ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 1(3) / 2012

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

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: i-secur@mail.ru**

В НОМЕРЕ

LEGAL ASPECT OF INFORMATION SECURITY

ISSUES AND OPINIONS

COMPUTER SECURITY

INFORMATION ENGINEERING PROTECTION

MARKET OF INFORMATION PROTECTION

REVIEW

TRIBUNE FOR YOUNG SCIENTIST

THE REGIONAL ATTESTATIVE CENTER SUSU

REQUIREMENTS TO THE ARTICLESTO BE PUBLISHED IN MAGAZINE

УДК 34.03:004.056.5, 34.03:[002:004]
ББК Х401.114, Х400.323

П. У. Кузнецов, П. Г. Андреев

СТРУКТУРА И СОДЕРЖАНИЕ МОДЕЛИ ЗАКОНА ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассматриваются вопросы совершенствования законодательства в сфере информационной безопасности. Приводится содержание модельного закона об обеспечении информационной безопасности.

Ключевые слова: *информационная безопасность, институт правового обеспечения информационной безопасности, базовые законы информационной сферы, субъекты и объекты информационной безопасности.*

P. U. Kuznecov, P. G. Andreev

THE STRUCTURE AND MAINTENANCE OF A MODEL OF A LOW ABOUT INFORMATIONAL SECURITY

The article is about problems of improvement of lows in the sphere of informational security. The article contains the maintains of a model Low about informational security.

Keywords: *informational security, institute of a legal providing of informational security, basic lows of informational sphere, subjects and objects of informational security.*

Проблема совершенствования правового регулирования информационной сферы общественных отношений тесно связана с необходимостью не только теоретического исследования вопросов влияния правотворческой деятельности на состояние законодательства, поскольку именно правотворчество является одним из условий совершенствования законодательства, но и непосредственно с процессом систематизации и кодификации действующего законодательства[1].

Законодательство в области правового обеспечения информационной безопасности содержит большой массив нормативных правовых актов, нормы которых разбросаны по многим отраслям права.

Выделение в системе права правового института обеспечения информационной безопасности вызывает необходимость акти-

визации правотворческой деятельности, направленной на упорядочивание законодательных актов и принятие единого закона, консолидирующего общие, основополагающие нормы, на основе которого будут устранены противоречия, существующие в специализированных законах.

Исследование этого аспекта законодательства в области обеспечения информационной безопасности свидетельствует о необходимости унификации терминологии и понятийного аппарата, цели, принципов данной деятельности, осуществляемой государственной политики на общенациональном уровне.

Как отмечает А. А. Стрельцов, совершенствование нормативного регулирования отношений предложено по двум основным направлениям: структурная систематизация нормативных правовых актов посредством их генеральной или частичной инкорпорации в единый сборник, и упорядочение юридических терминов, используемых в этих актах; устранение пробелов в законодательстве, затрудняющих эффективное противодействие угрозам безопасности объектов национальных интересов в информационной сфере[2].

В настоящее время в России приняты и реализуются доктринальные, концептуальные и программные документы, направленные на широкое использование и развитие информационных технологий. Среди них в первую очередь необходимо выделить Доктрину информационной безопасности Российской Федерации[3], в тексте которой значительное внимание уделено состоянию и развитию правового регулирования.

В последние годы наблюдается активный нормотворческий процесс в информационной сфере, особенно возросло число принимаемых законов, имеющих базовый характер.

Базовые законы информационного права занимают особое место в системе информационного законодательства. С момента их появления в отечественной правовой системе они были призваны выполнять две функции:

а) с помощью основных (общих) положений определять общий нормативный правовой климат правового обеспечения информационной сферы человеческой деятельности вне зависимости от отраслевой специфики;

б) непосредственно регулировать информационные правоотношения, возникающие по поводу информации и связанных с нею систем, а также в связи с использованием главных объектов права информационного характера (информационной системы, информационно-телекоммуникационных сетей, массовой информации и информации ограниченного доступа, электронной подписи, информационных технологий, защиты информации и информационной безопасности).

К общим положениям базовых федеральных законов правового регулирования информационной сферы общественных отношений относятся:

основные понятия информационной сферы и их определения;

принципы правового регулирования;

правовой статус основных субъектов информационных правоотношений;

общие правила поведения субъектов информационных правоотношений, содержащие общие дозволения, запреты и ограничения в информационной сфере.

Иначе говоря, нормы базовых законов информационного законодательства определяют *основные положения общего правового режима* информации и связанных с нею систем.

При этом правовые нормы базовых законов соотносятся как общие нормы по отношению к отраслевым нормам, в них содержатся общего характера правовые дозволения, запреты и ограничения, которые являются основой отраслевых правовых режимов объектов информационной природы.

Названные общие положения являются *основой* для формирования отраслевых норм права, призванных регулировать правоотношения, возникающие по поводу отраслевых объектов, имеющих информационный характер. Такие объекты формируются в связи с возникновением конкретных правоотношений в области гражданского права, трудового права, предпринимательского права, финансового права, уголовного права, экологического и земельного права, процессуальных отраслей права.

Следовательно, нормы базовых законов двуедино воздействуют на информационные правоотношения:

1) определяют *общие условия правового режима* информации применительно к отдельным её отраслевым подгруппам – трудовым, административным, уголовно-правовым и др.;

2) устанавливают *общие правила поведения* в области информации, информационных систем, информационных технологий, а также общие правила обеспечения правовой защиты интересов личности, общества и государства в информационной сфере.

Таким же требованиям на наш взгляд, должен соответствовать и базовый закон об информационной безопасности. Он должен содержать термины и их определения, основополагающие принципы обеспечения информационной безопасности, содержать предмет правового регулирования, основные задачи правового регулирования в данной сфере, исходя из угроз охраняемым законом информационным интересам личности, общества и государства. Также в данном законе должен быть определен перечень органов, обеспечивающих информационную безопасность, обозначены сферы их деятельности (например, защита государственной тайны, государственный контроль в сфере защиты персональных данных, лицензирование в сфере защиты информации и пр.) В законе должны быть закреплены основные положения в области обеспечения защиты информации с различным правовым режимом, правового регулирования деятельности по защите информации, включая основы лицензирования, а также общие условия ответственности за нарушение законодательства об информационной безопасности.

Принятие базового закона об информационной безопасности должно создать фундамент для комплексного преобразования законодательства, регулирующего соответствующие отношения в различных сферах деятельности, устранения существующих в них противоречий и восполнения пробелов.

Создание закона об информационной безопасности должно иметь теоретическое обоснование, исходящее из наличия в структуре российского права самостоятельного комплексного правового института обеспечения информационной безопасности, соответствующего ему правового института в российском законодательстве, в настоящее время раздробленного по ряду законодательных актов. Отсутствие состояния упорядоченности, гармонии требует от законодателя систематизации данного института в рамках одного закона.

При разработке закона необходимо исходить из комплексной природы правового института обеспечения информационной безопасности, его взаимодействия со смежными отраслевыми правовыми институтами системы права. Подобный подход означает необходимость формирования внутренне непротиворечивой системы законодательства обеспечения информационной безопасности, направленной на достижение реальной защищенности основополагающих информационных прав и законных интересов личности, общества и государства, обеспечение разумного баланса их законных интересов.

При построении модели законы об информационной безопасности нам представляется целесообразным использование положений Модельного информационного кодекса для государств – участников СНГ[4].

В первой главе закона, по нашему мнению, следует определить цель и сферу действия закона, субъекты и объекты, основные понятия, перечень законодательных актов, регулирующих данную сферу, принципы обеспечения информационной безопасности.

Общие положения закона наиболее целесообразно сформулировать в соответствии с Доктриной информационной безопасности Российской Федерации, нормами и принципами международного права и Конституции Российской Федерации. Соответственно, под информационной безопасностью в законе целесообразно будет понимать состояние защищенности сбалансированных интересов личности, общества и государства в информационной сфере. Среди прочих терминов целесообразно привести дефиниции понятий «информационная безопасность», «жизненно важные интересы в информационной сфере», «защита информации», «безопасность информации», «информационно-психологическая безопасность», «угрозы информационной безопасности», «объекты информационной безопасности», «средства и методы информационного воздействия», «система обеспечения информационной безопасности» и др.

Представляется, что объектом информационной безопасности могут быть жизненно важные интересы в информационной сфере, материальные и нематериальные объекты, а также отношения, возникающие в связи с возникновением угроз правам и законным интересам личности, общества и государства в информационной сфере (в том числе – в результате информационного воздействия на сознание человека и общества). Субъектами информационной безопасности могут быть

общество, государство, государственные органы, органы местного самоуправления, уполномоченные на обеспечение информационной безопасности, а также лица, чьи права и законные интересы были нарушены в результате противоправных посягательств в отношении информации и информационных объектов либо – путем информационного воздействия.

Важным моментом является закрепление в законе системы законодательства об информационной безопасности, а также приоритетное значение закона об информационной безопасности по отношению ко всем остальным законам, которые должны соответствовать его общим положениям. Следовательно, принятие закона повлечет необходимость мониторинга действующего законодательства на предмет соответствия содержащихся в нем норм положениям базового закона.

В качестве основных принципов обеспечения информационной безопасности предлагается выделить следующие принципы: приоритет прав и свобод человека и гражданина (как основополагающий принцип, закрепленный в международном праве); баланс интересов личности, общества и государства; адекватность мер безопасности существующим угрозам; государственная монополия на разработку и производство специальных средств информационного оружия[5]; гласность и общественный контроль в сфере обеспечения информационной безопасности.

Угрозы информационной безопасности, на нейтрализацию которых должна быть направлена деятельность по обеспечению информационной безопасности следует определить, по нашему мнению, исходя из перечня данных угроз, закрепленного в Доктрине информационной безопасности Российской Федерации.

Во вторую главу закона, по нашему мнению, целесообразно включить общие основы государственной системы обеспечения информационной безопасности, направленной на последовательную реализацию требований закона органами исполнительной власти. Важным элементом такой системы является необходимость обеспечения единого информационного и духовного пространства Российской Федерации, традиционных устоев общества и общественной нравственности, развитие правосознания и правовой культуры граждан в области обеспечения информационной безопасности (в том числе – в среде Интернет), обучение населения методам самозащиты от негативных информационных (информационно-психологических) воздействий, основам безопасного поведения в современной информационной среде и др.

В системе обеспечения важным является также определение органа, осуществляющего координацию деятельности в данной сфере (по нашему мнению, целесообразным было бы наделить данными полномочиями Совет Безопасности Российской Федерации).

Не менее важными элементами системы обеспечения информационной безопасности являются защита государственных информационных систем, выявление и учет субъектов, осуществляющих негативные информационные воздействия, ведение мониторинга данных воздействий, разработка и совершенствование средств и методов противодействия угрозам информационной безопасности, обеспечение предупреждения информационной противоправной деятельности, обеспечение подготовки квалифицированных кадров в сфере информационной безопасности (в технической, правоведческой и иных сферах), организация системы лицензирования, сертификации, экспертизы и контроля в сфере информационной безопасности, организация разработки и принятия стандартов в сфере информационной безопасности и др. Особое место в деятельности органов государственной власти должна занять деятельность, направленная на содействие принятию актов, посвященных данной проблеме, на международном уровне, взаимодействие с зарубежными государствами в целях обмена опытом, взаимной гармонизации законодательства, сотрудничеству в сфере противодействия угрозам, существующим в информационной сфере.

Третью главу закона целесообразно посвятить общим вопросам обеспечения безопасности информации ограниченного доступа, а именно: установить общие принципы отнесения информации к разряду конфиденциальной или секретной, виды информации ограниченного доступа (государственная тайна, коммерческая тайна, служебная тайна, личная тайна, семейная тайна, разновидности профессиональной тайны, персональные данные), общие требования к ее защите.

Четвертую главу закона следовало бы посвятить вопросам защиты общедоступной

информации от неправомерного воздействия (блокирования, искажения и проч.). Отдельно здесь следует выделить принципы защиты информации, содержащейся в государственных информационных сетях общего пользования, требования к их защите. Кроме того, в данном параграфе, по нашему мнению, следует урегулировать вопросы, связанные с организацией защиты объектов интеллектуальной собственности (кроме гражданско-правовых способов защиты), таких как государственная аккредитация организаций по коллективному управлению объектами авторских и смежных прав, государственная регистрация отдельных объектов интеллектуальной собственности и т. п.

Пятая глава закона может включать положения, связанные с защитой от вредоносной и недостоверной информации. В данную главу целесообразным представляется комплексно включить положения, содержащиеся в настоящее время в Федеральном законе «О защите детей от информационной продукции, причиняющей вред их здоровью, нравственному и духовному развитию»[6]. Необходимость отражения отдельных специализированных положений последнего очевидна ввиду нарастания в обществе психологической напряженности в связи с предполагаемым использованием некоторыми государственными организациями, корпоративными группами и отдельными людьми специальных средств и методов воздействия на психику человека.

В этой же главе необходимо также выделить угрозы, связанные с негативными информационно-психологическими воздействиями, результатом которых может быть: причинение вреда здоровью человека, блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости; манипуляция общественным сознанием и др. Эти угрозы реализуются через разработку, создание и применение специальных средств и методов воздействия.

Следует установить исчерпывающий перечень случаев, когда применение государством специальных средств и методов воздействия на психику людей может быть оправданно, таким образом реализуется принцип государственной монополии на использование таких средств.

Отдельное внимание следует уделить защите прав граждан, общества и государства от распространения недостоверной информации. При этом должно ограничиваться распространение недостоверной информации, наносящей вред интересам личности, общества и государства. К таковым могут быть отнесены материалы, распространяемые посредством российских и зарубежных СМИ с целью дестабилизации ситуации в государстве, подрыва традиционных общественных устоев, диффамации в отношении отдельных граждан. Должен быть установлен принцип права пострадавшей стороны на получение компенсации и публичного опровержения недостоверной информации.

Шестую главу закона целесообразно посвятить вопросам противодействия информационному экстремизму, установив четкие критерии признания информации угрожающей конституционному строю Российской Федерации, исключающие возможное широкое толкование (которое по сути будет означать введение цензуры). Одним из таких критериев должно выступать точное определение умысла распространителя информации, контекст распространения и т. п. Отдельно необходимо урегулировать вопрос проведения специальной экспертизы, устанавливающей экстремизм информации.

В седьмой, заключительной главе закона следует закрепить общие условия ответственности, применяемые в целях обеспечения информационной безопасности (уголовная, административная, гражданская, дисциплинарная), установить порядок финансового обеспечения деятельности по обеспечению информационной безопасности. Необходимо учесть, что расходы на реализацию закона зависят от создания в рамках государственной системы обеспечения информационной безопасности специального федерального органа. Если такой орган будет создаваться, то для обеспечения его деятельности потребуется дополнительное бюджетное финансирование. Если функции государственной системы обеспечения информационной безопасности будут распределены между существующими федеральными органами государственной власти, то дополнительных расходов федерального бюджета не потребуется.

Принятие закона об информационной безопасности потребует системного реформирования ряда законов, фрагментарно регулирующих данный вопрос: Федерального закона «Об информации, информационных

технологиях и о защите информации», Закона РФ «О государственной тайне», Федерального закона «О коммерческой тайне», Федерального закона «О персональных данных», Федерального закона «О лицензировании отдельных видов деятельности», внесения изменений в КоАП РФ, УК РФ – в части ответственности за информационные правонарушения, в ГК РФ – в той части, которая будет определена в законе об информационной безопасности.

Данный закон, консолидировав нормы, относящиеся к институту правового обеспечения информационной безопасности, в дальнейшем может быть использован в целях кодификации информационного законодательства в рамках информационного кодекса РФ.

Примечания

[1] Развитие информационных технологий и систематизации информационного законодательства. Т. А. Полякова // Информационные технологии и связь в Российской Федерации: 2005–2006 годы : федеральный справочник. – М. : Центр стратегических программ, 2006. – С. 87–98; Она же: Правовое обеспечение информационной безопасности при построении информационного общества в России. : автореферат диссертации на соискание ученой степени доктора юридических наук. – М., 2008. – С. 34.

[2] *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России : автореферат диссертации на соискание ученой степени доктора юридических наук. – М., 2004. – С. 25.

[3] Российская газета. – 2000. – 9 сент.

[4] Информационный бюллетень. Межпарламентская Ассамблея государств – участников Содружества Независимых Государств. – 2008. – № 42. – С. 223 – 251.

[5] Например, *Лопатин В. Н.* Информационное оружие: правовые запреты // Информационное право». – 2007, № 2; *Бегишев И. Р.* Информационное оружие как средство совершения преступлений // Информационное право. – 2010. – № 4. – С. 23 – 25.

[6] Собрание законодательства РФ, 03.01.2011 г. – № 1. – Ст. 48.

Кузнецов Петр Уварович, доктор юридических наук, профессор, заведующий кафедрой информационного права Уральской государственной юридической академии. E-mail: petr_kuznecov@mail.ru.

Андреев Павел Геннадьевич, соискатель кафедры информационного права Уральской государственной юридической академии, консультант отдела контрактов и планово-аналитической деятельности Комитета муниципального заказа администрации Волгограда. E-mail: andreevpg84@mail.ru.

УДК 347.1;347.4
ББК 67.4

А. В. Новоструев

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 27.06.2010 № 210–ФЗ «ОБ ОРГАНИЗАЦИИ ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ»

Универсальная электронная карта (УЭК) – это современное средство получения гражданином государственных и муниципальных услуг и проведения безналичных расчетов. Возможность совмещения этих видов сервиса на одной карте весьма проблематична с позиций сегодняшнего законодательства.

Ключевые слова: *Универсальная электронная карта, национальная платежная система, идентификация, аутентификация.*

A. Novostruev

PROBLEMS REALIZATION OF FEDERAL STATUTE OF 27.06.2010 № 210-FS «ABOUT ORGANIZATION PRESENTATION GOVERNMENT AND MUNICIPAL SERVICES»

Universal Electronic Card (UEC) is the modern means of getting state and municipal services and bank exchanges by a citizen. According to modern legislation acts the combination possibility of these kinds of services on one card is quite problematic.

Keywords: *Universal Electronic Card, national payment system, identification, authentication*

В последние годы правительства во всем мире начали интенсивно использовать информационно-коммуникационные технологии (ИКТ) с целью повышения эффективности и качества своих услуг. Эти инициативы и программы получили название «Электронное правительство» (E-Government). Мировой опыт показывает, что внедрение техноло-

гий «Электронного правительства» предоставляет гражданам и бизнесу доступ к высококачественным услугам государственных органов и одновременно уменьшает стоимость этих услуг.

Подготовка федеральной целевой программы «Электронная Россия» началась после подписания В. Путиным Окинавской хартии. Всемирный Саммит по информационному обществу был проведен в два этапа. Первый – в декабре 2003 г. в Женеве, второй – в ноябре 2005 г. в Тунисе. В это же время начала готовиться и обсуждаться в экспертном сообществе «Стратегия развития информационного общества в России», которая была одобрена в 2007 г.

Проблемы, которые предполагается решить в Российской Федерации с внедрением электронного правительства, лежат в основе необходимости реформирования государственной службы и формулируются следующим образом:

– постоянный рост совокупной занятости и расходов на заработную плату в государственном секторе увеличивает нагрузку на бюджеты разных уровней;

– слабая мотивация труда госслужащих и нехватка квалифицированного персонала приводят к снижению эффективности функционирования государственного аппарата;

– развитие протекционизма и коррупции определяет низкий уровень общественного доверия к чиновникам и государственному аппарату в целом;

– неспособность госаппарата реагировать на изменения вызывает операционную неэффективность и низкое качество государственных услуг.

Одним из способов упростить бюрократические процедуры, улучшить качество государственных услуг, повысить информированность граждан о своих правах, а также способствовать развитию безналичных расчётов является введение в оборот универсальной электронной карты (УЭК) как средства платежа и идентификации личности гражданина.

Созданию единой общенациональной информационно-платежной системы на основе универсальной электронной карты положил начало Федеральный закон от 27.06.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Закон), который определил федеральные электронные приложения, обеспечивающие:

1) идентификацию пользователя универсальной электронной картой в целях получения им при ее использовании доступа к государственным услугам и услугам иных организаций;

2) получение государственных услуг в системе обязательного медицинского страхования (полис обязательного медицинского страхования);

3) получение государственных услуг в системе обязательного пенсионного страхования (страховое свидетельство обязательного пенсионного страхования);

4) получение банковских услуг (электронное банковское приложение).

Для реализации обсуждаемого проекта распоряжением Правительства РФ федеральной уполномоченной организацией по выпуску, выдаче и обслуживанию УЭК назначена компания «Универсальная электронная карта» (ОАО «УЭК»).

В настоящее время запущен ряд пилотных проектов по выпуску УЭК (в Татарстане, Башкортостане, Астраханской области, Москве и др.). В реализации программы их использования (в любом из регионов, осуществляющих пилотные проекты, вне зависимости от места их выдачи) участвуют государственные и муниципальные организации, в том числе в области здравоохранения.

Однако использование УЭК в полном объеме имеет как положительные, так и отрицательные моменты как для их пользователей, так и для субъектов, их обслуживающих.

На сегодняшний день можно выделить четыре группы проблем, возникших при реализации проекта: правовые, технические, экономические и организационные.

Правовые проблемы использования УЭК

Существует ряд противоречий принятого закона с Конституцией РФ и действовавшими на момент его принятия другими федеральными законами (в том числе, раз это услуга, то с Гражданским кодексом, Законом о защите прав потребителей). А именно: в соответствии с пунктами 5 и 6 статьи 2, пунктом 10 статьи 5 и главой 4 данного закона, в организации предоставления государственных услуг участвует многофункциональный центр предоставления государственных и муниципальных услуг (МФЦ), которым, в частности, является российская организация, независимо от организационно-правовой формы,

уполномоченная на организацию предоставления государственных и муниципальных услуг. Между тем функции по организации исполнения функций исполнительной власти неотделимы от самой деятельности исполнительной власти, и до принятия данного закона являлись ими и остаются таковыми независимо от его принятия. В соответствии со статьей 16 закона в качестве основных функций за МФЦ закреплены, в частности:

– прием запросов заявителей о предоставлении государственных или муниципальных услуг;

– представление интересов заявителей при взаимодействии с органами, предоставляющими государственные услуги;

– представление интересов органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, при взаимодействии с заявителями;

– взаимодействие с государственными органами и органами местного самоуправления по вопросам предоставления государственных и муниципальных услуг;

– выдача заявителям документов органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги, по результатам предоставления государственных и муниципальных услуг;

– прием, обработка информации из информационных систем органов, предоставляющих государственные услуги, и органов, предоставляющих муниципальные услуги;

– иные функции, указанные в соглашении о взаимодействии.

Перечень функций, переданных МФЦ, может быть значительно (и при желании неограниченно) расширен.

Таким образом, в соответствии с положениями данного Закона российским организациям, в частности принадлежащим лицам на праве частной собственности, вменяется в обязанность реализация функций государственной власти и, соответственно, передаются властные полномочия, связанные с ее исполнением.

Получается, что в соответствии с данным законом, взаимодействие государства и гражданина в части обеспечения и соблюдения государством социальных прав последнего может, а значит, потенциально будет осуществляться исключительно при посредничестве бизнес-структур (в том числе транснациональных корпораций), де-юре наделенных полномочиями государственных исполнительных органов, что прямо противоречит статьям 2, 3 и 11 Конституции Российской Федерации.

В соответствии с пунктом 3 статьи 1 главы 1 обсуждаемого закона, услуги, предоставляемые государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание, предоставляются в электронной форме в соответствии с опубликованным перечнем. Высший исполнительный орган государственной власти субъекта Российской Федерации вправе утвердить дополнительный перечень услуг, оказываемых в субъекте Российской Федерации государственными и муниципальными учреждениями, предоставляемых в электронной форме.

Эта статья позволяет любые государственные услуги осуществлять исключительно в электронном виде, причем без какой-либо альтернативы. Перечень государственных функций органов исполнительной власти, исполнение которых происходит в электронной форме, может быть неограничен и может охватывать все стороны взаимоотношений граждан и государства по обеспечению государством их конституционных прав и свобод. Формулировки главы 1 закона, а также положение части 3 статьи 15 этого же закона прямо противоречат статье 33 Конституции Российской Федерации, гласящей: «Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления». Также они противоречат положениям действующего Федерального закона № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Функционал УЭК, заявленный при её внедрении, а именно – возможность в последующем заменить такие документы, как паспорт гражданина РФ и водительское удостоверение, также вступил в ряд противоречий с действующим законодательством. При оказании государственных услуг Федеральная миграционная служба РФ (ФМС) обязана удостоверять наличие у заявителя российского гражданства, поскольку данные услуги предоставляются только имеющим его лицам. Сегодня согласно статье 10 закона от 31.05.2002 г. № 62-ФЗ «О гражданстве РФ» единственным документом, подтверждающим гражданство РФ, является паспорт. С позиции ФМС, УЭК не является и не может являться документом, подтверждающим рос-

сийское гражданство, так как ОАО «УЭК» – это коммерческий хозяйствующий субъект, который не уполномочен осуществлять функции по контролю и надзору в сфере миграции. Такая позиция ФМС нашла поддержку в правительстве. Против универсальности электронных карт гражданина выступило и МВД РФ, которое полагает целесообразным использовать УЭК не в качестве водительского удостоверения, а лишь в качестве документа, который подтверждает его наличие. Сегодня права относятся к числу документов, удостоверяющих личность гражданина. В случае лишения УЭК данной функции замена действующего удостоверения картой невозможно.

Технические проблемы использования УЭК

Одной из основных проблем является сложная и потенциально рискованная совместимость двух составляющих – идентификационной (для доступа к государственным услугам) и коммерческой (для доступа к платежным услугам).

На сегодняшний день нет мирового опыта успешного внедрения банковских и идентификационных (удостоверяющих личность) услуг на едином электронном носителе. Существующие виды носителей успешно функционируют лишь при разделении на банковские (коммерческие) и носители, позволяющие получать государственные услуги. Это происходит потому, что не решен вопрос с блокированием УЭК и удержанием её банкоматом в случае неоднократного неправильного ввода пароля. Согласно требованиям международных платежных систем, банкомат в указанных случаях обязан заблокировать и изъять из обращения заблокированную универсальную карту. Однако при изъятии УЭК банкоматом ее владелец лишается не только платежеспособности, но и возможностей реализации своих гражданских прав и полномочий, установленных в Российской Федерации законом. Данную проблему предполагалось решить внедрением национальной платежной системы (НПС). Её введение столкнулось с серьезным противодействием от международных платежных систем VISA и MasterCard, занимающих более 85% карточного рынка в России и имеющих возможность по своему усмотрению в любой момент блокировать значительную часть карточных расчетов в России, так как процессинговые центры находятся за пределами последней. (Введение НПС может лишить эти системы около 4 млрд долларов США комиссионных в год.)

Немаловажными являются и другие технические проблемы: платформа, на которой будет строиться УЭК, а также вопрос аутентификации на основе электронной цифровой подписи (ЭЦП) и ее защиты.

На момент принятия закона не было современных микрочипов, на которых должна храниться вся необходимая информация, и соответствующего программно-аппаратного обеспечения российского производства. Использование чипов и программ иностранного производства ставит национальную безопасность в зависимость от их возможности реализовывать незадекларированные функции (блокирование информации, ее несанкционированное копирование, искажение и т. д.). Вопрос о создании отечественного микрочипа с заданными параметрами на сегодняшний день решен. В январе 2012 года заводом «НИИМЭ и Микрон» передано открытому акционерному обществу «УЭК» 10 тыс. чипов для универсальных электронных карт. ОАО «УЭК» завершило сертификацию первой партии чипов и готовит их к отправке в уполномоченные организации субъектов РФ.

Но вопрос с разработкой и внедрением собственных программно-аппаратных средств остается открытым.

Также не реализовано в должной мере межведомственное электронное взаимодействие. Министерства, ведомства, муниципальные образования и коммерческие организации России строили свои информационные системы не по единым стандартам, что на сегодняшний день не дает возможности полноценного межведомственного информационного взаимодействия и делает невозможным *предоставление услуг в электронном виде на Едином портале государственных и муниципальных услуг (функций) с использованием Единой системы идентификации и аутентификации и иных систем инфраструктуры электронного правительства.*

Кроме того, не решена проблема доступа большого количества граждан России к получению государственных услуг с помощью УЭК. По последним официальным статистическим данным, в сельской местности проживает более 37 миллионов человек в более чем 153 тысячах сельских населенных пунктах. Далеко не в каждом из них есть почтовое отделение, оборудованное пунктом коллективного доступа к сети Интернет. Реализация

предложения сотовых операторов по предоставлению доступа к сети Интернет в любой точке страны с использованием в этих целях ридеров весьма сомнительна в связи с низкой платежеспособностью сельских жителей (стоимость ридера около 50 долларов США плюс стоимость интернет–трафика мобильного оператора).

Экономические проблемы использования УЭК

Это необходимость колоссальных финансовых вложений, объем которых окончательно еще не определен: от 165 млрд (по оценке Минэкономразвития РФ) до 450 млрд рублей (по оценке Сбербанка России). Вложения обусловлены расходами: на выпуск карт; региональный и федеральный процессинг; инфраструктуру приема карт – банковскую, небанковскую, а также электронного правительства; уплату тарифов за транзакции по оказанию государственных и коммерческих услуг.

Главными источниками средств могут быть инвестиции частные (банков – участников платежной системы УЭК, провайдеров услуг и др.) и государственные (федерального и региональных бюджетов). По оценкам Минэкономразвития РФ, основную нагрузку должны нести банки: выпуск карт – 40 млрд руб., региональный процессинг – 12 млрд руб., инфраструктура приема карт – 70–100 млрд руб. Государство готово оплатить расходы на проведение трансакций (10 млрд руб.). Банки будут зарабатывать на эквайринговой сети и использовании остатков на счетах граждан. Государство получит выгоду от экономии на штате чиновников. Однако банки, главные потенциальные участники, не проявляют большой активности из-за неясностей деталей: у кредитных организаций нет достаточного экономического интереса, проект они считают социальным.

Организационные проблемы использования УЭК

Большие сложности возникают в привлечении всех, казалось бы заинтересованных, сторон к участию в проекте. Наблюдается серьезное отставание готовности и противоречивости ведомственных нормативно-правовых и нормативно-технических актов по использованию УЭК.

До сих пор активным предметом исследования остается взаимодействие банков, коммерческих и государственных структур. Данная проблема решается последовательно, в рамках пилотных проектов. Постепенно внедряются универсальные электронные карты в Москве, Татарстане, Башкортостане и других регионах. Введены и реализуются общие технические требования по совмещению этих региональных проектов.

К проблемам следует отнести реально существующее ведомственное сопротивление к введению УЭК в обращение.

Немаловажным является отношение общества в целом, и каждого его члена в отдельности, к так называемой «чипизации». Согласно проведенным опросам, около 20 процентов людей в России – против введения УЭК. Причина – нежелание быть хоть как-то зарегистрированным и идентифицированным на основании машинного кода. Это происходит как по религиозным соображениям, так и из-за неуверенности в надежной защищенности данных о себе или по иным причинам.

Поэтому актуальным становится проведение информационной и разъяснительной работы среди граждан по использованию электронных карт, иными словами, повышение финансовой и информационной грамотности населения. Минэкономразвития готово потратить 20 млн рублей, чтобы выяснить, боятся ли россияне введения универсальной электронной карты (УЭК) и какие именно фобии у них присутствуют в отношении «электронного паспорта». Проведенное исследование ляжет в основу информационной кампании по пропаганде УЭК среди населения.

Проведенное нами исследование показывает, что проблема национального использования универсальной карты все еще не нашла своего полного и органичного разрешения во всех сферах взаимодействия государства и гражданина. И если в сфере банковских услуг есть заметный прогресс, то в сферах правовой и организационной гармонизации ситуация далека от разрешения.

Новоструев Андрей Викторович, старший преподаватель кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: bigus2@yandex.ru

УДК 004.056:34.03, 343.222:[002:004]
ББК Х408.132.20, Х408.135

И. Р. Бегишев

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В настоящее время дискуссионной является проблема установления уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Автор рассматривает данную проблему с разных позиций и предлагает вариант ее решения.

Ключевые слова: *уголовная ответственность, нарушение правил эксплуатации, компьютерная информация, средства хранения, обработки или передачи информации.*

I. R. Begishev

RESPONSIBILITY FOR VIOLATING SERVICE REGULATIONS ON THE MEANS FOR DATA STORING, PROCESSING AND TRANSFERRING AND INFORMATION AND TELECOMMUNICATION NETWORKS

Currently, the issue of determining criminal responsibility for violating service regulations on the means for data storing, processing or transferring and telecommunication networks is a topic for discussions. The author addresses this issue from various positions and provides an option to solve it.

Keywords: *criminal responsibility; violating service regulations; data; means for storing, processing and transferring information*

Всеобщая информатизация общества все больше влияет на нашу жизнь. В силу этого нарушения работы информационно-телекоммуникационных устройств, их систем и сетей могут привести к катастрофическим последствиям.

Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей законодателем установлена в ст. 274 УК РФ «Нарушение правил эксплуатации средств

хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Данная норма является бланкетной и отсылает, как правило, к нормативно-правовым актам, инструкциям и правилам, устанавливающим правила эксплуатации средств хранения, обработки или передачи компьютерной информации.

При описании объективной стороны данного вида общественно опасного посягательства указание в диспозиции статьи на действие (бездействие) носит общий характер: используются слова «нарушение правил». Конкретное содержание этих правил раскрывается в нормативных актах других отраслей права. Ими могут быть федеральные законы, постановления правительства Российской Федерации, правила, инструкции, предписания, например, такие как Общероссийские временные санитарные нормы и правила для вычислительных центров, паспорта качества, технические описания и инструкции по эксплуатации, а также инструкции по использованию компьютерных программ. Правила эксплуатации средств хранения, обработки или передачи компьютерной информации могут быть предусмотрены как в общих требованиях по технике безопасности и эксплуатации компьютерной техники и периферийных устройств, так и в специальных правилах и инструкциях, регламентирующих особые условия эксплуатации средств хранения, обработки или передачи компьютерной информации (например, продолжительность работы и последовательность операций).[1]

Видимо, к средствам хранения, обработки или передачи компьютерной информации относятся персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается. Исходя из этого, было бы правильнее обобщить указанные средства хранения, обработки или передачи компьютерной информации и указать вместо них в названии и диспозиции ст. 274 УК РФ более широкие по смыслу информационно-телекоммуникационные устройства, их системы и сети.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации может выражаться в двух формах: в несоблюдении установленных правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо в нарушении информационно-телекоммуникационных сетей. Так, например, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации могут заключаться: в несоблюдении сроков технического обслуживания компьютеров; в некачественном проведении профилактических работ по обслуживанию компьютеров и их программ; в использовании несертифицированных программных средств; в ошибочных подключениях устройств и т. д.[2]

На наш взгляд, для привлечения нарушителей работы информационно-телекоммуникационных устройств, их систем и сетей к уголовной ответственности по ст. 274 УК РФ требуется принять общие нормы и правила использования информационно-телекоммуникационных устройств, их систем и сетей, которые должны быть обязательными для всех.

По мнению А. В. Сизова, причинение крупного имущественного ущерба не следует рассматривать в качестве тяжких последствий. Он считает, что если имущественный ущерб нанесен вследствие дезорганизации информационной системы посредством преступных действий, направленных на компьютерную информацию, то данный ущерб будет входить в понятие существенного вреда, предусмотренного частью 1 рассматриваемой статьи. А имущественный вред, причиненный собственнику в результате нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, целью которого не являлась информационная безопасность, должен квалифицироваться по совокупности ч. 1 ст. 274 УК РФ и по соответствующим статьям главы 21 УК РФ[3].

При определении тяжких последствий в каждом случае должна устанавливаться причинно-следственная связь между нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и указанными в диспозиции последствиями. Уничтожение, блокирование, модификация либо копирование компьютерной информации обязательно должны быть следствием нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации, а они, в свою очередь, должны быть причиной наступления тяжких последствий.

Представляется оригинальной позиция Н. А. Лопашенко, которая предлагает декриминализировать состав преступления, предусмотренный ст. 274 УК РФ. Она считает, что использование законодателем двух уровней последствий в качестве обязательных признаков состава подчеркивает то, что опасность самого деяния невелика. Не достигает степени преступного и деяние, сопровождаемое ближайшими, неотдаленными (существенный вред) последствиями. Следовательно, вполне возможно влиять на такое поведение мерами других правовых отраслей, прежде всего гражданского и административного. Распространенность подобных деяний также едва ли свидетельствует о необходимости самостоятельного уголовно-правового запрета. И, наконец, ст. 274 УК дает нам пример избыточной криминализации. Очевидно, что при ее проведении преследовалась цель привлечения к ответственности как раз тех лиц, которые, используя свое служебное положение, совершали хищения, применяя высокие технологии. Хищение — это материальный состав; для его наличия требуется причинение материального вреда. Состав нарушения правил, если можно так выразиться, дважды материальный, одно из возможных последствий — существенный вред. Однако если имеется в виду тот же вред, который причиняется хищением, мы нарушаем принцип справедливости уголовного законодательства и дважды привлекаем к уголовной ответственности за одно и то же[4].

В то же время ряд исследователей также предлагают исключить из УК РФ преступление, предусмотренное ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». К их числу можно отнести таких исследователей, как Т. Л. Тропина[5] и М.А. Зубова[6].

Аналогичного мнения придерживается и Д. В. Добровольский, который предлагает декриминализировать ст. 274 УК РФ путем исключения её из УК РФ, так как отсутствует реальная необходимость в уголовной наказуемости такого отклоняющегося поведения[7].

А.Ж. Кабанова[8] также предлагает декриминализировать состав преступления, предусмотренный ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», и перевести указанный состав правонарушения в сферу регулирования административного права.

Думается, что такой перевод в русло административного права невозможен ввиду того, что при наступлении таких последствий, повлекших уничтожение, блокирование, модификацию либо копирование компьютерной информации, вызванных нарушениями правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, обнаруживается повышенная общественная опасность и причинение существенного вреда обществу и государству.

Одним из самых распространенных на сегодняшний день способов дистанционной дестабилизации информационно-телекоммуникационных устройств, их систем и сетей является отказ в обслуживании.

Отказ в обслуживании угрожает не самой информации, а автоматизированной системе, в которой эта информация обрабатывается. При возникновении отказа в обслуживании уполномоченные пользователи системы не могут получить своевременный доступ к необходимой информации, хотя имеют на это полное право[9].

Случаются и другие способы нарушения информационно-телекоммуникационных устройств. Так, по мнению С. В. Щеголевой, нарушение работы компьютеров может быть следствием поражения управляющей компьютерной информации, выхода из строя программного обеспечения при активизации недокументированных команд, захвата вычислительных ресурсов компьютеров и мощностей каналов связи[10].

Следует отметить, что У. В. Зинина считает сформулированную диспозицию ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ как бланкетную, т. е. требующую обращения к конкретным правилам, что затрудняет применение данной статьи в полном объеме в связи с нередким отсутствием соответствующих правил. Более того, общественная опасность этого деяния состоит не в нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации как таковых, что подтверждается анализом зарубежного законодательства, а в тех по-

следствиях, к которым такие нарушения приводят, т. е. в нарушении работы информационных систем или информационно-телекоммуникационных сетей[11].

Е. В. Красненкова предлагает конкретизировать диспозицию рассматриваемой статьи и изложить её как «нарушение правил эксплуатации компьютерных и иных автоматизированных электронных систем обработки данных, а также их сетей и систем»[12]. Такой подход представляется вполне оправданным, так как он учитывает устоявшуюся сегодня терминологию в сфере безопасности информационных технологий.

Учитывая всё вышесказанное, мы предлагаем своё видение рассматриваемой статьи, изложенной в следующей редакции:

Статья 274. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей

1. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом цифровой информации, причинившее крупный ущерб, –

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Примечания

[1] *Дворецкий М. Ю., Копырюлин А. Н.* Правоприменение ст. 274 Уголовного кодекса РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2008. – № 2. – С. 495.

[2] *Кузнецов А. П.* Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети // Правовые вопросы связи. – 2007. – № 2. – С. 25–29.

[3] *Сизов А. В.* Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. – 2007. – № 4. – С. 27–30.

[4] См.: *Лопашенко Н. А.* Уголовно-правовая и криминологическая политика государства в области высоких технологий // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – Киев: Национальная академия наук Украины, 2003. – С. 89–97.

[5] См.: *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. … канд. юрид. наук. – Владивосток, 2005. – С. 11.

[6] См.: *Зубова М. А.* Компьютерная информация как объект уголовно-правовой охраны : автореф. дис. … канд. юрид. наук. – Казань, 2008. – С. 14.

[7] *Добровольский Д. В.* Актуальные проблемы борьбы с компьютерной преступностью : автореф. дис. … канд. юрид. наук. – М., 2005. – С. 9.

[8] *Кабанова А. Ж.* Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты) : автореф. дис. … канд. юрид. наук. – Ростов-на-Дону, 2004. – С. 6.

[9] *Скляров Д. В.* Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – С.10.

[10] *Щеголева С. В.* Характеристика неправомерного доступа к компьютерной информации органов внутренних дел как противоправных действий // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 163.

[11] *Зинина У. В.* Преступления в сфере компьютерной информации в российском и зарубежном праве : автореф. дис. … канд. юрид. наук. – М., 2007. – С. 14.

[12] *Красненкова Е. В.* Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : автореф. дис. … канд. юрид. наук. – М., 2006. – С. 10.

Бегишев Ильдар Рустамович, соискатель кафедры уголовного права и процесса ЧОУ ВПО «Институт экономики, управления и права (г. Казань)». E-mail: infolaw@bk.ru

УДК 34.03:004.056.5, 34:002
ББК Х401:114, Х404.022

П. Г. Андреев

ОПТИМИЗАЦИЯ ЗАКОНОДАТЕЛЬНОГО ОБЕСПЕЧЕНИЯ СЛУЖЕБНОЙ ТАЙНЫ

В статье рассматриваются ситуация о правовой неопределенности режима служебной тайны и вопросы совершенствования законодательства в этой сфере общественных отношений.

Ключевые слова: *информационная безопасность, служебная тайна, институт тайнообразования, закон об информации*

Andreyev P. G.

ENHANCEMENT OF LEGISLATIVE SECURITY FOR OFFICIAL SECRECY

The paper provides an overview of legislative ambiguity concerning the official secrecy regime, as well as the issues of enhancing legislation in that sphere of social relations.

Keywords: *information security, official secrecy, institute of secrecy generation, information law*

В настоящее время в законодательстве, регулирующем отношения, связанные с обеспечением информационной безопасности, имеется весьма значимый пробел, касающийся защиты служебной тайны. В то же время служебная тайна широко упоминается в законодательстве (в том числе – предусматривающем юридическую ответственность за разглашение)[1].

Действовавшая до вступления в силу Федерального закона от 18.12.2006 № 231-ФЗ статья 139 ГК РФ рассматривала понятия «коммерческая тайна» и «служебная тайна» как однородные по своему значению. Данный подход не раз подвергался критике со стороны ученых, отмечавших, в частности, что такое смешение двух совершенно разнородных понятий только внесло дополнительную путаницу[2]. Отмечалось и то, что информация, находящаяся в режиме служебной тайны, может и не иметь коммерческой ценности, а конфиденциальность ее охраняется не столько в силу ее ценности, столько в силу служебных обязанностей[3], что у данной информации отсутствует гражданская оборотоспособность[4] и, как следствие – действительная или потенциальная коммерческая ценность, что основанием отсутствия свободного доступа к служебной тайне (в отличие от коммерческой) является трудовое законодательство и заключенный на его основе трудовой договор, служебные отношения[5].

В настоящее время четкого законодательного определения указанного термина не существует, а сам объект обозначается как минимум четырьмя терминами: «служебная тайна», «служебная информация», «служебная информация ограниченного распростра-

нения», «информация для служебного пользования», что также не прибавляет ясности. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»[6] определил служебную тайну как служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами. Следовательно, субъектами, осуществляющими непосредственное ограничение доступа к служебной тайне, являются органы государственной власти, вследствие чего говорить о наличии у такой информации коммерческой ценности становится проблематично. Вместе с тем, данное определение, как отмечают исследователи, противоречит нескольким федеральным законам, где служебная тайна понимается совершенно иначе. Не вносит ясности и Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»[7], относящее к служебной информации ограниченного распространения «несекретную информацию, касающуюся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью» (по сути – речь идет о выделении информации особого рода – ограниченного распространения, не относящейся ни к информации ограниченного доступа, ни, соответственно, к служебной тайне). Отсутствие четких критериев отнесения сведений к служебной информации привело к тому, что указанное Постановление уже дважды оспаривалось в Верховном Суде РФ, который определил, что право граждан на информацию данным актом нарушено не было[8].

Неопределенность правовой ситуации, связанной с определением понятия «служебная тайна», дополняет еще и текст Федерального закона «Об информации, информационных технологиях и о защите информации», в ст. 11 которого законодатель среди прочих видов тайн употребляет и наименование «служебная тайна», однако не дает ему определение.

В целях устранения системных недостатков, связанных с регулированием отношений, связанных с обеспечением безопасности информации, составляющей служебную тайну, учеными был выдвинут ряд предложений. Так, И. Ю. Мирских предложила в целях устранения споров вокруг термина «служебная тайна» заменить его термином «трудовая тайна»[9] отражающим сущность служебной тайны и основания ее возникновения. Развивая данную позицию, а также учитывая, что возможность установления обязанности неразглашения служебной тайны установлена ст. 57 ТК РФ, представляется, что термин «служебная тайна» носит многогранный характер, который в целом сводится к трудовым (служебным) обязанностм по неразглашению конфиденциальной информации, однако не исчерпывается им. В частности, не может сводиться к трудовым отношениям ситуация, когда информация, относимая к служебной тайне, находится в распоряжении органов государственной власти или органов местного самоуправления.

Следует отметить мнение И. Ю. Павлова, который, исследуя вопрос, связанный с обеспечением безопасности служебной тайны, отметил, что использование двух категорий в отношении собственной секретной информации государственных органов представляется излишним – здесь уже применяется категория «государственная тайна». Соответственно понятие служебной тайны он предлагает использовать для обозначения «не относящейся к государственной тайне, полученной государственным органом или органом местного самоуправления информации, доступ к которой ограничен в соответствии с федеральным законом в интересах иных лиц»[10]. Например, режим служебной тайны частично может применяться при защите персональных данных, находящихся в базах данных государственного органа. Здесь возникает проблема, связанная с тем, что в отношении данной информации может действовать режим личной или семейной тайны. Для решения ее целесообразно обратиться к мнению В. Н. Лопатина, который, предлагая упорядочить работу с конфиденциальной информацией в сфере государственного управления, считает необходимым отдельное урегулирование вопроса о способах изменения режимов ограниченного доступа (в том числе замены одного режима другим)[11]. Данное упорядочение требует систематизации нормативной базы, прежде всего – принятия отдельного законодательного акта, определяющего перечень сведений, составляющих служебную тайну, общих принципов правовой охраны данной информации, с последующей конкретизацией данных общих норм в отрас-

левых законах. Однако соответствующий законопроект[12], разрабатывавшийся одновременно с проектом федерального закона «О введении в действие части четвертой Гражданского кодекса Российской Федерации», не получил нормативного воплощения. Фактически это может свидетельствовать о неполноте урегулирования вопросов, связанных с обеспечением информационной безопасности с применением норм гражданского законодательства.

Упомянутые выше правовые коллизии и пробелы, по нашему мнению, могут свидетельствовать о практически полном отсутствии системного подхода законодателя к решению проблемы урегулирования проблемы обеспечения деятельности, связанной с использованием служебной тайны. Оптимизация законодательного обеспечения данного вида деятельности видится в систематизации норм, входящих в единый комплексный правовой институт тайнообразования, в рамках единого законодательного акта, посвященного вопросам обеспечения информационной безопасности, приведение норм, регулирующих данную деятельности и содержащихся в отраслевых законодательных актах, в соответствие с данным законом.

Примечания

[1] Помимо УК РФ и КоАП РФ, термин «служебная тайна» содержится в Федеральном законе от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» // СЗ РФ. 2003. № 50. Ст. 4859; Федеральном законе от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности» // СЗ РФ. 2001. № 33 (часть I). Ст. 3430; Федеральном законе от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» // СЗ РФ. 1996. № 17. Ст. 1918 и мн. др.

[2] Информационное право: актуальные проблемы теории и практики: колл. монография / под. общ. ред. И. Л. Бачило. – М.: Издательство Юрайт, 2009. – С. 469.

[3] Комментарий к части первой Гражданского кодекса / под ред. О. Н. Садикова. М.: 1998. – С. 154.

[4] *Отнюкова Г. Д.* Коммерческая тайна // Закон. – 1998. – № 2. – С. 56.

[5] *Дозорцев В. А.* Интеллектуальные права: Понятие. Система. Задачи кодификации : Сборник статей. М., 2005. – С. 132.

[6] СЗ РФ. 10.03.1997. № 10. Ст. 1127.

[7] СЗ РФ, 2005, № 30 (часть 2). Ст. 3165.

[8] Решение Верховного Суда РФ от 22.12.2005 № ГКПИ05-1426 // БВС РФ. 2006. № 12; Определение Кассационной коллегии Верховного Суда РФ от 07.03.2006 № КАС06-45 // Там же; Решение Верховного Суда РФ от 12.02.2007 № ГКПИ06-1417; Определение Кассационной коллегии Верховного Суда РФ от 17.05.2007 № КАС07-164 [Электронный ресурс]. – Электрон. дан. – Институт Развития Свободы Информации. – Режим доступа: http//www.svobodainfo.org/info/page/rus?tid=633200066, свободный.

[9] *Мирских И. Ю.* Коммерческая тайна как вид конфиденциальной информации: Трудоправовой и цивилистический аспекты : дис. ... кандидата юридических наук. Пермь, 2005. С. 51.

[10] *Павлов И. Ю.* Правовое обеспечение доступа к официальной информации. Дис. … канд. юрид. наук. – М., 2008. – С. 12-13, 79-81.

[11] См.: *Лопатин В. Н.* Правовая охрана и защита служебной тайны // Государство и право. – 2000. – № 6. – С. 85.

[12] Проект федерального закона «О служебной тайне» № 124871-4 // СПС «КонсультантПлюс».

Андреев П. Г., соискатель кафедры информационного права Уральской государственной юридической академии. E-mail: andreevpg84@mail.ru

УДК 347.23.03
ББК Х404.022, Х401.114, Х404.3

А. В. Минбалеев

ПРОБЛЕМНЫЕ ВОПРОСЫ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

В статье рассматриваются проблемы применения правовых норм режима коммерческой тайны и вопросы совершенствования законодательства в этой сфере общественных отношений.

Ключевые слова: *объекты интеллектуальной собственности, коммерческая тайна, секрет производства (ноу-хау), Федеральный закон «О коммерческой тайне»*

A. V. Minbaleev

PROBLEMATIC ISSUES OF BUSINESS SECRET REGIME

The article covers the problems of application of legal provisions for business secret regime and problems of improvement of legislation in this area of public relations.

Keywords: *intellectual property, business secret, production secret (know-how), Federal Law «On Business Secret»*

С вступлением в силу с 1 января 2008 года части четвертой Гражданского кодекса Российской Федерации (далее – ГК РФ) в очередной раз изменилось законодательство о коммерческой тайне, что связано с признанием секретов производства (ноу-хау) в качестве объекта интеллектуальной собственности, а не информации. В соответствии со ст. 1465 ГК РФ под секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. Обладателю секрета производства принадлежит исключительное право его использования любым не противоречащим закону способом (исключительное право на секрет производства), в том числе при изготовлении изделий и реализации экономических и организационных решений. Таким образом, в качестве секретов производства (ноу-хау) могут выступать практически любые сведения, в том числе и не имеющие никакого отношения к производству, например, сведения об особенностях управления деятельностью организации или учреждения, об особенностях организации системы охраны и т. п. И все сведения, которые ранее охранялись как сведения, составляющие коммерческую тайну, сегодня могут быть признаны секретами производства и охраняться в качестве объекта интеллектуальной собственности.

Сегодня мы уже можем говорить об определенной практике применения новых норм о секретах производства (ноу-хау) и пробле-

мах, возникающих при защите режима коммерческой тайны.

Одним из обязательных условий приобретения теми или иными сведениями правового режима секретов производства (ноу-хау) является введение обладателем в отношении них режима коммерческой тайны. По новому законодательству в целом сохраняются особенности данного режима, связанные с рядом обязательных и рекомендуемых мер, которые должен осуществлять обладатель сведений, в отношении которых планируется засекречивание. Согласно Федеральному закону «О коммерческой тайне»[1] к числу обязательных мер, которые должен применять обладатель информации, желающий установить в отношении нее режим секретов производства (ноу-хау), относятся правовые (регулирование отношений по использованию секретов производства работниками и контрагентами, закрепление перечня секретов производства) и организационные меры (определение перечня, ограничение доступа, учет лиц, получивших доступ, нанесение на материальные носители (документы) грифа). Также предусматривается возможность применять при необходимости средства и методы технической защиты конфиденциальности, а также другие, не противоречащие законодательству Российской Федерации меры, например, оценку секретов производства.

В то же время законодатель включил ряд отдельных положений, которые сегодня приводят к ряду проблем. В частности, в ст. 1467 ГК РФ установлено положение о том, что исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. При этом ни в ГК РФ, ни в Федеральном законе «О коммерческой тайне» не предусматриваются основания для утраты конфиденциальности. В результате возникает вопрос о том, является ли раскрытие секретов производства одному или нескольким лицам основанием для признания утраты конфиденциальности?

По ранее действующему законодательству сведения, составляющие коммерческую тайну, в некоторых случаях не утрачивали правовую охрану в случаях их разглашения. Единственным условием при этом, которое должен был выполнить обладатель сведений, составляющих коммерческую тайну, – это принятие достаточных мер для восстановления их конфиденциальности и продолжение извлечения прибыли от использования этих сведений в силу неизвестности их третьим лицам и (или) закрепленного в договоре соглашения о сохранении конфиденциальности сведений лицом, их получившим.

Такое положение вещей было вполне допустимо ввиду особого правового режима информации как объекта гражданских прав, поскольку правовая охрана информации устанавливалась преимущественно в силу наличия определенного интереса обладателя к принадлежащей ему информации. И именно обладатель информации самостоятельно определял многие условия охраноспособности той или иной информации. Сегодня, когда секреты производства рассматриваются в качестве объекта интеллектуальной собственности, охрана которого напрямую зависит от условия сохранения конфиденциальности сведений, составляющих содержание секретов производства, любое разглашение (даже единичное) уже может быть основанием для прекращения действия исключительного права. Сегодня правоприменитель уже сталкивается с проблемой признания факта прекращения действия исключительного права на секреты производства. В связи с этим можно порекомендовать обладателям информации, устанавливающим режим коммерческой тайны, а также правообладателям охраняемых секретов производства в правовых актах организаций, закрепляющих порядок защиты коммерческой тайны, включать условие следующего содержания: «В случае разглашения секретов производства третьим лицам правообладатель может принять решение об отсутствии факта утраты конфиденциальности, если предприняты достаточные меры для предотвращения дальнейшего распространения данной информации и соблюдаются условия конфиденциальности охраняемой информации». Данное положение может признаваться основанием продолжения действия режима коммерческой тайны в случае его нарушения. При этом необходимо учитывать, что в законодательстве регулируется ряд случаев, при которых утрата конфиденциальности должна признаваться абсолютной. Например, в случае размещения информации в информационно-телекоммуникационных сетях общего пользования. В данном случае, если использовать по аналогии ст. п. 11 ч. 2 ст. 1270 ГК РФ (доведение до всеобщего сведения), происходит доведение до всеобщего сведе-

ния таким образом, что любое лицо может получить доступ к информации из любого места и любое время. В этом случае применение каких-либо оговорок в локальных актах или договорах не повлияет на сохранение режима коммерческой тайны и у правообладателя исключительное право на секреты производства прекратит существование.

Во всех случаях утраты конфиденциальности необходимо осознавать, что режим конфиденциальности утрачивается прежде всего по отношению к субъектам, которые получили доступ к ней. Для большинства других же этот режим может существовать. Более того, поскольку ГК РФ допускает возможность одновременной охраны одних и тех же ноу-хау разными субъектами, можно предположить, что разглашение (утрата конфиденциальности) в отношении определенных лиц может быть оформлена правообладателем как передача секретов производства (возможна устная договоренность о дальнейшей охране полученных сведений несколькими субъектами).

Из части четвертой ГК РФ не совсем ясно, можно ли устанавливать режим коммерческой тайны и охранять в качестве секрета производства ту или иную информацию повторно, если она ранее охранялась в таком режиме, а впоследствии режим коммерческой тайны был прекращен. Полагаем, что на данный вопрос следует ответить положительно при условии, что информация отвечает всем критериям охраноспособности в качестве секретов производства.

Другим спорным вопросом является сохранение секретов производства, созданных или полученных работниками в ходе осуществления трудовой функции, после прекращения трудовых отношений. Согласно ГК РФ, гражданин, которому в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства (ч. 2 ст. 1470). При этом доказать факт разглашения отдельных сведений конкретным работником является весьма непростой задачей, особенно при размещении сведений в информационно-телекоммуникационных сетях, в том числе в сети Интернет. В связи с этим сегодня первостепенной задачей при защите конфиденциальности оказывается человеческий фактор. Именно учет последнего должен ставиться в качестве приоритетного любым предпринимателем при защите секретов производства (ноу-хау).

Одним из наиболее проблемных вопросов сегодня является необходимость развития законодательства о коммерческой тайне и секретах производства (ноу-хау). В частности, в проекте изменений в Гражданский кодекс Российской Федерации и в ФЗ «О коммерческой тайне» предлагается следующее.

Секретом производства (ноу-хау) предлагается понимать сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к этим сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает *разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны* (выделено мной. – *А. М.*). При этом устанавливается также, что секретом производства не могут быть признаны сведения, обязательность раскрытия которых или недопустимость ограничения доступа к которым установлены законом или иным правовым актом.

В ФЗ «О коммерческой тайне» предлагается вернуть категорию «информация, составляющая коммерческую тайну», и понимать под ней сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. Предметом ФЗ «О коммерческой тайне» предлагается рассматривать отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерче-

скую ценность в силу неизвестности ее третьим лицам.

Таким образом, законодатель предлагает рассматривать различные виды информации, составляющей коммерческую тайну, – секреты производства (ноу-хау), а также иную информацию, составляющую коммерческую тайну. Информация, составляющая коммерческую тайну, при этом может быть объектом интеллектуальной собственности, а может и не быть таковым (например, сведения о скидках клиентам). Секреты производства (ноу-хау) не связаны с режимом коммерческой тайны. Их правообладатель может предпринимать иные разумные меры для соблюдения их конфиденциальности.

В ФЗ «О коммерческой тайне» предлагается также установить права обладателя информации, составляющей коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Также предлагается «вернуть» нормы об охране конфиденциальности информации в рамках трудовых отношений, в частности:

– предлагается, что в целях охраны конфиденциальности информации работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях, в том числе после прекращения действия трудового договора, в течение всего срока действия режима коммерческой тайны;

3) возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну;

– предлагается закрепить, что работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к такой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если информация разглашена в течение срока действия режима коммерческой тайны. Причиненные работником или лицом, прекратившим трудовые отношения с работодателем, убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанности по обеспечению режима коммерческой тайны;

– предлагается закрепить, что трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответ-

ственность за обеспечение охраны ее конфиденциальности. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством;

– предлагается закрепить, что работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Анализ вышеуказанных новелл свидетельствует о том, что законодатель учел опыт негативного рассмотрения любых сведений, охраняемых в режиме коммерческой тайны, в качестве объекта интеллектуальной собственности. В то же время также сегодня очень сложно сказать, насколько сможет российский бизнес 4-й раз за последние двадцать лет перестроиться в вопросах защиты коммерческой тайны. Подобная неопределенность законодателя, его «поиски» нужного решения делают данный институт для многих непонятным и формируют отторжение. Полагаем, что в целом верная концепция изменений все же не учитывает реализации на практике механизма разграничения секретов производства (ноу-хау) и информации, составляющей коммерческую тайну, что вызовет очень много вопросов и проблем.

Примечания

[1] ФЗ РФ «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ // Собрание законодательства РФ. – 2004. – № 32. – Ст. 3283.

Минбалеев А. В., к.ю.н., доцент кафедры конституционного и административного права ФГБОУ ВПО «Южно-Уральский государственный университет (национальный исследовательский университет)». E-mail: alexmin@bk.ru

УДК 347.23 + +342 739
ББК Х404.01

Дубровин О.В.

ВИДЫ ПУБЛИЧНОЙ СОБСТВЕННОСТИ

В статье в конституционно-правовом ракурсе рассматриваются виды и специфика публичной собственности.

Ключевые слова: *публичная собственность, виды собственности.*

O.V. Dubrovin

TYPES OF PUBLIC PROPERTY

The article in the constitutional-legal perspective discusses the types and specific of public property.

Keywords: *public property, the types of property.*

Одну из классификаций публичной собственности можно провести по такому критерию как субъект права.

Согласно п.2. ст. 8 Конституции Российской Федерации, в Российской Федерации признаются и защищаются равным образом частная, государственная, муниципальная и иные формы собственности.

Как было сказано ранее, действующее законодательство понятием публичная собственность объединяет государственную (федеральную собственность, собственность субъектов Федерации) и муниципальную собственность.

Согласно ст. 215 Гражданского кодекса Российской Федерации[1], муниципальной собственностью является имущество, принадлежащее на праве собственности городским и сельским поселениям, а также другим муниципальным образованиям.

К муниципальным образованиям в соответствии с Федеральным законом от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» относятся городские или сельские поселения, муниципальный район, городской округ либо внутригородская территория города федерального значения[2].

Конституция России в ст. 130 и Гражданский кодекс Российской Федерации в ст. 212, определили, что муниципальная собственность является обособленной формой собственности, но поскольку она, как федеральная собственность и как собственность субъектов Федерации, обеспечивает общественные интересы, ее следует рассматривать в качестве одного из вариантов публичной собственности.

Можно согласиться с мнением Е.Н. Абрамовой, которая считает, что право муниципальной собственности по характеру, природе, принципам правового регулирования, близко к праву государственной собственно-

сти, но при всем том, право муниципальной собственности имеет принципиальное отличие:

- его субъект не имеет суверенитета;

- его объектом не является имущество, изъятое из оборота;

- только в силу прямого указания закона, имущество, ограниченное в обороте, может быть объектом муниципальной собственности;

- принципы определения земли и других природных ресурсов к объектам муниципальной собственности, как в случае с частной собственностью и противопоставляются законодателем, принципам отнесения к государственной собственности[3].

В частности, п. 2 ст. 214 Гражданского кодекса Российской Федерации земля и другие природные ресурсы являются государственной собственностью, если не находятся в собственности частной либо муниципальной. При этом в научной литературе единства в вопросе толкования данной нормы нет.

Так, В.П. Мозолин данный принцип называет остаточным и утверждает, что он противоречит основным направлениям в развитии законодательства России. В том числе, он вообще не распространяется на недра и многие другие природные ресурсы, а также отдельные категории земель[4].

Существует и противоположенное мнение, например, В.В. Чубарова, с которым можно согласиться, в соответствии с ним в норме определено отнесение земли и других природных ресурсов к объектам государственной собственности, в случае если отсутствуют какие-либо доказательства принадлежности их к собственности граждан, юридических лиц или муниципальных образований[5].

Политика нашего государства в отношении муниципальной собственности определяется «Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года»[6], в соответствии с которой для повышения эффективности политико-правовых институтов и обеспечения исполнения законодательства необходимо решение следующих задач:

- повышение эффективности управления государственным имуществом, включая последовательное сокращение использования института хозяйственного ведения;

- сокращение объема имущества, находящегося в государственной и муниципальной собственности, с учетом задач обеспечения полномочий органов государственной власти и органов местного самоуправления.

Имущество, находящееся в муниципальной собственности в соответствии с п. 3. ст. 215 Гражданского кодекса Российской Федерации, состоит из двух частей:

имущество, закрепленное за муниципальными предприятиями и учреждениями во владение, пользование и распоряжение на праве хозяйственного ведения и оперативного управления;

муниципальная казна - средства местного бюджета и иное муниципальное имущество, не закрепленное за муниципальными предприятиями и учреждениями.

Одним из оснований разделения муниципального имущества, по нашему мнению, можно считать деление имущественной ответственности между муниципальным образованием и созданными им юридическими лицами по их долгам.

Федеральным законом от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», именуемом далее по тексту «Федеральный закон № 131-ФЗ» в ст. 50 установлен перечень имущества, которое может находиться в собственности муниципальных образований

В соответствии с п. 5 ст. 50 Федерального закона № 131-ФЗ, в случаях возникновения у муниципальных образований права собственности на имущество, не предназначенное для осуществления отдельных государственных полномочий, переданных органам местного самоуправления, для обеспечения деятельности органов местного самоуправления и должностных лиц местного самоуправления, муниципальных служащих, работников муниципальных предприятий и учреждений либо не относящееся к видам имущества, предназначенным для решения вопросов местного значения, указанное имущество подлежит перепрофилированию (изменению целевого назначения имущества) либо отчуждению. Порядок и сроки отчуждения такого имущества устанавливаются федеральным законом.

Хотя названная норма Федерального закона №131-ФЗ и предусматривает наличие федерального закона регламентирующего порядок и сроки отчуждения имущества, но на сегодняшний день такой закон не принят, что значительно затрудняет ее применение на практике.

Здесь же следует отметить, что ст. 50 Федерального закона №131-ФЗ не препятствует муниципальным образованиям использовать установленные законом способы привлечения денежных средств и иного имущества для формирования доходов местных бюджетов, в том числе иметь имущественные права и получать дотации из иных бюджетов, для решения вопросов местного значения, а также получать субвенции на осуществление органами местного самоуправления отдельных государственных полномочий, а потому не может рассматриваться как формирующая закрытый перечень видов муниципального имущества, не допускающая наличия в муниципальной собственности иного имущества, имеющего такое же целевое предназначение, что и имущество, названное в данной статье, и как нарушающая конституционные правомочия муниципальных образований и гарантии муниципальной собственности. Об этом было прямо указано в п.4.2 Определения Конституционного Суда РФ от 2 ноября 2006 г. № 540-О [7].

Таким образом, сложившаяся правоприменительная практика, по сути закрепившая отказ от установления закрытого перечня имущества, которое может находиться в муниципальной собственности, противоречит концепция Федерального закона № 131-ФЗ и долгосрочного социально-экономического развития Российской Федерации.

По нашему мнению, объекты, находящиеся в муниципальной собственности должны служить интересам социально-экономического развития муниципального образования, получения налоговых доходов в бюджет муниципального образования, развития экономического потенциала территории, с учетом различия вопросов местного значения отнесенных к компетенции муниципальных образований. Полагаем, что перечень объектов муниципального имущества можно привести в соответствие с вопросами, отнесенными к компетенции муниципального образования, основываясь на принципе его эффективного использования. Кроме того, органы местного самоуправления вправе самостоятельно решать, какие объекты муниципальной собственности требуются им для решения соответствующих вопросов местного значения, в пределах установленного перечня.

Субъектом права федеральной собственности является Российская Федерация. Перечень объектов федеральной собственности законодательством России не ограничен.

Состав субъектов Российской Федерации определен ст. 65 Конституции, в него входят республики, края, области, города федерального значения, автономная область, автономные округа.

В научной литературе отмечается, что субъекты России не обладают суверенитетом, а именно он является один из неотъемлемых свойств государства. Кроме того, суверенитет лежит в основе таких общепризнанных принципов международного права, как суверенное равенство государств, взаимное уважение государственного суверенитета, невмешательство государств во внутренние дела друг друга и др.

Следовательно, называть собственность субъектов Российской Федерации государственной не точно. Так для более правильного определения термина, Е.В. Кулешов Е.В. предлагает собственность субъектов Российской Федерации называть региональной собственностью[8].

В перечень объектов собственности субъектов Российской Федерации не могут входить объекты, находящиеся в исключительной федеральной собственности Российской Федерации.

Действующим законодательством РФ установлены такие виды объектов, которые могут находиться только в государственной или муниципальной собственности, а именно **ст. 27** Земельного кодекса РФ, **ст. 5** Федерального закона от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии»[9], **ст. 5** Федерального закона от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия»[10] и некоторых других законодательных актах специального характера, установлен перечень объектов, которые могут находиться исключительно в собственности государства или муниципальных образований.

Основанием для отнесения объектов к публичной собственности явилось принятое 27 декабря 1991 г. Постановление Верховного Совета РФ № 3020-1 «О разграничении государственной собственности в Российской Федерации на федеральную собственность, государственную собственность республик в составе Российской Федерации, краев, областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга»[11]. В приложениях № 1, 2, 2 к постановлению были указаны объекты, относящиеся исключи-

тельно к федеральной собственности; к федеральной собственности, которые могут передаваться в государственную собственность республик в составе Российской Федерации, краев, областей, автономной области, автономных округов, городов Москвы и Санкт-Петербурга, а так же к муниципальной собственности.

Постановлением Конституционного Суда РФ от 10 сентября 1993 г. № 15-П пункты 2 и 3 раздела IV настоящего приложения в части отнесения к объектам исключительно федеральной собственности предприятий топливно-энергетического комплекса и предприятий и объектов электроэнергетики признаны не соответствующими частям второй и третьей статьи 11-1, пункту «г» части первой статьи 84-11 Конституции РФ в редакции от 21 апреля 1992 г. и Федеративному договору.

В последствие эти объекты были приватизированы, кроме того, были приватизированы, как известно и другие объекты, вошедшие в перечень, такие как предприятия железнодорожного, воздушного транспорта и др.

Хотя Постановление Верховного Совета РФ № 3020-1 и перечисляет объекты исключительной публичной собственности, но реально не отражает перечень, поскольку его принятие было мерой по разграничению единого фонда государственного имущества, в том числе и для целей его возможной приватизации), а не установить ограничение оборотоспособности перечисленных объектов публичной собственности.

В настоящее время одной из проблем является формирование единообразного механизма разграничения различных видов публичной собственности.

Так, например, перечень полномочий автономных округов входящих в состав края или области оказывается сокращенным.

Сам термин «вхождение» стал предметом толкования Конституционного Суда РФ. Постановлением Конституционного Суда РФ от 14 июля 1997 г. № 12-П установлено, что вхождение автономного округа в состав края, области и по смыслу ч. 4 ст. 66 Конституции РФ означает такое конституционно-правовое состояние, при котором автономный округ, будучи равноправным субъектом Федерации, одновременно составляет часть другого субъекта Федерации - края или области[12].

Как отметил Конституционный Суд РФ в Постановлении от 11 мая 1993 г. № 9-П «По делу о проверке конституционности Закона Российской Федерации от 17 июня 1992 года «О непосредственном вхождении Чукотского автономного округа в состав Российской Федерации», нахождение автономного округа в крае или области не означает по действующему законодательству поглощение его территории, являющейся составной частью территории Российской Федерации. Взаимоотношения указанных субъектов Федерации при этом определяются законами Российской Федерации, актами органов государственной власти края (области) и автономного округа и договорами между ними[13].

Некоторые вопросы возникают при разграничении собственности, относящейся к совместному ведению Российской Федерации и ее субъектов.

Статья 72 Конституции РФ определяет исчерпывающий перечень, в который в том числе входят вопросы владения, пользования и распоряжения землей, недрами, водными и другими природными ресурсами, природопользование, разграничение государственной собственности.

Кроме того, ст. 76 Конституции определяет, что по предметам совместного ведения издаются федеральные законы и принимаемые в соответствии с ними законы и иные нормативные правовые акты субъектов Федерации; законы и иные нормативные правовые акты субъектов Федерации не могут противоречить федеральным законам, принятым по предметам ведения РФ, а также по предметам совместного ведения.

Таким образом, использовав в принципе традиционное деление собственности на частную и публичную, Конституция РФ подразделяет публичную собственность на государственную и муниципальную. Тем самым, во-первых, подчеркивается самостоятельность местного самоуправления, во-вторых, такая классификация позволяет выделять федеральную собственность и собственность субъектов Российской Федерации, что предопределяет особенности правового положения различных объектов, находящихся соответственно в федеральной собственности или собственности субъектов РФ.

Примечания

[1] Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ. СЗ РФ. 1994 г. № 32 ст. 3301.

[2] Федеральный закон от 6 октября 2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» СЗ. РФ. 2003 г. № 40 ст. 3822.

[3] Гражданское право: учебник: в 3 т. Т. 1. / Е.Н. Абрамова, Н.Н. Аверченко, Ю.В. Байгушева [и др.]; под ред. А.П. Сергеева. - М.: «РГ Пресс», 2010.

[4] Комментарий к Гражданскому кодексу Российской Федерации, части первой / под ред. Т.Е. Абовой, А.Ю. Кабалкина. М., 2004. С. 603

[5] Комментарий к Гражданскому кодексу Российской Федерации, части первой / под ред. О.Н. Садикова. М., 2005. С. 568

[6] Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утверждена распоряжением Правительства РФ от 17 ноября 2008 г. // СЗ РФ. - 2008.- №47.- Ст. 5489.

[7] Определение Конституционного Суда РФ от 2 ноября 2006 г. № 540-О. «По запросу Правительства Самарской области о проверке конституционности статьи 1, частей 6 и 8 статьи 2 Федерального закона «О внесении изменений и дополнений в Федеральный закон «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации» и статьи 50 Федерального закона «Об общих принципах организации местного самоуправления в Российской Федерации» // Вестник Конституционного Суда Российской Федерации. - 2007. -№ 2.

[8] Кулешов Е.В. Государственная собственность субъектов Российской Федерации как основа их экономической самостоятельности // Государство и право. 2005. № 6. С. 41.

[9] Федеральный закон от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии». СЗ РФ. 1995. № 48. Ст. 4552.

[10] Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия». СЗ РФ. 1997. № 18. Ст. 2105.

[11] Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР от 16 января 1992 г., № 3, ст. 89

[12] Постановление Конституционного Суда РФ от 14 июля 1997 г. № 12-П «По делу о толковании содержащегося в части 4 статьи 66 Конституции Российской Федерации положения о вхождении автономного округа в состав края, области» Вестник Конституционного Суда Российской Федерации. - 1997. - № 5.

[13] Постановление Конституционного Суда РФ от 11 мая 1993 г. № 9-П «По делу о проверке конституционности Закона Российской Федерации от 17 июня 1992 года «О непосредственном вхождении Чукотского автономного округа в состав Российской Федерации». Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. - 1993. - № 28. - Ст. 1083.

Дубровин О. В., соискатель кафедры конституционного и административного права Южно-Уральского государственного университета, помощник члена Совета Федерации Федерального Собрания Российской Федерации Р.У. Гаттарова по работе в Челябинской области Правительство Челябинской области. E-mail: dov1974@mail.ru

УДК 65.012.810;004.056;004.7
ББК 32.973-018.2

Д. И. Дик, В. М. Солодовников

АНАЛИЗ БЕЗОПАСНОСТИ СЕРВИСА ПРИЕМА ПЛАТЕЖЕЙ ROBOKASSA

В настоящее время большой популярностью пользуются сервисы, предоставляющие он-лайн продавцами услуги получения платежей. В статье проводится анализ безопасности одного из таких сервисов – сервиса ROBOKASSA.

Ключевые слова: *сервис приема платежей, безопасность.*

D. Dik, V. Solodovnikov

ROBOKASSA SERVICE SECURITY ANALYSIS

ROBOKASSA — is the service, that allows sellers (on-line stores) to receive payments by plastic cards, in every e-currency, using mobile commerce services, E-invoicing via leading banks in Russia, through ATMs, through instant payment terminals, through Contact remittances, and with the iPhone application. The article present analysis of security of this service.

Keywords: *payment service, security*

В настоящее время с развитием систем электронной торговли нашли широкое применение сервисы, позволяющие он-лайн продавцам принимать платежи от покупателей. Одним из таких сервисов является сервис ROBOKASSA[1].

Согласно описанию разработчиков «сервис ROBOKASSA построен таким образом, что, в отличие от случая "подключения" непосредственно к серверу платежной системы, отпадает необходимость в усиленной защите данных в процессе обмена. Для интеграции кассы в сайт магазина или сайт, предоставляющий платный доступ к контенту, нет необходимости в установлении исходящих SSL-соединений, подключении дополнительных компонент на сервере Клиента и т. п. В этом заключено главное преимущество применения системы ROBOKASSA»[2].

Действительно, использование сервиса ROBOKASSA избавляет продавца от необходимости самостоятельной поддержки системы получения средств от покупателя.

Однако остается открытым вопрос, действительно ли в полной мере обеспечивается защищенность системы оплаты.

Принцип работы сервиса ROBOKASSA заключается в следующем.

1) После выбора покупателем в он-лайн магазине товара магазин подсчитывает сумму заказа и посылает запрос к серверу, на котором расположен сервис ROBOKASSA. Сервис возвращает серверу он-лайн магазина код формы выбора валюты оплаты или кнопки оплаты, который встраивается на страницу он-лайн магазина.

Данный шаг может быть опущен. В этом случае код запроса к сервису ROBOKASSA

размещается на странице оплаты сайта продавца.

2) Покупатель выбирает на сайте Клиента или на странице Сервиса ROBOKASSA валюту платежа и приступает к платежу, нажав на кнопку оплаты.

3) После завершения операции в зависимости от ее исхода Покупатель перенаправляется на страницу исполненного платежа (в случае если он осуществил оплату), либо на страницу неисполненного (если он отказался от оплаты). После оплаты сервис отправляет сообщение магазину на указанный при регистрации URL адрес, передавая ему параметры совершенного платежа.

Рассмотрим подробнее указанные шаги.

На первом шаге, как уже было сказано, существуют две возможности:

а) На страницу магазина внедряется JScript-код следующего вида:

```
<script language='javascript' type='text/
javascript' src='https://merchant.
roboxchange.com/Handler/
MrchSumPreview.
ashx?MrchLogin=sMerchantLogin&
OutSum=nOutSum&
InvId=nInvId&
Desc=sInvDesc&
SignatureValue=sSignatureValue
IncCurrLabel=sIncCurrLabel&
Culture=sCulture&
Encoding=sEncoding
[&shpa=yyy&shpb=xxx…] – пользовательские параметры, начинающиеся с SHP в сумме до 2048 знаков
'></script>
```

Анализ существующих магазинов показал, что вместо адреса https://merchant.roboxchange.com/Handler/MrchSumPreview.ashx может использоваться адрес http://www.roboxchange.com/mrh_summpreview.asp, использующий незащищенное соединение.

Результатом выполнения скрипта является внедрение на страницу формы выбора способа оплаты;

б) На странице магазина создается ссылка на сервис оплаты в виде:

```
https://merchant.roboxchange.com/Index.
aspx?
MrchLogin=sMerchantLogin&
OutSum=nOutSum&
InvId=nInvId&
Desc=sInvDesc&
SignatureValue=sSignatureValue
IncCurrLabel=sIncCurrLabel&
Culture=sCulture&
Encoding=sEncoding
[&shpa=yyy&shpb=xxx…] – пользовательские параметры начинающиеся с SHP в сумме до 2048 знаков,
```

где:

sMerchantLogin – логин магазина на сервисе (обязательный параметр);

nOutSum – требуемая к получению сумма (обязательный параметр);

nInvId – номер счета в магазине (должен быть уникальным для магазина). Если содержит пустое значение, вовсе не указан, либо равен «0», то при создании операции ей будет автоматически присвоен уникальный номер счета;

sInvDesc – описание покупки, можно использовать только символы английского или русского алфавита, цифры и знаки препинания. Максимальная длина 100 символов;

sSignatureValue – контрольная сумма MD5 (обязательный параметр). Формируется по строке, содержащей следующие параметры, разделенные ':', с добавлением sMerchantPass1 (пароль, используемый интерфейсом инициализации оплаты) – sMerchantLogin:nOutSum: nInvId:sMerchantPass1[:пользовательские параметры, в отсортированном алфавитном порядке]. При инициализации оплаты вы можете передать дополнительные параметры, которые необходимы для работы вашего магазина. Переданные дополнительные параметры будут возвращены магазину на URL адреса Result Url, Success Url и Fail Url. Наименование дополнительных параметров должно начинаться с "SHP" в любом регистре. Например: Shp_item, SHP_1, ShpEmail, shp_oplata, ShpClientId и т. д. При инициализации оплаты каждый из передаваемых дополнительных параметров должен быть включён в подсчёт контрольной суммы (MD5). Например, если переданы пользовательские параметры shpb=xxx и shpa=yyy, то подпись формируется из строки: sMerchantLogin:nOutSum:nInvId:sMerchantPass1:shpa=yyy:shpb=xxx;

sIncCurrLabel – предлагаемая валюта платежа. Пользователь может изменить ее в процессе оплаты;

sCulture – опционально, язык общения с клиентом. Значения: en, ru;

sEncoding – кодировка, в которой возвращается HTML-код кассы. По умолчанию: windows-1251.

На третьем шаге в случае успешного про-

ведения оплаты сервис ROBOKASSA посылает магазину оповещение об оплате на адрес Result URL, задаваемый при регистрации, метод GET/POST/Email с указанием следующих параметров:

OutSum=nOutSum&
InvId=nInvId&
SignatureValue=sSignatureValue
[&пользовательские_параметры],
где:

nOutSum – полученная сумма. Сумма будет передана в той валюте, которая была указана при регистрации магазина;

nInvId – номер счета в магазине;

sSignatureValue – контрольная сумма MD5. Формируется по строке, содержащей некоторые параметры, разделенные ':', с добавлением sMerchantPass2 (пароль, используемый интерфейсом оповещения о платеже) – nOutSum:nInvId:sMerchantPass2[:пользовательские параметры в отсортированном порядке]. К примеру, если при инициализации операции были переданы пользовательские параметры shpb=xxx и shpa=yyy, то подпись формируется из строки ...:sMerchantPass2:shpa=yyy:shpb=xxx.

Если в настройках в качестве метода отсылки данных был выбран E-mail, то в случае успешного проведения оплаты робот системы отправит сообщение на e-mail, указанный в качестве Result URL, с указанием параметров, указанных выше.

Скрипт, находящийся по Result URL, должен проверить правильность контрольной суммы и соответствия суммы платежа ожидаемой сумме.

Данный запрос производится после получения денег, однако до того, как пользователь сможет перейти на Success URL. Перед скриптом магазина, расположенным по Success, URL обязательно отрабатывает скрипт запроса к Result URL.

Факт успешности сообщения магазину об исполнении операции определяется по результату, возвращаемому системе. Результат должен содержать «OKnMerchantInvId», т. е. для счета #5 должен быть возвращен текст «OK5».

После успешного исполнения платежа Покупатель перенаправляется по адресу Success URL. При этом передаются следующие параметры («чек» об оплате):

OutSum=nOutSum&
InvId=nInvId&
SignatureValue=sSignatureValue&
Culture=sCulture
[&пользовательские_параметры].

Схема вычисления контрольной суммы идентична схеме вычисления контрольной суммы, передаваемой на адрес Result URL.

Переход пользователя по данному адресу с корректными параметрами (соответствия кода MD5) означает, что платеж по реквизитам продавца выполнен успешно. Сервис несет финансовую ответственность перед продавцом в соответствии с соглашением за достоверность такого подтверждения.

Однако для дополнительной защиты рекомендуется, чтобы факт оплаты платежа проверялся скриптом, исполняемым при переходе на Result URL, или путем запроса XML-интерфейса о результате данной платежной операции, и только при реальном наличии счета с номером nMerchantInvId в БД магазина.

В случае отказа от исполнения платежа покупатель перенаправляется по данному адресу Fail URL. Для того, чтобы продавец мог разблокировать заказанный товар на складе при отказе от его оплаты методом, выбранным при регистрации, будут переданы параметры:

OutSum=nOutSum&
InvId=nInvId&
SignatureValue=sSignatureValue&
Culture=sCulture
[&пользовательские_параметры].

Схема вычисления контрольной суммы идентична схеме вычисления контрольной суммы, передаваемой на адрес Result URL.

Переход пользователя по данному адресу, вообще говоря, не означает окончательного отказа Покупателя от оплаты, нажав кнопку «Back» в браузере он может вернуться на страницы ROBOKASSA. Поэтому в случае блокировки товара на складе под заказ для его разблокировки желательно проверять факт отказа от платежа запросом запроса XML-интерфейса о результате данной платежной операции, используя в запросе номер счета nMerchantInvId, имеющийся в БД магазина (Продавца).

Очевидно, что данная система оплаты, как и другие системы Web оплаты, является слабо защищенной от использования вредоносного программного обеспечения типа «троянский конь».

Для защиты целостности ссылки на оплату и извещений об оплате используется код аутентичности сообщения, построенный на основе хеш функции MD5[3] и известных толь-

ко магазину и сервису пары паролей. Стойкость кода аутентичности сообщений определяется исключительно надежностью пароля. В настоящий момент существует значительное количество программ для атаки на MD5 хеш путем перебора значений. Использование таких программ для атаки на систему ROBOKASSA требует лишь незначительной их модификации. Таким образом, неудачно выбранные владельцем магазина пароли ставят систему оплаты под угрозу.

Для защиты от несанкционированного доступа к платежным реквизитам путем перехвата сетевого трафика используется протокол SSL.

Этот же протокол предположительно должен обеспечивать защиту от атак типа «человек посередине».

К сожалению, защищенность от данных атак оставляет желать лучшего. В случае возможности перенаправления трафика через «себя» атакующий получает возможность реализации целого ряда атак:

1) Фальсификация сервера сервиса ROBOKASSA путем перенаправления на сервер атакующих дейтаграмм, отправляемых с компьютера покупателя на адрес сервиса: merchant.roboxchange.com. Для аутентификации сервиса и защиты от атаки «человек посередине» используется подписанный центром сертификации сертификат, однако с учетом сложившейся практики, когда пользователи мало обращают внимание на содержимое сертификатов и подтверждение факта их выдачи уполномоченным центром сертификации, наличие такого сертификата не является достаточной гарантией от реализации атаки.

2) Фальсификация сервера сервиса ROBOKASSA путем модификации URL адреса сервиса на странице магазина. Реализация данной атаки требует возможность перехвата и модификации веб-страниц, передаваемых с сервера интернет-магазина на компьютер покупателя. Данная атака реализуема по причине того, что какая-либо защита данных страниц не предполагается.

3) Фальсификация номера счета, на который должна поступать оплата с сервиса ROBOKASSA. Реализация данной атаки идентична предыдущей. В большинстве случаев применения сервиса единственной возможностью для покупателя проверить правильность оплаты является число, содержащее номер счета, по которому осуществляется оплата, и сумма платежа. При совпадении сумм платежа выглядит маловероятным, что покупатель будет осуществлять проверку номера счета.

4) Фальсификация отклика об оплате. Реализация данной атаки требует возможность перехвата и модификации откликов (HTTP запросов или электронных писем), передаваемых от сервиса интернет-магазину. Возможность данной атаки обеспечивается идентичностью кодов аутентичности сообщений, передаваемых во всех видах откликов, что дает атакующему возможность заменить один вид отклика на другой.

Таким образом, анализ показывает, что сервис оплаты ROBOKASSA недостаточно защищен от атак типа «человек посередине». Кроме того, вызывает опасение возможность использования продавцом недостаточно стойких паролей.

Примечания

[1] Организация приема электронных платежей ROBOKASSA / ЗАО "Центр интернет-платежей". URL: http://www.robokassa.ru/ru/ (дата обращения: 23.03.2012).

[2] ROBOKASSA. Описание интерфейсов / ЗАО "Центр интернет-платежей". URL: http://www.robokassa.ru/ru/Doc/Ru/Interface.aspx (дата обращения: 23.03.2012).

[3] *Столлингс В.* Основы защиты сетей. Приложения и стандарты. М.: Издательский дом «Вильямс», 2002. 432 с.

Дик Дмитрий Иванович, кандидат технических наук, доцент кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: ddi@kgsu.ru

Солодовников Вячеслав Михайлович, кандидат физико-математических наук, доцент, заведующий кафедрой «Безопасность информационных и автоматизированных систем» Курганского государственного университета. E-mail: vmsolodovnikov@yandex.ru

УДК 519.151, 519.725, 519.165
ББК 22.311

Н. В. Медведев, С. С. Титов

О ПОЧТИ ПОРОГОВЫХ МАТРОИДАХ И СХЕМАХ РАЗДЕЛЕНИЯ СЕКРЕТА

В статье рассмотрены вопросы информационной безопасности, связанные с разделением секрета. Обсуждается проблема реализации сложных структур доступа, соответствующих схем разделения секрета на примере задачи существования почти пороговых матроидов. Построена бесконечная серия почти пороговых матроидов, схем разделения секрета, связанных с кодами Рида – Маллера.

Ключевые слова: *почти пороговые матроиды, циклы, схема разделения секрета, эллиптические кривые, код Рида-Маллера.*

N. V. Medvedev, S. S. Titov

ON ALMOST-THRESHOLD MATROIDS AND SECRET SHARING SCHEMES

The article is devoted to the questions of information security related to the sharing of secret. Realizations of complicated access structures and corresponding secret sharing schemes are discussed on the example of the problem of the existing almost-threshold matroids. The infinite series of almost-threshold secret sharing schemes and matroids is built based on Reed-Muller codes.

Keywords: *almost-threshold matroids, loops, secret sharing scheme, elliptic curves, Reed-Muller code.*

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая, являясь системообразующим фактором жизни общества, активно влияет на состояние безопасности различных сфер деятельности. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать[1]. Поэтому вопросы, связанные с криптографическими методами зашиты информации и математическими задачами криптологии, являются чрезвычайно важными[1]. Такие вопросы приводят также и к сложным задачам разграничения доступа к информации и разделения секрета[2, 3, 4, 5].

Одним из основных криптографических примитивов в теории и практике защиты информации является набор *схем разделения секрета* (СРС). Компьютерной метафорой здесь выступает «красная кнопка», которая может быть нажата только при наличии ключей доступа у достаточно полной коалиции доверенных лиц. Основная идея СРС состоит[2] в раздаче *долей секрета* участникам таким образом, чтобы заранее заданные коалиции участников (разрешенные коалиции) могли однозначно восстановить секрет (совокупность этих множеств называется *структурой доступа*), а неразрешенные – не получали никакой дополнительной, к имеющейся априорной, информации о возможном значении секрета. Такие СРС называются *совершенными*. *Идеальными* называются СРС, где размер доли секрета, предоставляемый участнику, не больше самого размера секрета[2]. Такова, например, схема разделения секрета Шамира[6], где доли секрет-

ного ключа раздаются N участникам СРС, используя многочлен степени n-1, и только объединившись, не менее чем n участников такой *пороговой* схемы «n из N» могут однозначно восстановить секрет. Как известно[2, 7], разрешенные коалиции идеальной схемы разделения секрета определяются циклами некоторого связного *матроида* (см. далее), изучение которого и дает структуру доступа. Поэтому очевидна актуальность вопросов, связанных с изучением СРС и их свойств.

В пороговых СРС все участники равноправны, и любая коалиция из n участников может однозначно восстановить секрет. Непростой задачей является организация сложной структуры доступа, в частности, если имеется неравноправность участников, проявляющаяся, например, в том, что не все n-элементные коалиции являются разрешенными. Такие СРС естественно назвать *почти пороговыми*, важный вопрос существования и реализации таких СРС и рассмотрен ниже.

Напомним[8], что на множестве H определен матроид, если некоторые его подмножества названы *независимыми* (остальные – *зависимыми*), причём удовлетворяются аксиомы матроида; так, в терминах *циклов* – минимальных (по включению) зависимых подмножеств из H – аксиом всего две: 1) нет цикла в цикле, т. е. если $C,\ D$ – циклы, и $C \subset D$, то C=D; 2) если $C_1 \neq C_2$ – циклы, и $x \in C_1 \cap C_2$, то $C_1 \cup C_2 \setminus \{x\}$ содержит цикл. Любое максимальное независимое подмножество B, содержащееся в H, называется *базой* матроида H. Матроид называется *связным*, если для любых двух его элементов существует содержащий их цикл. Матроид называется *простым*, или *комбинаторной геометрией*, если в нем нет одноэлементных и двухэлементных циклов[8]. Отметим, что в идеальных СРС естественно рассматривать только простые матроиды, т. к. наличие цикла из двух участников можно интерпретировать как скрытую идентичность этих участников[5]. При $|H|$=N возможно реализовать пороговую схему разделения секрета «*(n-1)* из *(N-1)*», например СРС Шамира, которую определяет матроид, который естественно назвать *пороговым*, т. е. все его *n*-элементные подмножества – циклы.

В работе[9] представлена почти пороговая почти совершенная СРС, основанная на использовании многочленов степени n на эллиптической кривой[10,11,12], точки которой применяются для параметризации участников. Эта СРС названа почти пороговой, т. к. добавление в неразрешенную коалицию из n участников любого другого участника, не состоящего в этой коалиции, делает данную коалицию разрешенной. В данной работе, в развитие статьи[9], исследуется проблема существования простых связных почти пороговых матроидов и реализации таких СРС.

Перейдем к рассмотрению этой задачи, рассматривая только конечные матроиды. Естественно назвать матроид *почти пороговым*, если все его циклы n-элементны, но не все его n-элементные подмножества – циклы. Предположим, что связный почти пороговый, но не пороговый, матроид H существует, тогда для его циклов должны выполняться обе аксиомы матроида. Первая аксиома выполняется, т. к. все циклы почти порогового матроида имеют одинаковую мощность, и цикла в цикле быть не может. Для мощности цикла $n \geq 3$ почти пороговые матроиды являются простыми.

Для мощности цикла n=2 существование связного почти порогового непорогового матроида противоречит связности, т. к. каждая пара элементов должна входить в некоторый цикл, что доказывает

Утверждение 1. Для мощности цикла два связного почти порогового непорогового матроида не существует.

Рассмотрим теперь поставленную задачу для мощности цикла n=3. Допустим, что связный почти пороговый, но непороговый, матроид существует, и его трехэлементное подмножество $\{1,2,3\}$ – не цикл. С точки зрения разделения секрета это можно интерпретировать как «поражение в правах» этой коалиции участников по сравнению с «более равноправными» трехэлементными коалициями участников, составляющих циклы. Тогда оно независимо, и его можно дополнить до базы матроида мощности r≥3. Из-за связности матроида каждой паре элементов в базе соответствует хотя бы один элемент вне базы матроида, дополняющий эту пару до цикла. Циклами этого матроида будут, в частности, трехэлементные подмножества A=$\{1,2,a\}$, B=$\{2,3,b\}$, причем $a \neq b$. Проверим, выполняется ли вторая аксиома циклов матроида: $C = A \cup B \setminus \{2\} = \{1,2,3,a,b\} \setminus \{2\} = \{1,3,a,b\}$. По этой аксиоме в четырехэлементном множестве C=$\{1,3,a,b\}$ должен быть хотя бы один цикл, по нашему предположению – трехэлементный. Во множестве C всего четыре трехэлементных подмножества: D=$\{1,3,a\}$, E=$\{1,3,b\}$, F=$\{3,a,b\}$, G=$\{1,a,b\}$. Подмножество D – не цикл, т. к.

происходит нарушение второй аксиомы матроида: $M = D \cup A / \{a\} = \{1,2,3\}$, где $\{1,2,3\}$ – не цикл. Аналогично, подмножество E – не цикл: $E \cup B / \{b\} = \{1,2,3\}$. Проверим, будут ли циклами трехэлементные подмножества F и G. Пусть $F=\{3,a,b\}$ – цикл, тогда по второй аксиоме матроида в подмножестве $K = F \cup B / \{b\} = \{2,3,a\}$ должен содержаться цикл, но этого не происходит, т.к. $A=\{1,2,a\}$ – цикл, ведь тогда подмножество $K \cup A / \{a\} = \{1,2,3\}$ должно было бы быть циклом, вопреки нашему предположению. Это нарушение второй аксиомы матроида, следовательно, $F=\{3,a,b\}$ – не цикл.

Аналогично, пусть $G=\{1,a,b\}$ цикл, тогда по второй аксиоме матроида в подмножестве $L = G \cup A / \{a\} = \{1,2,b\}$ должен содержаться цикл, но этого не происходит, т. к. $\{2,3,b\}$ – цикл, следовательно, $G=\{1,a,b\}$ – не цикл.

Получается, что в подмножестве C нет ни одного трехэлементного цикла, что не соответствует аксиоме. Следовательно, наше предположение почти пороговости привело к противоречию, что доказывает

Утверждение 2. Для мощности цикла три связного почти порогового непорогового матроида не существует.

Однако ситуация меняется при $n > 3$. Например, для мощности цикла четыре $n=4$ удается построить простой связный почти пороговый непороговый матроид H, $|H|=8$, что доказывает

Утверждение 3. Для мощности цикла четыре простой связный почти пороговый непороговый матроид существует.

Подробно опишем этот пример. Назначим циклами следующие четырехэлементные подмножества H, кодируя их битами функции выбора:

$1=\{0,1,2,3\}=(1\ 1\ 1\ 1\ 0\ 0\ 0\ 0)$,
$2=\{2,3,4,5\}=(0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$,
$3=\{0,1,4,5\}=(1\ 1\ 0\ 0\ 1\ 1\ 0\ 0)$,
$4=\{4,5,6,7\}=(0\ 0\ 0\ 0\ 1\ 1\ 1\ 1)$,
$5=\{2,3,6,7\}=(0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$,
$6=\{0,1,6,7\}=(1\ 1\ 0\ 0\ 0\ 0\ 1\ 1)$,
$7=\{0,2,4,6\}=(1\ 0\ 1\ 0\ 1\ 0\ 1\ 0)$,
$8=\{1,3,5,7\}=(0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$,
$9=\{1,3,4,6\}=(0\ 1\ 0\ 1\ 1\ 0\ 1\ 0)$,
$10=\{0,3,5,6\}=(1\ 0\ 0\ 1\ 0\ 1\ 1\ 0)$,
$11=\{1,2,5,6\}=(0\ 1\ 1\ 0\ 0\ 1\ 1\ 0)$,
$12=\{0,2,5,7\}=(1\ 0\ 1\ 0\ 0\ 1\ 0\ 1)$,
$13=\{0,3,4,7\}=(1\ 0\ 0\ 1\ 1\ 0\ 0\ 1)$,
$14=\{1,2,4,7\}=(0\ 1\ 1\ 0\ 1\ 0\ 0\ 1)$.

Таким образом, эти циклы представлены в виде байтов, т.е. восьмибитовых строк. Они построены так, что каждая пара циклов имеет либо два общих элемента, либо ни одного. Проверяемая аксиома матроида выполняется в более сильной форме: если разные циклы C и D пересекаются, то $C \oplus D = C \cup D / \{C \cap D\}$ содержит цикл. В нашем случае верно еще более сильное утверждение: если $C \cap D \neq \varnothing$, $C \neq D$, то множество $C \oplus D$ является циклом. Итак, почти пороговый матроид построен. Отметим, что циклы с добавлением пустого множества $\varnothing=0=(0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$ и всего множества $H=(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$ образуют подгруппу G_8 в абелевой группе по сложению восьмибитовых строк Z_2^8 с операцией симметричной разности $\oplus$. Групповая структура показывает: если $C \neq D$, то $S = C \oplus D \neq \varnothing$, причем либо S есть цикл, если $C \cap D \neq \varnothing$, либо $S=H$, если $C \cap D = \varnothing$ (и тогда $C \cup D = H$).

Ранг данного простого связного почти порогового непорогового матроида H равен четырем, например, $B=\{0,1,4,7\}$ – одна из баз матроида, максимальное независимое множество. Легко проверить, что добавление любого элемента из H в базу матроида будет давать цикл: добавление элемента 2 даст цикл $14=\{1,2,4,7\}$, добавление элемента 3 даст цикл $13=\{0,3,4,7\}$, добавление элемента 5 даст цикл $3=\{0,1,4,5\}$, добавление элемента 6 даст цикл $6=\{0,1,6,7\}$.

Из утверждения 3 следует, что почти пороговые матроиды существуют, но возможно ли их реализовать в качестве СРС? Ведь общая проблема описания матроидов, соответствующих схемам разделения секрета, пока не решена[2]. Покажем, что построенный простой связный почти пороговый непороговый матроид H с мощностью цикла четыре может использоваться для реализации идеальной СРС. Разберем пример построения *битовой* схемы разделения секрета, где нулевой элемент матроида – хранитель секретного бита $s_0 \in \{0,1\}$, а с первого по седьмой его элементы – участники СРС, где биты s_1, s_2, s_3, …, s_7 – их доли секрета. Метафорой здесь выступает тумблер, изначально находящийся в «нейтральном» положении, где, например, «вверх» – означает включение устройства, а «вниз» – включение тревоги, причем участникам СРС неизвестно, какое положение тумблера за что отвечает.

Матрица M, составленная из битовых строк, кодирующих циклы связного матроида H, является проверочной матрицей кода, составленного из строк матрицы СРС. Зная одну из баз матроида – $B=\{0,1,4,7\}$ и доли секрета участников, составляющих эту базу, можно получить доли секрета оставшихся участников СРС: $s_2=s_1+s_4+s_7$, $s_3=s_0+s_4+s_7$, $s_5= s_0+s_1+s_4$, $s_6= s_0+s_1+s_7$, эти линейные преобразования вместе с базовыми значениями s_0, s_1, s_4 и s_7 определяют порождающую матрицу M_1. Все s_i для i вне базы находятся из s_j (где j – в базе) линейным образом, т. е. как суммы некоторых базовых s_j.

$$M = \begin{pmatrix} 1&1&1&1&0&0&0&0 \\ 0&0&1&1&1&1&0&0 \\ 1&1&0&0&1&1&0&0 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 1&1&0&0&0&0&1&1 \\ 1&0&1&0&1&0&1&0 \\ 0&1&0&1&0&1&0&1 \\ 0&1&0&1&1&0&1&0 \\ 1&0&0&1&0&1&1&0 \\ 0&1&1&0&0&1&1&0 \\ 1&0&1&0&0&1&0&1 \\ 1&0&0&1&1&0&0&1 \\ 0&1&1&0&1&0&0&1 \end{pmatrix}$$

$$M_1 = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&1&1&1 \\ 1&0&1&1 \\ 0&0&1&0 \\ 1&1&1&0 \\ 1&1&0&1 \\ 0&0&0&1 \end{pmatrix}$$

Минимальными разрешенными коалициями будут $\Gamma_{\min}=\{\{3,5,6\}, \{3,4,7\}, \{2,4,6\}, \{2,5,7\}, \{1,4,5\}, \{1,6,7\}, \{1,2,3\}\}$, т. е. участники, образующие цикл с хранителем секрета, в данном случае с нулевым участником. Это и есть структура доступа. Максимальными неразрешенными коалициями $\Gamma_{\max}$ являются четырехэлементные циклы, не содержащие участника, который является хранителем секрета. Рассмотрим доказательство этого утверждения. Если пятиэлементное множество $E=\{a,b,c,d,e\}$, где $0 \notin \{a,b,c,d,e\}$ является максимальной неразрешенной коалицией, то оно не содержит часть, которая после добавления нуля становится циклом. Если в E нет ни одного цикла, то это независимое множество, чего быть не может, т. к. ранг H равен четырем. Значит, в E есть цикл. Пусть $\{a,b,c,d\}$ – цикл, тогда если в E нет коалиций из $\Gamma_{\min}$, то в $\{0,a,b,c,d,e\}$ нет циклов, содержащих нуль. Остается в H еще два участника – f и g, и каждый цикл, содержащий нуль, включает либо f, либо g, либо f и g. Перебором всех циклов проверим, что таких двух элементов нет, т. е. для любых двух ненулевых элементов найдется цикл, содержащий нуль, в которых ни одного из этих элементов нет. Например, коалиция участников $\{1,4,7\}$ неразрешенная, т. к. не образует цикл с нулем, но не максимальная: она часть цикла $\{1,2,4,7\}$.

Данная непороговая схема разделения секрета будет БД-совершенной[2], т. к. любая неразрешенная коалиция участников встречается в коде СРС, представленном в табл. 1, два раза, со всеми возможными значениями секрета $s_0=0$ и $s_0=1$, поэтому они не получают информации о секрете.

Таблица 1

№	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	1	1
2	1	0	0	1	0	1	1	0
3	1	0	0	1	1	0	0	1
4	1	0	1	0	1	0	1	0
5	1	0	1	0	0	1	0	1
6	0	0	1	1	1	1	0	0
7	0	0	1	1	0	0	1	1
8	1	1	0	0	1	1	0	0
9	1	1	0	0	0	0	1	1
10	0	1	0	1	1	0	1	0
11	0	1	0	1	0	1	0	1
12	0	1	1	0	1	0	0	1
13	0	1	1	0	0	1	1	0
14	1	1	1	1	1	1	1	1
15	1	1	1	1	0	0	0	0

Покажем на примере, что СРС будет совершенной, т. е. неразрешенная коалиция участников не получает никакой информации о секрете. Возьмем неразрешенную коалицию из четырех участников с номерами $4, 5, 6, 7$. Пусть секрет пытаются восстановить четыре участника с секретами $s_4=0$, $s_5=1$, $s_6=1$ *и* $s_7=0$. Рассмотрим, какую информацию о секрете получают участники. Пусть секрет пытается восстановить один злоумышленник – участник с секретом $s_7=0$, в результате он получит четыре варианта строк табл. 1 со значением $s_0=0$ и столько же вариантов строк со значением $s_0=1$, т.е. имеющаяся у него информация не позволяет сделать вывод о значении секрета. Если бы злоумышленник, например, получил два варианта строк со значением $s_0=0$ и шесть вариантов строк со значением $s_0=1$, то он с большой вероятностью (а именно $p=6/8=0{,}75$) смог бы сделать вывод, что значение секрета $s_0=1$, но в нашем случае оба значения секретного бита остаются равновероятными ($p=1/2$) для всех неразрешенных коалиций. Пусть секрет пытаются восстановить два участника с секретами $s_6=1$ *и* $s_7=0$, в результате они получат два варианта строк со значениями $s_0=0$ и столько же вариантов строк со значением $s_0=1$, т. е. узнать секрет равносильно подбрасыванию монеты. Пусть секрет пытаются восстановить три участника с секретами $s_5=1$, $s_6=1$ и $s_7=0$, в результате они получат один вариант строки с номером 13, где $s_0=0$, и один вариант строки с номером 2, где $s_0=1$, т. е. по-прежнему значение секрета равновероятно. Пусть секрет пытаются восстановить все эти четыре участника с секретами $s_4=0$, $s_5=1$, $s_6=1$ *и* $s_7=0$, хотя это им не разрешено. В результате они получат один вариант строки с номером 13, где $s_0=0$, и один вариант строки с номером 2, где $s_0=1$, т. е. никакой информации о секрете не получают, что и означает совершенность этой СРС.

Рассмотрим пример восстановления секрета разрешенной коалицией, когда первый, второй и третий участники объединились для восстановления секрета. Эта коалиция разрешенная, т. к. вместе с нулевым участником эти три участника образуют цикл – $\{0,1,2,3\}$. СРС является битовой, поэтому возможно всего восемь вариантов раздачи долей секрета для трех участников $\{0,0,0\}$, $\{0,0,1\}$,…, $\{1,1,1\}$. Пусть $s_1=0$, $s_2=1$, $s_3=1$, тогда они однозначно восстанавливают секрет, а именно, поскольку во всех строках табл. 1 (с номерами 6 и 7) с такими значениями s_1, s_2, s_3 значение s_0 равно нулю. Итак, $s_0=0$. Также они могут восстановить доли секрета остальных участников – s_4, s_5, s_6, s_7, но неоднозначно, получается два варианта строк с тем же значением секрета s_0, что отображено в строках 6 и 7 табл. 1.

Перейдем теперь к построению почти пороговых СРС большей мощности циклов. Для построения простого связного почти порогового непорогового матроида с мощностью цикла восемь $n=8$, $|H|=16$ воспользуемся следующим методом. Возьмем все битовые строки, соответствующие циклам почти порогового матроида с мощностью цикла четыре, представленные в табл. 1, и заменим каждый элемент битовой строки на два таких же, т. е. $(1\ 1\ 1\ 1\ 0\ 0\ 0\ 0)$ заменим на $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$. Таким образом, получим 16 циклов с $\varnothing$ и всем множеством H. Для предотвращения «скрытой идентичности» добавим цикл $(0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$ и $(1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0)$. В результате, складывая получившиеся циклы каждый с каждым, получим множество циклов матроида, которые при добавлении пустого множества и единичной строки образуют абелеву группу по сложению из 32 элементов, следовательно, из-за групповой структуры вторая аксиома выполняется, и почти пороговый матроид с мощностью цикла восемь существует. Нетрудно заметить, что здесь имеется изоморфизм групп $G_{2^4} = G_{16} = G_8 \oplus Z_2 \cong Z_2^5$, где $Z_2 = \{0,1\}$. Аналогично, в общем случае, пусть построен почти пороговый матроид с мощностью цикла $n=2^{m-1}$, $|H|=2^m$. Чтобы построить почти пороговый матроид с мощностью цикла $n=2^m$, $|H|=2^{m+1}$, «расширим» все битовые строки, соответствующие циклам почти порогового матроида с мощностью цикла $n=2^{m-1}$, т. е. заменим каждый элемент битовой строки на два таких же. Таким образом, после предотвращения «скрытой идентичности», т. е. добавления двух циклов $(0\ 1\ 0\ 1\ \ldots\ 0\ 1)$ и $(1\ 0\ 1\ 0\ \ldots\ 1\ 0)$, получим 2^{m+1}-2 циклов, которые после добавления $\varnothing$ и всего множества H образуют абелеву группу относительно побитового сложения, что доказывает

Утверждение 4. В простом связном почти пороговом непороговом матроиде с мощностью 2^m имеется изоморфизм групп $G_{2^m} \cong Z_2^{m+1}$.

Интересно отметить, что образованные битовые строки в табл. 1 есть циклы самого матроида H, при $n=4$, а также не что иное, как код Рида – Маллера первого порядка – $RM(1,3)$. Из утверждения 4 следует, что в общем случае циклы связного почти порогового

матроида с $n=2^{m-1}$ мощности $N=2^m$ и соответствующие СРС описываются кодами Рида – Маллера[13] первого порядка $RM(1,m)$, что доказывает

Утверждение 5. Существует бесконечная серия связных простых почти пороговых непороговых матроидов с мощностью 2^m, которые описываются кодами Рида – Маллера первого порядка.

Итак, доказана

Теорема 1. Существует бесконечная серия идеальных битовых почти пороговых совершенных СРС, основанных на кодах Рида – Маллера первого порядка, при $n=2^{m-1}$, $N=2^m$.

Код $RM(1,m)$ – это $[n,k,d]$-код со следующими основными параметрами: $n=2^m$, $k=m+1$, $d=2^{m-1}$. Как известно[13], имеется важный параметр кода $RM(1,m)$ – радиус покрытия r_m. Радиус покрытия кода $RM(1,m)$ является важной криптографической характеристикой. Возможно, изучение почти пороговых матроидов и их свойств позволит приблизиться к решению этой задачи.

В статье показана сложность и важность задач СРС. В рамках концепций информационной безопасности, связанных с разделением секрета, решены конкретные задачи о почти пороговом разделении секрета, а именно доказано, что почти пороговых матроидов и СРС для мощности цикла два и три не существует. Приведен и подробно разобран пример связного простого почти порогового матроида для мощности цикла четыре. Построена бесконечная серия таких матроидов мощности 2^m. Рассмотрен вопрос реализации соответствующих им битовых СРС. Доказано, что существует бесконечная серия таких СРС. Установлена взаимосвязь между почти пороговыми матроидами, СРС и кодами Рида – Маллера первого порядка.

Примечания

[1] Доктрина информационной безопасности [Электронный ресурс]. Российская газета [сайт]. URL: http://www.rg.ru/oficial/doc/min_and_vedom/ mim_bezop/doctr.shtm

[2] Введение в криптографию / под общ. ред. В. В. Ященко. СПб: Питер, 2001. 288 с.

[3] *Гайдамакин Н. А.* Автоматизированные информационные системы, базы и банки данных. Вводный курс : Учебное пособие. М.: Гелиос АРВ, 2002. 368 с.

[4] *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд. Урал. ун-та, 2003. 328 с.

[5] *Болотова Е. А., Коновалова С. С., Титов С. С.* Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противод. терроризму : матер. IV междунар. науч. конф. М.: МЦНМО, 2009. Т. 2. С. 71–86.

[6] *Shamir A.* How to share a secret // Communications of the ACM. NY, USA: ACM, 1979. Т. 22. No. 11. P. 612–613.

[7] *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра : учебник для вузов. М.: Гелиос АРВ, 2003. 336 с.

[8] *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 288 с.

[9] *Медведев Н. В., Титов С. С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады Томского государственного университета систем управления и радиоэлектроники. Томск: Издательство Томского государственного университета систем управления и радиоэлектроники, № 1 (23), ч. 1, 2011. С. 91-96.

[10] Медведев Н.В., Баутин С.П., Титов С.С. Проблема разделения секрета на эллиптических кривых // Проблемы прикладной математики и механики: сб. научн. тр. Екатеринбург: УрГУПС, 2008, № 65(148). С. 160–174.

[11] Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А. А. Болотов [и др.]. М.: КомКнига, 2006. 328 с.

[12] Математические и компьютерные основы криптологии : уч. пособие для вузов / Ю. С. Харин [и др.]. Минск: Новое знание, 2003. 381 с.

[13] *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.

Медведев Никита Владимирович, аспирант кафедры «Высшая и прикладная математика» Уральского государственного университета путей сообщения (УрГУПС). E-mail: itcrypt@gmail.com

Титов Сергей Сергеевич, д-р физ.-мат. наук, профессор кафедры «Высшая и прикладная математика» Уральского государственного университета путей сообщения (УрГУПС). E-mail: sergey.titov@usaaa.ru

УДК 342.51
ББК Х401.011.2

А. А. Захаров, Е. А. Оленников, А. В. Широких, А. М. Воробьев

О НЕКОТОРЫХ ПОДХОДАХ К ИНФОРМАЦИОННОЙ ЗАЩИТЕ ЭЛЕКТРОННОЙ ОЧЕРЕДИ ЛПУ

В статье анализируются основные угрозы, связанные с функционированием электронной очереди ЛПУ, анализируются методы минимизации рисков, связанных с реализацией данных угроз. Авторы также изучают возможности использования средств защиты для создания дополнительных сервисов в электронной медицинской истории болезни.

Ключевые слова: *электронная очередь, виртуальная регистратура, информационная безопасность, защита.*

A. A. Zaharov, E. A. Olennikov, A. V. Shirokih, A. M. Vorobiev

ABOUT SOME APPROACHES FOR INFORMATION SECURITY OF E-HEALTH FACILITY QUEUE

The paper analyzes the main threats associated with the functioning of e-health facility queue, methods to minimize the risks associated with the implementation of these threats. The authors also examine the possibilities of the usage of protective equipment for the creation of additional services in the electronic medical history.

Keywords: *e-health facility queue, virtual registry, information security, protection.*

Повышение качества и доступности медицинской помощи – один из приоритетов государственной политики. Подтверждением этого является Концепция развития системы здравоохранения в Российской Федерации до 2020 года[1], в которой большое внимание уделено вопросам развития и применения информационных технологий в здравоохранении с целью повышения доступности и качества медицинской помощи населению. В крупных российских городах для повышения доступности медицинских услуг создаются и внедряются компьютерные программы «Электронная очередь» или «Виртуальная регистратура»[2]. Обеспечивая возможность самозаписи пациентов к специалистам через Интернет, эти программные продукты создают новые сервисы – электронную очередь (далее – ЭО) в медицинских информационных системах (МИС). Однако ЭО может являться источником угроз для безопасности конфиденциальной информации, хранящейся в этих системах. Речь идет и о персональных данных пациентов, и о не подлежащих разглашению сведений, составляющих врачебную тайну.

В настоящее время внедрение ЭО еще не стало массовым, поэтому на данном этапе актуальной задачей является классификация угроз информационной безопасности медицинским системам и выработка рекомендаций для минимизации этих угроз. Ориентируясь на будущее широкое внедрение ЭО, авто-

ры также изучают возможность использования технологий защиты систем самозаписи и для создания дополнительных функционалов в МИС «Электронная карта пациента».

Все внешние угрозы безопасности ЭО условно можно разделить на два класса:

1. *Угрозы безопасности бизнеса*. Реализация угроз данного класса приводит к частичному нарушению работы ЭО или полному ее отказу. Данные угрозы могут быть реализованы, например, с целью дискредитации ЛПУ со стороны недобросовестных конкурентов.

2. *Угрозы конфиденциальности данных*. Реализация угроз данного класса направлена на хищение или искажение персональных и/или медицинских данных пациентов.

Угрозы безопасности бизнеса

1. Классические угрозы, которым подвержен любой электронный сетевой сервис: различные виды DoS и DDoS-атак, дифейсмент, SQL-injection[3] и т. д. Методы борьбы с подобными угрозами хорошо изучены и могут успешно применяться для защиты ЭО. Методы и стоимость противодействия DDoS-атакам зависят от их масштаба[4]. Если в атаке на сервис участвует небольшое количество хостов, можно заблокировать их IP-адреса или ввести ограничение на создание множества одновременно посылаемых запросов, например, с помощью технологии CAPTCHA[5]. В противном случае, для эффективного противостояния DDoS-атаке требуется дорогостоящее оборудование и программное обеспечение (ПО), которое должно быть установлено не в ЛПУ, а на стороне провайдера Интернет.

Однако если учесть, что DDoS-атаки не организуют против случайно выбранных Web-ресурсов, а преследуют, как правило, экономические интересы, то можно считать вероятность угрозы DDoS-атак на ЭО ЛПУ маловероятной.

2. Формирование большого количества ложных заявок на запись, ввод ложной информации, запись от имени другого лица, запись с целью продажи места в очереди. Важность противодействия таким угрозам обусловлена особенностями ЭО ЛПУ, которые отличают ее от ЭО других учреждений (ФНС, ГИБДД, банки и пр.). Это небольшое количество мест в очереди. В зависимости от специализации и других факторов врач может принять в день лишь ограниченное число пациентов. Кроме того, невозможность записаться на прием может иметь серьезные негативные последствия для пациента.

Для борьбы с подобными угрозами необходимо реализовать комплекс защитных мер, исключающих возможность анонимной записи и использования автоматизированных средств для создания заявок на запись:

– процедура записи должна включать тест, позволяющий удостовериться, что запись осуществляет именно человек, а не машина. Для этого можно использовать технологию CAPTCHA;

– в сервис ЭО должен быть включен модуль, позволяющий использовать черные списки и фильтрацию электронной почты.

Для исключения возможности анонимной записи может использоваться процедура аутентификации через предварительную регистрацию на сайте ЛПУ.

1. *Регистрация пользователя с подтверждением его личности через e-mail*. Процедура регистрации может быть завершена только тогда, когда пользователь воспользуется кодом активации, который система вышлет на указанный электронный адрес.

Плюсы: ЛПУ не несет дополнительных затрат, т. к. отправка кода активации на электронный адрес осуществляется бесплатно и может быть полностью автоматизирована. Впоследствии на электронный адрес пациента может отправляться полезная информация.

Минусы: подобная регистрация применяется на многих веб-ресурсах, метод является стабильным, однако уже ненадежным. За несколько минут можно бесплатно завести новый адрес на обычных серверах электронной почты или можно воспользоваться сервисом, позволяющим бесплатно без регистрации генерировать электронные адреса (например, http://10minutemail.com). Таким образом, данный метод защиты позволит лишь сократить количество ложных записей, но не исключить их совсем.

2. *Регистрация пользователя с подтверждением его личности через отправку смс на мобильный телефон абонента*. Система высылает код активации в виде смс-сообщения на указанный номер мобильного телефона; процедура регистрации будет завершена, когда пользователь отправит смс-сообщение с кодом активации на специальный номер.

Плюсы: более надежная защита от спамеров, так как процедура регистрации большого количества сотовых номеров требует и финансовых вложений, и времени; возможность оперативной связи с пациентом, т. к. на ука-

занный номер мобильного телефона пациента может отправляться полезная информация.

Минусы: если в системе рассылки смс-сообщений не заблокирована возможность отправки сообщений на короткие номера, злоумышленник может подписать ЛПУ на платные контент-услуги, указав соответствующий номер при регистрации. Ввиду простоты исполнения вероятность наступления негативных последствий можно оценить как высокую.

В качестве средств защиты можно предложить фильтрацию вводимых в систему номеров телефонов и ограничение количества вводов разных номеров телефонов за единицу времени с одного IP-адреса.

3. *Платная регистрация пользователя*. Может быть использован любой из способов регистрации, однако пользователь должен будет внести небольшую сумму на счет ЛПУ. Впоследствии данная сумма может быть возвращена пациенту, например, включением этой суммы в счет оплаты услуг.

Плюсы: снижается риск регистрации пользователей из хулиганских побуждений.

Минусы: необходимо включить в систему дополнительные модули для организации возможности оплаты регистрации; процедура регистрации усложняется, что может оттолкнуть некоторых пациентов. Повышается привлекательность спуфинга сервиса ЭО с целью незаконного получения средств клиентов ЛПУ. Кроме того, данная процедура не вполне законна и вполне может быть оспорена в суде, поскольку нарушает принцип оплаты только оказанных услуг.

4. *Запись на прием с использованием секретного идентификатора пациента (СИП), выдаваемого ЛПУ без предварительной регистрации на сайте ЛПУ*. При посещении ЛПУ пациент получает уникальный идентификатор, подтверждающий его личность. Впоследствии данный идентификатор может быть использован и при записи на прием, и как основа для штрих-кода, который может печататься на внутренних документах ЛПУ, например, для обезличивания результатов анализов.

Плюсы: исключает возможность анонимной записи при условии того, что секретный идентификатор будет держаться в тайне; пациентам не нужно проходить предварительную регистрацию на сайте; упрощается программная реализация ЭО.

Минусы: необходимость личного посещения ЛПУ для получения СИП; при несоблюдении мер безопасности СИП может быть доступен злоумышленнику.

5. *Интеграция сервиса ЭО с системой «Электронное правительство» (или подобными системами)*[6]. Предоставление доступа к сервису ЭО через портал системы «Электронное правительство».

Плюсы: полностью исключает возможность анонимной записи; надежная процедура регистрации и, главное, в отличие от регистрации, описанной в п. 4, этот подход можно использовать для доступа к разным ЛПУ.

Минусы: система к ЭО должна удовлетворять определенным требованиям, предъявляемым к сервисам, которые подключаются к системе «Электронное правительство», поэтому может потребоваться переработка уже имеющейся системы ЛПУ.

Угрозы конфиденциальности данных

1. Перехват данных, которые пациент отправляет/получает в процессе записи на прием в ЛПУ, а также в процессе регистрации на сайте ЛПУ.

Наиболее опасными угрозами с этой точки зрения являются спуфинг и фишинг[7]. Суть подобных атак заключается в следующем. Пациент попадает на поддельный сайт, где его обманом заставляют ввести конфиденциальные сведения: имя пользователя и пароль, номер паспорта или СНИЛС, номер телефона.

Использование номера телефона поддельным сайтом для получения кода «подтверждения» представляет отдельную опасность для клиента. В этом случае злоумышленник может подписать клиента без его ведома на услуги так называемых контент-провайдеров. Для этого под предлогом подтверждения регистрации запрашивается номер телефона, на который оформляется подписка. Клиенту посылается смс с «кодом подтверждения», который ничего не подозревающий клиент вводит на сайте. После этого злоумышленники получают возможность окончательного оформления подписки на псевдоуслуги.

Рекомендуется при записи на прием требовать ввода минимума персональных данных, а, по возможности, вовсе не указывать никакой конфиденциальной информации. Этого можно добиться, например, созданием общедоступного источника персональных данных, куда, следуя п. 1 ст. 8 ФЗ № 152 о персональных данных[8] (в ред. Федерального закона от 25.07.2011 № 261-ФЗ), «…с письмен-

ного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес…». Этих данных достаточно для идентификации пациента, и желательно, чтобы модуль ЭО оперировал только с ними. Иными словами:

– ПДн пациента должны храниться только в БД медицинской информационной системы ЛПУ, которая защищается в соответствии со стандартами информационной безопасности;

– для обслуживания ЭО должна использоваться отдельная база данных (БД ЭО);

– БД ЭО должна содержать данные пациента, необходимые для авторизации на сайте ЭО, и уникальный идентификатор пациента (УИП), а все услуги ЭО реализуются через промежуточный уровень, основу которого могут составлять, например, web-сервисы.

Выводы

Атаки на ЭО с целью получения прибыли на сегодняшний день маловероятны. При «правильной» организации системы ЭО доступ к ПДн пациента в принципе получить не удастся (их попросту может не быть).

Попытки остановить сервис ЭО реально никакого ущерба (кроме, возможно, репутационного) ЛПУ не нанесут, поскольку есть живая очередь и запись по телефону. ЭО – это пока дополнительная, но не основная возможность записи на прием. Однако по мере перехода к ЭО и постепенного отказа от живой очереди вероятность последующих угроз будет повышаться:

– запись с целью продажи места (известны реальные случаи);

– кража ПДн пациентов.

Методы противодействия этим угрозам – исключение возможности анонимной записи. Такие методы рассмотрены, проанализированы их достоинства и недостатки. Наиболее приемлемыми авторы считают приведенные выше методы 4 и 5.

Примечания

[1] Концепция развития здравоохранения до 2020 года [электронный ресурс]. URL: http://www.zdravo2020.ru/concept (дата обращения: 13.03.2012)

[2] Веб-регистратура [сайт]. URL: http://www.med-registratura.ru (дата обращения: 13.03.2012)

[3] Крис Касперски. Компьютерные вирусы изнутри и снаружи. – Питер. – СПб.: Питер, 2006. — С. 527.

[4] Как уберечься от DDoS-атак [электронный ресурс]. URL: http://www.pcweek.ru/security/article/detail.php?ID=121148 (дата обращения: 13.03.2012)

[5] Completely Automatic Public Turing Test to Tell Computers and Humans Apart [электронный ресурс]. URL: http://www.captcha.ru (дата обращения: 13.03.2012)

[6] Государственные услуги. Портал государственных и муниципальных услуг [сайт]. URL: http://www.gosuslugi.ru/ru/ (дата обращения: 13.03.2012)

[7] *Медведовский И. Д., Семьянов П. В., Леонов Д. Г.* Атака на Internet. // Москва, ДМК, 2000 – 336 с.

[8] О персональных данных: Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 [электронный ресурс]. URL: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html (дата обращения: 13.03.2012)

Александр Анатольевич Захаров, доктор технических наук, профессор, заведующий кафедрой информационной безопасности ГОУ ВПО «Тюменский государственный университет». E-mail: azaharov@utmn.ru

Евгений Александрович Оленников, кандидат технических наук, доцент кафедры информационной безопасности ГОУ ВПО «Тюменский государственный университет». E-mail: olennikov@utmn.ru

Андрей Валерьевич Широких, кандидат технических наук, доцент кафедры информационной безопасности ГОУ ВПО «Тюменский государственный университет». E-mail: maxwide@utmn.ru

Воробьев Артем Максимович, менеджер интернет-проектов ООО «УК “Гранд Медиа”». E-mail: artandvor@gmail.com

УДК 519.642
ББК 22.19

А. А. Каширин, С. И. Смагин

ЧИСЛЕННОЕ РЕШЕНИЕ ТРЁХМЕРНОЙ ЗАДАЧИ ДИФРАКЦИИ АКУСТИЧЕСКИХ ВОЛН

Рассматривается стационарная задача дифракции акустических волн на трёхмерных однородных включениях. Она формулируется в виде граничных интегральных уравнений первого рода с одной неизвестной функцией, что позволяет существенно понизить вычислительную сложность задачи. Приводятся результаты численных экспериментов, демонстрирующие возможность предлагаемого подхода.

Ключевые слова: *задача дифракции, уравнение Гельмгольца, граница, интегральное уравнение, численное решение.*

A. A. Kashirin, S. I. Smagin

THE NUMERICAL SOLVING THREE-DIMENSIONAL DIFFRACTION PROBLEM OF ACOUSTIC WAVES

We consider the stationary diffraction problem of acoustic waves on the three-dimensional homogenous inclusions. It formulates as the boundary integral equations of the first kind with single unknown function. It significantly reduces the computational complexity of the problem. We give the results of the numerical experiments, which illustrate the possibilities of this approach.

Keywords: *diffraction problem, Helmholtz equation boundary, integral equation, numerical solution.*

Введение

Математическое моделирование процессов распространения стационарных волн в средах с трёхмерными включениями играет важную роль в различных областях науки и техники и приводит к постановке достаточно сложных задач математической физики. Такие задачи принято называть задачами дифракции. Они встречаются, например, в радиофизике, дефектоскопии, оптике, акустике океана и атмосферы, геофизике.

Аналитические решения задач дифракции могут быть найдены только в исключительных случаях, когда граница включения имеет достаточно простую геометрическую форму. Поэтому основным методом исследо-

вания дифракционных процессов является прямое компьютерное моделирование.

Поскольку компьютер может оперировать только конечными наборами данных, возникает необходимость в построении дискретных аналогов исходных задач, которое может быть проведено различными способами. При этом следует учитывать, что решения рассматриваемых задач зависят от трёх пространственных переменных, отыскиваются в неограниченных областях, где должны удовлетворять условиям излучения на бесконечности, и при больших действительных волновых числах являются быстро осциллирующими функциями.

Отмеченные свойства приводят к тому, что дискретные аналоги задач дифракции, построенные методами конечных элементов или конечных разностей, предъявляют весьма высокие требования к ресурсам компьютера. С вычислительной точки зрения более эффективной представляется дискретизация исходных задач, сформулированных в виде эквивалентных им граничных интегральных уравнений. В этом случае неизвестные функции отыскиваются на двумерных замкнутых многообразиях, что особенно важно при численном решении, т. к. при этом существенно понижается вычислительная сложность исходных задач.

Переход к интегральным постановкам задач дифракции может быть осуществлён различными способами. В данной работе, в отличие от общепринятого подхода, когда задачи дифракции формулируются в виде систем двух граничных интегральных уравнений с двумя неизвестными функциями[1], получены и используются слабо сингулярные интегральные уравнения Фредгольма первого рода с одной неизвестной функцией, каждое из которых равносильно исходной задаче. Эти уравнения обладают сложной для теоретического анализа структурой, что компенсируется возможностью построения на их основе эффективных численных алгоритмов[2].

Для численного решения интегральных уравнений разработан не требующий триангуляции поверхности согласованный с шагом сетки алгоритм осреднения интегральных операторов со слабыми особенностями в ядрах, позволяющий строить дискретные аналоги исходных задач по достаточно простым аналитическим формулам[3].

Аппроксимирующие интегральные уравнения системы линейных алгебраических уравнений (СЛАУ) имеют плотно заполненные матрицы комплексных коэффициентов порядка нескольких десятков тысяч. Приближённые решения этих СЛАУ находятся численно при помощи обобщённого метода минимальных невязок (GMRES)[4]. Расчёты показывают, что число итераций, необходимых для отыскания решений СЛАУ данным методом, невелико по сравнению с размерностью систем и зависит от неё весьма слабо.

После того как приближённое решение интегрального уравнения найдено, искомое приближённое решение исходной задачи дифракции может быть одинаково просто и точно вычислено как в ближней, так и в дальней зоне.

1. Исходная задача и интегральные уравнения

Рассмотрим трёхмерное евклидово пространство R^3 с ортогональной системой координат $ox_1x_2x_3$, заполненное однородной изотропной средой с плотностью ρ_e, скоростью распространения акустических колебаний c_e и коэффициентом поглощения γ_e, в котором имеется ограниченное произвольной замкнутой липшицевой поверхностью Γ однородное изотропное включение с плотностью ρ_i, скоростью звука c_i и коэффициентом поглощения γ_i. Области R^3, занятые включением и вмещающей средой, обозначим через Ω_i и Ω_e ($\Omega_e = R^3 / \overline{\Omega}_i$).

Сформулируем исходную задачу.

Задача 1.1 (обобщённая постановка задачи дифракции). Найти функции $u_{i(e)} \in H^1(\Omega_{i(e)})$, удовлетворяющие интегральным тождествам

$$\int\limits_{\Omega_{i(e)}} \nabla u_{i(e)} \nabla \overline{v}_{i(e)} dx - k^2_{i(e)} \int\limits_{\Omega_{i(e)}} u_{i(e)} \overline{v}_{i(e)}\, dx = 0 \quad \forall v_{i(e)} \in H^1_0\left(\Omega_{i(e)}\right), \qquad (1.1)$$

условиям сопряжения на границе раздела сред из Ω_i и Ω_e

$$\left\langle u_i - u_e, \mu \right\rangle_\Gamma = \left\langle u_0, \mu \right\rangle_\Gamma \quad \forall \mu \in H^{-1/2}(\Gamma), \qquad (1.2)$$

$$\left\langle \eta, p_i N u_i - p_e N u_e \right\rangle_\Gamma = \left\langle \eta, p_e u_1 \right\rangle_\Gamma \quad \forall \eta \in H^{1/2}(\Gamma),$$

и условию излучения на бесконечности

$$\partial u_e / \partial |x| - ik_e u_e = o\left(|x|^{-1}\right), \quad |x| \to \infty, \tag{1.3}$$

если на границе включения Γ заданы функции $u_0 \in H^{1/2}(\Gamma)$ и $u_1 \in H^{-1/2}(\Gamma)$.

Здесь $\langle \cdot, \cdot \rangle_{\tilde{A}}$ – отношение двойственности на $H^{1/2}(\Gamma) \times H^{-1/2}(\Gamma)$, обобщающее скалярное произведение в $H^0(\Gamma)$, $Nu \in H^{-1/2}(\Gamma)$ – нормальная производная u, понимаемая в смысле распределений[5], ω – круговая частота колебаний,

$$p_{i(e)} = \left[\rho_{i(e)} \omega \left(\omega + i\gamma_{i(e)} \right) \right]^{-1}, \quad k_{i(e)}^2 = \omega \left(\omega + i\gamma_{i(e)} \right) \Big/ c_{i(e)}^2, \quad \mathrm{Im}\left(k_{i(e)} \right) \geq 0.$$

Замечание 1.1. Если $\mathrm{Im}(k_e)=0$, то $u_e \in H^1_{\mathrm{loc}}(\Omega_e)$.

Определения используемых здесь и далее функциональных пространств имеются в работе[5].

Теорема 1.1[2]**.** Задача 1.1 имеет не более одного решения.

Введём следующие обозначения:

$$A_{i(e)} q \ (x) \equiv \left\langle G_{i(e)}(x, \cdot), q \right\rangle_\Gamma, \qquad B_{i(e)} q \ (x) \equiv \left\langle N_x G_{i(e)}(x, \cdot), q \right\rangle_\Gamma, \tag{1.4}$$

$$\left(B'_{i(e)} q \right)(x) \equiv \left\langle N_{(\cdot)} G_{i(e)}(x, \cdot), q \right\rangle_\Gamma, \ G_{i(e)}(x, y) = \exp\left(ik_{i(e)} |x - y| \right) \Big/ \left(4\pi |x - y| \right).$$

Решение задачи 1.1 будем искать в виде потенциалов

$$u_e(x) = \left(A_e q \right)(x), \quad x \in \Omega_e, \tag{1.5}$$

$$u_i(x) = p_{ei} \left(A_i (N u_e + u_1)^+ \right)(x) - \left(B'_i (u_e + u_0)^+ \right)(x), \quad x \in \Omega_i,$$

где $q \in H^{-1/2}(\Gamma)$ – неизвестная плотность, $u_0 \in H^{1/2}(\Gamma)$, $u_1 \in H^{-1/2}(\Gamma)$, $p_{ei} = p_e / p_i$, а знаком "+" отмечаются предельные значения соответствующих выражений на Γ, когда $x \to \Gamma$ из области Ω_e.

Ядрами интегральных операторов здесь являются фундаментальные решения уравнений Гельмгольца и их нормальные производные, поэтому $u_{i(e)}$ удовлетворяют тождествам (1.1) и условию излучения (1.3) для u_e. Кроме того, выполнение для них первого из условий сопряжения (1.2) автоматически влечёт за собой выполнение второго условия сопряжения. Подставляя потенциалы (1.5) в условия сопряжения (1.2), получаем слабо сингулярное интегральное уравнение Фредгольма первого рода для определения неизвестной плотности q:

$$\left\langle (Cq), \mu \right\rangle_\Gamma = \left\langle v_0, \mu \right\rangle_\Gamma \quad \forall \mu \in H^{-1/2}(\Gamma), \tag{1.6}$$

$$(Cq)(x) \equiv \left(\left(0.5 \left(A_e + p_{ei} A_i \right) + \left(B'_i A_e - p_{ei} A_i B_e \right) \right) q \right)(x),$$

$$v_0(x) = -0.5 u_0(x) + p_{ei} \left(A_i u_1 \right)(x) - \left(B'_i u_0 \right)(x). \tag{1.7}$$

Теорема 1.2[2]**.** Пусть $u_0 \in H^{1/2}(\Gamma), u_1 \in H^{-1/2}(\Gamma), \gamma_e > 0$ или ω не является собственной частотой задачи

$$\Delta u + k_e^2 u = 0, \quad x \in \Omega_i, \qquad u = 0, \quad x \in \Gamma. \tag{1.8}$$

Тогда уравнение (1.6) корректно разрешимо в классе плотностей $q \in H^{-1/2}(\Gamma)$ и формулы (1.5) дают решение задачи 1.1.

Потенциалы (1.5) предпочтительней использовать, когда необходимо рассчитать отражённое волновое поле в области Ω_e, поскольку в этом случае расчёты проводятся по достаточно простой формуле. Если же необходимо вычислить проходящее волновое поле в области Ω_i, предпочтительнее использовать потенциалы следующего вида:

$$u_i(x) = \left(A_i q \right)(x), \quad x \in \Omega_i, \tag{1.9}$$

$$u_e(x) = \left(A_e(u_1 - p_{ie} N u_i)^- \right)(x) - \left(B'_e(u_0 - u_i)^- \right)(x), \quad x \in \Omega_e,$$

где $q \in H^{-1/2}(\Gamma)$ – неизвестная плотность, $u_0 \in H^{1/2}(\Gamma)$, $u_1 \in H^{-1/2}(\Gamma)$, $p_{ie} = p_i / p_e$, а знаком "–" отмечаются предельные значения соответствующих выражений на Γ, когда $x \to \Gamma$ из области Ω_i.

И в этом случае задача 1.1 сводится к слабо сингулярному интегральному уравнению Фредгольма первого рода:

$$\left\langle (Dq), \mu \right\rangle_\Gamma = \left\langle u_0, \mu \right\rangle_\Gamma \quad \forall \mu \in H^{-1/2}(\Gamma), \tag{1.10}$$

$$(Dq)(x) \equiv \left(\left(0.5(A_i + p_{ie} A_e) + (p_{ie} A_e B_i - B'_e A_i) \right) q \right)(x).$$

Теорема 1.3[2]**.** Пусть $u_0 \in H^{1/2}(\Gamma), u_1 \in H^{-1/2}(\Gamma), \gamma_e > 0$ или ω не является собственной частотой задачи (1.8). Тогда уравнение (1.10) корректно разрешимо в классе плотностей $q \in H^{-1/2}(\Gamma)$ и формулы (1.9) дают решение задачи 1.1.

2. Численный метод

Применяемый метод численного решения представляет собой развитие методики, предложенной и впервые апробированной в работе[6]. Кратко опишем схему его реализации.

Построим покрытие поверхности Γ системой $\{\Gamma_m\}_{m=1}^M$ окрестностей узловых точек $x'_m \in \Gamma$, лежащих внутри сфер радиусов h_m с центрами в x'_m, и обозначим через $\{\varphi_m\}$ подчинённое ему разбиение единицы. Тогда

$$\sum_{m=1}^{M} \varphi_m(x) = 1 \quad \forall x \in \Gamma, \quad 0 \le \varphi_m \le 1, \quad \operatorname{supp} \varphi_m \subset \Gamma_m.$$

В качестве φ_m будем использовать функции

$$\varphi_m(x) = \varphi'_m(x) \left(\sum_{n=1}^{M} \varphi'_n(x) \right)^{-1}, \quad \varphi'_n(x) = \varphi'(r_n / h_n), \quad \varphi'(t) = \begin{cases} \left(1 - t^2\right)^3, & t < 1, \\ 0, & t \ge 1, \end{cases}$$

где $r_n = |x - x'_n|$.

Приближённые решения интегральных уравнений будем искать на сетке $\{x_m\}$,

$$x_m = (\overline{\varphi}_m)^{-1} \int_\Gamma x \varphi_m \, d\Gamma, \quad \overline{\varphi}_m = \int_\Gamma \varphi_m \, d\Gamma,$$

узлами которой являются центры тяжестей функций φ_m. В дальнейшем будем предполагать, что для всех m, $n = 1, 2, \ldots, M$ выполняются неравенства

$$0 < h' \le r_{mn}, \quad m \ne n, \quad h' \le h_n \le h, \quad h / h' \le q_0 < \infty.$$

Здесь $r_{mn} = |x_m - x_n|$, h', h – положительные числа, зависящие от M, q_0 не зависит от M.

Вместо заданной на Γ неизвестной функции q будем рассматривать обобщённую функцию $q\delta_\Gamma$, действующую по правилу

$$\left(q\delta_\Gamma, \psi \right)_{R^3} = \left\langle q, \psi \right\rangle_\Gamma, \quad \forall \psi \in H^1\left(R^3\right).$$

Эту функцию будем приближать выражением

$$q(x)\delta_\Gamma(x) \approx \sum_{n=1}^{M} q_n \overline{\varphi}_n \psi_n(x), \quad \psi_n(x) = \left(\pi \sigma_n^2 \right)^{-3/2} \exp\left(-r_n^2 / \sigma_n^2 \right), \quad x \in R^3,$$

где q_n – неизвестные коэффициенты, $\sigma_n^2 = 0.5 \overline{\varphi}_n$.

Интегральный оператор Фредгольма первого рода из (1.4) аппроксимируем по формулам[3]:

$$\int_{\Gamma}\left(A_{i(e)}q\right)\varphi_m d\Gamma \approx \overline{\varphi}_m\sum_{n=1}^{M}A_{i(e)}^{mn}q_n,\quad m=1,2,...,M, \tag{2.1}$$

$$A_{i(e)}^{mn}\equiv A_{mn}\left(k_{i(e)}\right),\quad A_{mn}=0.5\beta_{mn}\exp\left(-\gamma_{mn}^2\right)\left(w\left(z_{mn}^{+}\right)-w\left(z_{mn}^{-}\right)\right)\Big/r_{mn},\quad n\neq m,$$

$$A_{mm}=\beta_{mm}\left(2\left(\pi\sigma_{mm}^2\right)^{-1/2}+ikw\left(\mu_{mm}\right)+2\pi^{1/2}\left(1-\mu_{mm}^2/3\right)\sigma_{mm}/\overline{\varphi}_m\right),$$

$$\beta_{mn}=\overline{\varphi}_n\left(4\pi\left(1-\mu_{mn}^2+0.5\mu_{mn}^4\right)\right)^{-1},\quad \sigma_{mn}^2=\sigma_m^2+\sigma_n^2,\quad \mu_{mn}=0.5k\sigma_{mn},$$

$$z_{mn}^{\pm}=\pm\gamma_{mn}+i\mu_{mn},\quad \gamma_{mn}=r_{mn}/\sigma_{mn},\quad i^2=-1,$$

$$w(z)=\exp\left(z^2\right)\left(1+\operatorname{erf}(z)\right),\quad \operatorname{erf}(z)=\frac{2}{\sqrt{\pi}}\int_0^z\exp\left(-t^2\right)dt.$$

Интегральный оператор Фредгольма второго рода из (1.4) аппроксимируем по формулам[7]:

$$\int_{\Gamma}\left(aq+B_{i(e)}q\right)\varphi_m d\Gamma \approx \overline{\varphi}_m\sum_{n=1}^{M}B_{i(e)}^{mn}q_n,\ m=1,2,...,M, \tag{2.2}$$

$$B_{i(e)}^{mn}=\left(4\pi r_{mn}^3\right)^{-1}n_{mn}^{*}\exp\left(ik_{i(e)}r_{mn}\right)\left(ik_{i(e)}r_{mn}-1\right)\overline{\varphi}_n,\quad n_{mn}^{*}=\sum_{l=1}^{3}n_{lm}\left(x_{lm}-x_{ln}\right),$$

$$B_{i(e)}^{mn}=-\mathrm{Gs}(x_m)\quad \text{ï ðè } a=0.5,\quad B_{i(e)}^{mn}=-1-\mathrm{Gs}(x_m)\quad \text{ï ðè } a=-0.5,$$

$$\mathrm{Gs}(x_m)=\sum_{n\neq m}^{M}\frac{n_{mn}^{*}\overline{\varphi}_n}{4\pi r_{mn}^3}\approx\frac{1}{4\pi}\int_{\Gamma}N_y\frac{1}{\left|x_m-y\right|}d\Gamma_y=-\frac{1}{2}.$$

Интегральные операторы в левых частях уравнений (1.6) и (1.10) являются композицией интегральных операторов (2.1) и (2.2), поэтому аппроксимируем их по формулам[3]:

$$\int_{\Gamma}\left(Cq\right)\varphi_m d\Gamma \approx \sum_{n=1}^{M}\left(A_e^{mn}B_i^{mn}-p_{ei}A_i^{mn}B_e^{mn}\right)q_n,\quad m=1,2,...,M, \tag{2.3}$$

$$\int_{\Gamma}\left(Dq\right)\varphi_m d\Gamma \approx \sum_{n=1}^{M}\left(p_{ie}A_e^{mn}B_i^{mn}-A_i^{mn}B_e^{mn}\right)q_n,\quad m=1,2,...,M, \tag{2.4}$$

а правые части уравнений (1.6) и (1.10) – по формулам

$$\int_{\Gamma}v_0\varphi_m d\Gamma \approx \overline{\varphi}_m\left(\mathrm{Gs}\left(x_m\right)u_0\left(x_m\right)+\sum_{n=1}^{M}\overline{\varphi}_n\left[p_{ei}A_i^{mn}u_1\left(x_n\right)-u_0\left(x_n\right)B_i^{nm}\right]\right),$$

$$\int_{\Gamma}u_0\varphi_m d\Gamma \approx \overline{\varphi}_m u_0\left(x_m\right),\quad m=1,2,...,M.$$

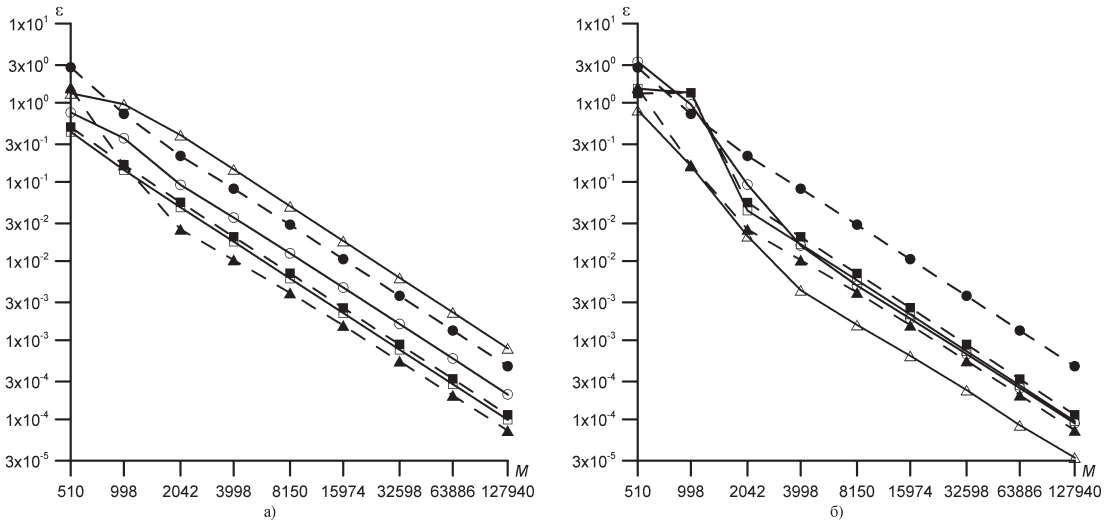

Рис. 3.1. Погрешности вычисления решений задач дифракции из примера 3.1:
а) найденных по формулам (1.5); б) найденных по формулам (1.9)
(сплошная линия – во внутренней области, пунктир – во внешней области)

3. Результаты численных экспериментов

Пример 3.1. Рассматривается задача дифракции плоской акустической волны на однородном единичном шаре с центром в начале координат. Граничное условие: $u_0(x)=\exp(ik_e x_3)$, $u_1(x)=ik_e\exp(ik_e x_3)n_3$. Параметры сред: $k_i=12.5$, $\rho_i=4$, $k_e=8$, $\rho_e=3$ (I); $k_i=7$, $\rho_i=2$, $k_e=16.5$, $\rho_e=5$ (II); $k_i=21$, $\rho_i=7$, $k_e=13.5$, $\rho_e=4.5$ (III).

Точное решение этой задачи имеется в работе[8]. По теореме 1.2 данная задача эквивалентна интегральному уравнению (1.5), а по теореме 1.3 – интегральному уравнению (1.9), численно решив которые, получаем приближённые решения задачи дифракции.

Пример 3.1 приведён для демонстрации возможностей метода численного решения. С этой целью результаты расчётов представлены в виде графиков в двойных логарифмических переменных $\lg\varepsilon$ от $\lg M$, где ε – относительная погрешность вычисления. При точном степенном законе убывания погрешности эти графики будут асимптотически переходить в прямые линии с наклоном $\mathrm{tg}\alpha=-p/2$, где p – порядок аппроксимации относительно «шага» $h\sim M^{-1/2}$ заданной на граничной поверхности сетки.

Графики погрешностей для первого набора параметров помечены квадратами, для второго – треугольниками, для третьего – кругами, погрешности решений во

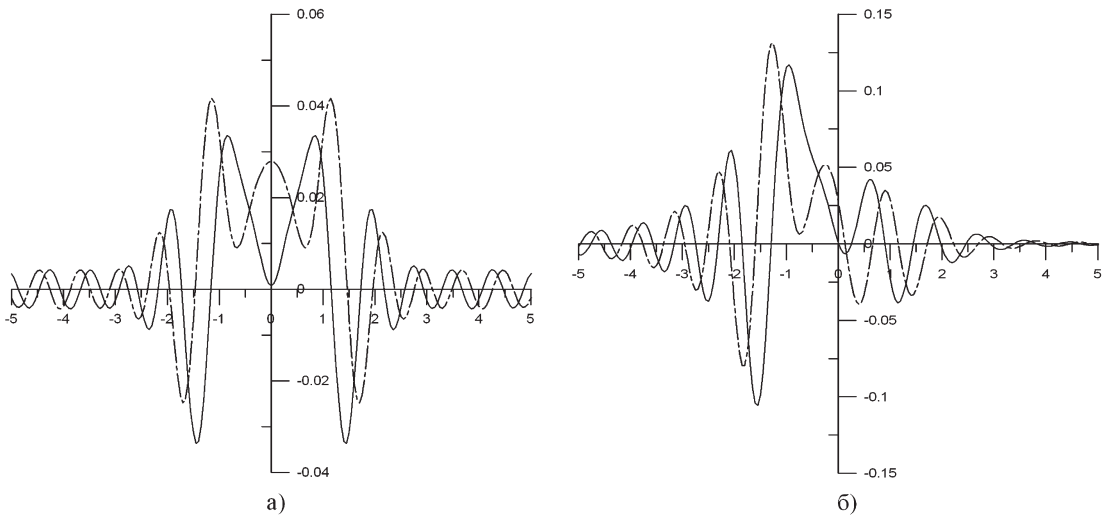

Рис. 3.2. Отражённое поле u_e из примера 3.2 на отрезках
а) $|x_1|\le 5$, $x_2=0$, $x_3=0$; б) $x_1=0$, $|x_2|\le 5$, $x_3=0$
(сплошная линия – вещественная часть, пунктир – мнимая часть)

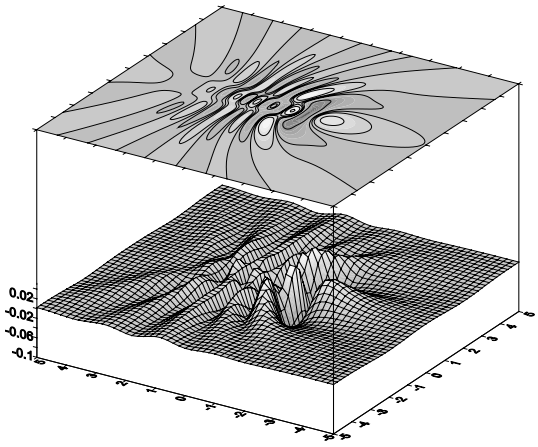

Рис. 3.3. Добавочное поле $\Delta|u_e|$ на квадрате $\{-5\le x_1, x_2\le 5, x_3=0\}$

внутренней области изображены сплошной линией, во внешней области – пунктиром.

Количество точек дискретизации M варьировалось от 500 до 128000, решения СЛАУ находились численно при помощи GMRES[4] с точностью до 10^{-9}. Эксперименты проводились на кластере ВЦ ДВО РАН. Распараллеливанию подвергались наиболее трудоёмкие модули: решение СЛАУ, вычисление точных и приближённых решений, вычисление погрешности решений.

На рис. 3.1 приведены погрешности решений задачи дифракции, полученные в результате подстановки решений уравнений (1.6) и (1.10) в формулы (1.5) и (1.9) соответственно. Погрешности вычислены в норме пространств сеточных функций $H_h^0(\Omega_{i(e)})$. Видно, что при достаточно больших M погрешность решений имеет порядок не хуже $h^2 \sim M^{-1}$.

Пример 3.2. Рассматривается задача дифракции акустических волн на включении, границей которого является эллипсоид (0.75, 1, 0.5) с центром в точке (0, 0, –1). Падающее поле создается точечным источником вида

$$u_0(x) = \exp\left(ik_e\left|x-y\right|\right)\Big/\left|x-y\right|,$$

расположенным в точке (0, 2, 2). Параметры сред: $c_e=0.125$, $\rho_e=3$, $\gamma_e=0.05$, $c_i=0.07$, $\rho_i=5$, $\gamma_i=0.02$. На рис. 3.2 изображены вещественные и мнимые части отражённого поля u_e на отрезках $|x_1|\le 5$, $x_2=0$, $x_3=0$ и $x_1=0$, $|x_2|\le 5$, $x_3=0$, а на рис. 3.3 – добавочное поле $\Delta|u_e|=|u_e+u_0|-|u_0|$ на квадрате $\{-5\le x_1, x_2\le 5, x_3=0\}$.

По результатам численных экспериментов можно сделать вывод, что, несмотря на свою простоту, используемый метод обладает весьма высокой точностью при решении трёхмерных стационарных задач дифракции. Он позволяет проводить расчёты в достаточно широком диапазоне волновых чисел и эффективен как на регулярных, так и на нерегулярных сетках.

Примечания

[1] *Колтон Д., Кресс Р.* Методы интегральных уравнений в теории рассеяния. М.: Мир, 1987. 311 с.

[2] *Каширин А. А., Смагин С. И.* Обобщённые решения интегральных уравнений скалярной задачи дифракции // Дифференциальные уравнения, 2006. Т. 42. № 1. С. 79–90.

[3] *Каширин А. А.* Исследование и численное решение интегральных уравнений трёхмерных стационарных задач дифракции акустических волн : Дисс. … канд. физ.-мат. наук. Хабаровск, 2006. 118 с.

[4] *Saad Y.* and *Schultz M.* GMRES: A generalized minimal residual algorithm for solving nonsymmetric linear systems // SIAM J. Sci. Statist. Comput., 7 (1986). P. 856–869.

[5] *McLean W.* Strongly elliptic systems and boundary integral equations. Cambridge: Cambridge University Press, 2000. 372 p.

[6] *Смагин С. И.* Численное решение интегрального уравнения I рода со слабой особенностью для плотности потенциала простого слоя // Журнал вычислительной математики и математической физики. 1988. Т. 28, № 11. С. 1663–1673.

[7] *Ершов Н. Е., Смагин С. И.* Численное решение трёхмерной стационарной задачи дифракции акустических волн на упругом включении. Препринт. Владивосток: ДВО АН СССР, 1989. 46 с.

[8] *Тихонов А. Н., Самарский А. А.* Уравнения математической физики. М.: Издательство Московского университета, 1999. 799 с.

Каширин Алексей Алексеевич, кандидат физико-математических наук, доцент, старший научный сотрудник лаборатории «Вычислительной механики» ВЦ ДВО РАН. E-mail: elomer@mail.ru.

Смагин Сергей Иванович, член-корреспондент РАН, профессор, директор ВЦ ДВО РАН. E-mail: smagin@as.khb.ru.

УДК 004.056, 34.03:004.056.5
ББК Х401.114

А. В. Рожков, С. А. Рожков

РОССИЙСКАЯ ИНФОРМАТИЗАЦИЯ И ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ ТЕРМИНАЛЬНЫХ СИСТЕМ НА ПРИМЕРЕ ОРИГИНАЛЬНОЙ СИСТЕМЫ WTPRO

Статья посвящена вопросу современной практической реализации идеи мэйнфреймов (mainframe) – терминальным системам, их классификации, а также решению проблемы их защищенности на основе применения стандартных методов дискретной математики и теории групп. Проблемы иллюстрируются на примере созданной авторами статьи и продвигаемой на рынке терминальной системы WTPRO.

Ключевые слова: *информатизация, терминальная система, защита информации.*

A. V. Rozhkov, S. A. Rozhkov

INFORMATIZATION IN RUSSIA AND THE ISSUES OF TERMINAL SYSTEMS SECURITY AS EXEMPLIFIED BY WTPRO ORIGINAL SYSTEM

The paper provides an overview of current practices of mainframe implementation and focuses on terminal systems and their classification together with the issue of their security that can be solved by the use of standard methods of discrete mathematics and group theory. The issues are exemplified by the WTPRO original system; this product is created by the authors of the paper and well promoted on the market.

Key words: *informatization, terminal system, information security.*

1. Российская информатизация

На очередном российском интернет-форуме «РИФ+КИБ 2012» (Российский интернет-форум + конференция «Интернет и бизнес»), проходившем 18–20 апреля 2012 г., было обнародовано много интересных фактов.

Директор Российской ассоциации электронных коммуникаций (РАЭК) Сергей Плуготаренко со ссылкой на данные Фонда «Общественное мнение» привел следующие цифры: на сегодняшний день ежемесячная аудитория Рунета составляет 57,8 млн человек (это порядка 50% населения России в возрасте старше 18 лет). Рост аудитории за год составил 15%. При этом количество пользователей, выходящих в Сеть ежедневно, в нашей

стране составляет 44,3 млн человек (38% населения России в возрасте старше 18 лет). По этому показателю рост за год составил 22%. Сравнивая аудиторию Рунета с остальными медиа, эксперты отмечают, что на сегодняшний день в возрастных группах до 45 лет Интернет превосходит по охвату все остальные медиа, включая телевидение. Знаковым событием стало то, что ***осенью прошлого года по размеру национальной аудитории интернет-пользователей Россия вышла на первое место среди европейских стран.*** В мире по этому показателю наша страна занимает шестое место.

По оснащенности электронными устройствами с памятью и средствами коммуникации (компьютеры, смартфоны, телефоны, электронные книги и т. д.) мы также входим в первую десятку в мире – на одного россиянина приходится более двух подобных устройств, без учета компьютерных устройств на рабочих местах.

А вот по эффективности использования этого людского и технического потенциала в государственном управлении, бизнесе и народном хозяйстве мы не входим даже в первую сотню стран мира.

Материальная часть информатизации и техническая подготовленность населения страны выше всех похвал. Нормативно-правовая база также не вызывает нареканий. Последние два-три года лавинообразно нарастает число нужных и своевременных документов в этой сфере.

Речь идет и о федеральных законах, например, [1, 2] и о постановлениях и распоряжениях правительства, в первую очередь [3, 4]. Общий объем документов, регламентирующих информационную сферу, в том числе и ее защиту, составляет около 2000 документов федерального уровня.

Причина отставания информатизации социальной и производственной сфер жизни общества в сути этих самых социально-экономических отношений. Они сводятся к тому, что все делается по принципу: «глаза в глаза», «из рук в руки». Электронным бумагам, защищенным премудрой цифровой подписью, основанной на эллиптических кривых над полями Галуа, никто в здравом уме не верит!

Тем не менее, государство прилагает титанические усилия для выведения должностных и финансовых отношений на интернет-орбиту. Стартовал вдохновляемый банками мегапроект «Универсальная электронная карта», правда, его внедрение перенесено на 2013 г. В мае 2012 г. министр связи и массовых коммуникаций И. О. Щеголев обещает начать практическую реализацию проекта «Государственная электронная почта» для связи граждан с органами местного и государственного управления.

На местах власти и энтузиасты реализуют региональные информационные проекты.

В нашей работе речь идет об информатизации малых предприятий и органов местного самоуправления. О современной реализации старой идеи мэйнфреймов (mainframe) – терминальных системах: сильный сервер – слабые тонкие клиенты. В качестве этих клиентов может выступать огромный парк морально устаревшей электроники, имеющейся в больших количествах на многих рабочих местах.

2. Современные терминальные системы

Разработкой терминальных решений занимаются такие крупные корпорации, как Microsoft, Citrix, AT&T, Medialogic S.p.A., Famatech, а также ряд отечественных компаний АстраСТ (г. Челябинск), ОКБ САПР (г. Москва) и другие. Компании-разработчики больше внимания уделяют расширению функциональных возможностей решений, практически не затрагивая вопросы безопасности. В силу этого базовые технологии работы тонких клиентов не изменились с 80-х годов прошлого века и не обеспечивают необходимого сегодня уровня защищенности.

Исследованиями в области терминальных систем занимаются зарубежные и отечественные ученые: С. В. Конявская, Д. Ю. Счастный, И. А. Бажитов., М. Д. Муха, Т. У. Мазерс, Д. Холме, С. Каплан, Т. Ризер, А. Вуд, Б. Трич и другие.

Однако в большинстве работ рассматриваются в основном вопросы архитектуры системного и программного обеспечения терминальных систем, проблемы реализации и функционирования их аппаратной части. Проблемы же защищенности подобных систем от внешних и внутренних угроз их информационной безопасности рассматриваются недостаточно глубоко.

Например, вопросы доверенной загрузки операционной системы по сети до сих пор практически не изучались и, соответственно, не создавались программные продукты, реа-

лизующие указанную процедуру.

Классификация терминальных систем.

По способу исполнения терминалы делят на следующие типы.

1. Аппаратные. Полностью аппаратных терминальных клиентов сейчас практически не производят. Исключением являются тонкие клиенты Ncomputing, производимые в США.

2. Программно-аппаратные. В настоящее время большое распространение получили терминалы, построенные на той же компонентной базе и поддерживающие такую же систему команд, что и персональные компьютеры. На эти терминалы устанавливается специальное программное обеспечение, которое управляет работой терминала.

3. Программные. Программная реализация терминала предполагает, что на терминале уже установлена какая-либо операционная система, а для подключения к терминальному серверу запускается специальная программа.

По программной платформе, к которой подключаются терминалы, разделение определяется наиболее распространенными семействами операционных систем: Windows и Unix/Linux.

Терминалы также классифицируют по способу загрузки программного обеспечения.

1. Загрузка терминала происходит по сети, в самом терминале отсутствуют накопители информации.

2. Загрузка операционного терминала с локального накопителя, чаще всего используется IDE Flash или жесткий диск.

3. Запуск терминальной программы из операционной системы.

4. Загрузка через Интернет. Для доступа к удаленной системе используется интернет-браузер и/или Java-приложение.

По способу применения различают следующие типы терминальных систем.

1. Для удаленного доступа к приложениям.

2. Для замены рабочего стола.

3. Для выполнения специализированных задач.

4. Интернет-терминалы.

По уровню представления информации: различаются текстовые и графические терминалы.

В настоящее время на рынке наибольшее распространение получили следующие терминальные серверы: Microsoft Windows Terminal Server, Citrix MetaFrame, X Window System, NComputing Terminal Server, AT&T Real VNC, 2X ThinClientServer, NX NoMachine.

Из терминальных клиентов наиболее известны:

• На открытом исходном коде: Thinstation, LTSP, PXES

• Коммерческие: WindowsCE, WtWare, WtPro, DosRDP, JWT, а также программные реализации терминальных клиентов, поставляемые вместе с терминальными серверами.

Нами предложена терминальная система WTPRO [5, 6], функционал ее описан в [7, 8]. В настоящее время система WTPRO успешно используется примерно в 300 организациях стран СНГ, в том числе и в г. Челябинске. На нее имеется 5 патентов государственной регистрации программ, она отражена в монографической литературе, например в [9].

3. Проблемы защищенности терминальных систем

Созданная одним из авторов статьи, им же развиваемая и продвигаемая на рынке система WTPRO поддерживает четыре терминальных протокола – два текстовых: telnet – небезопасный протокол, ssh – защищенный аналог telnet; и два графических: RDP – удаленный рабочий стол Windows, VNC – открытый протокол для доступа как к Windows, так и к UNIX серверам.

Возможность тонкой настройки терминальной системы на едином сервере, почти полное исключение человеческого фактора позволяют заблокировать многие угрозы НСД. Вместе с тем, терминальная система подвержена новым атакам, актуальным только для нее. Источником большинства проблем безопасности является то, что на терминале нет предустановленной ОС – она загружается по сети. Используемые при этом протоколы, разрабатывались в 80-х годах прошлого века и не обеспечивают необходимого сегодня уровня защищенности. Собственно говоря, угрозу безопасности начинает представлять и фон-неймановская архитектура компьютерного «железа» и сама методология функционирования многих современных ОС.

Одним из авторов этой статьи разработаны расширения для виртуальных каналов RDP-протокола, расширяющие функциональные возможности сервера терминалов, позволяющие производить идентификацию и аутентификацию клиента и сервера. Их прак-

тическое удобство состоит в том, что пользователь работает графической легко различаемой информацией.

В свою очередь, в работах [10, 11] предложены модель и работающий в ней алгоритм, позволяющий локально формализовать проблему анализа протоколов взаимодействия двух субъектов. Например, сервера и терминального клиента.

Каждое сообщение сервера и клиента является некоторым двоичным словом. Пусть у нас взаимодействуют два субъекта. Как принято в криптографии – Алиса и Боб (A и B).

A посылает некоторое бинарное v сообщение B. В свою очередь, B, проанализировав его, отсылает A модифицированное сообщение $w = f(v)$.

В работе рассматриваются две возможные формализации данного взаимодействия, позволяющие применить стандартные методы дискретной математики и теории групп.

Первое, пусть сообщения, которыми обмениваются субъекты, имеют фиксированную длину. Данная ситуация хорошо моделируется стандартной процедурой, когда необходимо расставить флаги в интерфейсе взаимодействия. Если считать, что флаг принят – это 1, флаг сброшен – 0, то протокол взаимодействия является функцией обработки n-мерного бинарного вектора. То есть $f : Z_2^n \to Z_2^n$ отображение, заданное в линейном пространстве. Поскольку нет никаких надежд, что это отображение является линейным, то лучше рассматривать двоичный вектор v как код бинарного дерева T. При этом сообщения длины n будут образовывать n-слой T_n дерева T. В этом случае взаимодействие будет описываться некоторым отображением дерева T в себя: $f : T \to T$.

Если дополнительно разбить каждую трансакцию взаимодействия на элементарные трансакции, при которых в слове v изменяется только один символ, то мы получим отображение f, являющееся автоморфизмом дерева T.

Если система взаимодействия работает штатно, то среди автоморфизмов $Aut\ T$ дерева T выделяется подмножество $True$ допустимых взаимодействий. Если же в процессе взаимодействия возникло взаимодействие $h \notin True$, то система выдает сигнал опасности.

Не слишком большой натяжкой является допущение, что выполнение друг за другом (суперпозиция) двух допустимых преобразований f и g снова будет допустимым преобразованием $f \circ g$ и что тождественное преобразование (т. е. отсутствие реальных преобразований) тоже является допустимым преобразованием. В любом случае $True$ является, с алгебраической точки зрения, как минимум моноидом.

Обратимость преобразования f, т. е. восстановление прообраза v по известному сообщению $w = f(v)$, возможно далеко не всегда. Часто обработка разных допустимых запросов на выходе имеет одну и ту же последовательность допустимых бит. Впрочем, и здесь часто можно выбрать некую естественную (каноническую) ветвь многозначной функции f^{-1}. В этом случае некоторое семейство подмножеств $Gset = \{G \mid G \subseteq True\}$ моноида $True$ будет состоять из множеств, порождающих группы $gr(G) \le AutT$.

Вторая математическая модель более проста в использовании и не требует глубокой детализации протокола взаимодействия. Множество преобразований при трансакциях субъектов можно представить в виде дерева Forest возможных исходов. Вершиной дерева Forest будет исходное сообщение v Алисы. Всевозможные ответы Боба $W=\{w|w \in W\}$ конкатенируем с сообщением v и получаем первый слой дерева $Forest$ $Forest_1 = \{vw|w \in W\}$. Множество ответов $U=\{u|u \in U\}$ Алисы на ответы Боба конкатенируем во второй слой дерева $Forest_2 = \{vwu|w \in W, u \in U\}$ и т. д.

Возникающее дерево $Forest$ будет слойно однородным с фиксированной начальной вершиной – кодом запуска протокола. Выполнение протокола будет случайным блужданием по дереву $Forest$.

Сложность состоит в том, что количество вершин в этом дереве растет экспоненциально и равно произведение чисел $|W| \cdot |U| \cdot \ldots$ и даже при 5 проходах протокола и при 10 возможных исходах каждой трансакции получится порядка 100 тысяч вершин.

Следующее упрощение ситуации состоит в том, что разные ответы Алисы и Боба при взаимодействии имеют существенно различную вероятность. Проведя серию натурных экспериментов, можно составить таблицу вероятностей (вернее условных вероятностей) исходов событий, принадлежащих множествам $W, U, \ldots$ После этого ввести новую кодировку дерева $Forest$, например классическим кодом Хаффмана. В этом случае дерево $Forest$ преобразуется в двоичное дерево F. Двоичное дерево F будет иметь ту же мощность, что

и дерево $Forest$. Но отбросив его ветви, вероятность попадания на которые будет меньше некоторой пороговой величины, например, 10^{-3}, мы сможет существенно прорядить дерево F во многих важных для практики случаях до мощности $|W|+|U|+...$. Назовем такое проряженное дерево логарифмическим деревом LF.

В работе получены некоторые интересные результаты анализа протоков аутентификации в тонком клиенте WTPRO на языке автоморфизмов деревьев T и LF.

Выводы

Российская информатизация полностью готова к достижению общемирового уровня функциональности как по техническим параметрам, так и по уровню подготовленности персонала. Соответствует мировому уровню и организационно-правовая поддержка информатизации.

Учитывая отставание страны в области производства собственной элементной базы и программного обеспечения, упор в информатизации переносится на свободное программное обеспечение (СПО) и собственные малобюджетные разработки, учитывающие специфику и потребности российских пользователей. В первую очередь, программно-аппаратные комплексы для использования в офисах малых фирм и муниципальных органов власти.

В силу необходимости исполнения законов о защите информации, в первую очередь № 152-ФЗ о персональных данных, весьма актуальна проблема защищенности разрабатываемых индустриальных продуктов.

Система WTPRO, обсуждаемая в данной статье, является типичным примером подобной чисто российской разработки, служащей продвижению защищенной информатизации в российских регионах.

Литература

1. Федеральный закон. Об организации предоставления государственных и муниципальных услуг от 27.07.2010 № 210-ФЗ (ред. от 03.12.2011 № 383-ФЗ).

2. Федеральный закон. Об электронной подписи от 06.04.2011 № 63-ФЗ (ред. от 01.07.2011 № 169-ФЗ).

3. Распоряжение Правительства РФ. О государственной Программе Российской Федерации «Информационное общество (2011–2020 годы)» от 20.10.2010 № 1815-р (ред. от 30.12.2011 № 2438-р).

4. Распоряжение Правительства РФ. О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения 2011–2015 от 17.12.2010 № 2299-р.

5. Рожков, С. А. Терминальная система «ElinuxT»: Свидетельство об официальной регистрации программы для ЭВМ № 2006611848. Зарегистрировано в Реестре программ 30.05.2006.

6. Рожков С. А. Защищенная терминальная система WTPRO: Свидетельство о государственной регистрации программы для ЭВМ № 2009611320. Зарегистрировано в Реестре программ 04.03.2009.

7. Рожков С. А. Защищенные терминальные системы [текст] / С. А. Рожков // Доклады ТУСУР, т. 1 (19), часть 2, 2009. С. 62–64.

8. Рожков С. А. Терминальная система ELINUX: архитектура, функциональность, схема применения /С. А. Рожков // Вестник ЮУрГУ. Компьютерные технологии, управление, радиоэлектроника. № 26 (159), выпуск 10, 2009. С. 52–56.

9. *Стахнов А.* Linux-сервер в Windows-окружении. – СПб.: БХВ, 2007. 656 с.

10. Рожков А. В. Применение теории групп в задачах защиты информации [текст] / А. В. Рожков// Наука ЮУрГУ: материалы 60-й юбилейной научной конференции. Секция технических наук. – Челябинск: Изд-во ЮУрГУ, 2008. – Т. 2. – с. 111–115.

11. *Рожков, А. В.* Место и роль компьютерной безопасности в системе обеспечения информационной безопасности региона [текст] / А. В. Рожков// Вестник УрФО. Безопасность в информационной сфере, № 1, 2011. – Челябинск: Изд-во ЮУрГУ, с. 54–57.

А. В. Рожков, д.ф.-м.н., профессор, кафедра БИС. E-mail: urvest@mail.ru

С. А. Рожков, директор ООО «Deep Systems». E-mail: urvest@mail.ru

УДК 316.77:34
ББК Х401.114

И. Л. Бачило

ОТЗЫВ О ДИССЕРТАЦИИ АЛЕКСЕЯ ВЛАДИМИРОВИЧА МИНБАЛЕЕВА, ВЫПОЛНЕННОЙ НА ТЕМУ: «ТЕОРЕТИЧЕСКИЕ ОСНОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ МАССОВЫХ КОММУНИКАЦИЙ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА»

I. L. Bachilo

OPINION ON DISSERTATION OF ALEKSEY VLADIMIROVICH MINBALEEV: «THEORETICAL BASIS FOR LEGAL REGULATION OF MASS COMMUNICATIONS UNDER CONDITIONS OF INFORMATION SOCIETY DEVELOPMENT»

Исследование, представленное диссертационной работой А. В. Минбалеева **«Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества»,** является актуальным и весьма перспективным в плане развития информационного права и совершенствования практики

применения института массовых коммуникаций.

Интернет формирует сферу массовых коммуникаций, правовая основа которых до сих пор самостоятельно не исследовалась с точки зрения правового регулирования комплекса отношений, реализуемых субъектами в этом информационном пространстве. Критерии включения государственно-правовых механизмов в эту сферу отношений до сих пор представляют проблему, требующую согласования и нормативного определения механизмов регулирования как на уровне отдельных государств, так и их международного взаимодействия.

Автор ставил перед собой задачу теоретического обоснования и конструирования концепции правового регулирования массовых коммуникаций в условиях развития информационного общества, и это определило цель исследования и структуру представленной на защиту диссертации

Объектом диссертационного исследования являются общественные отношения, возникающие в сфере массовых коммуникаций в условиях развития информационного общества. *Предметом* исследования выступили правовые нормы, регулирующие отношения в сфере массовых коммуникаций в условиях информационного общества, а также соответствующие нормы международного права, нормы законодательства зарубежных стран, решения высших судебных инстанций и иная правоприменительная практика, механизмы саморегулирования по исследуемой проблематике.

Задача и цели исследования раскрыты в структуре работы. Она представлена: введением, четырьмя главами и 14-ю параграфами, а также заключением, которые позволили автору сосредоточить внимание на проблемах: 1 – понятие и правовая природа массовых коммуникаций в условиях развития информационного общества; 2 – закономерности развития и функционирования средств массовых коммуникаций; 3 – закономерности регулирования массовых коммуникаций в условиях развития информационного общества; 4 – обоснование теоретических и методологических основ регулирования массовых коммуникаций. Это позволило сформулировать и предложить для публичного обсуждения ряд авторских выводов и предложений по углублению научного видения рассматриваемой проблемы и ряд предложений в области совершенствования российского информационного законодательства.

Диссертация опирается на анализ обширного, разнопланового нормативного материала и достаточную эмпирическую базу. Автор проявил несомненные способности самостоятельно формулировать научные проблемы, имеющие важное значение для развития науки информационного права, использовал большой объем зарубежных источников, что позволило ему сформулировать свои самостоятельные выводы и предложения по одной из важных проблем современного права и практики информационно-коммуникативных отношений.

Методологическая и эмпирическая основы работы над диссертацией представлены комплексным рассмотрением и применением принципа единства всеобщего, общенаучных и специальных методов познания. Особенно значимы материалы российской и зарубежной судебной практики по вопросам правового регулирования информационных отношений; опыт правового регулирования отношений в информационной сфере в зарубежных странах (в Австралии, Великобритании, Германии, Гонконге, Дании, Индии, Китае, США, Украине, Франции, Швеции, Японии и др.); аналитические материалы, отчеты ряда международных, зарубежных и отечественных организаций, российских органов государственной власти в информационной сфере.

Научная новизна диссертационного исследования определяется тем, что в нем представлен широкий, системно обоснованный подход к видению и исследованию мало изученной научной и практической проблемы современного этапа развития общества. В диссертации предложен ряд новых положений, ценных выводов и рекомендаций по совершенствованию правового регулирования массовых коммуникаций в условиях развития информационного общества. Наиболее значимые из них вынесены автором на обсуждение в процессе защиты исследования в качестве докторской диссертации.

Рассмотрение положений, характеризующих новизну работы и выносимых на защиту 15 позиций, позволяет остановиться на следующих вопросах.

1. В рамках авторской концепции массовые коммуникации определены как «система взаимосвязанных средств, технологий передачи и получения массовой информа-

ции, предназначенной для определенной цели посредством использования законных средств и способов для ее достижения». Позитив этой формулы заключается в обозначении дихотомической зависимости средств коммуникации и информационного ресурса, которым заполняются сетевые системы связи. Понимая важность формы информации как «массовой», автор формулирует и свое понимание этой сущностной части института массовой коммуникации. Он определяет ее как «предназначенные и распространяемые для неограниченного или неопределенного круга лиц сведения (данные, сообщения), материалы независимо от формы их представления, средств и методов их распространения». (Глава 1 и п. 1 выносимых на защиту положений).

Отметим как позитивный признак исследования предложения по авторскому определению таких понятий, как «связь с общественностью», «сайт» и др.

Заметим, что и в этой части предлагаемых определений не помешала бы отсылка на соответствие правил выбора и распространения информации требованиям закона. Это тем более важно, что в положении 2 автор переходит к значению усвоения опыта работы средств массовой информации, но основное внимание уделяет только одной части правоотношений – *доступу распространяемой информации в Интернет*. Этот уклон неизбежно сузит область правового регулирования в среде отношений по массовым коммуникациям. Это важно, т. к. автор во второй главе диссертации считает, что «сеть Интернет, как и другие информационно-теле-коммуникационные сети, нельзя рассматривать как форму массовых коммуникаций» (параграф 4 главы второй и стр. 23 автореферата).

2. В части позитивных результатов исследования отметим выносимые на защиту положения, в которых автор характеризует информацию «как идеальное благо особого рода». Оценку этого «блага» диссертант определяет через «интерес» субъекта права к ней (информации) в процессе ее введения в оборот. Определяющим при этом он справедливо считает значение содержания, смысла, заложенного в информацию. Немного приглушает этот вывод уравнение смысла с формой предоставления информации потребителю (смысл и (или) форма) – пишет автор.

3. К позитивной стороне исследования стоит отнести позицию автора относительно общности норм, регулирующих такие формы массовых коммуникаций, как реклама, социальная реклама, связи с общественностью, СМИ при *традиционных формах* распространения и *новых* формах распространения этих видов информации в интернет-среде, как основных базовых требований к правовому регулированию. При этом важно внимание к дополнительным условиям правового регулирования в Интернете с учетом понимания автора широкой и узкой трактовки Интернета и адаптации методов регулирования с учетом новых средств массовых коммуникаций (стр. 9-12 автореферата – п. 7, 8, 10).

4. Отмечу и значение понимания метода саморегулирования и сорегулирования в области массовых коммуникаций в интернет-среде и конкретных предложений автора в этой части работы.

5. Значительное внимание уделено автором вопросам развития информационного права с учетом широкого использования массовых коммуникаций через потенциал интернет-среды и предложениям по совершенствованию законодательства за счет подготовки и принятия ряда закон федерального уровня. Можно только сожалеть, что эта часть авторских предложений не включена в характеристику новизны и положений, выносимых на защиту. Здесь проявилась скромность автора в оценке результатов своей работы.

Отмечая позитивные стороны диссертационного исследования автора, стоит обратить внимание и на некоторые спорные или требующие уточнения вопросы.

1. В работе автор неоднократно обращается к институту правового режима информации и отмечает в п. 3, вынесенном на защиту, что и массовая информация обладает всеми признаками для «разграничения правовых режимов», но имеет свою специфику. Такой тезис важен, хотя и может толковаться неоднозначно. Однако его значение не выявляется полностью, и особенно для распространителей информации, так как в авторском тексте все признаки массовой информации, а это и требования к ее содержанию и форме, адресованы исключительно к функции «контроля». *Но именно контроль в сфере массовых коммуникаций и является камнем преткновения в обеспечении чистоты и полезности социальной среды Интернета и блага ресурса массовых коммуникаций.*

Относительно функции контроля есть и такая авторская формулировка, как: «кон-

троль соответствия единым закономерностям существования информационной сферы…» (стр. 12, 29 автореферата, глава третья, 3-й параграф). Здесь и в некоторых других важных положениях концепции желательно бы уделить большее внимание субъектам, имеющим и реализующим права на доступ к сети «Интернет» и образующим область видов и форм правоотношений (глава 2-я и автореферат, стр. 10. п. 9).

В этой же связи желательно более точное определение информационных ресурсов, относимых к категории «ограниченного распространения». Автор уделяет внимание преимущественно «вредной информации», определение которой весьма затруднительно и может быть чисто субъективным. При этом теряется вопрос о несанкционированном вынесении в Интернет других категорий информационных ресурсов – тайны государственной, коммерческой; персональных данных и личной частной информации; авторской информации.

2. Основное внимание автора к таким формам массовой информации, как реклама, СМИ (обычные и электронные), связь с общественностью (кого и в каких формах?), не закрывает раскрытия и других форм массовых коммуникаций и распространяемой информации. Например. Поисковые, информационные системы, другие формы информирования пользователей интернет-ресурсами, определение природы интернет-переписки конкретных пользователей и доступа к этой информации через системы ЖЖ, блоги, «Одноклассники» и др. не снимает доступа широкой общественности к ним и социально-психологического влияния их на культуру информационного общения. Например, справочно-поисковые системы в Интернете большое благо для распространения научных знаний. Это тоже сфера массовых коммуникаций.

3. Методологическое значение для всего комплекса проблем информационного права имеет позиция автора относительно признания связи информационного общества с его характеристиками как гражданского, социально, демократического и правового и одновременного утверждения, что «государство» и гражданское общество существуют совместно (а это значит и отдельно), что склоняет автора к характеристике роли государственных и правовых институтов к их патерналистской трактовке, их обязывании обеспечить требования субъектов гражданского общества. Это снижает и роль государственного участия в реализации задач массовых коммуникаций, а также значимости саморегулирования и сорегулирования процессов и отношений.

4. Автор рекомендует подготовку и принятие ряда законов РФ, включающего такие, как: базовый закон РФ «О массовых коммуникациях», базовый закон «Об основах регулирования отношений в Интернете», поправки в законы и СМИ и рекламе в российском национальном законодательстве. Это полезно. Но как может действовать закон одного государства в области регулирования отношений в Интернете, вопрос непростой. Он требует учета масштаба и сложности сетевой природы, пространства жизни интернет-коммуникаций и информационной среды и возможных дискуссий по этой проблеме с учетом позиций таких конвенций, как, например, Конвенция о киберпреступности, которая обнажает проблемы обеспечения суверенитета каждого участника ее, проблемы координации применения разных юрисдикций в интернет-среде.

Отмечу, что появление вопросов к автору исследования – хороший признак. Это научно-практическое исследование открывает весьма важный аспект правового регулирования правоотношений в сфере, пока не поддающегося единой, комплексной и целостной системе правового регулирования. В этом несомненная заслуга автора диссертации – Алексея Владимировича Минбалеева.

Разработка проблемы представленного исследования потребовала основательной теоретической подготовки и высокой юридической культуры исследователя. Судя по диссертации, этими качествами автор обладает. Диссертант продемонстрировал глубокое знание отечественной литературы по общей теории права, информационному, административному и другим отраслям права, а также широкого круга зарубежных источников соответствующей проблематики.

Особо следует отметить, что имеем дело с первой научно-квалификационной работой докторского уровня, представляющей современное комплексное и системно организованное исследование по недостаточно изученной в науке информационного права теме, имеющей большое теоретическое и непосредственно практическое значение для развития правоотношений в сфере массовых

коммуникаций. Эта работа существенно дополняет область правового регулирования массовых коммуникаций, наличие и развитие которых формирует базу и ресурс нового этапа информационной культуры в условиях глобализации по всем направлениям формирования современной цивилизации. Одновременно соискатель поднимает и пытается на концептуальном уровне решить проблемы как сущности информационного права, так и места в нем института массовых коммуникаций.

К оригинальным теоретическим новациям и наиболее практически значимым результатам этого исследования необходимо отнести его практическую значимость, возможность использования полученных результатов и выводов для оживления дискуссионного ракурса науки информационного права, совершенствования информационного законодательства, разработки курсов учебных дисциплин, а также при создании учебных и учебно-методических пособий по информационно-правовой проблематике в образовательных учреждениях высшего профессионального образования. Частично они уже используются в образовательном процессе и научно-исследовательской деятельности Южно-Уральского государственного университета (национального исследовательского университета).

Впечатляет апробация автором выводов и положений, полученных им в ходе работы над темой. Результаты диссертационного исследования докладывались более чем на 46 научных и научно-практических конференциях и семинарах, в том числе профильных по теме диссертации зарубежных и международных конференциях и семинарах; они получили отражение в публикациях автора, о которых даны сведения в автореферате и по ходу изложения материала диссертации.

Диссертант принимал участие в выполнении научно-исследовательских работ по финансируемым Российской Федерацией программам, являлся научным руководителем поисковых научно-исследовательских работ в рамках мероприятия «Проведение научных исследований научными группами под руководством кандидатов наук» в рамках Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы по теме «Правовое регулирование деятельности средств массовой информации в условиях развития информационного общества в России».

Таким образом, изучение содержания данной диссертации и автореферата показывает высокую степень обоснованности, достоверность и новизну сформулированных автором научных положений, выводов и рекомендаций. Высказанные суждения и замечания в данном отзыве на диссертацию ни в коем случае не колеблют ее высокой оценки как самостоятельного и творческого научно-исследовательского труда и имеют в основном дискуссионный характер.

Диссертация А. В. Минбалеева на тему «Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества» является самостоятельным, творческим, структурно обоснованным и законченным исследованием, соответствующим профилю научной специальности 12.00.14 – административное право, финансовое право, информационное право.

Автореферат диссертации и публикации соискателя отражают основные положения проведенного диссертационного исследования.

Оформление рецензируемой диссертации соответствует установленным требованиям.

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

Вывод: диссертационное исследование на тему «Теоретические основания правового регулирования массовых коммуникаций в условиях развития информационного общества» соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени доктора юридических наук (ч. 1 п. 7 и п. 8 Положения о порядке присуждения ученых степеней, утвержденного Постановлени-

ем Правительства Российской Федерации от 30 января 2002 г. № 74 (в редакции Постановления Правительства Российской Федерации от 20 июня 2011 г. № 475), а диссертант – Алексей Владимирович Минбалеев заслуживает присуждения ученой степени доктора юридических наук по специальности 12.00.14 – административное право, финансовое право, информационное право.

И. Л. Бачило, зав. сектором информационного права Института государства и права Российской академии наук, заслуженный юрист Российской Федерации, доктор юридических наук, профессор. E-mail: urvest@mail.ru

УДК 316.77:34, 34:070
ББК Х401.114

П. У. Кузнецов

РЕЦЕНЗИЯ НА МОНОГРАФИЮ МИНБАЛЕЕВА АЛЕКСЕЯ ВЛАДИМИРОВИЧА НА ТЕМУ «ТЕОРЕТИЧЕСКИЕ ОСНОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ МАССОВЫХ КОММУНИКАЦИЙ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА»

P. U. Kuznecov

REVIEW OF THE MONOGRAPH OF ALEKSEY VLADIMIROVICH MINBALEEV: «THEORETICAL BASIS FOR LEGAL REGULATION OF MASS COMMUNICATIONS UNDER CONDITIONS OF INFORMATION SOCIETY DEVELOPMENT»

Монография А. В. Минбалеева посвящена исследованию важнейшей в современном для науки информационного права проблемы – выявлению теоретических оснований правового регулирования массовых коммуникаций и созданию весьма важной концепции правового регулирования массовых коммуникаций в рамках отрасли информационного права. Развитие авторской концепции реализуется посредством использования методологического построенного приема – познания закономерностей развития и функци-

онирования явления применительно к определенной парадигме – системе правовых взглядов, идей, представлений о теоретических основаниях правового регулирования массовых коммуникаций в условиях развития информационного общества.

Автор при проведении исследования теоретических оснований правового регулирования массовых коммуникаций в условиях развития информационного общества направил свои усилия на решение крупной научно-практической проблемы, имеющей существенное значение как для развития доктрины современного информационного права, так и для совершенствования российского законодательства, регулирующего отношения в сфере массовых коммуникаций.

Актуальность исследования не вызывает сомнений, поскольку на современном этапе развития общества мы наблюдаем стремительное развитие огромного количества форм и видов массовых коммуникаций. С появлением и развитием сети Интернет их количество возросло во много раз и уже сегодня практически не поддается точному подсчету. В этой связи возникает необходимость теоретического обобщения правовой природы массовых коммуникаций, а также имеющегося опыта их регулирования в целях выработки единых теоретических оснований для дальнейшего правового регулирования отдельных массовых коммуникаций. В этой связи настоящее исследование, бесспорно, представляется весьма своевременным, поскольку позволяет начать юридический анализ отношений в сфере массовых коммуникаций. Актуальность работы также обусловлено отсутствием в юридической науке комплексных исследований в сфере правового регулирования массовых коммуникаций.

Большая заслуга А. В. Минбалеева заключается в том, что он исследует вопросы, которые в науке информационного права не получали глубокого изучения и соответствующего развития в течение последних нескольких лет.

Цель исследования достигается тем, что автор поставил и решил такие задачи, как: определение места и роли массовых коммуникаций в становлении и развитии информационного общества; изучение особенности информации как объекта правоотношений и ее системообразующее значение для массовых коммуникаций; анализ правовой природы массовой информации и массовых коммуникаций; выявление закономерности функционирования и развития отдельных средств массовых коммуникаций на современном этапе; исследование закономерности регулирования массовых коммуникаций; выявление и исследование отраслевых и методологических основ правового регулирования массовых коммуникаций на этапе становления и развития информационного общества в Российской Федерации. Решение названных задач позволило автору разработать и обосновать принципиально новую концептуальную модель целостного системного регулирования правоотношений, возникающих по поводу массовых коммуникаций.

Это позволяет ему обосновать вывод об обособлении в рамках информационного права специальной подотрасли российского права – права массовых коммуникаций. Такой вывод является важнейшим теоретическим основанием для дальнейшего правового регулирования массовых коммуникаций в условиях развития информационного общества. Такой подход автора в установлении главных исследовательских приоритетов обеспечивает высокий теоретический уровень проведенной научной работы, выражающийся в полномасштабном решении поставленных задач, формулировании нескольких важных с точки зрения научной новизны теоретических положений.

Одним из важных для науки информационного права положений является авторский анализ правовой природы массовых коммуникаций в условиях развития информационного общества. В этой связи он показывает, что массовые коммуникации, в первую очередь средства массовой информации, оказали огромное влияние на формирование и развитие информационного общества. Автор подвергает теоретическому осмыслению феномен существования массовых коммуникаций как особого объекта информационных правоотношений. На основе такого анализа в работе сформулировано авторское определение массовых коммуникаций как «система взаимосвязанных средств, технологий передачи и получения массовой информации, предназначенной для определенной цели, посредством использования законных средств и способов для ее достижения».

Важным является и то, что впервые в науке подвергнуто исследованию понятие «массовой информации» как системообразующей категории и приводится его определение –

«предназначенные и распространяемые для неограниченного или неопределенного круга лиц сведения (данные, сообщения), материалы независимо от формы их представления, средств и методов их распространения».

Наиболее важным концептуальным положением работы являются выводы об институциональном развитии информационного права, выделении характерных признаков такого развития, определении места информационного права в системе российского права. Автор обосновал предназначение информационного права как «единого центра управления» регулирования информационных отношений, поскольку информационные отношения пронизывают многие складывающиеся сегодня правоотношения. Данный вывод обусловлен обеспечением всех других отраслей права категориальным аппаратом, базовыми информационно-правовыми нормами и принципами регулирования информационных отношений, а также единством и разнообразием использования комплексного метода правового регулирования. В задачу информационного права, как правильно подчеркивает автор, входит контроль соответствия принимаемых норм, регулирующих информационные отношения, единым закономерностям существования информационной среды. Автор обосновал такой вывод практикой регулирования тех или иных отношений в информационной сфере другими отраслями права, что свидетельствует о появлении огромного количества коллизий и противоречий с существующими закономерностями информационной сферы.

Комплексный анализ существующих правовых средств регулирования позволил А. В. Минбалееву впервые на монографическом уровне описать существование самостоятельного метода правового регулирования, характерного исключительно для информационного права. Автор справедливо подчеркивает, что «главной функцией отраслевого метода информационного права в условиях развития информационного общества является создание целенаправленного инструментария упорядочения общественных отношений в информационной сфере сообразно основным закономерностям развития глобального информационного общества и информационной политики государства, а целью отраслевого метода информационного права – создание гармоничной универсальной системы способов, приемов, средств, позволяющих упорядочить общественные отношения в информационной сфере в условиях стремительного изменения технических, организационных и иных условий функционирования информационной среды».

Автор обосновал вывод о том, что специфика метода информационного права отражается в уникальном сочетании способов правового регулирования: запретов, позитивных обязываний, дозволений, поощрений, правовых рекомендаций. При этом важное место отведено саморегулированию как особому способу правового регулирования, включая договорно-правовое регулирование.

Отраслевой метод информационного права представлен как система способов, приемов, средств правового регулирования общественных отношений в информационной сфере, специфика которого проявляется в совокупности императивных и диспозитивных начал, обусловленных предметом данной отрасли, а также в особенностях развития государства и права в условиях глобального информационного общества, применении ряда специфических способов правового регулирования, в том числе интегрированных из других наук и областей знаний.

Вместе с тем, отдельные положения и выводы исследования А. В. Минбалеева являются спорными, что вызывает вопросы, а также замечания и пожелания.

1. В работе автор последовательно и обоснованно отмечает дуалистическую природу информации как объекта правоотношений и указывает, что «информация есть сложное явление, являющееся, с одной стороны, проявлением свойства объектов живой природы (субъектов) отражать в форме психических ощущений движение объектов окружающего мира (содержательная сторона информации – сведения), а с другой стороны – проявлением способности некоторых объектов живой природы передавать через сообщения испытанные им и переработанные ощущения другим объектам живой природы (представительная сторона информации – сообщение).

При исследовании правовой природы массовых коммуникаций автор также указывает на их дуалистическую природу, отмечая роль информации и формы ее распространения. Однако в работе, как представляется, автор не развивает и недостаточно обосновывает выявленную закономерность дуалистичности данных объектов. Исходя из названия

второго параграфа первой главы, вероятно, автору следовало бы привести аргументацию и проследить системообразующее значение информации как объекта правоотношений для массовых коммуникаций как объектов правоотношений.

В связи с этим возникает вопрос о том, каким образом связана дуалистическая природа информации и массовых коммуникаций? Какие связи возникают между ними в условиях именно развития информационного общества? В чем заключается системообразующее значение информации для массовых коммуникаций? Какие закономерности их взаимодействия можно выявить на современном этапе? Есть ли обратная связь массовых коммуникаций на информацию как объекты правоотношений?

2. Первый параграф второй главы работы А. В. Минбалеева посвящен исследованию правовой природы традиционных средств массовой информации в условиях развития информационного общества. Автором используется понятие «традиционные средства массовой информации», но автором не в достаточной степени обосновывается, почему им вводится и используется данный термин. При анализе традиционных средств массовой информации автор недостаточно уделяет внимание особенностям правового режима периодических печатных изданий, теле- и радиовещания. Между тем, автор более детально обращается к специализированным средствам массовой информации.

В связи с вышесказанным возникает вопрос, какими критериями руководствовался автор при разграничении традиционных средств массовой информации от иных? Что представляют собой специализированные средства массовой информации и как они соотносятся с традиционными и новыми средствами массовой информации?

3. Разделяя озабоченность автора бесконтрольным распространением «грязной» информации и позицию о необходимости правового регулирования использования массовых коммуникаций в сети Интернет в рамках отдельной Концепции противодействия использованию сети Интернет в противоправных целях, следует отметить, что автором недостаточно уделено места в исследовании такой новой формы распространения массовой информации, как комментарии и высказывания в сети Интернет, в том числе размещение их в такой среде, как «Блогосфера».

Руководствуясь нормами о свободе распространения информации любым законным способом (ст. 29 Конституции Российской Федерации), авторы таких высказываний нередко нарушают законные интересы других лиц и установленные нормы нравственности. Несмотря на то что п. 3 ст. 55 Конституции Российской Федерации устанавливает возможность ограничения прав и свобод человека и гражданина федеральным законом в таких случаях, все же законодатель пока относится пассивно к решению этой проблемы. Позиция автора в этой части никак не отражена в работе.

Однако высказанные замечания носят дискуссионный характер, они никак не влияют на общую положительную оценку работы и не снижают ее научного уровня и практической значимости.

Исследование А. В. Минбалеева является первым монографическим трудом в области комплексного исследования массовых коммуникаций как правового феномена. Предложения и рекомендации автора могут содействовать улучшению качества правотворчества в области законодательства об информации. Совершенствование законодательства на основе разработанной А. В. Минбалеевым концепции правового регулирования массовых коммуникаций в условиях развития информационного общества может позволить упорядочить отношения в сфере массовых коммуникаций, привести их в систему.

П. У. Кузнецов, заведующий кафедрой информационного права ФГБОУ ВПО «Уральская государственная юридическая академия», доктор юридических наук, профессор. E-mail: urvest@mail.ru

УДК 34.03:004.73(100)
ББК Х401.114, Х408.135, Х911.16

Д. А. Астахов

ПРОБЛЕМА ПОДГОТОВКИ КАДРОВ ДЛЯ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье выявляется противоречие между основными направлениями международного сотрудничества в области международной информационной безопасности и содержанием новых российских образовательных программ для подготовки международников. На основе анализа российского проекта «Конвенции международной информационной безопасности» и содержания зарубежных образовательных программ обосновывается необходимость совершенствования ФГОС-3 по направлению «Международные отношения».

Ключевые слова: *международное сотрудничество, международная информационная безопасность, информационная война, информационный терроризм, информационные правонарушения, образовательная программа.*

D. A. Astakhov

ISSUE OF PERSONNEL TRAINING TO ENSURE INTERNATIONAL INFORMATION SECURITY

The article shows the conflict arisen between basic areas of international cooperation in the domain of international information security and the content of new Russian education programs for international lawyers. Basing upon the analysis of Russian project "Convention of International Information Security" and the contents of foreign education programs, the author substantiates the necessity of improvement of the third generation of Federal State Education Standards (FGOS-3) in the area of "International Relation".

Keywords: *International cooperation, international information security, information war, information terrorism, information crimes, education program.*

Развитие глобального информационного общества носит необратимый характер, и, как любая культурная трансформация, вместе с позитивными последствиями вызывает и негативные проявления, усиливая угрозы правам человека, общественной нравственности и информационной безопасности государств. Совет Европы, НАТО, США, Великобритания, Канада и другие государства приняли свои стратегии кибербезопасности. Од-

нако очевидно, что столь глобальная проблема не может быть решена силами каждого отдельного государства – необходима консолидация международного сообщества для обеспечения международной информационной безопасности. Возможность деструктивных воздействий на информационные инфраструктуры различных государств и опасность их многократного повторения свидетельствуют о том, что пришло время выработки совместных решений относительно форм, методов и способов международного сотрудничества в области противодействия этим угрозам. Научное осмысление данной проблемы началось не только за рубежом, но и в России (1, 2 и др.).

А. В. Яковенко выделяет 5 основных направлений международного сотрудничества в области информационной безопасности:

1. Недопущение враждебного использования информационных и телекоммуникационных технологий в военно-политических и террористических целях. Противодействие компьютерной преступности, создание условий для дальнейшего интенсивного развития трансграничного информационного взаимодействия, а также обеспечение свободы распространения информации в глобальном информационном пространстве.

2. В условиях развивающегося информационного обмена, открытости сети Интернет, разветвленного характера социальных сетей информационное пространство становится все более привлекательным для террористических организаций и лиц, причастных к террористической деятельности. В рамках усилий по предотвращению негативного использования информационного пространства важное место отводится борьбе с компьютерной преступностью.

3. Обеспечение безопасности объектов критической информационной инфраструктуры. Эта проблема чрезвычайно актуальна, и в ее решении могли бы сыграть значительную роль распространение лучшего опыта и организация центров оказания консультативной помощи тем государствам, которые в этом нуждаются. Кроме того, достаточно перспективным представляется достижение межгосударственных договоренностей относительно взаимного уведомления о попытках организации компьютерных атак на инфраструктуры критически важных объектов, а также совместного поиска злоумышленников.

4. Обеспечение трансграничного информационного взаимодействия. Это динамично развивающая сфера приложения достижений информационных и телекоммуникационных технологий. Однако ее функционирование возможно только при условии устойчивости и безопасности глобального информационного пространства, во многом базирующегося на глобальной информационной инфраструктуре и, в частности, на сети Интернет.

5. Обеспечение свободы распространения информации в глобальном информационном пространстве (2).

Считаем необходимым дополнить названный перечень еще двумя актуальными направлениями международного сотрудничества в области информационной безопасности.

Первое направление – разработка межгосударственной программы повышения уровня информированности международного сообщества об угрозах информационной безопасности, формирования культуры информационной безопасности граждан. Начиная с 2009 года, США, Великобритания, Канада и ряд других стран опубликовали свои национальные стратегии кибербезопасности, согласно которым в этих странах запущены масштабные программы от воспитания населения в духе понимания киберугроз до создания государственных центров мониторинга безопасности по всей стране. Например, в США уже несколько лет проходит общенациональный месячник осведомленности населения по вопросам информационной безопасности. Он открывается президентом и в нем участвует огромное количество людей, общественных организаций, государственных структур. Как образно заметил М. И. Гришанков, «там бьют в информационный набат, начиная от детских садов, заканчивая министерствами и ведомствами» (3).

Второе направление – подготовка квалифицированных кадров для обеспечения международной информационной безопасности, на чем мы остановим более пристальное внимание.

28 октября 2010 года в ходе 65-й сессии Генеральной Ассамблеи ООН Первым комитетом Генассамблеи консенсусом был принят обновленный российский проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая призывает к рас-

смотрению существующих и потенциальных угроз в сфере информационной безопасности, определению основных понятий, оценке целесообразности разработки соответствующих международных принципов. Число соавторов российского проекта увеличилось до 36 государств и включает всех наших партнеров по Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества и другие государства, такие как США, Япония, Германия и Канада.

Итоги деятельности Группы правительственных экспертов ООН по международной информационной безопасности, международные договоры в этой области, консультации экспертов и представителей научных кругов, многочисленные конференции и семинары по данной проблематике делают очевидной необходимость принятия под эгидой ООН акта, определяющего правила поведения государств в информационном пространстве и позволяющего объединить их усилия по противодействию угрозам в информационной сфере. Видение России таких форм и принципов закреплено в распространенном в качестве официального документа 66-й сессии Генеральной Ассамблеи ООН проекте «Правила поведения в области обеспечения международной информационной безопасности». Это совместная инициатива России, Китая, Узбекистана и Таджикистана, основная цель которой – стимулировать широкое международное обсуждение данной проблематики на мировой арене.

Главной задачей «Правил» является выработка кодекса ответственного поведения государств в сфере международной информационной безопасности с учетом военно-политических, криминальных и террористических вызовов и угроз. Документ предполагает противодействие использованию информационных и телекоммуникационных технологий в целях, не совместимых с задачами обеспечения международной стабильности, мира и безопасности. Он также предусматривает соблюдение прав и свобод человека в информационном пространстве, уважение суверенитета, территориальной целостности и политической независимости всех государств, а также создание многостороннего транспарентного и демократического международного механизма регулирования сети Интернет.

На второй международной встрече высоких представителей, курирующих вопросы безопасности, в Екатеринбурге (21–22 сентября 2011 года) Россия представила концепцию Конвенции об обеспечении международной информационной безопасности. По мнению главы Минкомсвязи России И. О. Щеголева, предложенная концепция Конвенции об обеспечении международной информационной безопасности заложит основу для выработки универсальной международной конвенции под эгидой ООН и позволит объединить усилия мирового сообщества на этом направлении (4).

Согласно проекту Конвенции, международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. В документе сформулированы основные угрозы международной безопасности в информационной сфере, предложена система мер по противодействию этим угрозам: меры предотвращения и разрешения военных конфликтов в информационном пространстве; меры противодействия использованию информационного пространства в террористических целях; меры противодействия правонарушениям в информационном пространстве.

Каждое из трех названных направлений обеспечения международной информационной безопасности весьма специфично и имеет инновационный характер для практики международных отношений. Очевидно, что решение столь актуальных, новых и масштабных задач в области международной информационной безопасности требует соответствующего кадрового обеспечения. Специалистов в этой области и в России, и за ее пределами готовят в рамках направления «Международные отношения».

Сравнительный анализ программ бакалавриата по направлению «Международные отношения» в России (ФГОС-3) и Австралии (The University of Queensland) выявил результат не в пользу России. Австралийская программа, в отличие от российской, методологически основана на проблемах международной безопасности. Так, в числе профессиональных дисциплин, изучаемых будущими австралийскими бакалаврами международных отношений, в названном университете изучаются: Проблемы азиатско-тихоокеанской безопасности; Терроризм и его вмешательство в международную политику; Между-

народная безопасность; Вооруженные силы и политика; США и эволюция международного порядка; Безопасность человека в международной политике; Разведка и национальная безопасность; Права человека и международная политика; Власть и мировой порядок; Этика в международной политике (5).

В числе профессиональных компетенций в российском ФГОС-3 по направлению «Международные отношения» для подготовки бакалавров названы «умение и навыки слежения за динамикой основных характеристик среды международной безопасности и понимание их влияния на национальную безопасность России (ПДК-3)», однако профессиональными дисциплинами эти компетенции почти не подкреплены. Единственной дисциплиной стандарта, формирующей названные компетенции, является «Основы международной безопасности». Остальные дисциплины: БЖД, История международных отношений 1900–1991, Современные международные отношения 1991–2010, Мировая политика, Теория международных отношений, Теория и история дипломатии, Экономические и политические процессы в СНГ (6).

Примерная основная образовательная программа высшего профессионального образования для подготовки магистра по направлению 031900 «Международные отношения», утвержденная в МГИМО, не содержит дисциплину «Международная информационная безопасность», в отличие от «Международной энергетической безопасности». Правда, в примерный учебный план по направлению магистратуры включены дисциплины, в рамках которых гипотетически могли бы изучаться вопросы международной информационной безопасности: «Глобальная безопасность», «Новые риски в международной политике», «Безопасность и сотрудничество приграничных территорий». Однако в аннотациях к названным дисциплинам нет даже упоминания о проблемах международной информационной безопасности. Так, структура курса «Глобальная безопасность» предполагает изучение следующих тем: Фактор безопасности в международных отношениях и мировой политике; Теоретические подходы к анализу логики глобальной безопасности; Новые параметры современной глобальной безопасности; Формирование новой повестки дня глобальной безопасности; Контроль над вооружением; Правовые аспекты глобальной безопасности; Региональное измерение глобальной безопасности; Проблемы безопасности на Ближнем и Среднем Востоке; Проблемы безопасности в АТР; Европейская безопасность; Формирование региональной безопасности на евразийском постсоветском пространстве; Перспективы формирования новой системы глобальной безопасности (7).

Таким образом, ФГОС-3 по направлению «Международные отношения» не соответствуют актуальным требованиям сегодняшнего времени, в котором небывалую остроту приобрели проблемы международной безопасности и международной информационной безопасности. Из этого следует, что начавшаяся в 2011 году подготовка бакалавров и магистров по международным отношениям по новым образовательным стандартам, если ничего не менять, ничего не принесет, кроме неспособности выпускников-международников противодействовать информационным войнам, информационному терроризму, а также информационным правонарушениям в международном пространстве. Надеемся, что России удастся избежать столь пессимистичного сценария и новое поколение международников сможет внести свой ощутимый вклад в обеспечение международной информационной безопасности.

Список литературы

1. *Федоров, А. В.* Информационная безопасность в мировом политическом процессе. – М.: Изд-во «МГИМО-Университет», 2006.–219 с.

2. *Яковенко, А. В.* London-Cyber: как можно противодействовать угрозам информационной безопасности (Электронный ресурс)// http://rus.rusemb.org.uk/article/85

3. Выступление М. И. Гришанкова на Инфофоруме-2012. (Электронный ресурс) // http://2012.infoforum.ru/2012/program

4. Выступление главы Минкомсвязи России И. О. Щеголева на Международной конференции по вопросам киберпространства в Лондоне (Электронный ресурс) //http://rus.rusemb.org.uk/article/89

5. Bachelor of International Studies (BIntSt) – Course List. Information valid for students commencing 2012 // The University of Queensland, Australia: Официальный сайт. (Электронный ресурс) http://www.uq.edu.au/study/program_list.html?acad_prog=2316

6. Примерная основная образовательная программа ВПО для подготовки бакалавра по направлению «Международные отношения» // Московский государственный институт международных отношений: Официальный сайт. (Электронный ресурс) http://www.mgimo.ru/files/8972/int-rel_bac.pdf

7. Примерная основная образовательная программа ВПО для подготовки магистра по направлению «Международные отношения» // Московский государственный институт международных отношений: Официальный сайт. (Электронный ресурс) http://www.mgimo.ru/files/8972/int-rel_mag.pdf

---

Астахов Дмитрий Александрович, студент ЮУрГУ. E-mail: urvest@mail.ru

РЕГИОНАЛЬНЫЙ АТТЕСТАЦИОННЫЙ ЦЕНТР ЮУрГУ

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

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

2) осуществление мероприятий по оказанию услуг в данной области;

3) повышение квалификации сотрудников режимно-секретных подразделений.

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

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

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

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

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

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

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

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

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

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

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

Программа предусматривает изучение следующих дисциплин:

1) Правовое и нормативное обеспечение защиты государственной тайны;

2) Организация комплексной защиты информации в организациях;

3) Организация режима секретности в организации;

4) Организация защиты информации, обрабатываемой средствами вычислительной техники;

5) Организация защиты информации при осуществлении международного сотрудничества;

6) Допуск граждан к сведениям, составляющим государственную тайну;

7) Организация и ведение секретного делопроизводства;

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

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

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

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

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

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

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

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

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

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

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

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

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

Контактные адреса и телефоны:

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

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

Редакция просит авторов при направлении статей в печать руководствоваться приведенными ниже правилами и прилагаемым образцам 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)	

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 «Проблемы права».
Или по почте по адресу:
Россия, 454091, г. Челябинск, ул. Васенко, д. 63, оф. 401.

ВЕСТНИК УрФО
Безопасность в информационной сфере № 1(3)/2012

Подписано в печать 30.03.2012. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 6,30. Тираж 300 экз. Заказ 167/355.
Цена свободная.

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