции. При этом, согласно официально принятому в США определению, под кибернетическим пространством понимается некое условное (виртуальное) пространство, возникающее в процессе использования электронных и электромагнитных средств хранения, обработки и обмена данными в компьютерных сетях и связанных с ними физических инфраструктурах[5].

Согласно отчету, подготовленному по результатам ежегодного саммита по угрозам в киберпространстве, прошедшего 15 октября 2008 года, определен перечень наиболее серьезных киберугроз. К их числу было отнесено:

• распространение вирусных программ, способных наносить ущерб программному и аппаратному обеспечению;

• скрытое дистанционное управление информационными системами (перегрузка каналов, рассылка спама, хищение информационных ресурсов);

• активизация боевых действий в киберпространстве;

• перехват IP-адресов и мобильного телефонного трафика;

• экономическая и финансовая преступность в кибернетическом пространстве[6].

В 2011 году организацией Североатлантического договора (НАТО) была принята Доктрина кибербезопасности, текст которой на сегодняшний день не представлен широкому кругу лиц. При этом организацией Североатлантического договора создаются органы коллективной кибербезопасности:

• Совет по кибероборонe (NATO Cyber Defence Management Board – CDMB) для координации вопросов обороны в киберпространстве в штаб-квартире НАТО основных командных центров Организации;

• Совет по консультациям, контролю и командованию (The NATO Consultation, Control and Command – NC3) как основной орган, отвечающий за технические и прикладные аспекты кибероборонe;

• Военное руководство НАТО (NATO Military Authorities – NMA) и Агентство по консультациям, контролю и командованию (Consultation, Control and Command Agency – NC3A) имеют определенные полномочия по определению стандартов оборонного потенциала в области кибербезопасности, а также закупок для его развития;

• Агентство по связи и информационным услугам НАТО (NATO Communication and Information Services Agency – NCSA) отвечает за предоставление технических и оперативных услуг в области кибербезопасности по всей организации Североатлантического договора. Агентство отвечает за противодействие любой киберагрессии против членов НАТО[7].

Специализированный центр по обороне в сфере кибербезопасности НАТО (CCDCOE) в Таллине при участие 20 экспертов и консультантов

– сотрудников Международного комитета Красного Креста и Киберкомандования США разработал пособие о ведении санкционированных онлайн-атак.

Согласно принципам спланированной хакерской атаки, указанным в пособии, нападениям не должны подвергаться такие важные гражданские объекты, как больницы, дамбы и атомные электростанции, при этом атаки на ключевые гражданские объекты могут рассматриваться как нарушения Женевской конвенции[8].

Руководитель экспертной группы по созданию пособия Майкл Шмитт заявил, что применение силы возможно только в том случае, если разразился вооруженный конфликт[9]. В документе также рассмотрены и вопросы поиска инициаторов атаки.

Представляется необходимым отметить интерес Соединенных Штатов Америки в заключении соглашений по вопросам кибербезопасности со странами, не являющимися участниками Североатлантического договора.

В апреле 2013 г. приняли решение начать диалог по вопросу кибербезопасности Соединенные Штаты Америки и Китай, которые на протяжении последних лет обвиняли друг друга в хакерских атаках.

Исключением не является и Российская Федерация. В июне 2013 г. между Правительством Соединенных Штатов Америки и Правительством Российской Федерации было заключено соглашение об организации линии прямой шифрованной связи между уполномоченными представителями Соединенных Штатов Америки и Российской Федерации по вопросам угроз в сфере использования информационно-коммуникационных технологий и самим информационно-коммуникационным технологиям[10].

Главная опасность виртуальных кибератак есть возможность наносить дистанционный реальный урон экономической и политической независимости государства средствами информационных и телекоммуникационных технологий.

Все большее количество жизнеобеспечивающей инфраструктуры государства – электронное правительство, платежные системы, он-лайн-банкинг, интернет-трейдинг и т. д. – становится потенциальными объектами для кибератак. Например, программные закладки в программном обеспечении компьютеров в посольстве станут отправлять секретные данные злоумышленникам, которые смогут выставить их на продажу. Кража баз данных банка может привести к массовому выводу денег со счетов населения. Киберугрозам может подвергаться кто угодно – государство в целом, предприятия и организации, личность, все это может оказать влияние на независимость государства.

При рассмотрении данного вопроса следует обратить внимание на деятельность Временной комиссии Совета Федерации по развитию информационного общества, председателем которой является член Совета Федерации Федерального Собрания Российской Федерации Р. У. Гаттаров.

В марте 2013 г. при инициативе членов Временной комиссии Совета Федерации по развитию информационного общества был разработан проект национальной Стратегии кибербезопасности России[11], в котором были определены основные угрозы в области кибербезопасности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) кибершпионаж (таргетированные атаки на информационные массивы государственных структур, бизнеса и граждан)

5) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности государства, бизнеса, гражданина;

6) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде;

7) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

К основным направлениям Стратегии кибербезопасности России были отнесены:

1) безопасность онлайн-бизнеса. Исследование «Экономика Рунета» показало, что объем российского сегмента интернет-рынка достигает 1% ВВП с прогнозом роста в 30% в год. Со стороны государства необходимо оказывать определенную поддержку этому рынку, как, например, делают в США. Прежде всего речь идет о защите финансовых онлайн-операций, противостоянии и расследовании киберпреступлений;

2) обеспечение гарантий прав граждан. Каждый все больше доступен по каналам цифровой коммуникации, и потому более уязвим. Растет количество случаев онлайн-мошенничества, краж персональных данных, преследования. Гражданин должен иметь право на защиту его личной жизни и данных;

3) защита национальной информационно-коммуникационной инфраструктуры. Речь идет как об органах государственного управления, так и крупных объектах, таких, как атомные станции и трубопроводы;

4) реализация современных систем управления с использованием информационно-коммуникационных технологий. Электронное правительство, электронный парламент, электронные выборы – все эти инновационные системы могут быть очень уязвимы для манипуляций по каналам цифровой коммуникации. Это очень опасно, т. к. нарушается функционирование ключевых государственных механизмов и теряется управляемость, поэтому нужно обеспечить их защищенность;

5) построение эффективных механизмов борьбы с киберпреступлениями. Сегодня расследуется малая доля киберпреступлений, и практически все они – на нашей территории. Наиболее опасные операции проводятся с территорий других государств, поэтому расследование и привлечение ответственности сильно усложняется, поскольку дело выходит на межнациональный уровень. Для решения проблемы нужно ратифицировать Конвенцию по борьбе с киберпреступностью;

6) противодействие массированным кибератакам. США, страны Западной Европы, Китай, Южная Корея и другие страны активно развивают свои службы по ведению кибероперациий. Они включают как оборону, так и нападение. России необходимо быть готовой защищать свои цифровые границы от краж секретных данных, которые налажены в фоновом режиме, и нанесения ущерба в случае обострения отношений.

Следует отметить, что в целях защиты информационного пространства Российской Федерации стратегией кибербезопасности России предложено:

1) создание государственного ситуационного центра, функционирующего в режиме 24/7, с целью изучения киберугроз и реагирования на них;

2) создание портала, содержащего статистическую информацию об инцидентах в сфере кибербезопасности, потенциальных уязвимостях информационных систем и способах их компенсации, а также предоставляющего гражданам РФ возможность публиковать сообщения о проблемах в области кибербезопасности, обсуждать их и предлагать конструктивные решения, получать обратную связь от уполномоченных государственных органов;

3) организация национальных учений в области кибербезопасности с участием военных подразделений, правоохранительных органов, государственных органов, а также руководства критически важных объектов;

4) полноценный запуск и переход на широкое использование инфраструктуры электронной цифровой подписи;

5) разработка и принятие государственных стандартов кибербезопасности Российской Федерации, а также реализация механизмов их регулярного пересмотра в соответствии с лучшими мировыми практиками и новейшими технологиями;

6) предоставление правоохранительным органам полномочий, расширяющих их оперативные возможности по борьбе с киберугрозами;

7) принятие программы развития отечественных программных средств обеспечения кибербезопасности;

8) обязательная публикация под свободной лицензией ПО, разработанного по госзаказу (кроме особых случаев);

9) пересмотр квалификационных требований к государственным служащим в области информационных технологий с учётом современных тенденций отрасли.

Представляется необходимым высоко оценить профессионализм и актуальность разработки стратегии кибербезопасности России, при этом считаем, вопрос ее принятия и реализации должен входить в перечень первоочередных и стратегических вопросов Правительства Российской Федерации.

Также следует отметить необходимость объединения усилий государств в разработке и принятии международных Конвенций по вопросам кибербезопасности в целях совершенствования законодательной базы и снижения барьеров при поиске и поимке киберпреступников, обеспечения национальной безопасности стран.

Литература

[1] Бирюкова Т. А., Белякова Е. Г., Копьев А. В., Морозов С. Ю., Хлистун Ю. В., Юдина А. Б. Комментарий к Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи» // СПС «ГАРАНТ». 2012.

[2] Об утверждении Положения о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи (ГППСС) и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем»: Приказ Гостелекома РФ от 21 июля 1999 г. № 22 // Российская газета. 1999. № 247.

[3] U.S. National Security Strategy 2010 // National Strategy Forum URL: http://www.nationalstrategy.com/NSFReview/Winter2009Vol19No1USNSS2010.aspx (дата обращения: 15.09.2013 г.).

[4] Конышев В. Н., Сергунин А. А. Стратегия национальной безопасности Б. Обамы: старое вино в новых мехах? // Обозреватель – Observer. 2010. № 12 (251).

[5] Бедрицкий А. В. Американская политика контроля над кибернетическим пространством // Москва. 2012. № 6.

[6] Там же.

[7] КИБЕРКОМ займется конфликтом Google и Китая // Интернет-портал. Независимая газета. URL: http://nvo.ng.ru/forces/2011-10-07/11_cybercom.html (дата обращения: 15.09.2013 г.).

[8] Женевская Конвенция о защите гражданского населения во время войны // Действующее международное право. 2007. т. 2.

[9] Искусство кибервойны: НАТО выпустила руководство для хакеров. // Интернет-портал ТВ-новости. URL: http://russian.rt.com/article/5929 (дата обращения: 15.09.2013 г.).

[10] О заключении Соглашения между Правительством Российской Федерации и Правительством Соединенных Штатов Америки об организации линии прямой шифрованной связи между уполномоченными представителями Российской Федерации и Соединенных Штатов Америки по вопросам угроз в сфере использования информационно-коммуникационных технологий и самим информационно-коммуникационным технологиям: Распоряжение Правительства РФ от 15 июня 2013 г. № 983-р. // СЗ РФ. 2013. № 25. ст. 3196.

[11] Проект Стратегии национальной кибербезопасности РФ. Интернет-портал. URL: http://gattarovruslan.ru/?dir=initiative&index=4 (дата обращения: 15.09.2013 г.).

References

[1] Biryukova T.A., Belyakova E.G., Kop'ev A.V., Morozov S.Yu., Khlistun Yu.V., Yudina A.B. Kommentarii k Federal'nomu zakonu ot 7 iyulya 2003 g. № 126-FZ «O svyazi» [Commentaries to the Federal Law as of July 7, 2003 No. 126-Fz 'On communications']// Sistema GARANT. - 2012.

[2] Ob utverzhdenii Polozheniya o poryadke, obshchikh usloviyakh i printsipakh ispol'zovaniya na territorii Rossiiskoi Federatsii sistem global'noi podvizhnoi personal'noi sputnikovoi svyazi (GPPSS) i trebovaniyakh po obespecheniyu informatsionnoi bezopasnosti dlya rossiiskikh segmentov ukazannykh sistem»: Prikaz Gostelekoma RF ot 21 iyulya 1999 g. № 22 [On the affirmation of the provision on procedures, general interpretation and principles of the use of the systems of global portable personal satellite communications and security requirements for the Russian segments of the abovementioned systems: Order of the State Telecommunication Agency of the Russian Federation as of July 21, 1999 No.22]// Rossiiskaya gazeta [Russian post]. 1999. No. 247.

[3] U.S. National Security Strategy 2010 // National Strategy Forum URL: http://www.nationalstrategy.com/NSFReview/Winter2009Vol19No1USNSS2010.aspx (data obrashcheniya: 15.09.2013g.).

[4] Konyshev V.N., Sergunin A.A. Strategiya natsional'noi bezopasnosti B. Obamy: staroe vino v novykh mekhakh? [Strategy of national security of Barak Obama: Old wine in new bottles?]// Obozrevatel'–Observer. 2010. No. 12 (251).

[5] Bedritskii A.V. Amerikanskaya politika kontrolya nad kiberneticheskim prostranstvom [American policy of control over cyber space]// Moscow. 2012. No. 6.

[6] Bedritskii A.V. Amerikanskaya politika kontrolya nad kiberneticheskim prostranstvom [American policy of control over cyber space] // Moskva. 2012. No. 6.

[7] KIBERKOM zaimetsya konfliktom Google i Kitaya [CYBERCOM will manage the conflict of Google and China]// Internet-portal. Nezavisimaya gazeta. URL: http://nvo.ng.ru/forces/2011-10-07/11_cybercom.html (date of compellation: 15.09.2013g.).

[8] Zhenevskaya Konventsiya o zashchite grazhdanskogo naseleniya vo vremya voiny [Geneva Convention Relative to the Protection of Civilian Persons in Time of War] // Deistvuyushchee mezhdunarodnoe pravo [Present international law]. 2007. V. 2.

[9] Iskusstvo kibervoiny: NATO vypustila rukovodstvo dlya khakerov [The art of cyber war: NATO has issued the guidance for hackers]// Internet – portal TV- novosti. URL: http://russian.rt.com/article/5929 (date of compellation: 15.09.2013).

[10] O zaklyuchenii Soglasheniya mezhdu Pravitel'stvom Rossiiskoi Federatsii i Pravitel'stvom Soedinennykh Shtatov Ameriki ob organizatsii linii pryamoi shifrovannoi svyazi mezhdu upolnomochennymi predstavitelyami Rossiiskoi Federatsii i Soedinennykh Shtatov Ameriki po voprosam ugroz v sfere ispol'zovaniya informatsionno-kommunikatsionnykh tekhnologii i samim informatsionno-kommunikatsionnym tekhnologiyam: Rasporyazhenie Pravitel'stva RF ot 15 iyunya 2013 g. № 983-r. [On conclusion of the agreement between the Government of the Russian Federation and the Government of the United States of America on the establishment of the line of direct cypher communication between the authorized representatives of the Russian Federation and the United States of America on the issues of threats in the sphere of the use of information and communication technologies: Decree of the Government of the Russian Federation as of June 15, 2013 No. 983-r] // SZ RF [Official Gazette of the Russian Federation]. 2013. No. 25. Art. 3196.

[11] Proekt Strategii natsional'noi kiberbezopasnosti RF [Project of the strategy of national cyber security of the Russian Federation]. Internet portal. URL: http://gattarovruslan.ru/?dir=initiative&index=4 (date of compellation: 15.09.2013).

Дубровин Олег Владимирович, кандидат юридических наук, доцент кафедры конституционного и административного права Южно-Уральского государственного университета, 454136, г. Челябинск, пр. Победы, д. 293, кв. 339, т. м.+79128082228. E-mail: dov1974@mail.ru.

Dubrovin Oleg Vladimirovich, Candidate of Juridical Sciences, The Associate Professor of Constitutional and Administrative Law, South Ural State University, 454136, Chelyabinsk, Pobedy Prospect, B.293, Apt. 339, bw: +79128082228. E-mail: dov1974@mail.ru.

УДК 342.518:004.7.056.5
ББК Х401.114 + Х401.011

Патраков А. В.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В статье рассматриваются проблемы обеспечения информационной безопасности системы электронного правительства. Автор считает актуальным сегодня подготовку системы нормативных правовых актов, регламентирующих вопросы информационного взаимодействия государства, граждан и бизнеса, а также предусматривающих использование информационно-коммуникационных технологий в новых административных процессах. Совершенствование нормативно-правовой базы позволит устранить отставание законодательства в этой области от потребностей общества и характера общественных отношений, а также создать целостную правовую систему регулирования государственных услуг, оказываемых через информационно-телекоммуникационные сети.

Ключевые слова: *электронное правительство, кибербезопасность, информационная безопасность, служебная тайна.*

Patrakov A. V.

PROBLEMS OF INFORMATION SECURITY SYSTEMS E-GOVERNMENT

This article discusses the information security system of e-government . The author considers relevant today training system of normative legal acts regulating the issues of information cooperation between the state , citizens and businesses , as well as incorporating the use of information and communication technologies in the new administrative processes. Improving the regulatory framework will eliminate the backlog of legislation in this area on the needs of society and the nature of social relations, and create a coherent legal system of regulation of public services provided through information and telecommunications networks.

Keywords: *e-government, cyber security, information security, official secrecy.*

Одним из ключевых проблем в сфере информационной безопасности в целом, а также кибербезопасности в частности, является вопрос обеспечения информационной безопасности системы электронного правительства. Угрозы безопасности инфраструктуры электронного правительства, как крупнейшей в России государственной информационной системы, имеют широчайший спектр. Это могут быть внутренние угрозы (со стороны людей, имеющих доступ к инфраструктуре электронного правительства), внешние (со стороны внешних по отношению к системе пользователей, киберпреступников, киберспецслужб), а

также угрозы объективного характера (потеря информации вследствие техногенных катастроф, природных катаклизмов). Поэтому при проектировании системы обеспечения информационной безопасности для инфраструктуры электронного правительства упор был сделан на комплексный подход. Система интегрирует разнородные средства защиты информации, необходимые для нейтрализации угроз безопасности для всех ее компонент, в единую взаимосвязанную среду, обеспечивающую выполнение целевых задач по информационной безопасности, вытекающих из моделей угроз и моделей нарушений, общесистемной политики безопасности и частных разделов политики безопасности.

Информационная безопасность является одной из важных компонент предоставления государственных услуг в электронном виде. При создании единого портала государственных услуг проводилась работа по анализу возможных угроз, на основе которых сформированы требования по защите информации при использовании портала государственных услуг. В системе безопасности портала используется обширный набор механизмов безопасности: межсетевые экраны, средства анализа содержимого, средства предотвращения вторжений, антивирусные средства защиты информации, средства мониторинга и контроля защищенности.

Программное обеспечение портала государственных услуг проходит сертификацию по требованиям информационной безопасности и отсутствию недекларированных возможностей. Вместе с этим портал государственных услуг аттестован по требованиям ФСТЭК на обработку конфиденциальной информации и персональных данных по требованиям класса К1.

Для доступа на портал используется система аутентификации на основе электронной подписи, реализованная с помощью решений, прошедших сертификацию в ФСБ. Также для обеспечения защищенного межсетевого взаимодействия органов исполнительной власти и организаций, оказывающих государственные услуги, используется система защищенного документооборота. На уровне субъектов РФ утверждаются требования к информационной безопасности электронного правительства, регламентирующие принципы обеспечения информационной безопасности, требования к подсистемам защиты информации.

Основную платформу системы электронного правительства составляет телекоммуникационная инфраструктура ОАО «Ростелеком» – защищенная, сертифицированная корпоративная сеть передачи данных. Все внутренние каналы связи в рамках инфраструктуры электронного правительства защищены средствами криптографической защиты.

В соответствии со своим назначением и политикой информационной безопасности электронного правительства система не накапливает данных, связанных с персональной информацией граждан. Система призвана синхронизировать использование многочисленных учетных данных, которые ведутся различными ведомствами в соответствии с их полномочиями.

Обеспечение необходимого уровня информационной безопасности, в первую очередь персональных данных граждан, является одной из первоочередных проблем реализации программы электронного правительства, которая вызывает обоснованные опасения. И, несмотря на все преимущества электронного правительства, к вопросу информационной безопасности стоит подходить очень серьезно.

Несмотря на масштабы и темпы внедрения инфраструктуры электронного правительства существует ряд проблем, которые необходимо решить для успешного функционирования данной системы.

Во-первых, необходимо отметить, что наряду с переводом государственных услуг в электронный вид в настоящее время в отдельных федеральных законах имеются положения, ограничивающие предоставление государственных и муниципальных услуг в многофункциональных центрах и через портал государственных услуг. К таким положениям относятся нормы федеральных законов, прямо или косвенно ограничивающие и (или) создающие предпосылки для ограничения предоставления государственных и муниципальных услуг по принципу «одного окна», включающие обязательность предоставления заявителем документов, необходимых для получения государственных услуг, исключительно в орган, предоставляющий государственные услуги; наличие в федеральном законе требования получения результата государственной услуги заявителем исключительно в органе, предоставляющем государственные услуги; необходимость осу-

ществления личного взаимодействия заявителя уполномоченными представителями органов, предоставляющих государственные услуги, в целях совершения отдельных действий и процедур.

Во-вторых, выступая в качестве посредника между федеральными органами исполнительной власти, органами власти субъектов РФ, организациями, предоставляющими государственные услуги, и получателями государственных услуг, многофункциональные центры напрямую могут повлиять на результат оказания услуг, что может привести к негативным последствиям как для получателя услуги, так и для органа, ее предоставляющего. В свою очередь, законодательно не закреплена ответственность многофункциональных центров за ненадлежащее исполнение возложенных на них обязанностей в соответствии с нормативными правовыми актами и соглашением о взаимодействии.

Федеральный закон «Об организации предоставления государственных и муниципальных услуг»[1] лишь ссылается на то, что соглашения о взаимодействии, заключаемые между многофункциональными центрами и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, должны включать ответственность сторон за неисполнение или ненадлежащее исполнение возложенных на них обязанностей.

Решением вышеупомянутых проблем может стать принятие законопроекта, внесенного в Государственную Думу 7 марта 2012 г. – проект федерального закона № 33022-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в целях устранения ограничений для предоставления государственных и муниципальных услуг по принципу «одного окна»[2]. Цель – устранить ограничения для предоставления государственных и муниципальных услуг по принципу «одного окна». Проектом вносятся изменения в 23 закона в следующих сферах общественных отношений: образование и наука, здравоохранение, соцзащита, содействие занятости населения, имущественные отношения, предпринимательская деятельность, подтверждение гражданско-правового статуса и др.

Очевидной проблемой внедрения системы электронного правительства мы видим в недостаточности и недоработанности нормативно-правовой базы в области регулирования электронного документооборота, в области использования электронной подписи.

Предоставление государственных услуг в электронной форме включает в себя не только организацию межведомственного электронного взаимодействия, но и электронную подачу заявления на предоставление услуги, отслеживание хода ее предоставления. Однако здесь имеется противоречие с Указом Президента № 351 от 17.03.2008[3], согласно которому запрещается подключение к сети Интернет государственных информационных систем, содержащих сведения, составляющие служебную тайну (к числу которой относятся результаты предоставления государственных услуг). Таким образом, складывается парадоксальная ситуация: законом о предоставлении государственных услуг и другими подзаконными актами предусматривается предоставление государственных услуг в электронной форме, а техническая возможность такого предоставления, по сути, запрещена указом Президента.

На наш взгляд, указанные проблемы могут быть решены путем принятия Федерального закона «О служебной тайне» и согласования нормативных правовых документов, учитывая особенности правоотношений, возникающих в процессе предоставления государственных услуг. Категорирование на законодательном уровне информации, обрабатываемой органами власти в процессе предоставления государственных услуг, позволит определить принципы и правила ее использования в целях удовлетворения потребностей заказчиков государственных услуг и выполнения возложенных на органы власти обязанностей по их предоставлению.

Правительством Российской Федерации устанавливаются Правила использования простых электронных подписей при оказании государственных и муниципальных услуг, в том числе правила создания и выдачи ключей простых электронных подписей, а также перечень органов и организаций, имеющих право на создание и выдачу ключей простых электронных подписей в целях оказания государственных и муниципальных услуг. Также должны быть определены виды электронных подписей, использование которых допускается при обращении за получением государственных и муниципальных услуг. На сегодняшний день Правительством установлены

лишь правила использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой и требования к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой. Вопрос использования электронной подписи получателями услуг пока нормативно не урегулирован.

Остро стоит проблема обеспечения информационной безопасности инфраструктуры электронного правительства. В процессе предоставления государственных услуг происходит накопление большого объема как персональных данных, так и служебной информации органов государственной власти. На данном этапе вопрос информационной безопасности рассматривается лишь поверхностно и упоминается в качестве одного из показателей системы электронного правительства. Не разработаны документы, регламентирующие порядок обработки персональных данных и служебной информации на уровне федеральных и региональных органов власти. Без должного уровня информационной безопасности технологические и социальные последствия компьютеризации и информатизации различных сфер общественной жизни весьма плачевны как для бизнеса и государства, так и для человека, учитывая то, что большая часть персональных данных о потребителях услуг будет сконцентрирована в рамках единой системы электронного правительства. Наблюдается несоответствие типовых форм документов по государственным услугам требованиям Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации[4].

В целях обеспечения безопасности информации, обрабатываемой в системе электронного правительства, необходимо в первую очередь привести законодательство в соответствие с требованиями времени и развитием информационных технологий, провести единую политику защиты информации, разработать единую методику оценки угроз для объектов информатизации, входящих в электронное правительство. Необходимо также уточнить сферы компетенции федеральных органов исполнительной власти в области информационной безопасности. Для обеспечения приемлемого уровня защиты информационных ресурсов электронного правительства необходимо создание комплексной системы обеспечения информационной безопасности. Система обеспечения информационной безопасности должна консолидировать правовые, технологические, организационные, технические и физические меры и способы защиты. Она должна иметь продуманную долгосрочную политику, обеспечивающую повышение уровня информационной безопасности в соответствии с появлением новых источников и средств реализации угроз.

Наряду с проблемами в области права, существуют технологические и социальные проблемы, препятствующие оказанию государственных услуг в электронном виде. А. А. Тедеев выделяет следующие проблемы развития и внедрения концепции электронного правительства:

- низкий уровень развития телекоммуникаций;
- низкий уровень компьютерной культуры населения и должностных лиц государственных органов власти и органов местного самоуправления;
- психологическая неготовность общества[5].

Многие граждане до сих пор не имеют представления о системе электронного правительства, не говоря уже о посещении портала государственных услуг и многофункциональных центров. Граждане по-прежнему сами предоставляют в государственные органы полный комплект документов, необходимый для получения государственной услуги. Причина такой ситуации кроется в том, что ведомства, возможно, не донесли до граждан информацию о том, что теперь нет необходимости предоставления документов в бумажном виде, но также не исключено, что граждане не имеют доверия к электронным документам.

Еще одной проблемой, препятствующей эффективному развитию системы электронного правительства, является «информационное неравенство» – понятие, которое отражает социальную дифференциацию населения по принципу возможностей доступа к информационно-коммуникационным технологиям и выступает одной из серьезных угроз реализации информационных прав человека в условиях глобализации информационной среды.

Для осуществления качественного прорыва в данной сфере, о котором сегодня так много говорится, необходимым представляется подготовка системы нормативных правовых актов, регламентирующих вопросы информационного взаимодействия государства, граждан и бизнеса, а также предусматривающих использование информационно-коммуникационных технологий в новых административных процессах. Совершенствование нормативно-правовой базы позволит устранить отставание законодательства в этой области от потребностей общества и характера общественных отношений, а также создать целостную правовую систему регулирования государственных услуг, оказываемых через информационно-телекоммуникационные сети.

Литература

[1] См.: ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета. 2010. 30 июля.

[2] Проект федерального закона № 33022-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в целях устранения ограничений для предоставления государственных и муниципальных услуг по принципу "одного окна" // http://www.garantkey.ru/monitoring/buhgalter/1703/index.php.

[3] Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03. 2008 № 351 // СЗ РФ. 2008. № 12. Ст. 1110.

[4] Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // СЗ РФ. 2008. № 38. Ст. 4320.

[5] Тедеев А. А. Информационное право: учебник. М.: Изд-во Эксмо, 2005. С. 75.

References

[1] Federal Law «On provision of state and municipal services» as of 27.07.2010 No. 210-FZ // Rossiiskaya gazeta. July 30, 2010.

[2] Draft Federal Law No.33022-6 «On amendments in certain statutory acts of the Russian Federation for the purposes of removal of constraints for provision of state and municipal services on one-stop» // http://www.garantkey.ru/monitoring/buhgalter/1703/index.php.

[3] Presidential Decree of the Russian Federation «On information security measures in the process of use of information and telecommunication networks of international informational exchange» as of 17.03. 2008 No. 351 // Sobranie Zakonodatel'stva Rossiiskoi Federatsii. 2008. No. 12. Art. 1110.

[4] Decision of the Government of the Russian Federation «On affirmation of the Resolution on peculiar features of processing of personal data performed without the use of automation means» as of 15.09.2008 No.687 // Sobranie Zakonodatel'stva Rossiiskoi Federatsii. 2008. No.38. Art. 4320.

[5] Tedeev A. A. Informatsionnoe pravo: uchebnik [Informational law: Course book]. Moscow: Izd-vo Eksmo, 2005. p. 75.

Патраков Алексей Владимирович, студент магистратуры кафедры конституционного и административного права ЮУрГУ. E-mail: avpatrakov@gmail.com.

Patrakov Alexey, graduate student of constitutional and administrative law SUSU. E-mail: avpatrakov@gmail.com.

УДК 004.7.056.5 + 343.35
ББК Х408.135

Попов К. И., Майоров А. В.

ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

В статье рассматриваются отдельные аспекты противодействия преступлениям в сфере компьютерной информации. Автором рассматриваются правовые основы противодействия в целом и преступлениям в сфере компьютерной информации. Делается вывод, что при разработке и совершенствовании нормативного регулирования необходимо учитывать опыт зарубежных стран, которые, значительно раньше приступив к борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств и методов противодействия преступлениям в сфере компьютерной информации.

Ключевые слова: *компьютерные преступления, компьютерная информация, противодействие, борьба, преступность.*

Popov K. I., Mayorov A. V.

LEGAL BASIS OF PREVENTING CRIME IN COMPUTER INFORMATION ON THE INTERNET

The article considers some aspects of counteraction to crimes in the sphere of computer information. The author considers the legal basis of counteraction to the whole, and crimes in the sphere of computer information. It is concluded that the development and improvement of the regulatory framework must take into account the experience of foreign countries, which is much earlier and came to fight crime in the sphere of high technologies, developed a system of effective legal means and methods used to combat crimes in the sphere of computer information.

Key words: *computer crime, computer information, fighting, fighting, crime.*

В правовом государстве борьба с преступностью является одной из ключевых и первоочередных задач, которая осуществляется посредством противодействия целой системы его социальных институтов. Непосредственно же решением данной задачи занимается ограниченный круг государственных органов. Это специализированные органы, которые существуют только для выполнения такой роли в рамках своей компетенции.

Оперативно-розыскная деятельность, являясь государственно-правовой формой борьбы с преступностью, осуществляется в строгом соответствии с законом и имеет правовое регулирование, понимаемое как нормативно-правовое опосредование общественных отношений, их государственно-властное нормирование, облеченное в правовые нормы.

В этой связи предпосылки эффективного осуществления оперативно-розыскных мероприятий в сети Интернет напрямую связаны с наличием полноценной правовой основы, под которой многими авторами понимается совокупность законодательных и иных нормативных актов, регламентирующих возникающие при этом отношения.

Противодействие преступлениям в сфере компьютерной информации с использованием сети Интернет является важнейшей межгосударственной и внутренней криминологической и правовой проблемой нашей страны, основывающейся на соответствующей правовой базе, к которой относятся Конституция РФ и федеральные законы.

В целом же следует отметить, что нормативное урегулирование информационных отношений, в том числе и отношений, возникающих при пользовании компьютерной информацией, в РФ находится на достаточно высоком уровне[1]. Уже в 90-е гг. XX в. в России происходит активное нормотворчество в сфере информационных технологий. Так, в этот период были приняты: Федеральный закон от 27 декабря 1991 г. «О средствах массовой информации»[2]; Федеральный закон от 5 марта 1992 г. «О безопасности» (*утративший силу в 2010 г. в связи с принятием нового Закона*)[3]; Федеральный закон от 21 июля 1993 г. «О государственной тайне»[4]; Федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»[5]; Указ Президента РФ от 28 июня 1993 г. № 966 «О Концепции правовой информатизации России»[6]; Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»[7]; Указ Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию»[8]; Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»[9]; Указ Президента РФ от 24 января 1998г. № 61 «О Перечне сведений, отнесенных к государственной тайне»[10]; Доктрина информационной безопасности РФ, утвержденная распоряжением Президента РФ от 9 сентября 2000 г. № 1895.

В настоящий период действует ФЗ «Об информации, информационных технологиях и о защите информации» от 8 июля 2006 г.[11] В УК РФ целая глава посвящена преступлениям в сфере компьютерной информации.

Глава 28 Уголовного кодекса Российской Федерации (далее – УК РФ) «Преступления в сфере компьютерной информации» включает в себя три состава преступлений: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» и ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Появление данной главы в УК РФ в 1996 г. было крайне обоснованным и весьма своевременным в связи с интенсивным развитием информационных технологий. В то же время в силу относительной новизны регулируемых данной главой правоотношений она страдала многочисленными недостатками – главным образом в понятийной сфере, начиная с отсутствия нормативной дефиниции самого понятия компьютерной информации и заканчивая множеством спорных моментов, связанных с объективной частью каждой из включенных в нее статей[12]. В последующем указанные и другие недостатки были устранены в уголовном законодательстве путем внесения соответствующих изменений и дополнений.

Правовую основу противодействия компьютерным преступлениям посредством осуществления оперативно-розыскной деятельности органами внутренних дел составляют нормативно-правовые акты различной юридической силы:

- Конституция Российской Федерации;
- Федеральный закон Российской Федерации «Об оперативно-розыскной деятельности»;
- другие федеральные законы и принятые в соответствии с ними иные нормативно-правовые акты и международные договоры Российской Федерации.

Виртуальная природа сети Интернет не выводит его из-под юрисдикции Российской Федерации и на возникающие здесь отношения в полном объеме распространяется действие российского законодательства, при ре-

шении указанных проблем нельзя не учитывать надгосударственный характер глобальных сетей, который объективно требует развития международного правового регулирования в этой области, более детальной регламентации в соответствующих актах вопросов организации проведения оперативно-розыскных мероприятий в глобальных компьютерных сетях.

Среди законодательных актов, оказывающих влияние на организацию оперативно-розыскной деятельности в глобальных сетях, следует особо выделить Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи». В этом Законе установлен порядок взаимодействия операторов связи с субъектами оперативно-розыскной деятельности. В соответствии со ст. 64 указанного Закона, операторы связи независимо от ведомственной принадлежности и форм собственности... обязаны оказывать содействие и предоставлять органам, осуществляющим оперативно-розыскную деятельность, возможность проведения оперативно-розыскных мероприятий на сетях связи.

Между тем Законом «О связи» детально не определены формы содействия оператора связи субъектам ОРД, что влечет возникновение коллизий при попытках оперативных служб получить требуемую информацию. Решение данной проблемы возможно путем более четкого закрепления на законодательном уровне обязанностей операторов связи. Внесение соответствующих изменений и дополнений в Закон о связи позволило бы, в отличие от достаточно неопределенной формулировки о «содействии», четко регламентировать порядок предоставления субъектам ОРД доступа к информации на узлах связи.

Правовую основу осуществления оперативно-розыскных мероприятий в глобальных компьютерных сетях в соответствии с ч. 2 ст. 4 Закона «Об оперативно-розыскной деятельности» создают и нормативные акты, издаваемые органами, осуществляющими оперативно-розыскную деятельность. Положения, содержащиеся в нормативных актах МВД России (приказах, инструкциях, наставлениях), должны учитываться при осуществлении оперативно-розыскной деятельности в глобальных компьютерных сетях.

Противодействие сетевым преступлениям требует согласованности и оперативности, наличия системы устойчивых и эффективных связей правоохранительных органов разных государств. Предпринимаемые в этой сфере усилия ведут к реальному укреплению международного взаимодействия правоохранительных органов. Как утверждают эксперты, к настоящему моменту между правоохранительными структурами большинства наиболее развитых стран достигнуты прямые соглашения о сотрудничестве в борьбе с компьютерными преступлениями, и Россия интенсивно участвует в этих процессах. Важную роль играет сотрудничество по линии Интерпола.

Во взаимодействии на международном уровне осуществляется сотрудничество в следующих формах:

а) обмена информацией, в том числе:

- о готовящихся или совершенных преступлениях в сфере компьютерной информации и причастных к ним физических и юридических лицах;
- о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в данной сфере;
- о способах совершения преступлений в сфере компьютерной информации;
- о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации;

б) исполнения запросов о проведении оперативно-розыскных мероприятий, а также процессуальных действий в соответствии с международными договорами о правовой помощи;

в) планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

г) оказания содействия в подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров и учебных курсов;

д) создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

е) проведения совместных научных исследований по представляющим взаимный

интерес проблемам борьбы с преступлениями в сфере компьютерной информации;

ж) обмена нормативными правовыми актами, научно-технической литературой по борьбе с преступлениями в сфере компьютерной информации;

з) в других взаимоприемлемых формах[13].

Таким образом, можно сказать, что в настоящее время не завершен процесс формирования правовой основы по противодействию компьютерным преступлениям, совершаемым с использованием сети Интернет, которую составляет совокупность содержащихся в законодательных и иных нормативных актах правовых норм, создающих правовые условия либо непосредственно регламентирующих его осуществление. Вместе с тем интенсивное изменение технологий опережает соответствующую реакцию законодателя и возможности правоохранительных органов. Поскольку законодательное решение должно основываться на глубоком осмыслении практики, требуется время для того, чтобы в законе и иных нормативно-правовых актах была дана адекватная регламентация отношений, возникающих в рассматриваемой сфере.

Вполне очевидно, что при разработке и совершенствовании нормативного регулирования необходимо учитывать опыт зарубежных стран, которые, значительно раньше приступив к борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств и методов противодействия преступлениям в сфере компьютерной информации.

Примечание:

[1] Гулян А. Р. К вопросу о концептуальных направлениях предупреждения компьютерных преступлений в РФ/ А. Р. Гулян // Общество и право. – 2009. – № 2. – С. 132.

[2] См.: Федеральный закон от 27 декабря 1991 г. «О средствах массовой информации» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 7. Ст. 300.

[3] См.: Федеральный закон от 5 марта 1992 г. «О безопасности» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. № 15. Ст. 769.; Федеральный закон от 28 декабря 2010 № 390-ФЗ «О безопасности» // «КонсультантПлюс» : Режим доступа http://www.consultant.ru/document/cons_doc_LAW_108546/

[4] См.: Федеральный закон от 21 июля 1993 г. «О государственной тайне» // Российская газета. 1993. 21 сент.

[5] См.: Федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31. Ст. 3448.

[6] См.: «О Концепции правовой информатизации России»: Указ Президента РФ от 28 июня 1993 г. № 966 // Собрание актов Президента и Правительства РФ. 1993. № 27. Ст. 2521.

[7] См.: «Об основах государственной политики в сфере информатизации»: Указ Президента РФ от 20 января 1994 г. № 170 // Собрание актов Президента и Правительства РФ. 1994. № 4. Ст. 305.

[8] См.: «О дополнительных гарантиях прав граждан на информацию»: Указ Президента РФ от 31 декабря 1993 г. № 2334 // Собрание актов Президента и Правительства РФ. 1994. № 2. Ст. 74.

[9] См.: «Об утверждении Перечня сведений, отнесенных к государственной тайне»: Указ Президента РФ от 30 ноября 1995 г. № 1203 // Собрание законодательства РФ. 1995. № 49. Ст. 4775.

[10] См.: «О Перечне сведений, отнесенных к государственной тайне»: Указ Президента РФ от 24 января 1998 г. № 61 // Собрание законодательства РФ. 1998. № 5. Ст. 561.

[11] См.: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 31.07.2006, № 31 (1 ч.). Ст. 3448.

[12] См.: Амелин Р. В. О возможном решении проблемы неполноты главы 28 УК РФ / Р. В. Амелин // Уголовно-исполнительная система: право, экономика, управление. – 2009. – № 5. – С. 5–6.

[13] Ястребов Д. А. Международно-правовое сотрудничество государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации / Ястребов Д. А. // Юридический мир. – 2008. – № 12. – С. 75.

References

[1] Gulyan A.R. K voprosu o kontseptual'nykh napravleniyakh preduprezhdeniya komp'yuternykh prestuplenii v RF [To the question of conceptual areas of focus of computer crime protection in the Russian Federation] // Obshchestvo i pravo. – 2009. – No. 2. – p. 132.

[2] Federal law as of December 27, 1991 «On mass media» // Vedomosti S»ezda narodnykh deputatov RF i Verkhovnogo Soveta RF. 1992. No. 7. Art. 300.

[3] Federal law as of March 5, 1992 «On security» // Vedomosti S»ezda narodnykh deputatov RF i Verkhovnogo Soveta RF. 1992. No. 15. Art. 769.; Federal Law as of December 28, 2010 No. 390-FZ «On security» // Konsul'tant Plyus: http://www.consultant.ru/document/cons_doc_LAW_108546/

[4] Federal Law as of July 21, 1993 «On state secret» // Rossiiskaya gazeta. September 21, 1993.

[5] Federal law as of July 27, 2006 «On information, information technologies, and information security» // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 2006. No. 31. Art. 3448.

[6] «On the concept of legal informatization of Russia» Presidential Decree of the Russian Federation as of June 28, 1993 No. 966 // Sobranie aktov Prezidenta i Pravitel'stva RF. 1993. № 27. St. 2521.

[7] Sm.: «Ob osnovakh gosudarstvennoi politiki v sfere informatizatsii» Presidential Decree of the Russian Federation as of January 20, 1994 No. 170 // Sobranie aktov Prezidenta i Pravitel'stva Rossiiskoi Federatsii. 1994. No. 4. Art. 305.

[8] «On additional guarantees of the rights of citizens for information» Presidential Decree of the Russian Federation as of December 31, 1993 No. 2334 // Sobranie aktov Prezidenta i Pravitel'stva Rossiiskoi Federatsii. 1994. No. 2. Art. 74.

[9] «On information classified as state secret» Presidential Decree of the Russian Federation as of November 30, 1995 No. 1203 // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 1995. No. 49. Art. 4775.

[10] «On information classified as state secret» Presidential Decree of the Russian Federation as of January 24, 1998 gNo. 61 // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 1998. No. 5. Art. 561.

[11] Federal law as of 27.07.2006 No. 149-FZ «On information, information technologies, and information security» // Sobranie zakonodatel'stva Rossiiskoi Federatsii. 31.07.2006, No. 31 (Part 1), Art. 3448.

[12] Amelin R.V. O vozmozhnom reshenii problemy nepolnoty glavy 28 UK RF [On possible solution of the problem of the incompleteness of Chapter 28 of the Criminal Code of the Russian Federation] // Ugolovno-ispolnitel'naya sistema: pravo, ekonomika, upravlenie. – 2009. – No. 5. – p.5–6.

[13] Yastrebov D.A. Mezhdunarodno-pravovoe sotrudnichestvo gosudarstv - uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v bor'be s prestupleniyami v sfere komp'yuternoi informatsii [International and legal cooperation of the members of the Commonwealth of Independent States in Computer Information Security Crime Prevention] // Yuridicheskii mir. – 2008. – No. 12. – p. 75.

Попов Константин Иванович, канд. юрид. наук, доцент кафедры правовых дисциплин, филиал ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ) в г. Озерске. 456783 , Челябинская область, г. Озерск, ул. Бажова, 14, каб. 210. E-mail: tiulpanovfm@susu.ac.ru

Майоров Андрей Владимирович, канд. юрид. наук, доцент, заведующий кафедрой государственных и гражданско-правовых дисциплин факультета подготовки сотрудников правоохранительных органов, доцент кафедры правовых дисциплин филиала в г. Озёрске ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ), 454081, Челябинск, ул. Артиллерийская, 100, каб. 210. Тел.: 8 (351) 243-05-25. E-mail: AB_Majorov@mail.ru

Popov Konstantin Ivanovich, candidate of law, assistant professor of of State and Civil Disciplines Department, Faculty of Law Enforcement Officials Training «South Ural State University» (national research university) in Ozersk. 454081, Ozersk, 14 Baqova st., 208 of. E-mail: popovki@susu.ac.ru

Mayorov Andrey Vladimirovich, candidate of law, associate Professor, head of State and Civil Disciplines Department, Faculty of Law Enforcement Officials Training «South Ural State University» (national research university), 454081, Chelyabinsk, 100 Artilleryskay st., 210 of. Tel.: 8 (351) 243-05-25. E-mail: AB_Majorov@mail.ru

УДК 342.951:608
ББК Х401.114 + Х404.321.1

Минбалеев А. В.

ОТЗЫВ НА ДИССЕРТАЦИЮ КУЛАКОВА Н. А. НА ТЕМУ «АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ЗАЩИТЫ ПРАВ ПАТЕНТООБЛАДАТЕЛЕЙ»

Отзыв официального оппонента подготовлен на диссертацию, защита которой состоится в диссертационном совете при Южно-Уральском государственном университете. Диссертация посвящена актуальной проблеме административно-правового регулирования защиты прав патентообладателей. В работе рассматриваются проблемы правового регулирования патентной защиты информации.

Ключевые слова: *административное право, защита, патентообладатель, отзыв, диссертация.*

Minbaleev A. V.

REVIEWED BY N.A. KULAKOV THESIS ENTITLED «ADMINISTRATIVE AND LEGAL REGULATION IN THE SPHERE OF PROTECTION OF THE RIGHTS OF PATENT HOLDERS»

Review prepared by the official opponent thesis defense will take place in the dissertation council at the South-Ural State University. The thesis is devoted to the actual problem of administrative and legal regulation of the rights of patent holders. The paper deals with problems of legal regulation of patent protection information.

Keywords: *administrative law, protection, patent, review, thesis.*

Диссертационная работа Николая Андреевича Кулакова посвящена актуальной и сложной теме – вопросам административно-правового регулирования в сфере защиты прав патентообладателей. Избранные автором вопросы исследования актуальны на современном этапе развития государства, поскольку сегодня активно ставятся задачи по созданию благоприятных условий для творческой и изобретательской активности, поощрения отечественных исследований и разработок, обеспечения их конкурентоспособности на внутреннем рынке и за рубежом, стимулирования и внедрения результатов интеллектуальной деятельности, а также дальнейшего совершенствования государ-

ственной политики в области интеллектуальной собственности.

Осознавая важность интеллектуальной собственности для развития инновационной экономики, Российская Федерация уделяет особое внимание вопросам повышения эффективности функционирования института интеллектуальной собственности. Государственные инвестиции в научные исследования и разработки за последние 8 лет возросли в 2 раза (со 143 млрд рублей в 2005 г.), превысив 400 млрд рублей. Стратегия инновационного развития Российской Федерации на период до 2020 года предусматривает индикатор «коэффициент изобретательской активности», который должен увеличиться с 2,0 в 2010 году до 2,8 в 2020 году. Количество ежегодно подаваемых заявок на изобретения к 2020 году должно вырасти как минимум на 40%. Однако текущая практика свидетельствует о недостаточно эффективном функционировании института интеллектуальной собственности. Так, количество патентных заявок за последние 8 лет увеличилось всего лишь на 28 %. В обществе складывается негативная оценка эффективности защиты прав патентообладателей, что приводит к низкой инновационной активности предпринимателей и предпочтению ими иных способов защиты технических решений механизму патентования.

С 1 января 2008 года с принятием части четвертой Гражданского кодекса Российской Федерации появилось кодифицированное законодательство об интеллектуальной собственности, практика применения которого за прошедшие годы показала низкую степень эффективности как административной, так и судебной защиты прав патентообладателей. Гражданско-правовые средства защиты прав патентообладателей все чаще оказываются неэффективными. В этой связи перед государством стоит серьезная задача по созданию комплексной системы защиты данных прав. Одним из ключевых компонентов этой защиты, бесспорно, должен стать действенный механизм административно-правового регулирования в сфере защиты прав патентообладателей. Право интеллектуальной собственности, согласно современной позиции многих исследователей, является комплексным институтом, который включает в себя как гражданско-правовые, так и административно-правовые механизмы защиты. Последние требуют повышенного внимания, поскольку сами патентообладатели, как показывает практика, сегодня не в состоянии защитить свои права и законные интересы.

Актуальность темы обусловливается также вступлением Российской Федерации во Всемирную торговую организацию. Данный факт, связанный с началом действия в России ряда новых международных актов в сфере интеллектуальной собственности, а также новых экономических правил, заставляет сегодня пересматривать государственную политику в сфере защиты прав национальных патентообладателей. Бесспорно, в данном процессе ведущую роль должны играть именно административно-правовые средства защиты прав и законных интересов национальных патентообладателей. В этой связи актуальным является уже сама постановка автором диссертационного исследования проблем системы административно-правового регулирования защиты прав патентообладателей.

Еще одним фактом, обосновывающим актуальность выбранной темы исследования, является начавшаяся реформа государственного управления в сфере интеллектуальной собственности. В России не позднее 1 июля 2014 г. планируется создание Федеральной службы по интеллектуальным правам, которая будет создана на основе Федеральной службы по интеллектуальной собственности. Новая служба консолидирует обязанности всех министерств и ведомств по учету, контролю и хранению интеллектуальной собственности, вплоть до ее экспорта, позволит преодолеть ведомственную разобщенность в этой сфере, вносящую сейчас свой вклад в торможение экономического роста. Новый орган должен будет разработать и принять правила рассмотрения и разрешения споров по защите нарушенных интеллектуальных прав в административном порядке; будет осуществлять проверку в установленном порядке деятельности государственных заказчиков и организаций-исполнителей; аттестацию и осуществлять регистрацию патентных поверенных Российской Федерации, выдачу им регистрационных свидетельств, а также контроль за выполнением ими требований, предусмотренных законодательством Российской Федерации; осуществлять рассмотрение и разрешение в административном порядке споров, возникающих в связи с защитой интеллектуальных прав в отношениях, связанных с подачей и рассмотрением заявок

на выдачу патентов на изобретения, полезные модели, промышленные образцы и других результатов интеллектуальной деятельности, с их государственной регистрацией, с выдачей соответствующих правоустанавливающих документов, с оспариванием предоставления этим результатам и средствам правовой охраны или с ее прекращением. В связи с появлением нового ведомства актуальным является вопрос об эффективности и проблемах функционирования Федеральной службы интеллектуальной собственности и необходимости создания в рамках новой системы защиты прав патентообладаталей, в том числе и с использованием административно-правовых средств защиты.

Все это дает основание полагать, что избранная диссертантом научная проблема, сформулированная в наименовании диссертационного исследования, является по-настоящему актуальной.

Достоверность и обоснованность результатов исследования обеспечивается, прежде всего, тем, что полученные выводы и результаты базируются на результатах обобщения научных позиций ученых по исследуемому кругу вопросов, критического анализа правовой материи, а также практики реализации правовых норм. Этому способствовал системный подход к исследованию поставленных вопросов. В диссертации использован широкий круг источников, включающий в себя: Конституцию Российской Федерации, федеральные законы, а также многочисленные подзаконные акты, акты органов судебной власти. Кроме того, диссертантом использовались материалы научных публикаций, аналитические документы, обзоры, статистические сведения и другие материалы, в том числе характеризующие зарубежный опыт.

Выводы работы базируются как на теоретических материалах в области общей теории права, административного, административно-процессуального, конституционного права, права интеллектуальной собственности, так и на эмпирических данных, полученных в ходе детального исследования указанной проблематики, в том числе значительного количества дел из административной и судебной практики, что делает изложение, а также ряд выводов и предложений обоснованными и доказательственными.

Эмпирическую основу исследования составили официальные статистические данные, материалы обобщения судебной практики, практики Федеральной службы по интеллектуальной собственности. Кроме того, в рамках исследования использованы данные, полученные в ходе анкетирования сотрудников органов внутренних дел, членов Всероссийского общества изобретателей и рационализаторов. Это свидетельствует о достаточной степени достоверности научных положений, выводов и рекомендаций, сделанных диссертантом, а также репрезентативность эмпирического материала.

Диссертация отвечает требованию научной новизны сделанных научных положений, выводов и рекомендаций. Научная новизна обусловлена как самой постановкой проблемы, так и авторским подходом к исследованию административно-правового регулирования в сфере защиты прав патентообладателей в условиях модернизации российской экономики. Автором впервые в отечественной науке административного права проведено комплексное системное исследование административно-правовых средств защиты прав патентообладателей, на основе которого автором предложены меры по совершенствованию правового регулирования в указанной сфере. Исследование теоретико-правовых основ административно-правового регулирования в сфере защиты прав патентообладателей позволило автору сделать ряд предложений по повышению эффективности защиты патентных прав в административном порядке. Новым можно обозначить и разработанный в ходе диссертационного исследования комплекс практических рекомендаций по организации деятельности органов внутренних дел в сфере выявления и пресечения административных правонарушений в области патентного законодательства.

Наиболее существенные выводы и результаты исследования, характеризующие личное участие и вклад автора в разработку научной проблемы, можно представить совокупностью положений, обосновывающих необходимость совершенствования административно-правового регулирования в сфере защиты прав патентообладателей, а также совокупностью сделанных предложений по формированию важного для науки административного права и практики правоприменения понятийного аппарата.

Рассмотрим наиболее важные для науки административного права выводы автора, сделанные в работе.

В первой главе в рамках анализа теоретико-правовых основ административно-право-

вого регулирования в сфере защиты патентных прав исследуется сущность административно-правового регулирования в сфере патентных прав, определяются правовые основы охраны патентных прав, проводится ретроспективный анализ российского и зарубежного законодательства в указанной сфере, определяется административно-правовой статус органов исполнительной власти, наделенных компетенцией по защите прав патентообладателей.

Обозначая общую характеристику административно-правовой защиты прав патентообладателей, автор формулирует понятия административно-правовой охраны прав патентообладателей и административно-правовой защиты (с. 18 диссертации). Необходимо отметить, что в науке административного права данные определения даются впервые. Также впервые в науке административного права систематизировано административно-правовое регулирование в сфере патентования с учетом обновленного законодательства и норм международного права, ставших частью правовой системы Российской Федерации в связи со вступлением в ВТО.

Автором сформулировано понятие административной ответственности в области патентного законодательства, под которым он понимает применение в установленном порядке уполномоченными государственными органами предусмотренных законодательством административных наказаний за совершение административных правонарушений, посягающих на патентные права, с целью предупреждения совершения новых правонарушений как самим правонарушителем, так и иными лицами.

Предложенные автором определения обладают научной новизной и закладывают теоретическую основу для дальнейшего научного анализа вопросов административно-правового регулирования в сфере патентования.

Во втором параграфе автором исследуются история развития российского законодательства и зарубежное законодательство в сфере защиты патентных прав. Автором устанавливается ряд закономерностей в сфере административно-правового регулирования, начавшегося в России с XVIII в. до наших дней. Совершенно справедливым представляется вывод, что с самого начала перехода российского государства к рыночным отношениям существовала необходимость создания специализированного патентного суда, но законодатель попытался заменить специализированный патентный суд административным органом – Высшей патентной палатой Российской Федерации. Сегодня мы видим, что необходимость специализированного суда по вопросам интеллектуальных прав – это объективная необходимость для государства, которое ставит задачу инновационного развития.

В работе систематизирован опыт административно-правового регулирования в сфере защиты прав патентообладателей за рубежом, выработаны существующие модели административной ответственности за нарушение патентных прав. Проделанная работа позволяет автору в дальнейшем прийти к ряду обоснованных выводов. Многие идеи, высказанные автором, не нашли в работе дальнейшего отражения, но, бесспорно, станут основой для дальнейших исследований в сфере совершенствования административно-деликтного законодательства в сфере защиты прав патентообладателей.

В третьем параграфе анализируется административно-правовой статус Федеральной службы по интеллектуальной собственности. Автор приходит к обоснованному выводу, что одной из проблем защиты патентных прав в административном порядке является отсутствие правовой нормы, определяющей максимальный срок рассмотрения возражений Палатой по патентным спорам. В связи с чем последующее предложение по закреплению данных сроков является также обоснованным. К числу органов исполнительной власти, осуществляющих охрану патентных прав, автор относит МВД России. Автор отмечает, что между Роспатентом и МВД России заключено соглашение о взаимодействии, направленное на организацию информационного обмена. При этом в настоящий момент правовой механизм реализации данного соглашения на ведомственном уровне МВД России и Роспатента не сформирован.

Во второй главе «Модернизация административно-правового регулирования в сфере защиты прав патентообладателей» выявлены проблемы нормативно-правового регулирования защиты патентных прав в административном порядке, административной ответственности в сфере патентного законодательства, предложены пути решения данных проблем; разработаны рекомендации по повышению эффективности реализации административной ответственности в

области патентного законодательства органами внутренних дел.

В первом и втором параграфах автором исследована административная процедура рассмотрения патентных споров, осуществляемая Роспатентом и образованной при нем Палатой по патентным спорам, рассматриваются вопросы совершенствования законодательства об административных правонарушениях, посягающих на патентные права. Делается обоснованный вывод о том, что одной из гарантий справедливого разрешения патентных споров является совмещение преимуществ административного разбирательства с гарантиями справедливого рассмотрения дела в Суде по интеллектуальным правам. Наиболее эффективной для Российской Федерации является система, основанная на сочетании административной и судебной форм защиты патентных прав.

Делаются обоснованные предложения по совершенствованию законодательства в части:

• обязательного утверждения решений коллегии Палаты по патентным спорам руководителем Роспатента;

• введения административно-правовой нормы, устанавливающей максимальный срок рассмотрения возражений, поданных в Палату по патентным спорам;

• необходимость дополнения санкции ч. 2 ст. 7.12 КоАП РФ дополнительным видом административного наказания – конфискация орудия или предмета административного правонарушения.

В третьем параграфе анализируется деятельность органов внутренних дел по реализации административной ответственности в области патентного законодательства. Диссертант выявил направления повышения ее эффективности, в том числе:

• повышение качества взаимодействия органов внутренних дел с Всероссийским обществом изобретателей и рационализаторов;

• повышение качества реализации соглашения о взаимодействии МВД России и Роспатента путем закрепления механизма его реализации в ведомственных нормативных правовых актах;

• повышение уровня подготовки сотрудников органов внутренних дел в области патентного законодательства.

Делается ряд предложений по совершенствованию эффективного взаимодействия МВД России и Федеральной службы по интеллектуальной собственности.

В работе отражен ход и результаты проведенных социологических исследований, отражающих достоверность полученных выводов.

Необходимо отметить и подготовленный автором проект Соглашения о взаимодействии Министерства внутренних дел Российской Федерации и Всероссийского общества изобретателей и рационализаторов (приложение 7 диссертации), а также проект Примерной программы повышения квалификации сотрудников подразделений организации применения административного законодательства и подразделений по исполнению административного законодательства территориальных органов МВД России, осуществляющих профилактику и пресечение административных правонарушений в области патентного законодательства (приложение 8 диссертации).

Цель исследования – проведение комплексного анализа административно-правового регулирования в сфере защиты прав патентообладателей, обоснование и разработка рекомендаций по совершенствованию российского законодательства в указанной сфере. В соответствии с поставленной целью автором предпринята попытка разграничить категории «административно-правовая охрана» и «административно-правовая защита» прав патентообладателей; охарактеризовать административно-правовую защиту как элемент административно-правовой охраны патентных прав; исследовать ретроспекцию российского законодательства в сфере защиты патентных прав, а также особенности защиты прав патентообладателей в зарубежных странах; определить место и роль Роспатента в структуре федеральных органов исполнительной власти, а также выявить проблемы правового регулирования защиты патентных прав в административном порядке; разработать предложения и рекомендации по совершенствованию ведомственного правового регулирования защиты патентных прав в административном порядке; исследовать административную ответственность как способ защиты патентных прав и сформулировать конкретные предложения по ее совершенствованию; проанализировать специфику деятельности органов внутренних дел в сфере защиты прав патентообладателей, сформулировать предложения по повышению ее эффективности.

Анализ диссертационного исследования свидетельствует, что поставленные цель и задачи в работе выполнены в полном объеме.

Результаты проведенного исследования отражены в 14 публикациях, семь из которых опубликованы в журналах, рекомендованных в перечне ВАК Министерства образования и науки Российской Федерации для опубликования основных положений кандидатских и докторских диссертаций по юридическим специальностям, в том числе в ведущем журнале России, специализирующемся на вопросах интеллектуальной собственности «Право интеллектуальной собственности». Материалы диссертационного исследования нашли практическое применение в деятельности ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, УМВД России по Хабаровскому краю, а также в учебном процессе ФГКОУ ВПО «Дальневосточный юридический институт МВД России», ФГБОУ ВПО «Тихоокеанский государственный университет», докладывались на международных и всероссийских научно-практических конференциях, круглых столах.

Структура и объем диссертации, изложенной на 202 страницах, состоящей из введения, двух глав, заключения, библиографического списка литературы, приложений, представляются обоснованными, что позволило диссертанту логично и последовательно раскрыть содержание темы.

В то же время диссертационное исследование такой сложной и достаточно актуальной проблемы не может не вызывать ряда замечаний, в том числе и дискуссионного характера.

1. Ряд положений, выносимых на защиту, представляют собой частные аспекты имеющихся пробелов в процедуре рассмотрения патентных споров (положение второе и третье, выносимые на защиту) и не представляют собой теоретических положений, имеющих научную новизну. В защиту автора необходимо отметить, что в работе проводятся теоретические исследования по данным вопросам и делаются обоснованные выводы.

Аналогичное замечание можно сделать и в отношении положения пятого, выносимого на защиту. В данном случае не представляет научную новизну тезис о необходимости переноса статьи из одной главы Кодекса Российской Федерации об административных правонарушений в другую. Кроме того, учитывая тот факт, что патентообладателем могут выступать не только физические лица, но и юридические лица, государство и иные публичные образования, вряд ли обосновано перенесение именно в главу 5 КоАП РФ «Административные правонарушения, посягающие на права граждан». В связи с этим считаем необоснованным и вывод автора, что родовым объектом ч. 2 ст. 7.12 КоАП РФ, которая устанавливает ответственность за нарушение изобретательских и патентных прав, следует признать общественные отношения, возникающие в связи с охраной прав человека и гражданина.

2. Сложно однозначно согласиться с предложением диссертанта о необходимости замены категории «автор» формулировкой «заинтересованные лица». Под «заинтересованными лицами» предлагается рассматривать каждого соавтора, а также лиц, обладающих правом на получение патента в соответствии с гражданским законодательством или договором. При этом в качестве заинтересованных лиц сам автор (если он один) попадает косвенно, исходя из того, что он обладает правом на получение патента. Между тем, право на получение патента в соответствии со ст. 1357 ГК РФ принадлежит в первую очередь автору объекта патентного права. При этом данное право может перейти к иному лицу (как физическому, так и юридическому) по основаниям, предусмотренным законом. Кроме того, право на получение патента может быть передано автором иному лицу на основании гражданско-правового договора. Такими лицами и выступают заявители. Вряд ли стоит отдельно акцентировать внимание на соавторов.

3. Не представляется возможным согласиться с предложением изменить формулировку «сущность изобретения, полезной модели или промышленного образца» на «информация об изобретении, полезной модели или промышленном образце». Информация об изобретении, полезной модели или промышленном образце является более общей формулировкой и значительно расширяет перечень случаев возможного незаконного привлечения к ответственности лиц, распространивших данную информацию. Например, в случае использования конвенционного приоритета информация об изобретении, полезной модели или промышленном образце фактически может быть опубликована российскими авторами путем ее перепечатки из официальных изданий зарубежного патентного ведомства. Информация об изобретении может касаться тех или иных неох-

раняемых элементов изобретения и ряда других организационных аспектов. В связи с этим более логичным видится использование имеющейся законодательной конструкции.

4. Вывод автора о необходимости привлечения к административной ответственности за нарушение прав на селекционные достижения не представляет научной новизны, поскольку уже не раз высказывался на конференциях и круглых столах экспертами в сфере патентного права. Полагаем, что данная возможность вряд ли обоснована в связи со сложностью установления факта нарушения, поскольку если говорить о селекционном достижении, то доказательством нарушения должно быть устойчивое сохранение «контрафактных» признаков селекционного достижения на протяжении ряда поколений. В связи с этим процесс доказывания нарушения должен быть растянут на годы. Выявление же «контрафактных признаков» определенного селекционного достижения в первый год не предполагает, что они сохранятся в последующие годы, а значит, мы и не можем говорить о нарушении.

5. Анализируя в параграфе 3 первой главы место и роль Федеральной службы по интеллектуальной собственности в структуре федеральных органов исполнительной власти, к сожалению, автор не рассматривает имеющуюся концепцию реформирования данного федерального органа исполнительной власти и создание Федеральной службы по интеллектуальным правам. Реформирование планируется завершить в 2014 году, в связи с чем появится ряд особенностей в сфере именно административно-правовой защиты прав патентообладателей.

6. Автор говорит в исследовании о присоединении России во Всемирную торговую организацию, но при этом не учитывает всех особенностей произошедших для России изменений и не выстраивает эту специфику применительно к административно-правовому регулированию. К сожалению, автор не анализирует необходимость внесения изменений в КоАП РФ применительно к ч. 2 ст. 7.12 в связи со вступлением Российской Федерации в ВТО и присоединением к ряду международных документов в сфере патентного права.

7. В работе в ряде случаев используется некорректное применение аббревиатур (РФ, Президент РФ, Правительство РФ, ч. 4 Гражданского кодекса), достаточно много орфографических, пунктуационных и стилистических ошибок. На с. 5 не дается полное название Федеральной службы по интеллектуальной собственности, используется сокращение Роспатент. Ряд сокращений используется без обозначения их полного наименования при первом указании.

Несмотря на высказанные замечания, анализ диссертационного исследования в целом свидетельствует о научной новизне исследования как содержащего в себе ряд существенных для науки административного права выводов и положений. Высказанные замечания ставят под сомнение в определенной мере научную новизну ряда выводов, но на общую положительную оценку представленной к защите работы не влияют. Изучение диссертации и автореферата соискателя показывает достаточную степень обоснованности сформулированных автором в работе в целом ряда научных положений, выводов и рекомендаций.

Теоретическое и практическое значение исследования достаточно высокое и выражается в комплексном изучении широкого круга проблемных вопросов, затрагивающих административно-правовое регулирование защиты прав патентообладателей. Материалы диссертации обобщают и дополняют научные знания об особенностях административно-правового регулирования защиты прав патентообладателей.

Результаты проведенного исследования могут иметь значение для восполнения пробелов административно-правового регулирования в сфере защиты прав патентообладателей. Автором в этой связи разработаны и представлены предложения о внесении изменений в нормативные правовые акты, регулирующие исследуемые общественные отношения.

В ходе проведенной значительной исследовательской работы Н. А. Кулаков продемонстрировал достаточно глубокое знание отечественной литературы по общей теории права, административному праву и процессу, конституционному праву, праву интеллектуальной собственности и другим отраслям права. Диссертация опирается на анализ обширного, разноплановового как нормативного материала, так и правоприменительной практики. Обращает на себя внимание основательная апробация автором выводов и положений, полученных им в ходе работы над темой.

Диссертация Н. А. Кулакова на тему «Административно-правовое регулирование в сфере защиты прав патентообладателей» является самостоятельным, творческим, структурно обоснованным исследованием, соответствующим профилю научной специальности 12.00.14 – административное право; административный процесс.

Автореферат и публикации соискателя отражают основные положения проведенного диссертационного исследования. Автореферат диссертации Н. А. Кулакова отражает ее содержание, включает в себя все необходимые для такого рода работ атрибуты, концептуально объясняет сущность проведенного автором исследования.

Оформление рецензируемой диссертации соответствует установленным требованиям.

Диссертация Н. А. Кулакова свидетельствует о том, что соискателем самостоятельно выполнена актуальная, результативная, ценная в научном плане работа, характеризующаяся высоким, значимым для современной науки административного права потенциалом. Она является научно-квалификационной работой, в которой содержатся полученные лично автором теоретические положения, совокупность которых можно квалифицировать как новое научное достижение, имеющее существенное значение для развития теории права, науки административного права, законотворчества и повышения эффективности правоприменения.

Вывод: диссертационное исследование на тему «Административно-правовое регулирование в сфере защиты прав патентообладателей» соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата юридических наук (пп. 7 и 8 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 30 января 2002 г. № 74 (в ред. Постановления Правительства РФ от 20.06.2011 г. № 475), а диссертант – Николай Андреевич Кулаков заслуживает присуждения ученой степени кандидата юридических наук по специальности 12.00.14 – административное право; административный процесс.

Минбалеев Алексей Владимирович, д. ю. н., доцент, доцент кафедры конституционного и административного права ЮУрГУ. E-mail: alexmin@bk.ru.

Minbaleev Aleksey Vladimirovich, Associate professor in the Department of Constitutional and Administrative Law at the South Ural State University (national research university), Doctor of Law. E-mail: alexmin@bk.ru.

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

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

AUT VIAM INVENIAM AUT FACIAM

Приглашаем на программу повышения квалификации

«СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННО-ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ»

(в рамках указанной образовательной программы предоставляются дополнительные консультационные услуги)

Занятия проводят ведущие специалисты в области делопроизводства и информационных сетевых технологий Южно-Уральского государственного университета

Участникам выдается удостоверение о повышении квалификации государственного образца
Лицензия на образовательную деятельность № 0816 от 03.03.2011 г.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПРОГРАММЫ

Документационное обеспечение управления (ДОУ):

- Классификация документов;
- Особенности составления и оформления распорядительных, организационно-правовых, информационно-справочных документов;
- Требования к реквизитам бланков документа;
- Организация документооборота;
- Порядок движения документов в организации;
- Обработка документов (регистрация документов, контроль за исполнением документов) с помощью программы Excel;
- Номенклатура дел, порядок составления;
- Определение сроков хранения документов;
- Применение нового «Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения»;
- Формирование и оформление дел постоянного, временного (свыше 10 лет) хранения;
- Экспертиза ценности документов (ЭЦД);
- Порядок проведения ЭЦД;
- Подготовка документов к уничтожению;
- Правила оформления акта о выделении к уничтожению документов;
- Составление и оформление описей на дела постоянного, временного (свыше 10 лет) хранения.

Правовые основы:

• Современная нормативно-методическая база по делопроизводству;

• Правила выдачи и свидетельствования предприятиями, учреждениями и организациями копий документов;

• Организационно-правовые основы документирования управленческой деятельности.

Органы управления ДОУ:

• Службы документационного обеспечения управления;

• Положение о службе документационного обеспечения управления и должностные инструкции работников.

IT-технологии:

• Типы компьютерных сетей;

• Основные сведения о сети Интернет и локальной сети;

• Семейство протоколов TCP/IP и адресация компьютеров;

• Online-справочники;

• Поисковые системы;

• Принцип работы поисковых серверов;

• Web-каталоги и web-индексы;

• Электронная почта;

• Правила работы с электронным сообщением;

• Безопасность и защита информации при работе в Интернете.

Стоимость участия одного слушателя составляет 6480 руб.

(шесть тысяч четыреста восемьдесят) рублей 00 коп., НДС не облагается

При участии пяти и более человек от одной организации предоставляется скидка 10%

Оплата производится на расчетный счет

454080, г. Челябинск, пр. В. И. Ленина, 76.
ИНН 7453019764/КПП 745301001
УФК по Челябинской области (ФГБОУ ВПО «ЮУрГУ» (НИУ)
л/с 20696Х28730)
р/с 40501810600002000002
БИК 047501001, ОКПО 02066724
ОКАТО 75401000000, ОГРН 1027403857568
ГРКЦ ГУ Банка России по Челябинской области,
г. Челябинск, КБК 00000000000000000130
В платежном поручении в графе «назначение платежа» указать:
«За обучение Ф.И.О. по «Современным технологиям информационно-документационного обеспечения управления».
Копию платежного поручения иметь при себе.

Продолжительность программы составляет 72 часа

Предлагаем повысить Ваш квалификационный уровень по программе, содержащей курс лекций и практические занятия

Занятия проводятся по мере комплектования групп

Желаем успеха Вам и Вашему бизнесу!

Заявки на участие по программе повышения квалификации принимаются по телефонам:
(351) 267-90-51; 267-99-00 (факс)

E-mail: admin@susu.ac.ru / bov@susu.ac.ru
Сайт: www.susu.ac.ru
г. Челябинск

ЗАЯВКА

на обучение по программе повышения квалификации в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

ФИО участника: _____

Должность: _____

Наименование организации: _____
(полное и сокращенное)

_____

Руководитель организации: _____

Прошу внести меня в список обучающихся по программе повышения квалификации «Современные технологии информационно-документационного обеспечения управления».

_____/_____
(расшифровка подписи)

Реквизиты организации:

юр. адрес: _____	БИК: _____
_____	ОГРН: _____
р/с: _____	ОКПО: _____
в _____	телефон: (_____)_____
к/с: _____	тел. (факс): _____
ИНН/КПП: _____	e-mail: _____

Оплату услуг по настоящей заявке согласно выставленному Исполнителем счету гарантируем.

Руководитель организации _____/_____
М.П. (расшифровка подписи)

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

AUT VIAM INVENIAM AUT FACIAM

Приглашаем на программу повышения квалификации

«КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ»

Приглашаются должностные лица,
ответственные за организацию и обеспечение защиты персональных данных

Занятия проводят ведущие специалисты в области документационного обеспечения управления и защиты информации Южно-Уральского государственного университета

Участникам выдается удостоверение установленного образца
Лицензия на образовательную деятельность № 0816 от 03.03.2011 г.

В связи с подписанием Президентом РФ новой редакции Федерального закона «О персональных данных» от 25.07.2011 года организации, предприятия и учреждения обязаны разработать комплекс мер, обеспечивающих конфиденциальность персональных данных работников и клиентов, таким образом создать систему защиты персональных данных на предприятии и в его структурных подразделениях.

В соответствии с требованиями настоящей редакции закона Оператор обязан издать документы, определяющие политику оператора в отношении обработки персональных данных (ПДн) и устанавливающие процедуры, направленные на предотвращение нарушений законодательства.

Предлагаем повысить Ваш квалификационный уровень по программе, содержащей курс лекций и практические занятия.

По окончании обучения слушателю предоставляется раздаточный материал, включающий подборку нормативных правовых актов, документов, перечень web-порталов и иных полезных ресурсов сети Internet.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПРОГРАММЫ

• Классификация и правовые основы защиты сведений конфиденциального характера;

• Правовые основы защиты ПДн в организации;

• Внутренние документы организации, регламентирующие обработку (автоматизированную, неавтоматизированную) персональных данных;

• Организация работы со сведениями, составляющими служебную тайну;

• Организация работы по обеспечению безопасности ПДн;

• Правила осуществления допуска должностных лиц к обработке ПДн;

• Порядок осуществления внутреннего контроля обработки ПДн;

• Практикум «Разработка Положения о защите ПДн в организации».

Стоимость участия одного слушателя составляет 12 960 руб.
(двенадцать тысяч девятьсот шестьдесят) рублей 00 коп., НДС не облагается
При участии четырех и более человек от одной организации предоставляется скидка 10%

Иногородним участникам программы предлагается проживание в одно- и двухместных номерах различной степени комфортности гостиницы университета

Продолжительность программы составляет 72 часа

Оплата производится на расчетный счет
454080, г. Челябинск, пр. В. И. Ленина, 76.
ИНН 7453019764/КПП 745301001
УФК по Челябинской области (ФГБОУ ВПО «ЮУрГУ» (НИУ)
л/с 20696Х28730)
р/с 40501810600002000002
БИК 047501001, ОКПО 02066724
ОКАТО 75401000000, ОГРН 1027403857568
ГРКЦ ГУ Банка России по Челябинской области,
г. Челябинск, КБК 00000000000000000130
В платежном поручении в графе «назначение платежа» указать:
«За обучение Ф.И.О. по «Конфиденциальному делопроизводству и организации работы с персональными данными».
Копию платежного поручения иметь при себе.

Занятия проводятся по мере комплектования групп
Желаем успеха Вам и Вашему бизнесу!

Заявки на участие по программе повышения квалификации принимаются по телефонам:
(351) 267-90-51; 267-99-00 (факс)
E-mail: admin@susu.ac.ru / bov@susu.ac.ru. Сайт: www.susu.ac.ru
г. Челябинск

ЗАЯВКА

на обучение по программе повышения квалификации в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет)

ФИО участника: _____

Должность: _____

Наименование организации: _____
(полное и сокращенное)

_____

Руководитель организации: _____

Прошу внести меня в список обучающихся по программе повышения квалификации «Конфиденциальное делопроизводство и организация работы с персональными данными».

_____/_____
(расшифровка подписи)

Реквизиты организации:

юр. адрес: _____ БИК: _____

_____ ОГРН: _____

р/с: _____ ОКПО: _____

в _____ телефон: (_____)_____

к/с: _____ тел. (факс): _____

ИНН/КПП: _____ e-mail: _____

Оплату услуг по настоящей заявке согласно выставленному Исполнителем счету гарантируем.

Руководитель организации _____/_____
М.П. (расшифровка подписи)

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 № 3(9) / 2013

Подписано в печать 27.09.2013. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,60. Тираж 300 экз. Заказ 876/1.
Цена свободная.

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