Министерство юстиции Российской Федерации

Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции Российской Федерации»

ПРАВОВАЯ ИНФОРМАТИКА

Периодический научный журнал

Выпуск № 3 – 2012

Москва, 2012

УДК [004:342.951](470+571)
ББК 67.401.114(2Рос)
П 54

Правовая информатика. Выпуск 3–2012. — М. : ФБУ НЦПИ при Минюсте России, 2012. — 68 с.

ISSN 1994-1390

Редакционная коллегия

Сергин М.Ю	Главный редактор, доктор технических наук, профессор
Горбачева Е.В.	
Колмыкова И.Г.	
Макаренко Г. И.	
Матвиенко Ю.В.	кандидат медицинских наук
Морозов А.В.	доктор юридических наук, професор
Филатова Л.В.	кандидат юридических наук, старший научный сотрудник
Челнокова О.В.	ответственный секретарь

Редакционный Совет

Морозов А.В.	Председатель Совета, доктор юридических наук, профессор
Астанин В.В.	доктор юридических наук
Батурин Ю.М.	доктор юридических наук, профессор
Горбачева Е.В.	
Зубрин В.В.	кандидат юридических наук
Королев С.М.	
Макаренко Г.И.	
Матвиенко Ю.В.	кандидат медицинских наук
Михалевич В.В.	
Павлов И.Н.	кандидат юридических наук
Полякова Т.В.	доктор юридических наук, профессор
Рассолов И.М.	доктор юридических наук, профессор
Севостьянов В.Л.	кандидат технических наук
Сергин М.Ю	доктор технических наук, профессор
Филатова Л.В.	кандидат юридических наук, старший научный сотрудник

«Журнал» «Правовая информатика» является периодическим рецензируемым изданием. Подписка на журнал на 2013 год производится по объединенному каталогу «Пресса России» или направив письмо в редакцию.
Индекс подписки: 44723
Адрес редакции: 125437, Москва, Михалковская ул, 65, стр.1
Телефон: +7495-459-0504 (с 15 до 17 час), E-mail: informatika@scli.ru

ISSN 1994-1390 **© ФБУ НЦПИ при Минюсте России, 2012**

СОДЕРЖАНИЕ

Белявский Алексей Анатольевич, Комендантова Елена Владимировна
Организационно-правовая система правоохранительной деятельности противодействия правонарушениям в информационной сфере Российской Федерации 4

Бойченко Игнат Сергеевич
Актуальные вопросы развития информационного общества 9

Гобрусенко Константин Иванович, Коновалова Юлия Викторовна
Актуальные вопросы организации информационного обеспечения аналитических подразделений Росфинмониторинга 13

Евстифеева Наталья Александровна, Крылов Григорий Олегович, Рябков Виктор Ефимович
Признаковое пространство в задачах анализа репутационных рисков кредитных организаций как субъектов финансовой и информационной безопасности 17

Иванова Анна Юрьевна
Организационно-правовые методы защиты интеллектуальной собственности на созданные программные средстваи. 19

Крылов Григорий Олегович
Проблемы защиты информации при переводе денежных средств в Национальной платежной системе 25

Морозов Антон Андреевич, Арутюнова Лусине Борисовна
Формирование единого пространства юридически значимого электронного взаимодействия . . . 27

Никитина Виктория Леонидовна
Проблемы мониторинга универсальных электронных карт в национальной платежной системе 31

Гобрусенко Константин Иванович, Рябков Виктор Ефимович
Правовые вопросы информационного обеспечения аналитических подразделений Росфинмониторинга 33

Филатова Людмила Васильевна, Михалевич Владимир Владимирович
Информационно-правовые учетные системы федеральных органов исполнительной власти в «электронном государстве» 37

Бекетнова Юлия Михайловна, Крылов Григорий Олегович, Фомин Ярослав Алексеевич
Выявление рисков нарушения финансовой и информационной безопасности 44

Чеботарева Анна Александровна
Механизмы электронной демократии: возможности и проблемы их реализации в Российской Федерацие 49

Шамков Николай Степанович
Организационно-правовые проблемы внедрения системы электронного документооборота (СЭД) в органах государственного управления по материалам федеральной службы судебных приставове 54

Сведения об авторах 61

Annotations and key words 63

Белявский Алексей Анатольевич
Комендантова Елена Владимировна

Организационно-правовая система правоохранительной деятельности противодействия правонарушениям в информационной сфере Российской Федерации

Аннотация: *Рассматриваются ключевые вопросы информатизации деятельности правоохранительных органов в связи с изменениями в текущем законодательстве Российской Федерации. Показано, что информационная безопасность правотворческой и правоприменительной деятельности – приоритетная задача на ближайшее время.*

Ключевые слова: *информационная безопасность, информация, информационная сфера, правоохранительные органы, общедоступные сведения, информационные правонарушения.*

Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)» [1] в сфере обеспечения безопасности в информационном обществе определила такие, как:

- противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам Российской Федерации;
- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасности информации ограниченного доступа;
- обеспечение развития законодательства Российской Федерации и совершенствование правоприменительной практики в области информационных и телекоммуникационных технологий.

Для противодействия правонарушениям в информационной сфере в 2000 году была принята Доктрина информационной безопасности Российской Федерации, которая не потеряла свою актуальность до сих пор, и ряд федеральных законов, с помощью которых возможно принятие мер для обеспечения безопасности в информационной сфере.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения по использованию информации [2].

Данный Федеральный закон раскрывает понятие «обладатель информации» и устанавливает его права и обязанности.

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

- Обладатель информации при осуществлении своих прав обязан:
- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации [3]. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации [4].

В соответствии с федеральным законом «Об информации, информационных технологиях и о защите информации» в Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Этот закон определяет информацию как объект общественных отношений, а так же подразделяет её по категориям доступа: в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Также, законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Эта информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации [5].

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

При этом запрещено распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

На распространение прочей информации могут налагаться ограничения: ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами либо другими физическими лицами при исполнении ими профессиональных обязанностей или

организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами или по решению суда. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина, предоставившего такую информацию о себе.

Конституция Российской Федерации закрепляет за гражданами право на неприкосновенность частной жизни и семейную тайну [6]. Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещается требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина, если иное не предусмотрено федеральными законами. Порядок доступа к персональным данным граждан устанавливается федеральным законом «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [7]. За незаконное разглашение подобного рода информации установлена правовая ответственность.

Основными элементами организационной основы системы противодействия информационным правонарушениям в Российской Федерации (далее – РФ) являются: Президент РФ, Совет Федерации и Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и другие государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, в соответствии с законодательством РФ участвующие в решении задач обеспечения информационной безопасности РФ [8].

Президент РФ в пределах своих конституционных полномочий руководит органами и силами по обеспечению информационной безопасности РФ; санкционирует действия по обеспечению информационной безопасности РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности РФ; определяет в своих ежегодных посланиях Федеральному Собранию РФ приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания РФ на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности РФ.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию РФ приоритетных направлений в области обеспечения информационной безопасности РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности РФ, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности РФ, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности РФ, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента РФ в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту РФ и в Правительство РФ.

Межведомственные и другие государственные комиссии, создаваемые Президентом РФ

и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности РФ.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности РФ, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности РФ; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ.

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности РФ.

Органы судебной власти осуществляют правосудие по делам о правонарушениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ. В состав системы обеспечения информационной безопасности РФ могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности РФ, перечисленных в Доктрине информационной безопасности, предполагала разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом РФ [9].

Приоритетным направлением государственной деятельности в системе противодействия информационным правонарушениям является совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, которое предусматривает следующие меры: оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования; создание организационно-правовых механизмов обеспечения информационной безопасности; определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере; создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления; разработку проектов нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий; разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе; совершенствование системы подготовки соответствующих кадров [10].

Правовое регулирование отношений в информационной сфере должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере. Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом. Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ, при решении возникающих в информационной сфере конфликтов, неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере. Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ. Реализация гарантий конституционных прав и свобод человека и

гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства. Для организации реализации государственной деятельности в данной сфере предназначена система обеспечения информационной безопасности Российской Федерации [11].

Литература.

1. СЗ РФ. – 2010. – № 46. – Ст. 6026
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Ч. 1).
3. См. О средствах массовой информации: Закон Российской Федерации от 27.12.1991 № 2124-I // Ведомости Съезда народных депутатов и Верховного Совета РСФСР. – 1992. – № 7.- Ст. 300.
4. См. Об архивном деле в Российской Федерации: Федеральный закон от 22.10.2004 № 125-ФЗ // СЗ РФ. – 2004. – № 43. – Ст. 4169.
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Ч. 1).
6. Конституция Российской Федерации от 12.12.1993 // РГ. 1993. 25 дек.
7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (Ч. 1).
8. Доктрина информационной безопасности Российской Федерации, утв. Президентом РФ 09.09.2000 № Пр-1895 //РГ. 2000. 28 сент.
9. Доктрина информационной безопасности Российской Федерации, утв. Президентом РФ 09.09.2000 № Пр-1895 //РГ. 2000. 28 сент.
10. См.: В.В. Ершов, Д.А. Ловцов «Информационные отношения и право» Сборник научных трудов, выпуск первый, Москва 2006 г.
11. См.: Международные аспекты информационной безопасности//Бизнес и безопасность в Росси. 2007. №46. С.63

рецензент: ***Филатова Людмила Васильевна***
кандидат юридических наук, старший научный сотрудник

Бойченко Игнат Сергеевич

Актуальные вопросы развития информационного общества

Аннотация: *Проведен информационно-правовой обзор законодательства в сфере электронного взаимодействия государства и граждан, государственных органов, а также предоставления государственных услуг. Предложены меры по совершенствованию взаимодействия институтов информационного общества.*

Ключевые слова: *Общество, законодательство, информация, государство, услуги, взаимодействие.*

Информационное общество, как объект научного исследования, является очень многогранным и изучается различными науками: социологией, философией, политологией, юриспруденцией. В данной статье автор хочет рассмотреть наиболее актуальные вопросы развития информационного общества – электронное взаимодействие и электронные услуги.

В начале XXI века мировое сообщество разработало основы в информационного общества и закрепило их международных актах: Окинавская хартия Глобального информационного общества [1], Декларация принципов «Построение информационного общества». Положения этих международных документов дополнены статьей 19 Всеобщей декларации прав человека «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» [2].

Для Российской Федерации вопросы в сфере электронного взаимодействия, электронных услуг являются актуальными:

- во-первых, информационные технологии развиваются быстро, ежегодный прирост около 12 процентов [3];
- во-вторых, государственная политика направлена на развитие данной сферы;
- в-третьих, IT-сфера для международных рынков является одной из самых перспективных и быстрорастущих в мире, с учетом вступления России в ВТО, Россия может стать крупным «игроком» в данной сфере;
- в-четвертых, с помощью развития информационных технологий Россия может перейти от сырьевой экономики к высокотехнологичному и интеллектуальному производству и продукции, как основной составляющей экономики в информационном обществе.

В последние годы сформированы основные направления и принципы построения информационного общества, и они прописаны в Доктрине информационной безопасности Российской Федерации от 09.09.2000 № Пр-1895, в Стратегии развития информационного общества в Российской Федерации от 07.02.2008 № Пр-212, в Государственной программе Российской Федерации «Информационное общество» (2011 – 2020 годы) от 20.10.2010 №1815. Данные нормативно-правовые акты составляют базис правового регулирования построения информационного общества.

Дополняют положение вышеуказанных нормативно-правовых актов Федеральные законы: от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», от 09.02.2009. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», от 27.07.2010 № 210-ФЗ» Об организации предоставления государственных и муниципальных услуг» установили конституционно-правовой механизм реализации права на информацию, от 06.04.2011 № 63-ФЗ «Об электронной подписи, от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Стоит отметить, что Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации пре-

доставления государственных и муниципальных услуг» регламентирует порядок предоставления гражданам государственных и муниципальных услуг. Федеральный закон определяет принципы предоставления государственных и муниципальных услуг:

1) правомерность;
2) заявительный порядок обращения;
3) правомерность взимания с заявителей государственной пошлины;
4) открытость деятельности органов;
5) доступность обращения за предоставлением государственных и муниципальных услуг и предоставления государственных и муниципальных услуг, в том числе для лиц с ограниченными возможностями здоровья;
6) возможность получения государственных и муниципальных услуг в электронной форме [4].

«Повышение качества и доступности предоставляемых организациям и гражданам государственных услуг, упрощение процедуры и сокращение сроков их оказания, снижение административных издержек со стороны граждан и организаций, связанных с получением государственных услуг, а также внедрение единых стандартов обслуживания граждан.

Повышение открытости информации о деятельности органов государственной власти и расширение возможности доступа к ней и непосредственного участия организаций, граждан и институтов гражданского общества в процедурах формирования и экспертизы решений, принимаемых на всех уровнях государственного управления» [5].

Министерство связи и массовых коммуникаций Российской Федерации определило цели, направленные на повышения качества жизни в России с 2012 года по 2018 гг.[6]. Одним из приоритетных направлений являются электронные услуги, как составляющая информационного общества.

В связи с этим выделены следующие цели и задачи:

- возможность получить 100% государственных услуг самостоятельно и в любое время;

«Задача Минкомсвязи России — ускорить информатизацию органов государственной власти, чтобы полностью избавить жителей от необходимости собирать пакеты документов».

- 80% государственных услуг предоставляются в электронном виде;

Задача Минкомсвязи России — обеспечить эффективную и удобную работу портала государственных услуг, системы межведомственного электронного взаимодействия и гарантировать доступность всех госуслуг в электронном виде в любом регионе России. Необходимо создать среду, позволяющую сотням ИТ-компаний создавать полезные для жителей приложения и сервисы и интегрировать их с «электронным правительством».

- возможность оценить качество каждой оказанной государственной услуги;

«Задача Минкомсвязи России — через законодательные инициативы и автоматизацию обеспечить выполнение этого принципа всеми госорганами».

Министерством Юстиции Российской Федерации осуществляется предоставление государственных услуг в электронном виде: ведение государственного реестра казачьих обществ в Российской Федерации, предоставление информации физическим и юридическим лицам о зарегистрированных некоммерческих организациях, филиалах и представительствах иностранных некоммерческих неправительственных организаций, ведение реестров адвокатов субъектов Российской Федерации и выдаче адвокатам удостоверений, проставление в установленном порядке апостиля на официальных документах, подлежащих вывозу за границу и др.

Для успешного решения задач государственного управления в современном мире необходимо активное электронное взаимодействие государства и общества, а также переход к электронному взаимодействию между государственными органами. В этой связи необходимо отметить Постановление Правительства № 890 от 06.09.2012 г. «О мерах по совершенствованию электронного документооборота в органах государственной власти». Данное Постановление регламентирует обмен электронными документами. Стартует пилотный проект по обмену электронными документами «В период с 1 марта по 1 сентября 2013 г. осуществить реализацию пилотных проектов электронного документооборота между Аппаратом Правительства Российской Федерации и Министерством связи и массовых коммуникаций Российской Федерации, а также между Министерством связи и массовых коммуникаций Российской Федерации и Министерством юстиции Российской Федерации в части государственной регистрации нормативных правовых актов Министерства связи и массовых коммуникаций Российской Федерации».

Изменения коснулись и судебной системы РФ, а именно в возможности предоставления документов в электронном виде. В АПК были внесены соответствующие изменения.

Лица, участвующие в деле, вправе представлять в арбитражный суд документы в электронном виде, заполнять формы документов, размещенных на официальном сайте арбитражного суда в сети Интернет, в порядке, установленном в пределах своих полномочий Высшим Арбитражным Судом Российской Федерации [7].

А также получение судебных актов в электронном виде. Информация о деятельности судов может предоставляться в устной форме и в виде документированной информации, в том числе в виде электронного документа [8].

В статье 8 Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» перечислены права пользователя

Пользователь информации имеет право:

1) получать достоверную информацию о деятельности государственных органов и органов местного самоуправления;
2) отказаться от получения информации о деятельности государственных органов и органов местного самоуправления;
3) не обосновывать необходимость получения запрашиваемой информации о деятельности государственных органов и органов местного самоуправления, доступ к которой не ограничен;
4) обжаловать в установленном порядке акты и (или) действия (бездействие) государственных органов и органов местного самоуправления, их должностных лиц, нарушающие право на доступ к информации о деятельности государственных органов и органов местного самоуправления и установленный порядок его реализации;
5) требовать в установленном законом порядке возмещения вреда, причиненного нарушением его права на доступ к информации о деятельности государственных органов и органов местного самоуправления [9].

Законодательство Российской Федерации гарантирует гражданину право на доступ к информации, получения, распространения информации. Но реализовать это право гражданину сложно по следующим причинам:

1) нет технической возможности пользоваться электронными услугами [10];
2) неправомерные действия или бездействия должностных лиц [11];
3) недостаточные меры и механизм ответственности должностных лиц [12];
4) недостаточное внедрение и распространение специального программного обеспечения, либо его высокая стоимость.

В настоящее время активно развивается нормативно – правовая база в сфере электронного взаимодействия, электронных услуг, информационного общества и информационных технологий. Активно внедряются информационные технологии в государственные органы, в бизнес, в образование, медицину, что соответствует общей государственной политики в этой сфере. Существует и ряд проблем, технологического, технического, и правового характера. Поэтому нормативная база в этой сфере будет активно совершенствоваться и развиваться. Развитие государственных и муниципальных услуг с помощью ИКТ, является верным шагом и делает государственные и муниципальные услуги удобнее и доступнее, а электронный документооборот может сократить бюрократические и другие издержки. Государственные услуги в XXI должны быть доступными, оперативными, актуальными, достоверными.

Литература.

1. ст. 9 Окинавская хартия Глобального информационного общества от 22.07.2000 // Государственная политика информационной безопасности (основные документы). – Екатеринбург: Изд-во УрГЮА, 2001.
2. Всеобщая декларация прав человека, принята Генеральной Ассамблеей ООН 10.12.1948 // РГ. 1995. 5 апр.
3. Цели Минкомсвязи России http://2018 minsvyaz.ru/#1-1 – официальный сайт Минкомсвязи России (дата обращения 11.11.2012)

4. статья 4 Федеральный закон от 27.07.2010 # 210-ФЗ» Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. – № 31. – Ст.4179.,

5. Распоряжение Правительства Российской Федерации от 06.05.2008 №632-р «Об одобрении Концепции формирования в Российской Федерации электронного правительства до 2010 года» // СЗ РФ. 2008. №20. Ст.2372.
6. Цели Минкомсвязи России http://2018. minsvyaz.ru/#s – официальный сайт Минкомсвязи России (дата обращения 11.11.2012)

7. См.Приказ Высшего Арбитражного Суда Российской Федерации от 12.01.2011 №1 «Временный порядок подачи документов в арбитражные суды Российской Федерации в электронном виде» // Текст документа официально опубликован не был.// Консультант плюс.
8. См. Федеральный закон от 22.12.2008 №262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 2008. № 52 (ч.I). Ст.6217.
9. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст.776.
10. 55 миллионов Россиян пользуются сетью активно. http://www.rg.ru/2011/12/26/shyogolev-anons.html
11. Решением от 06.02.2006 Арбитражного суда г. Москвы по делу N А40-70178/05-106-546 Суд признал незаконным отказ о предоставлении кадастрового плана.
12. Статья 25. Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» устанавливает ответственность должностного лица, но нет механизма применения данной нормы.

рецензент: ***Морозов Андрей Витальевич***,
доктор юридических наук, профессор

Гобрусенко Константин Иванович,
кандидат юридических наук,
Коновалова Юлия Викторовна

Актуальные вопросы организации информационного обеспечения аналитических подразделений Росфинмониторинга

Аннотация: *Рассматриваются вопросы организации информационного обеспечения аналитических подразделений Росфинмониторинга в интересах противодействия легализации (отмывания) преступных доходов и финансирования терроризма.*

Ключевые слова: *противодействие легализации (отмыванию) денег, информационные ресурсы аналитических подразделений Росфинмониторинга, автоматизация информационных процессов, финансовое расследование.*

Введение

Результативность борьбы с преступными деяниями в сфере противодействия легализации (отмыванию) преступных доходов и финансированию терроризма (ПОД/ФТ) во многом зависит от надлежащей организации ее информационного обеспечения, представляющего собой систему сбора, обработки, накопления и использования информации, имеющей значение для выявления, предупреждения и раскрытия преступлений в сфере ПОД/ФТ, а так же от организации и проведения финансовых расследований.

Актуальность темы следует из анализа практики информационного обеспечения аналитических подразделений Федеральной службы по финансовому мониторингу (далее – Росфинмониторинг), который свидетельствует о том, что руководители и сотрудники этих подразделений испытывают настоятельную необходимость в получении различных видов сведений из министерств, служб, агентств и юридических лиц, не относящихся к организациям, перечисленным в Федеральном законе № 115-ФЗ [1]. Однако фактическая обеспеченность необходимыми данными не соответствует их информационным потребностям, что является одним из сдерживающих факторов повышения эффективности исполнения возложенных на Росфинмониторинг функций по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Особое значение для аналитиков имеет любая социальная информация, содержащая сведения, которые возможно использовать с целью борьбы с преступностью. Такие сведения должны обладать следующими необходимыми свойствами: иметь отношение ко всему процессу борьбы с преступностью или к какому-либо его элементу, быть конкретными, достаточно полными и достоверными.

Федеральная служба по финансовому мониторингу является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также по выработке государственной политики, нормативно-правовому регулированию и координации деятельности в этой сфере иных федеральных органов исполнительной власти. Росфинмониторинг осуществляет полномочия, возложенные Постановлением Правительства РФ «Об утверждении положения о Федеральной службе по финансовому мониторингу»[2].

Задачи, функции и полномочия Федеральной службы по финансовому мониторингу в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма устанавливаются в соответствии с Федеральным законом 115-ФЗ.

Одним из условий успешного решения задач в сфере противодействия отмывания доходов, полученных преступным путем, и финансирования терроризма является предварительный сбор, обработка, накопление и последующий

анализ информации, указывающей на различные признаки противоправной деятельности в сфере противодействия легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Многообразие способов совершения предикатных преступлений и преступлений, связанных с легализацией преступных доходов и финансирования терроризма, соединенное с применением различных и разнообразных приемов и средств маскировки существенно затрудняет обнаружение признаков таких преступлений. Вместе с тем для различных способов совершения преступлений в сфере ПОД/ФТ характерна устойчивая повторяемость, объективно обусловленная системой функционирования финансового механизма хозяйствующих субъектов экономики России, что позволяет проанализировать методы и тенденции (типологии) отмывания преступных доходов и создает предпосылки для описания использования современных информационных технологий в выявлении, предупреждении и раскрытии преступлений данной категории. Как показывает практика, в отдельных случаях только при помощи современных информационных технологий становится возможным выявление фактов легализации (отмывания) преступных доходов. Следовательно, научная разработка методик выявления фактов легализации преступных доходов и финансирования терроризма и применение при осуществлении финансового мониторинга современных информационных технологий является важным резервом повышения результативности проводимых правоохранительными и финансовыми органами мер по ПОД/ФТ и представляет важную в теоретическом и практическом отношении проблему.

Информационное обеспечение аналитических подразделений Росфинмониторинга формируется на основе различных информационных ресурсов, которые накапливаются в рамках разнообразных информационных систем.

Как показывает изучение практики, с позиции интересов информационного обеспечения аналитических подразделений на основе современных технологий, все информационные ресурсы целесообразно подразделять на две основные группы:

1) собственные информационные ресурсы аналитических подразделений Росфинмониторинга;
2) информационные ресурсы сторонних организаций, содержащие сведения, позволяющие характеризовать юридических и физических лиц и их финансово-хозяйственную деятельность.

К собственным информационным ресурсам аналитических подразделений Росфинмониторинга относятся:

- база данных сообщений об операциях, подлежащих контролю в соответствии с законодательством Российской Федерации;
- база данных (автоматизированное рабочее место, далее АРМ) «Спецделопроизводство».

Основным источником информации, используемой в деятельности Росфинмониторинга, для базы данных операций являются организации, осуществляющие операции с денежными средствами или иным имуществом. В соответствии с требованиями Федерального закона № 115-ФЗ эти организации предоставляют информацию в виде инициативных сообщений об операциях, подлежащих обязательному контролю, и о подозрительных операциях, выявляемых в процессе внутреннего контроля, а также в виде отчетов на информационные запросы Росфинмониторинга.

АРМ «Спецделопроизводство» предназначено для накопления, обработки, систематизации и хранения информации о документально подтвержденных фактических результатах мероприятий, проводимых аналитическими подразделениями Росфинмониторинга, а также поиска информации, координации деятельности и выявления пересечений по объектам, информационного обеспечения управленческой, аналитической и иной служебной деятельности упомянутых подразделений.

Для аналитических подразделений Росфинмониторинга особый интерес представляют справочные сведения, которые могут использоваться в идентификационных целях. Они могут содержаться как «в несистематизированной (разрозненной) документации, имеющейся в организациях, у должностных лиц и граждан, так и в различного рода ведомственных и вневедомственных картотеках и информационных массивах. Практика свидетельствует, что различные организации, учреждения, юридические и физические лица располагают автоматизированными информационными системами, содержащие информационные массивы в формате баз данных, сформированные на основе первичных документов.

В этой связи организация работы со второй группой информационных ресурсов предусматривает получение Росфинмониторингом от

организаций и индивидуальных предпринимателей и использование в поисково-справочной работе информационных массивов в формате баз данных, содержащих сведения о лицах и других объектах материального мира, об инфраструктуре экономики подведомственной территории, наличии природных ресурсов, демографических, миграционных и других особенностей регионов.

Для аналитических подразделений Росфинмониторинга особый интерес представляют справочные сведения, которые могут использоваться в идентификационных целях. Они могут содержаться как «в несистематизированной (разрозненной) документации, имеющейся в организациях, у должностных лиц и граждан, так и в различного рода ведомственных и вневедомственных картотеках и информационных массивах. Практика свидетельствует, что различные организации, учреждения, юридические и физические лица располагают автоматизированными информационными системами, содержащие информационные массивы в формате баз данных, сформированные на основе первичных документов.

В этой связи организация работы со второй группой информационных ресурсов предусматривает получение Росфинмониторингом от организаций и индивидуальных предпринимателей и использование в поисково-справочной работе информационных массивов в формате баз данных, содержащих сведения о лицах и других объектах материального мира, об инфраструктуре экономики подведомственной территории, наличии природных ресурсов, демографических, миграционных и других особенностей регионов.

В настоящее время Росфинмониторинг использует информационные ресурсы федеральных органов исполнительной власти и отдельных иных организаций, таких как Федеральной налоговой службы, Федеральной таможенной службы, Федеральной службы государственной статистики и др.

Например, информационные массивы налоговых органов «ЕГРЮЛ» и «ЕГРИП» содержат справочные сведения, которые используются аналитическими подразделениями Росфинмониторинга при проведении финансовых расследований в целях идентификации юридических лиц и индивидуальных предпринимателей, а также оценки их финансово-хозяйственной деятельности.

С развитием рыночных отношений и информационных технологий у Росфинмониторинга в связи с осуществлением своих функций возникает необходимость в получении информации, которой располагают юридические лица, не относящиеся к организациям, перечисленным в Федеральном законе № 115-ФЗ.

Практика свидетельствует, что различные организации (юридические лица) располагают автоматизированными информационными системами, содержащие предметно ориентированные информационные массивы в формате баз данных, накапливающие сведения в электронном виде, позволяющие ускорить анализ информации и которые могут быть использованы для эффективной реализации Федерального закона № 115-ФЗ. Доступ к информационным системам таких организаций (юридических лиц) может организовываться по письменным запросам или на основе двухсторонних соглашений об информационном взаимодействии.

Практика свидетельствует, что Росфинмониторинг с целью совершенствования информационного обеспечения аналитических подразделений, развития и использования информационных технологий не всегда может получать базы данных или организовать удаленный доступ к автоматизированным информационным системам различных организаций.

Во многих городских отделах записи актов гражданского состояния учетные данные заносятся в базы данных и вводятся в память ЭВМ. Данная информация оказывается востребованной при установлении: родственных связей; лиц, сменивших фамилию; юридических лиц и физических лиц с правом занятия предпринимательской деятельностью, зарегистрированных по паспортным данным умерших людей (что неоднократно встречается на практике), а также установлении родственных связей директорского корпуса крупных предприятий и руководителей государственных организаций.

Авиаперевозчики формируют базы данных, содержащие информацию о конкретных субъектах, пользующихся услугами воздушного транспорта, которые, в свою очередь, могут являться объектами расследования по делам Росфинмониторинга. Получение соответствующей информации из такой базы данных по субъекту, в отношении которого проводится финансовое расследование, позволит Росфинмониторингу с большой степенью достоверности обосновывать свои подозрения и устанавливать те или иные обстоятельства, имеющие существенное значение при реализации в рамках уголовно-процессуального законодательства

Российской Федерации собранных и переданных правоохранительным органам материалов. Вместе с тем, авиаперевозчики (юридические лица) не относятся к организациям, перечисленным в Федеральном законе № 115-ФЗ.

Для аналитических подразделений Росфинмониторинга, обеспечивающих обслуживание сферы оборота биоресурсов, большое значение имеют информационные массивы в формате баз данных, формируемые Федеральным агентством по рыболовству. Такие информационные массивы содержат справочные таблицы:

а) судовладельцев (идентификационные данные на юридических лиц, являющиеся владельцами промысловых судов);

б) морских портов, типов, назначений и состояний судов;

в) видов лова, орудий лова, объектов промысла;

г) режимов промысла, видов промысловых рыб, промысловых районов и портов; квот вылова.

Росфинмониторинг не располагает сведениями, необходимых для решения поставленных государством задач и содержащихся в банках данных Пенсионного фонда России, ГИБДД МВД России, Министерства юстиции Российской Федерации и ряда других организаций.

Размещение и интеграция на серверах Росфинмониторинга таких информационных массивов в формате баз данных позволяет создавать автоматизированный банк данных с целью поиска по нему сведений для последующего отождествления объектов финансовых расследований при проведении финансовых расследований. Такой банк данных условно назовем информационно-справочный банк данных вневедомственного характера.

Использование современных информационных технологий с целью автоматизации информационных процессов аналитических подразделений Росфинмониторинга и создания информационной системы на основе банка данных «информационно-справочного характера» является важным резервом повышения качества информационного обеспечения и результативности проведения финансовых расследований. Особое значение имеют банки данных двух групп ресурсов: собственные информационные ресурсы и информационные ресурсы сторонних организаций, которые позволяют наиболее эффективно решать стоящие перед аналитическими подразделениями задачи по выявлению признаков предикатных преступлений и фактов легализации.

В целях совершенствования правового регулирования информационного обеспечения служебной деятельности аналитических подразделений Росфинмониторинга ряд федеральных законов и иных нормативных правовых актов, мы считаем, необходимо дополнить положениями, дающих Росфинмониторингу право безвозмездно получать от федеральных министерств, служб, агентств, а также организаций независимо от форм собственности и физических лиц информационные массивы в формате баз данных, необходимые для решения поставленных перед ним государством задач, за исключением содержащих сведения, доступ к которым ограничен федеральными законами.

Выводы: назрела необходимость о нормативном закреплении обмена информационными массивами в формате баз данных между различными государственными структурами в целях повышения эффективности исполнения возложенных на них функций, а также о выделении координатора от Совета безопасности Российской Федерации при рассмотрении и подписании соглашений по информационному обмену и использованию автоматизированных информационных систем сторон.

Литература.

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», «Российская газета» от 29 июля 2006 г., N 165
2. Постановления Правительства РФ от 23.06.2004 N 307 «Об утверждении положения о Федеральной службе по финансовому мониторингу». «Российская газета» от 29 июня 2004 г., N 136,

Евстифеева Наталья Александровна

Крылов Григорий Олегович,
кандидат юридических наук

Рябков Виктор Ефимович

Признаковое пространство в задачах анализа репутационных рисков кредитных организаций как субъектов финансовой и информационной безопасности

Аннотация: *рассматривается проблема анализа кредитных организаций как субъектов финансовой и информационной безопасности. В статье приведены характеристики пространства признаков (признакового пространства) для репутационной оценки кредитных организаций.*

Ключевые слова: *оценка рисков, информационная безопасность, распознавание образов.*

Введение

Важнейшим условием обеспечения национальной безопасности государства является стабильность его экономической системы. Одним из основных элементов такой системы в любом развитом государстве являются кредитные организации, репутационные риски которых требуется оценивать.

Актуальность работы обусловлена тем, что на текущий момент особенно остро встает вопрос борьбы с коррупционными проявлениями и теневым сектором экономики. Необходимыми условиями их функционирования являются каналы, обслуживающие значительные объемы наличных денежных средств, мобильных финансовых инструментов, а также обеспечивающие вывод денежных средств за рубеж, в частности в оффшорные зоны. Обеспечение существенного объема этих потоков возможно только при непосредственном участии в процессе отдельных сотрудников банков, либо целиком конкретных проблемных кредитных организаций. Таким образом, своевременное выявление проблемных кредитных организаций является одним из важных аспектов поддержания стабильности и оздоровления экономики государства.

Одним из эффективных решений задачи выявления неблагонадежных кредитных организаций является их анализ в терминах теории распознавания образов [1]. Первым этапом данного исследования стало формирование признакового пространства.

Для целей всесторонней оценки благонадежности кредитной организации как ячейки экономической системы страны необходимо провести оценку следующих аспектов их функционирования:

- собственные экономические показатели банка;
- объем и состав клиентского портфеля банка;
- качество системы внутреннего контроля банка.

Каждый из перечисленных аспектов характеризуется своим набором признаков. Практически целесообразным представляется описанный ниже состав признакового пространства

I. Собственные экономические показатели банка:

1) Активы. Характеризуют объем имеющихся в распоряжении банка объектов собственности. Позволяют оценить благонадежность и устойчивость кредитной организации. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.
2) Капитал. Характеризует объем всего имеющегося в распоряжении банка имущества в денежном эквиваленте. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.

3) Ценные бумаги. Характеризует объем выпущенных организацией ценных бумаг. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

4) Обороты средств в банкоматах. Показывает интенсивность операций в банкоматах, может служить косвенным индикатором операций с наличными денежными средствами, проводимыми в организации. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

II. Объем и состав клиентского портфеля банка:

1) Кредиты предприятиям. Позволяет оценить объемы, в которых востребованы услуги данной организации у юридических лиц. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

2) Потребительские кредиты. Характеризует объемы услуг, оказываемых физическим лицам. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

3) Расчетные счета. Характеризует размеры клиентского портфеля организации. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.

4) Вклады физических лиц. Характеризует объем денежных средств населения, имеющихся в распоряжении банка. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

III. Качество системы внутреннего контроля банка:

1) Качественный состав предоставляемой подразделением информации. Оценивается соотношение количества сообщений, переданных организацией по кодам обязательного контроля, и по результатам работы внутреннего контроля (подозрительных операций). Причем целесообразно проводить оценку как по количеству сообщений, так и по общей сумме проводимых операций. При эффективной работе подразделения внутреннего контроля организации данные показатели должны быть более 50%, что при минимальном количестве нарушений свидетельствует об интенсивной работе организации по выявлению и информированию о подобных фактах.

2) Количество нарушений. Характеризует качественную составляющую предоставляемой информации. К нарушениям отнесем предоставление операций обязательного контроля по коду 6001, предоставление сообщений с существенным искажением информации, предоставление сообщений по кодам обязательного контроля на сумму ниже пороговой. Количество нарушений считаем как величину относительную. Нормирующей величиной будет являться общее число сообщений, переданных организацией.

3) Количество не представленных сообщений. Сообщения, не представленные организацией, выявляются путем проведения перекрестного анализа информации. Данный показатель также целесообразно рассматривать как относительный и нормировать на общее количество сообщений, переданных организацией.

Следует отметить, что перечисленный набор признаков не является исчерпывающим, однако он может быть необходимым для распознавания случаев легализации (отмывания) преступных доходов.

Выводы: Приведенные признаки кредитных организаций могут быть исходными в терминах теории распознавания образов для решения задачи противодействия легализации (отмывания) преступных доходов, поскольку они образуют упорядоченные наборы (векторы), что позволит получить интегральные оценки надежности кредитной организации, ее устойчивости, а также риски существенных нарушений в деятельности организации, которые могут повлечь за собой отзыв лицензии на банковскую деятельность (репутационные риски).

Литература

1. Фомин Я.А., «Распознавание образов. Теория и применение» М.: издательство «Фазис», 2012 г.

Иванова Анна Юрьевна

Организационно-правовые методы защиты интеллектуальной собственности на созданные программные средства

Аннотация: *проблемы защиты авторских прав на программные средства*

Ключевые слова: *программное обеспечение, программа для ЭВМ, базы данных, программный продукт, средства защиты авторских прав.*

Активное развитие информационных технологий и все большая компьютеризация нашего общества четко обозначает проблему обеспечения авторских прав на программные продукты.

Особенностью программного обеспечения для ЭВМ как предмета правового регулирования и правовой защиты является то, что это техническое понятие, определенное в ГОСТе 19781-90 как данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма. Это же определение было юридически сформулировано в Федеральном законе от 23 сентября 1992 г. «О правовой охране программ и баз данных для ЭВМ».

Данное определение без изменений перешло в ст. 1261 Гражданского кодекса Российской Федерации (далее – ГК РФ), где указано, что программа для ЭВМ – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Такое определение, с одной стороны, сужает круг охватываемых объектов, так как существуют программы, предназначенные не для получения результата, а, например, для обеспечения работоспособности устройств, работающих не только на компьютерных устройствах (яркий пример тому – современные телефоны). С другой стороны, охрана всех подготовительных материалов как программ, наоборот, расширяет круг объектов, относящихся к программам, по сути, ими не являющимися, так как подготовительные материалы очень разнообразны и охраняются авторским правом изначально – это, например, изображения, используемые в программе, или не являются объектом авторского права: алгоритм работы программы, техническое задание на ее разработку.

В настоящее время специалистами создаются как программы для ЭВМ, так и базы данных. Взаимная связь программ и баз данных с ЭВМ очевидна. Как ЭВМ не может функционировать без программного обеспечения, так и программное обеспечение имеет ценность лишь при его работе на ЭВМ. Поэтому вполне логично, что первые программы появились одновременно с изобретением ЭВМ, развивались параллельно с их совершенствованием.

Так, первое устройство подобного рода появилось в середине 40-х годов XX века, и одновременно с ним были созданы первые программы для его функционирования.

Усовершенствование ЭВМ неизбежно влекло за собой развитие программ и начало внедрения машин в различные сферы жизнедеятельности человека. Повсеместное распространение ЭВМ привело к необходимости охраны программ от незаконного использования.

Первоначально, на заре существования ЭВМ, не разграничивались понятия «програм-

мное» и «аппаратное» обеспечение, поскольку устройства для обработки данных воспринимались в это время (в 1940 – 1950-е гг.) как некое единое целое, именно так и продавались, а элементы их не могли становиться предметом отдельных договоров и являлись коммерческой тайной.

Владельцами программ в этот период были крупные производители ЭВМ, заинтересованные в сохранении своего полного контроля над новым изобретением и пользующиеся знакомым им инструментарием патентного права и правовой охраны коммерческой тайны.

Логическим следствием такого положения явилось то, что в эпоху первого поколения компьютерных устройств для регулирования охраны программного обеспечения применялись нормы патентного права и права на коммерческую тайну.

Компьютерные программы не являются «классическим» объектом авторского права. Они выполняют утилитарную функцию, представляя собой определенный набор команд и инструкций для компьютерных устройств. Основную ценность представляют собой «поведение» компьютерной программы, задачи, которые она выполняет, а не текст ее объектного кода. Именно функциональные характеристики программного продукта, а не «красота» программного кода являются предметом интереса со стороны пользователей. При этом «поведение» компьютерной программы и исходный код, лежащий в ее основе, являются достаточно независимыми: существует немало программ, обладающих схожими функциональными характеристиками, но в то же время имеющих в основе различный исходный код.

В силу указанной специфики в свое время Всемирная организация интеллектуальной собственности (далее – ВОИС) и некоторые страны (например, Япония) предлагали выработать особый правовой режим для компьютерных программ. Однако после того как в США компьютерные программы были признаны объектами авторского права на законодательном уровне, сработал «эффект домино» и аналогичный подход нашел отражение в большинстве остальных стран, включая страны Европы.

Понятно, почему с подобной инициативой выступала именно Япония, являющаяся основным производителем и экспортером программного обеспечения.

Обращаясь к истории защиты авторских прав на компьютерные программы, можно проследить следующую хронологию. В 1971 г. ВОИС впервые созвала группу экспертов по этой проблеме, а в 1978 г. были подготовлены Типовые положения об охране программного обеспечения вычислительных машин, предлагавшиеся национальным законодателям в качестве примерного образца при разработке соответствующих законодательств. В 1983 г. ВОИС предложила проект международного договора по данному вопросу.

В предлагавшихся решениях ВОИС, как и в работах ряда ученых-юристов того времени, предусматривалось создание системы, сочетавшей элементы патентного и авторского права. Однако такой комбинированный подход не встретил поддержки со стороны национальных законодателей и в настоящее время не актуален.

Как естественное следствие «демократизации» компьютерной техники, углубления юридического анализа данного вопроса на третьем этапе юридического осмысления проблемы охраны программ для ЭВМ ученые основывались на признании правового статуса программного обеспечения. Устанавливалось, что как сами компьютерные программы, так и все другие результаты процесса создания программного обеспечения (анализ и определение проблемы, разработка системы, кодирование, документация) отвечают тем требованиям, которые предъявляются законодательством, юридической теорией к понятию «произведение»: они являются результатом творческой деятельности автора и выражаются в объективной форме.

В 1980 – 1988 гг. в США (1980 г.), Великобритании (1988 г.), Франции (1985 г.), Венгрии, Японии (1985 г.) и других странах мира были приняты поправки к законодательству об авторском праве, которые обеспечивали достаточно эффективную защиту программного обеспечения.

При этом в Соединенных Штатах Америки фактически охрана программного обеспечения начала предоставляться ранее – с момента вступления в силу Закона об авторском праве США 1976 г.

Таким образом, с повестки дня ВОИС и Международной ассоциации промышленной собственности был фактически снят вопрос о введении специальной охраны программного обеспечения, вытекающий из Положений 1978 г. В связи с этим оказалось неактуальным и заключение соответствующего международного договора, так как охрана прав авторов программ обеспечивается в соответствии с положениями Всемирной конвенции об авторском праве 1952 г.

В настоящее время в большинстве стран мира программы для ЭВМ подлежат авторско-правовой охране. Однако лишь в некоторых странах (как в Российской Федерации до 1 января 2008 г.) существуют специальные законы, посвященные данной проблеме (в частности, в Южной Корее (1987 г.), Республике Узбекистан (1994 г.), Кыргызской Республике (1998 г.). В ряде стран программы для ЭВМ охраняются авторским правом наравне с другими объектами и лишь упомянуты среди возможных объектов охраны (как и сейчас в Российской Федерации).

В качестве основных аргументов в пользу выбранного, в том числе и в России подхода обычно указываются легкость приобретения данной защиты, связанная с отсутствием необходимости выполнения каких-либо формальностей, а также отсутствие значительных издержек, связанных с такой защитой, что делает ее общедоступной и демократичной.

Как программы для ЭВМ и базы данных, так и топологии интегральных микросхем для признания их охраноспособными должны обладать двумя признаками: они должны быть результатом творческого труда и выражены в объективной форме.

Кроме двух указанных признаков охраноспособности, несмотря на их отсутствие в законодательстве, в доктрине авторского права некоторые авторы, в частности В.Я. Ионас и М.И. Никитина, выделяют еще два признака: существенную новизну произведения (иными авторами включаемую обычно в признак творческого характера) и его воспроизводимость (включаемую в признак объективной формы), упоминание о которой было в Основах гражданского законодательства Союза ССР и союзных республик 1961 г., но отсутствует в современном законодательстве.

Вместе с тем, как и в России, в иностранных правопорядках не дается четкого определения того, какое произведение можно считать творчески созданным. Данный вопрос до сих пор является дискуссионным. С точки зрения французского права творческими являются произведения, если в них видны личность, дух автора, если оно является плодом человеческого ума. Точка зрения американских ученых, что произведение должно быть оригинальным (то есть не скопированным) и креативным (то есть в произведении должно быть по меньшей мере небольшое присутствие мысли). Англичане исходят из того, что произведение должно быть оригинальным (при этом под оригинальностью не понимается обязательно что-то новаторское, уникальное; должна быть некая, в каждом конкретном случае своя, мера труда, умения или усилия автора)

Выделяют технические, правовые и организационно-правовые средства защиты авторских прав.

Техническими признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

Правовые средства защиты предусмотрены ГК РФ.

В частности, одним из способов является согласно ст. 1262 ГК РФ возможность правообладателя в течение срока действия исключительного права на программу для ЭВМ или на базу данных может по своему желанию зарегистрировать такую программу или такую базу данных в федеральном органе исполнительной власти по интеллектуальной собственности.

В то же время Приказом Минюста от 21 января 2000 г. N 10 «Об утверждении концепции информатизации Министерства юстиции Российской Федерации» в целях упорядочения расходования бюджетных средств на разработку программного обеспечения был введен механизм регистрации созданных программ и баз данных.

Регистрация программ свидетельствует об использовании уже организационно-правовых средств. Регистрация программных продуктов свидетельствует и о их качестве и востребованности на рынке информационных услуг. Информационным письмом Минсвязи РФ от 04.03.2002 N 1341 введено понятие «Качество парка программных средств», который понимается как доля лицензированных программных средств, находящихся в эксплуатации.

Самым используемым способом защиты интеллектуальной собственности является заключение лицензионного договора.

Как известно, право использования программы для ЭВМ или базы данных может быть передано на основании лицензионного договора, заключаемого по общему правилу в письменной форме. Согласно ст. 1236 ГК РФ существует два вида лицензий – исключительная и неисключительная.

В соответствии с обоими видами лицензий лицензиат обязан:

- использовать результат интеллектуальной деятельности способами, предусмотренными договором, и на установленной им территории;
- воздерживаться от совершения действий, нарушающих исключительное право лицензиара.

Различие между исключительной и неисключительной лицензиями – в объеме прав.

Лицензиат, получивший соответствующее право на основании неисключительной лицензии, не может осуществлять защиту своих прав, его права ограничены временными рамками и иными условиями договора.

Лицензиар заключает лицензионные договоры на передачу неисключительных прав. Например, договор на передачу лицензий программы содержит такие права Лицензиата:

- установить одну лицензионную версию на одно рабочее место (ЭВМ);
- осуществлять действия, необходимые для функционирования программного продукта в соответствии с его назначением на требуемом количестве ЭВМ, в том числе, установку хранение и запуск клиентской части программного продукта пользователями сети муниципального образования Лицензиата.

И такие обязанности:

- не производить несанкционированного копирования программного продукта;
- не распространять копии программного продукта;
- не осуществлять действий по обходу технических средств защиты, встроенных в программу;
- использовать программу только в пределах территории Лицензиата;
- не осуществлять вскрытие технологии, декомпиляцию и дезассемблирование программы, кроме случаев, прямо оговоренных действующим законодательством;
- использовать программу как единое целое;
- не предоставлять программу в прокат или во временное пользование.

Однако такая процедура заключения лицензионного договора при больших тиражах программного продукта представляется неприемлемой. Следовательно, при массовой продаже программных продуктов лицензиару требуется другой подход к заключению договора о передаче прав от правообладателя к конечному пользователю.

Для таких случаев действующая редакция ГК РФ в п. 3 ст. 1286 предусматривает возможность заключения каждым пользователем программы для ЭВМ или базы данных с правообладателем договора присоединения, условия которого могут быть изложены на приобретаемом экземпляре программы для ЭВМ или базы данных либо на упаковке этого экземпляра. Начало использования таких программ или баз данных пользователем, как оно определяется этими условиями, означает его согласие на заключение договора. Этот вид лицензионного договора известен как оберточная лицензия.

Отметим, что возможность заключать такие договоры с массовыми пользователями предоставлялась и до введения в действие части IV ГК РФ. Так, положения п. 2 ст. 32 Закона РФ от 09.07.1993 N 5351-1 «Об авторском праве и смежных правах» разрешали при продаже экземпляров программ для ЭВМ и баз данных и массовом предоставлении доступа к ним применять особый порядок заключения договоров.

Данный порядок был установлен Законом РФ от 23.09.1992 N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных». В соответствии с п. 3 ст. 14 данного закона при продаже и предоставлении массовым пользователям доступа к программам для ЭВМ и базам данных допускается применение особого порядка заключения договоров, например, путем изложения типовых условий договора на передаваемых экземплярах программ для ЭВМ и баз данных.

Отдельно необходимо сказать о мерах ответственности, предусмотренных в российском законодательстве за незаконное использование программ.

Основанием применения гражданско-правовой ответственности является нарушение интеллектуальных прав – соответственно личных неимущественных, исключительного права на использование результата интеллектуальной деятельности или иных охраняемых законом прав. Такая ответственность наступает применительно к ст. 401 ГК РФ.

Первым видом мер ответственности, который может быть применен в случае нарушения исключительных прав на результаты интеллектуальной деятельности, является возмещение убытков.

Данный вид ответственности используется редко, поскольку, заявляя требование о возмещении убытков, автор (иной правообладатель) должен доказать не только сам факт нарушения

его прав ответчиком, но и конкретный размер понесенных убытков и причинную связь между ними. Вместе с тем даже данные о точном объеме реализованной контрафактной продукции (а их практически невозможно получить) не могут с точностью подтвердить убытки правообладателя – имея в виду разницу в стоимости легальной и контрафактной продукции, невозможно с достоверностью утверждать, что при отсутствии в продаже контрафактных экземпляров объем законно произведенных экземпляров вырос бы на соответствующую величину.

В случае, если нарушено исключительное право на использование программы для ЭВМ или базы данных (и как на объект авторских, и как на объект смежных прав), правообладатель вправе вместо возмещения убытков требовать от нарушителя выплаты компенсации.

Взыскание компенсации представляет собой особый вид гражданско-правовой ответственности (не носящий публичный характер, имея в виду ее взыскание в пользу потерпевшего от нарушения, а не в пользу государства), который, по сути, является упрощенным порядком возмещения правообладателем собственных имущественных потерь.

Компенсация в силу абзаца третьего п. 3 ст. 1252 ГК РФ может быть взыскана за каждый случай неправомерного использования программы для ЭВМ или базы данных либо за допущенное нарушение в целом.

Один из самых принципиальных и спорных вопросов, возникающих при применении мер защиты интеллектуальных прав, – о том, является ли вина нарушителя условием их применения или же одного факта нарушения интеллектуальных прав достаточно.

В настоящее время в научной литературе (а некоторое время назад и в судебной практике) дискуссии ведутся вокруг толкования положения, предусмотренного п. 3 ст. 1250 ГК РФ, о том, что отсутствие вины нарушителя не освобождает его от обязанности прекратить нарушение интеллектуальных прав, а также не исключает применение в отношении нарушителя мер, направленных на защиту таких прав.

Означает ли указанная норма то, что любые меры защиты как личных неимущественных, так и исключительного права на использование результата интеллектуальной деятельности (а соответственно и возмещение убытков, и взыскание компенсации – ст. 1252 ГК РФ) могут быть применены только в силу того, что доказан факт нарушения лицом этих прав, при этом вина лица не имеет значения?

Следующая мера – уголовная ответственность за незаконное использование объектов авторского права или смежных прав, предусмотренная ч. 2, 3 ст. 146 Уголовного кодекса Российской Федерации (далее – УК РФ). При этом стоит отметить, что нарушение авторских прав относится к области частного права, и такие дела, по нашему мнению, должны быть отнесены к делам частно-публичного обвинения, однако, как и большинство преступлений, они относятся к уголовным делам публичного обвинения. В России были попытки расширить список дел, которые должны быть отнесены к делам частно-публичного обвинения, однако такие изменения не были приняты.

Наличие программ для ЭВМ на компьютерах не является их использованием. Субъектом преступления является тот работник, который осуществил установку (инсталляцию) программы.

При запуске программы на исполнение создается лишь временная копия, которая является частью технологического процесса, имеющего единственной целью использование записи, при этом не создается нового экземпляра произведения.

Таким образом, запуск программы на исполнение или факт наличия программы на жестком диске компьютера не является использованием программы, а использованием программы является в том числе установка ее на ЭВМ. Соответственно, уголовной ответственности подлежит то лицо, которое осуществило установку программы на ЭВМ с нарушением гражданского законодательства. О том, что понятие контрафакта является юридическим, указано и в Постановлении Пленума Верховного Суда РФ N 15 от 19 июня 2006 г.

Третья мера – административная ответственность. Задача по борьбе с нарушениями авторских прав может быть успешно реализована при помощи административной ответственности, которая установлена ст. 7.12 Кодекса Российской Федерации об административных правонарушениях за незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах либо на экземплярах произведений или фонограмм указана ложная информа-

ция об их изготовителях, о месте их производства, а также об обладателях авторских и смежных прав, а равно иное нарушение авторских и смежных прав в целях извлечения дохода.

На сегодняшний день привлечение к административной ответственности по таким делам не получило особого распространения. Усиление мер административной ответственности, которое может включать в себя как установление ответственности за правонарушения, совершенные и без цели извлечения дохода, так и увеличение наказания, позволит тем самым частично отказаться от уголовного наказания за нарушение авторских прав.

Такие изменения не повлияют на возможность правообладателей обращаться в суд для защиты исключительных прав на результаты интеллектуальной деятельности на основании ст. 1252 ГК РФ, в которой перечислены основные способы защиты нарушенных прав.

Гражданские и уголовные дела о нарушении авторских прав на программы для ЭВМ связаны с тем, что в настоящее время большинство гражданских исков от правообладателей за незаконное использование программ заявляются в рамках уголовных дел, это связано с распределением бремени доказывания обстоятельств дела в судебном процессе, этот вопрос рассмотрен в п. 14 Постановления Пленума Верховного Суда РФ N 15, где указано, что:

- истец должен подтвердить факт принадлежности ему авторского права и (или) смежных прав или права на их защиту, а также факт использования данных прав ответчиком;
- ответчик обязан доказать выполнение им требований законодательства об авторском праве при использовании произведений и (или) объектов смежных прав. В противном случае физическое или юридическое лицо признается нарушителем авторского права и (или) смежных прав, и для него наступает гражданско-правовая ответственность в соответствии с законодательством Российской Федерации.

Данная позиция основывается на том, что в судебном процессе каждая сторона должна доказать те обстоятельства, на которые она ссылается (п. 1 ст. 56 Гражданского процессуального кодекса, п. 1 ст. 65 Арбитражного процессуального кодекса, отсюда следует обязанность истца доказать факт использования ответчиком программы для ЭВМ при обращении в суд.

В настоящее время, как показывает анализ материалов гражданских, административных и уголовных дел, существует необычная тенденция защиты гражданских прав правообладателя негражданско-правовыми способами. Большинство правообладателей для пресечения нарушения и наказания лица в первую очередь выбирают меры публично-правового принуждения и обращаются с заявлением о возбуждении уголовного дела или заявлением о наличии данных, указывающих на событие административного правонарушения. Как правило, лишь в случае, когда уголовное дело или дело об административном правонарушении по каким-либо основаниям прекращено, правообладатели обращаются за защитой своих гражданских прав.

Вместе с тем рассмотрение уголовного или административного дела и вынесение соответственно обвинительного приговора или постановления о привлечении лица к административной ответственности не препятствуют одновременной защите нарушенных интеллектуальных прав в гражданско-правовом порядке. Российское законодательство не допускает лишь одновременного применения двух мер публично-правовой ответственности за одно нарушение, возможность же применения гражданско-правовых мер защиты от применения или неприменения мер публичной ответственности не зависит.

Оправдательный приговор суда по уголовному делу также сам по себе не свидетельствует о невозможности применения мер гражданско-правовой ответственности в связи с тем, что состав преступления, предусмотренного ст. 146 УК РФ, отличается от состава нарушения гражданского законодательства. Так, УК РФ вводит дополнительные по сравнению с ГК РФ признаки: объективный – размер, субъективные – цель, вина. Кроме того, УК РФ устанавливает ряд оснований освобождения от уголовной ответственности, в частности, в связи с истечением срока давности, с деятельным раскаянием, с принятием акта амнистии. Очевидно, что ни одно из них не служит основанием освобождения от гражданской ответственности.

рецензент: ***Сергин Михаил Юрьевич,***
доктор технических наук, профессор

Крылов Григорий Олегович,
доктор физико-математических наук,
кандидат юридических наук

Проблемы защиты информации при переводе денежных средств в Национальной платежной системе

Аннотация: *рассматриваются проблемы защиты информации в национальной платежной системе после вступления России во Всемирную торговую организацию.*

Ключевые слова: *всемирная торговая организация, перевод денежных средств, защита информации.*

Актуальность, новизна, цель и практическая значимость работы обусловлены проблемами реализации Федерального закона от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе»[1], который преследует триединую задачу: уход от иностранной разведки российских финансовых транзакций – усиление национального финансового мониторинга в интересах противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма – уменьшение массы наличных денежных средств.

Основные положения нормативного обеспечения защиты информации при осуществлении переводов денежных средств в национальной платежной системе России приведены в анализируемом ниже Положении Центрального банка России от 9 июня 2012 г. N 382-П [2]

Анализируемое «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» по состоянию на 21 августа 2012 года в целом соответствует требованиям, предъявляемым к подзаконным нормативно-правовым актам. Однако, после вступления России во Всемирную торговую организацию (далее - ВТО) Федеральный закон от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе» и, следовательно, анализируемое Положение требуют дополнений по обязательствам России перед ВТО. В частности, согласно терминологии ВТО банковские операции относятся к банковским услугам. После присоединения к ВТО к оказанию таких банковских услуг в России будут допущены иностранцы из стран – членов ВТО на предусмотренных условиях. Россия присоединилась к ВТО 22 августа 2012 года путем ратификации соответствующих международных соглашений. После ратификации эти тексты стали частью международных соглашений России, которые, как известно, имеют бульшую силу, нежели любые внутренние российские законы. В случае противоречия между этими текстами и внутренними российскими законами в силу ч. 4 ст. 15 Конституции РФ применяться должны будут первые. После вступления России в ВТО в отношении оказания иностранными лицами из членов ВТО финансовых услуг в России / применительно к получателям в России / и из России будут действовать правила согласно принятым на себя Россией обязательствам. Кроме того, российские субъекты получат право входить на иностранные рынки финансовых услуг, причем с учетом тех обязательств, которые взяли на себя соответствующие члены ВТО.

В связи с получением Россией статуса члена ВТО для нее начали действовать десятки документов ВТО (как международные соглашения, образующие правовую основу ВТО, так и локальные документы органов ВТО). Важнейший из них — Генеральное соглашение о торговле услугами (General Agreement on Trade in Services), GATS (ГАТС). Сюда же следует отнести Международные стандарты ISO 13335, ISO 13569 (банковские и финансовые услуги), ISO 17799/BS 7799-2, », COBIT, серию стандартов ИСО/МЭК 27000 и др.

Необходимо отметить следующие резервы доработки Положения:

1. Целесообразно дополнить п.1.1. Положения ссылкой на «Положение о защите информации в платежной системе», утвержденное Постановлением Правительства РФ от 13 июля 2012 № 584;
2. Положение не содержит ссылки на ранее принятый Стандарт Банка России СТО БР ИББС-1.0-2010 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» без соблюдения которого, как отметил В. Лукацкий, крайне трудно выполнять требования Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», которым после 1 января 2011 года должны соответствовать все системы, обрабатывающие персональные данные. Проблема выполнения технических требований, вытекающих из этого закона ускорила процесс принятия кредитными организациями данного стандарта. Обсуждая вопрос внедрения СТО БР ИББС, стоит упомянуть и об Указании Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», в котором установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств 3 категорий операторов: платежных систем; услуг платежной инфраструктуры; по переводу денежных средств.
3. В соответствии с п. 2.9.1.Положения «В случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют средства криптографической защиты информации (СКЗИ) российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа». Однако, никак не урегулирован вопрос применения СКЗИ нероссийского производства. В Приложении 2 приведен перечень требований к СКЗИ без учета происхождения. Например, если длина ключей для симметричных СКЗИ, предназначенных для защиты финансовых транзакций составляет свыше 56 бит, то при наличии нотификации ФСБ, ввозятся такие СКЗИ, что фактически является разрешением и на эксплуатацию. Поэтому получается так, что в НПС могут применяться любые СКЗИ.
4. На оператора платежной системы возлагается большая работа по реагированию на инциденты, разработке методик анализа и реагирования, информирование операторов по переводу и операторов инфраструктуры о выявленных инцидентах и т.д. Оценка соответствия требованиям по ИБ проводится самостоятельно или с приглашением внешних организаций в соответствие с методикой, приведенной в приложении к Положению. При этом никак не урегулирован вопрос о наличии лицензии на техническую защиту конфиденциальной информмции у такой организации в соответствии с Постановлением Правительства РФ от 03.02.2012 г №79 «О лицензировании деятельности по технической защите конфиденциальной информации»
5. Перечень отмеченных замечаний не является исчерпывающим. Отдельного анализа требуют Приложения к анализируемому Положению. Особенно это относится к Приложению 1, которое содержит спорные утверждения из области многомерных экспертных оценок и не соотносится с международными моделями уровней зрелости организаций.

Выводы: Отмеченные замечания требуют дальнейшего анализа и доработки.

Литература.

1. Федеральный закон от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе». «Российская газета» от 30 июня 2011 г. № 139.
2. Положение Центрального банка России от 9 июня 2012 г.N 382-П «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», http://www.cbr.ru/, 2012 г.

Морозов Антон Андреевич
Арутюнова Лусине Борисовна

Формирование единого пространства юридически значимого электронного взаимодействия

Аннотация: *в статье подробно разбираются проблемы формирования единого пространства юридически значимого электронного взаимодействия, а так же способы преодоления таких проблем.*

Ключевые слова: *право, информационная безопасность, информационные технологии, государственные функции.*

Формирование единого информационного пространства является главной задачей для обеспечения электронного взаимодействия между государственными органами. Как уже отмечалось, для решения этой задачи 20 октября 2010 г Правительством Российской Федерации была утверждена Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)».

Согласно данной программе отрасль информационных и телекоммуникационных технологий (далее – информационные технологии) в 2000 – 2010 годах развивалась высокими темпами, ежегодный прирост составлял около 25 процентов, что существенно выше среднегодовых темпов роста валового внутреннего продукта и роста отдельных отраслей. Информационные технологии и информационные услуги стали достаточно существенной статьей российского несырьевого экспорта. Однако сводные индексы и межгосударственные сопоставления до сих пор характеризуют Россию не лучшим образом, что говорит о недостаточном уровне развития отрасли информационных технологий, об отставании от мировых лидеров, а также о нереализованности потенциала уже существующих инфраструктур и технологий.

С другой стороны, по ряду параметров Россия не сильно отличается от европейских стран, где доля сектора информационных технологий составляет около 5 процентов валового внутреннего продукта, около 30 процентов населения никогда не пользовались сетью Интернет и только 38 процентов граждан использовали сеть Интернет при получении государственной услуги (в основном для получения формы заявления).

Отмечавшиеся в указанный период достаточно высокие темпы роста были продемонстрированы во многом благодаря новым открывшимся рынкам, новым продуктам и услугам (сотовая связь, компьютерное оборудование, консалтинг и другие услуги) на фоне низкого начального уровня развития информационных технологий в России. В настоящее время становится очевидным, что для сохранения набранных темпов роста необходимо устранить целый ряд существующих барьеров.

Одним из факторов, негативно влияющих на уровень распространения информационных технологий и развитие информационного общества в России, является недостаточно высокий уровень социально-экономического развития многих субъектов Российской Федерации. Так, сохраняется высокий уровень различия в использовании информационных технологий в домашних хозяйствах регионов. В рейтинговой оценке российских регионов по их готовности к информационному обществу индекс лидера в 22 раза превышает показатель региона-аутсайдера. Остаются проблемы организации широкополосного доступа для конечных пользователей. На конец 2010 года только около 21,5 процента всех российских домашних хозяйств (11,4 млн. домашних хозяйств) имели широкополосный доступ в сеть Интернет, а средняя скорость доступа в регионах варьировалась от 128 Кбит/с до 1 Мбит/с, что существенно ниже, чем в Москве (7,5 Мбит/с) и Санкт-Петербурге (6 Мбит/с). В каждом втором регионе России удельный вес организаций, использующих широкополосный доступ, не превышает 27 процентов. Даже лидер по этому показателю (г. Москва) на 8 процентных пунктов отстает от уровня использования широкополосного доступа в странах Европейского союза. Для ускоренного развития в Российской Федерации информационного общества

необходимо обеспечить значительное снижение стоимости предоставляемых населению услуг на основе информационных технологий с одновременным повышением их качества на основе развития конкуренции между операторами связи и поставщиками оборудования.

Еще одним фактором, препятствующим ускоренному развитию в России информационного общества, является недостаточный уровень распространения в обществе базовых навыков использования информационных технологий. Это касается как населения в целом, так и государственных и муниципальных служащих. Требует корректировки и система воспроизводства кадров в сфере информационных технологий. Сегодня обучение в вузах осуществляется в основном по старым методикам. В результате из высших учебных заведений страны зачастую выходят специалисты, не владеющие современными технологиями и неспособные с их помощью повысить эффективность выполнения функций государственного и муниципального управления.

Следует отметить высокий уровень зависимости российского рынка от зарубежной продукции в сфере информационных технологий. В подавляющем большинстве создаваемых информационных систем в России сегодня используются в основном зарубежные разработки. Можно выделить еще ряд барьеров, препятствующих успешному развитию отечественной промышленности в сфере информационных технологий, среди которых критически значимым является низкий уровень правовой защиты интеллектуальной собственности.

Существенным препятствием ускоренному развитию информационного общества в России является отсутствие массового интерактивного взаимодействия граждан и организаций с государственными органами власти при оказании последними государственных услуг. При этом следует отметить, что до настоящего времени в России законодательно не утвержден даже перечень государственных и муниципальных услуг, оказываемых в электронном виде соответственно органами государственной власти и органами местного самоуправления. Не решен вопрос о признании на законодательном уровне электронного документа эквивалентом бумажного документа.

Использованию потенциала информационных технологий препятствует разрозненность государственных информационных ресурсов, невозможность сопоставить данные, содержащиеся в этих ресурсах, а также значительное дублирование информации. Необходимо обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения органов государственной власти.

Проблемы, препятствующие повышению эффективности использования информационных технологий в целях повышения качества жизни граждан, обеспечения конкурентоспособности России, развития экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствования системы принятия государственных управленческих решений, носят комплексный межведомственный характер и не могут быть решены на уровне отдельных органов государственной власти. Их устранение требует значительных ресурсов, скоординированного проведения организационных изменений и обеспечения согласованности действий органов государственной власти.

В результате отсутствия комплексного подхода к решению задачи формирования и развития информационного общества как одного из необходимых этапов модернизации экономики России проявились негативные тенденции, которые при сохранении текущей экономической ситуации могут усиливаться.

В соответствии со Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 (далее – Стратегия), целями формирования и развития информационного общества в Российской Федерации являются повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий. Таким образом, создание информационного общества рассматривается как платформа для решения задач более высокого уровня – модернизации экономики и общественных отношений, обеспечения конституционных прав граждан и высвобождения ресурсов для личностного развития.

Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденная рас-

поряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р, определяет в качестве целей государственной политики в области развития информационных технологий создание и развитие информационного общества, повышение качества жизни граждан, развитие экономической, социально-политической и культурной сфер жизни общества, совершенствование системы государственного управления, обеспечение конкурентоспособности продукции и услуг в сфере информационных и телекоммуникационных технологий. Для достижения поставленных целей в соответствии с распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1663-р утверждены Основные направления деятельности Правительства Российской Федерации на период до 2012 года и перечень проектов по реализации указанных направлений, в том числе проекты в области построения информационного общества, модернизации информационных процессов и качественного развития средств массовых коммуникаций.

Таким образом, цели государственной политики определяют необходимость решения задач не только в сфере информационных технологий, но и в других отраслях экономики, науке и технике, социальной сфере и государственном управлении. В число показателей развития информационного общества в Российской Федерации, контрольные значения которых определены Стратегией, также включены показатели, отражающие уровень развития информационных технологий и степень их использования в разных сферах деятельности.

Текущее состояние готовности России к информационному обществу определяет в соответствии со Стратегией необходимость не только развития отрасли информационных технологий, но и определения приоритетов ее развития, создания на ее основе сервисов и обеспечения готовности граждан и организаций к использованию технических возможностей. Таким образом, на первый план выходят задачи координации действий различных агентов, согласования их интересов и ресурсов.

Международные обязательства Российской Федерации, с одной стороны, предполагают соблюдение положений соответствующих документов в области формирования информационного общества, а с другой – обеспечивают участие в разработке международных норм права и механизмов, регулирующих отношения в области использования глобальной информационной инфраструктуры, международных исследовательских проектах по приоритетным направлениям развития науки, технологий и техники, а также создают возможность использовать лучший опыт. Необходимо создание атмосферы заинтересованности в инновациях, готовности к нововведениям, открытости и непрерывности обучения как основы информационного общества.

Стратегией также установлено, что информационное общество характеризуется высоким уровнем развития информационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти, то есть для создания информационного общества высокий уровень развития информационных технологий является необходимым, но не достаточным условием. Необходимо обеспечить возможность внедрения технологий и создать привычку их использования в повседневной жизни. Поскольку информационное общество по своей природе не может быть локальным, то для всех граждан Российской Федерации независимо от места их проживания и социального статуса должны соблюдаться единые минимальные федеральные стандарты доступности информационных технологий.

В соответствии с целями и задачами формирования и развития информационного общества в Российской Федерации, предусмотренными Стратегией, а также с учетом текущего состояния сферы создания и использования информационных технологий в Российской Федерации целью Программы является получение гражданами и организациями преимуществ от применения информационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий и радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе. Достижение цели Программы обеспечивается путем выполнения мероприятий, сгруппированных по подпрограммам. Состав мероприятий может корректироваться по мере решения задач Программы. Для каждой подпрограммы определены задачи, решение которых обеспечивает достижение цели Программы.

В настоящее время с учетом рекомендаций Совета Европы и европейского опыта в данной области необходимо проводить поиски опытных путей на введение новых систем реорганизации или замены системы судебного

управления и компьютеризованных правовых информационных систем на международном уровне. Необходимо также установить соответствующий уровень науки и техники относительно информационных технологических систем в правовом секторе с учетом общего знаменателя тенденций в этой области в Европе, что позволит улучшить качество, действенность и эффективность правового регулирования и правосудия в государствах — членах Совета Европы, это имеет большое значение для модернизации систем правосудия и правовых информационных систем на международном уровне.

Литература:

1. Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993.
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006.
3. Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)», утвержденная распоряжением Правительства Российской Федерации № 1815-р 20 октября 2010 года.
4. Бачило И. Л. Субъекты права в информационной сфере. Информационное право: Учебник / Под ред. акад. РАН Б. Н
5. Топорнина. 2-е изд., с изм. и доп. – СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005.
6. Калятин В. О. Правовые вопросы организации сети Интернет.

   Серго А.Г. Интернет и право. М.: Бестселлер.

рецензент: ***Филатова Людмила Васильевна,***
кандидат юридических наук, старший научный сотрудник

Никитина Виктория Леонидовна

Проблемы мониторинга универсальных электронных карт в национальной платежной системе

Аннотация: *рассматриваются проблемы мониторинга универсальных электронных карт в национальной платежной системе после вступления России во Всемирную торговую организацию.*

Ключевые слова: *всемирная торговая организация, национальная платежная система России, универсальные электронные карты, мониторинг.*

Вступление

В России вступил в силу Федеральный закон от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе» [1], а также Положение Центрального банка России от 9 июня 2012 г. N 381-П «О порядке осуществления надзора за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры требований Федерального закона от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе», принятых в соответствии с ним нормативных актов Банка России» (далее Положение) [2], что требует исследования особенностей их реализации.

Актуальность темы. Стратегические цели создания Национальной платежной системы (НПС) заключаются по существу в уходе от иностранной разведки российских финансовых трансзакций, в уменьшении массы наличных денежных средств, равно как в усилении национального финансового мониторинга в интересах противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма. После вступления России 22 августа 2012 года во Всемирную торговую организацию (далее – ВТО) Федеральный закон от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе» и, следовательно, Положение требуют дополнений по обязательствам России перед ВТО. В частности, согласно терминологии ВТО банковские операции относятся к банковским услугам. После присоединения к ВТО к оказанию таких банковских услуг в России будут допущены иностранцы из стран – членов ВТО на предусмотренных условиях. После вступления России в ВТО в отношении оказания иностранными лицами из членов ВТО финансовых услуг в России / применительно к получателям в России / и из России будут действовать правила согласно принятым на себя Россией обязательствам. Кроме того, российские субъекты получат право входить на иностранные рынки финансовых услуг, причем с учетом тех обязательств, которые взяли на себя соответствующие члены ВТО. В связи с получением Россией статуса члена ВТО для нее начали действовать десятки документов ВТО (как международные соглашения, образующие правовую основу ВТО, так и локальные документы органов ВТО), которые требуют отдельного анализа на предмет их сопряжения с Положением, если зарубежные операторы платежных систем и операторы услуг платежной инфраструктуры, не являющимися кредитными организациями, получат статус субъектов национальной платежной системы России. Частично эта ситуация предусмотрена ст. 37 Федерального закона N 161-ФЗ. В Положении не отражены уголовно-правовые отношения, которые неизбежно возникнут при массовом обороте универсальных электронных карт (УЭК) и инфоматов, которые придут на смену банкоматам. Кроме того в Положениии неполно отражены отношения Банка России с федеральными органами исполнительной власти при осуществлении надзора и наблюдения в национальной платежной системе, в частности отношения с Федеральной службой финансово-

го мониторинга. Частично эта ситуация предусмотрена ст. 36 Федерального закона от 27 июня 2011 года № 161-ФЗ, а также в изменениях и дополнениях в Федеральном законе от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [3], которые сводятся к следующим:

1. Основные изменения данного закона коснулись статьи 7 «Права и обязанности организаций, осуществляющих операции с денежными средствами или иным имуществом». В пункты 1.1. и 1.2. о возможности не проведения идентификации клиента и выгодоприобретателя в случаях, когда сумма операции не превышает 15 тыс. руб. включены также представители клиента. Добавлены аналогичные положения, касающиеся переводов без открытия счета, в том числе электронных денежных средств: «Идентификация клиента – физического лица, представителя клиента и (или) выгодоприобретателя не проводится при осуществлении кредитными организациями, в том числе с привлечением банковских платежных агентов, перевода денежных средств без открытия банковского счета, в том числе электронных денежных средств, если сумма перевода не превышает 15 000 рублей либо сумму в иностранной валюте, эквивалентную 15 000 рублей, за исключением случая, если у работников кредитной организации, банковских платежных агентов возникают подозрения, что указанная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма». Введены также соответствующие дополнения, согласующие положения Федерального закона N 161-ФЗ «О национальной платежной системе» о праве кредитной организации поручать на основании договора другой кредитной организации, организации федеральной почтовой связи, платежному агенту проведение идентификации клиента – физического лица, представителя клиента и (или) выгодоприобретателя в целях осуществления перевода денежных средств без открытия банковского счета, в том числе электронных денежных средств. Обозначена ответственность за несоблюдение установленных требований по идентификации всех участников процесса. Кроме того, кредитным организациям вменено в обязанность сообщать Банку России в установленном им порядке информацию о лицах, которым кредитной организацией поручено проведение идентификации.
2. До 30 дней увеличен срок приостановления уполномоченным органом операций лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму в случае, если полученная информация подтверждена, в случае, если по заявлению уполномоченного органа есть решение суда, то такие операции приостанавливаются до отмены такого решения в соответствии с действующим законодательством (ст. 8).

Выводы: Вступление России в ВТО требует дальнейшего исследования проблем надзора и мониторинга универсальных электронных карт в национальной платежной системе.

Литература

1. Федеральный закон N 161-ФЗ «О национальной платежной системе». «Российская газета» от 30 июня 2011 г. N 139
2. Положение Центрального банка России от 9 июня 2012 г. N 381-П «О порядке осуществления надзора за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры требований Федерального закона от 27 июня 2011 года N 161-ФЗ «О национальной платежной системе», принятых в соответствии с ним нормативных актов Банка России», http://www.cbr.ru/, 2012 г.
3. Федеральный закон от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». «Российская газета» от 9 августа 2001 г. N 151

рецензент: ***Сергин Михаил Юрьевич,***
доктор технических наук, профессор

Гобрусенко Константин Иванович,
кандидат юридических наук

Рябков Виктор Ефимович

Правовые вопросы информационного обеспечения аналитических подразделений Росфинмониторинга

Аннотация: *рассматриваются правовые вопросы информационного обеспечения аналитических подразделений Росфинмониторинга в интересах противодействия легализации (отмывания) преступных доходов и финансирования терроризма.*

Ключевые слова: *противодействие легализации (отмыванию) доходов, информационные технологии, презумпция открытости информации, электронный документооборот.*

Актуальность темы обусловлена тем, что многообразие способов совершения легализации (отмывания) преступных доходов и финансирования терроризма, соединенное с применением различных и разнообразных приемов и средств маскировки существенно затрудняет обнаружение признаков таких преступлений. Вместе с тем, для различных способов совершения таких преступлений характерна устойчивая повторяемость, объективно обусловленная системой функционирования финансового механизма хозяйствующих субъектов экономики каждого отдельного государства, что создает предпосылки для использования современных информационных технологий в выявлении, предупреждении и раскрытии преступлений данной категории. В отдельных случаях только при помощи современных информационных технологий становится возможным выявление фактов легализации (отмывания) преступных доходов и финансирования терроризма. Следовательно, научная разработка и применение современных информационных технологий при осуществлении финансового мониторинга является важным резервом повышения результативности проводимых правоохранительными и другими органами исполнительной власти мер по противодействию легализации (отмыванию) преступных доходов и финансированию терроризма.

Согласно статье 2 Федерального закона РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» под *информационными технологиями* следует понимать процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Вместе с тем, использование современных информационных технологий в информационном обеспечении любой деятельности возможно только при организации на должном уровне информационного обеспечения этой деятельности и наличии соответствующих информационных ресурсов. Следовательно, специального решения требует проблема организации информационного взаимодействия между правоохранительными и другими органами и информационного обеспечения их соответствующих подразделений.

Правовое регулирование информационного обеспечения деятельности аналитических подразделений Федеральной службы по финансовому мониторингу (Росфинмониторинга) основывается на нормативных правовых актах различного уровня, регламентирующих процессы сбора, фиксации, обработки, накопления, хранения, поиска и распространения различных видов информации.

Основу правового регулирования их информационного обеспечения составляют Конституция Российской Федерации.

В соответствии со статьей 29 Конституции РФ каждому гарантируется свобода поиска, получения, передачи, производства и распространения информации любым законным спосо-

бом. Рамки этой свободы определены статьями 23 и 24, в соответствии с которыми устанавливается неприкосновенность частной жизни, личной и семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, за исключением ограничения этих прав на основании судебных решений. Накладывается также запрет на сбор, хранение, использование и распространение информации, содержащей сведения о частной жизни лица, без его согласия на такие действия.

При этом органы государственной власти и органы местного самоуправления, а также их должностные лица обязаны обеспечить каждому гражданину возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Необоснованный отказ в предоставлении гражданину такой информации либо предоставление неполной или заведомо ложной информации наказывается в административном порядке (статья 5.39 КоАП РФ), а если эти деяния причинили вред правам и законным интересам гражданина, то они образуют состав преступления (статья 140 УК РФ).

В соответствии со статьями 5, 9 и 10 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ) [2] Росфинмониторинг получает необходимую для выполнения возложенных на него функций информацию от организаций, осуществляющих операции с денежными средствами или иным имуществом, а также от органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, Банка России и компетентных органов иностранных государств.

С учетом развития рыночных отношений и информационных технологий в связи с необходимостью решения задачи по повышению эффективности исполнения функций по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма у Росфинмониторинга возникает необходимость в получении информации, которой располагают юридические лица, не относящиеся к организациям, перечисленным в Федеральном законе № 115-ФЗ.

Практика свидетельствует, что различные компании располагают автоматизированными информационными системами, содержащие предметно ориентированные информационные массивы в формате баз данных, накапливающие сведения в электронном виде, позволяющие ускорить анализ информации и которые могут быть использованы для эффективной реализации мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, предусмотренных Федеральным законом № 115-ФЗ.

Организация информационного обеспечения Росфинмониторинга предполагает использование ведомственных и вневедомственных информационных ресурсов в виде информационных массивов, в том числе в формате баз данных, которые формируются и накапливаются в рамках разнообразных информационных систем. При этом информационные ресурсы образуют отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

В соответствии со статьей 212 Гражданского кодекса Российской Федерации (далее – ГК РФ) информационные ресурсы, в том числе, в виде электронных документов и отдельных информационных массивов в формате баз данных, хранящихся на магнитных носителях информации, могут быть как государственными, так и негосударственными, и как элемент состава имущества и объект права собственности могут находиться в собственности граждан и юридических лиц, а также Российской Федерации, субъектов Российской Федерации, муниципальных образований.

В этой связи доступ Росфинмониторинга к информационным ресурсам сторонних организаций должен организовываться в соответствии с законодательством Российской Федерации, устанавливающим специальные режимы сбора хранения и распространения отдельных категорий информации, в частности: сведений, составляющих государственную, служебную или коммерческую, банковскую, налоговую и иную охраняемую законом тайну.

Массовое использование для обработки информации средств вычислительной техники с программным обеспечением помимо возможности входить в современные открытые автоматизированные информационно-телекоммуникационные системы, позволяет сравнительно легко модифицировать, копировать и разрушать

информацию, содержащуюся в этих системах. Таким образом, по мере развития вычислительных, автоматизированных информационных и телекоммуникационных систем повышается и их уязвимость. Данная проблема затрагивает правовые аспекты безопасности информации, содержащейся в автоматизированных информационно-телекоммуникационных системах, и использования информационных технологий.

Практика свидетельствует, что Росфинмониторинг с целью развития и использования информационных технологий не всегда может получить базы данных или организовать удаленный доступ к автоматизированным информационным системам различных министерств, служб и агентств, хозяйствующих субъектов.

Понятие «база данных» рассматривается в ГК РФ. Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (статья 1260 ГК РФ).

Согласно статье 1225 ГК РФ базы данных являются результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью).

На любые созданные базы данных, представленные в объективной форме, независимо от их материального носителя, назначения и достоинства признаются интеллектуальные права которые включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных ГК РФ (статьи 1226 и 1227), также личные неимущественные права и иные права (право следования, право доступа и другие).

Исключительное право на программу для ЭВМ или базу данных, созданные по договору, предметом которого было их создание (по заказу), принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное (статья 1296).

Поскольку любой информационный массив в формате баз данных является результатом интеллектуальной деятельности, средством индивидуализации и объектом исключительных прав, то в соответствии с частью 2 статьи 138 Гражданского кодекса Российской Федерации использование ее третьими лицами может осуществляться только с согласия правообладателя.

Таким образом, для совершенствования системы информационного обеспечения Росфинмониторинга на основе использования различных баз данных и внедрения современных информационных технологий необходимо достигнутые соглашения об информационном взаимодействии между Федеральной службой по финансовому мониторингу и различными министерствами, федеральными службами и федеральными агентствами закреплять межведомственными нормативными правовыми актами.

В соответствии с Постановлением Правительства Российской Федерации от 13.08.97 г. № 1009 «Об утверждении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации» нормативные правовые акты, имеющие межведомственный характер, независимо от срока их действия, не прошедшие государственную регистрацию, не зарегистрированные Министерством юстиции Российской Федерации и официально не опубликованные, применяться не могут.

Следовательно, такие межведомственные нормативные правовые акты должны быть зарегистрированы Министерством юстиции РФ. Кроме того, по нашему мнению, назрела необходимость о нормативном закреплении обмена информационными массивами в формате баз данных между всеми правоохранительными органами, различными министерствами, службами и агентствами, а также о выделении координатора от Совета безопасности Российской Федерации при рассмотрении и подписании соглашений по информационному обмену и использованию автоматизированных информационных систем сторон.

Например, во многих городских отделах записи актов гражданского состояния учетные данные заносятся в базы данных и вводятся в память ЭВМ. Данная информация оказывается востребованной при установлении: родственных связей; лиц, сменивших фамилию; юридических лиц и физических лиц с правом занятия предпринимательской деятельностью, зарегистрированных по паспортным данным умерших людей (что неоднократно встречается на практике), а также установлении родственных связей директорского корпуса крупных предприятий и руководителей государственных организаций.

Исходя из вышеизложенного, мы считаем, что положения любых нормативных правовых

актов, регулирующие информационные процессы, должны следовать презумпции открытости информации, устанавливающей, что органам исполнительной власти разрешено получение любого информационного массива (в том числе и в формате баз данных), необходимого для решения поставленных перед ними государством задач, за исключением содержащих сведения, доступ к которым ограничен федеральными законами.

Как показывает изучение практики, большое количество информационных ресурсов создается в электронном виде и используется в составе автоматизированных информационных систем организаций различных министерств, служб, агентств, структурных подразделений органов государственной власти Российской Федерации и субъектов Российской Федерации. В этой связи, необходима более точная регламентация вопросов, связанных с дальнейшим развитием электронного документооборота и использованием информационных технологий, их внедрением в деятельность различных министерств, служб и агентств, органов государственной власти Российской Федерации и субъектов Российской Федерации.

В этой связи, по нашему мнению, имеется настоятельная необходимость разработки и принятия федерального закона, регламентирующего важнейшие вопросы электронного документооборота и использования информационных технологий в деятельности органов государственной власти, различных министерств, служб и агентств Российской Федерации, создания и эксплуатация автоматизированных информационных систем и обеспечения их безопасности.

Выводы: положения любых нормативных правовых актов, регулирующие информационные процессы, должны следовать презумпции открытости информации, устанавливающей, что органам исполнительной власти разрешено получение любого информационного массива (в том числе и в формате баз данных), необходимого для решения поставленных перед ними государством задач, за исключением содержащих сведения, доступ к которым ограничен федеральными законами.

Литература.

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», «Российская газета» от 29 июля 2006 г., N 165
2. Федеральный закон от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». «Российская газета» от 9 августа 2001 г., N 151

Филатова Людмила Васильевна,
кандидат юридических наук, старший научный сотрудник
Михалевич Владимир Владимирович

Информационно-правовые учетные системы федеральных органов исполнительной власти в «электронном государстве»

Аннотация: *статья посвящена структуре и задачам Информационно-правовых учетных систем исполнительной власти в «электронном государстве». Так же освещены принципы организации таких систем.*

Ключевые слова: *информация, информационное право, право, государство, электронное государство.*

Построение глобального открытого информационного общества привело к реализации практически во всех странах мира концепции электронного государства, основанной на трансформации государственного управления при широком использовании информационных технологий в процессе государственной деятельности и оказании государственных услуг.

В литературе различного рода, в которой применяются термины «электронное правительство», «информационное общество», «электронный государственный аппарат», «электронная инфраструктура государства», «государство информационного общества», фактически речь идет об «электронном государстве» и о самом этом обществе, которое превращается в информационное, приобретая совершенно новые и прежде несвойственные ему черты [1]. И уже в правовых актах закрепляется понятие «информационное государство». Так, Государственная программа Российской Федерации «Информационное общество (2011-2020 годы) содержит подпрограмму «Информационное государство».

В таком обществе его политико-правовая организация представляет собой способ взаимодействия органов государственной и муниципальной власти и общества в целях предоставления государственных услуг и обеспечения возможности участия в осуществлении власти населения с использованием информационно-телекоммуникационных технологий, обеспечивающую его единство и территориальную целостность, в том числе в электронном пространстве, осуществляющую посредством государственного электронного механизма управление делами общества, суверенную публичную власть, придающую праву общеобязательное значение, гарантирующую права, свободы граждан, законность и правопорядок [2].

27 июля 2010 г. в России принят Федеральный закон «Об организации предоставления государственных и муниципальных услуг», который дает право заявителям получить такую услугу, в том числе в электронном виде. Этому праву корреспондирует обязанность органов государственной власти совершать предоставление услуг в электронном виде. Для реализации данной идеи был создан единый интернет-портал – gosuslugi.ru.

Указанный Федеральный закон определяет предоставление государственных и муниципальных услуг в электронной форме как их предоставление с использованием информационно-телекоммуникационных технологий, в том числе с использованием портала государственных и муниципальных услуг, многофункциональных центров, универсальной электронной карты и других средств, включая осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями [3].

Более того, в целях обеспечения информационной открытости деятельности органов исполнительной власти и органов местного самоуправления, повышения качества и доступности, предоставляемых ими государственных и муниципальных услуг, Министерство экономического развития Российской Федерации – упол-

номоченный Правительством РФ федеральный орган исполнительной власти ведет Федеральный реестр государственных и муниципальных услуг (функций) [4].

Электронное государство необходимо понимать как форму организации деятельности органов государственной власти в виртуальном пространстве, обеспечивающую за счет широкого использования информационно-коммуникационных технологий оптимизацию государственного управления, усиление открытости государства и реализацию конституционных прав и свобод граждан. Одной из основных особенностей электронного государства является виртуализация (дублирование) объектов реальности, то есть перенесение их аналогов в электронную форму (например, получение сведений из государственного реестра прав на недвижимое имущество и сделок с ним, федерального регистра нормативных правовых актов, реестра адвокатов субъектов Российской Федерации и т.п.).

Для современного демократического государства информирование граждан о фактах деятельности государственных органов и публичное обсуждение этих фактов являются основой механизмов общественного контроля деятельности государства. Доступность информации о деятельности государства положена в основу механизмов гражданского общества, а также в основу механизмов демократии. Все развитые демократии мира строят и развивают системы обеспечения доступа граждан к информации государства.

Нужно особо отметить, что использование современных информационно – коммуникационных технологий (ИКТ) позволяет значительно повысить информационную прозрачность государства и снизить затраты граждан и хозяйствующих субъектов на ознакомление с информацией о деятельности государства. Раскрытие информации является важным аспектом в таких сферах взаимодействия граждан и государства, как государственный учет, оказание государственных услуг, надзор и контроль и т. д. Внедрение информационно – коммуникационных технологий позволяет представить информационную открытость процессов и результатов государственного управления. Появление «электронного государства», широко использующего информационно – коммуникационные технологии, позволяет обеспечить качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов.

20 октября 2010 года распоряжением Правительства Российской Федерации № 1815-р утверждена Государственная программа Российской Федерации «Информационное общество (2011-2020 годы)» [5], которая пришла на смену Федеральной целевой программы «Электронная Россия» и позволяет в процессе своей реализации существенно продвинуться во внедрении технологий «электронного государства».

В настоящее время создана инфраструктура электронного правительства как комплекс вычислительных и телекоммуникационных средств, программного обеспечения, нормативно-правового и методического обеспечения. Однако базы данных учетной информации о ключевых объектах государственного управления отрывочны и охватывают незначительный временной горизонт.

Государственный учет данных о лицах, объектах явлениях осуществляются **в целях**:

а) реализации права на поиск, получение, передачу, производство и распространение информации;

б) информационного обеспечения государственной политики Российской Федерации и повышения эффективности государственного управления;

в) интеграции информационных ресурсов государства;

г) создания системы государственных информационных услуг на основе межведомственного взаимодействия органов государственной власти с применением информационных технологий;

д) создания системы мониторинга информационных учетных систем, как информационных ресурсов для обеспечения полноты, достоверности и актуальности информации.

Государственные учетные системы федеральных, региональных и муниципальных информационных систем и содержащейся в них информации (информационных ресурсов), формируется и функционирует на основе следующих **принципов**:

а) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

б) открытости информации о деятельности государственных органов и органов местного

самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

в) достоверности информации и своевременности ее предоставления;

г) применения современных информационных технологий для обеспечения автоматизированной обработки сведений и их передачи по цифровым линиям связи;

д) соблюдения конфиденциальности информации ограниченного доступа;

е) применения средств электронной подписи или иных аналогов собственноручной подписи для подтверждения подлинности электронных документов.

Учет распространен в органах государственной власти и управления повсеместно, но известен под разными именами. Регистрация актов гражданского состояния, кадастровый учет земли и недвижимости, учет выданных лицензий, учет нормативных правовых актов, муниципальных образований и их уставов, учет водных объектов и других полезных ископаемых, персональный учет населения, учет адресных льгот – вот лишь небольшая часть перечня систем государственного учета. Создаются общие государственные информационные ресурсы (регистры, кадастры, реестры, классификаторы). В большинстве своем государственный учет связан с правовыми последствиями для объекта учета.

С ведением того или иного вида учёта связано выполнение большинства государственных функций, в том числе оказание всех государственных услуг. Интересы граждан требуют сделать деятельность по ведению государственного учёта (сбору и хранению данных государства) официальной, осуществляемой по публично известным правилам и влекущей правовые последствия в соответствии с законом.

В связи с построением информационного общества и внедрением современных информационных технологий во все сферы жизни особую актуальность в настоящее время приобретают вопросы реализации права на поиск, получение, передачу, производство и распространение информации, информационного обеспечения государственной политики Российской Федерации, направленной на повышение эффективности государственного управления. Органы государственной власти имеют право осуществлять сбор и хранение информации только в целях обеспечения возможности реализации, гражданами и юридическими лицами установленных законом прав и обязанностей, а также в целях осуществления установленных законом государственных функций. Без официального публичного информирования о видах сбора и хранения информации государством и о целях этой деятельности нельзя говорить о прозрачности и подконтрольности государства. Ведение учета должно быть закреплено законодательно, регламентировано и общеизвестно, включая учетные данные, процедуры ведения учета и получения доступа к данным.

Кроме того, государственный учет и регистрация информационных систем и ресурсов необходимы для создания системы навигации на основе мониторинга государственных (федеральных и региональных), а также муниципальных и иных информационных систем и ресурсов, их учета и интеграции, а также обеспечения решения задач по предоставлению государственных информационных услуг на основе применения информационных технологий в рамках системы межведомственного взаимодействия органов государственной власти.

Государственная программа Российской Федерации «Информационное общество (2011–2020 годы)», утвержденная распоряжением Правительства РФ от 20.10.2010 № 1815-р. предусматривает внедрение информационных технологий для осуществления учетной деятельности в автоматизированном режиме и обеспечение взаимосвязи всех видов учета и отчетности государственных органов, в том числе с показателями результативности их деятельности.

В настоящее время в соответствии с Распоряжением Правительства Российской Федерации от 25.04.2006 № 584-р «Об утверждении перечня регистров, реестров, классификаторов и номенклатур, отнесенных к учетным системам федеральных органов государственной власти» [6] в указанном перечне значатся 40 таких учетных систем. К сожалению, за 6 лет после принятия этого правового акта Правительства РФ перечень не получил своего развития. Не приняты предусмотренные указанным актом правила отнесения регистров, реестров, классификаторов и номенклатур к учетным системам федеральных органов государственной власти, в которых должно быть предусмотрено обязательное включение в число учетных систем федеральных органов государственной власти:

регистров, реестров, классификаторов и номенклатур, содержащих сведения, которые

оказывают непосредственное влияние на осуществление или ограничение прав граждан или организаций;

регистров, реестров, классификаторов и номенклатур, общих для федеральных органов государственной власти.

Также не приняты правила формирования и ведения перечня учетных систем федеральных органов государственной власти и обеспечения доступа к такому перечню.

Следует отметить, что государственная регистрация баз и банков данных, в том числе содержащие учетные данные, была введена в 1996 году в соответствии с Постановлением Правительства Российской Федерации от 28.02.1996 № 226 «О государственном учете и регистрации баз и банков данных». Указанный нормативный правовой акт признан утратившим силу в 2009 году в связи с принятием Постановления Правительства РФ от 10.09.2009 № 723 «О порядке ввода в эксплуатацию государственных информационных систем» [7]. Но в целом проблема с государственными учетными системами – государственными информационными ресурсами продолжает оставаться нерешенной.

Описание общих механизмов учёта и особенностей ведения учёта в органах государственной власти и управления необходимо для классификации систем учёта, уже существующих и вновь создаваемых в органах государственной власти и управления. Принятие нормативных актов, регламентирующих учётную деятельность, должно опираться на единую систему понятий.

Ведением учёта называют деятельность по сбору и хранению определённого состава индивидуализированных данных об идентифицируемых лицах, объектах и/или явлениях различной природы.

Такие понятия, как «регистрация» или «ведение реестра» являются синонимами учёта. Использование этих терминов для описания какой-либо деятельности служит признаком того, что данная деятельность включает ведение учёта.

Учётные данные – данные, являющиеся предметом сбора и хранения в рамках ведения учёта.

Учётное событие – любое изменение учётных данных.

Предмет учёта – субъекты, юридические факты, объекты или реальные обстоятельства, данные о которых подлежат сбору и хранению в рамках ведения учёта.

Система учёта, учётная система – совокупность:

- нормативно-правовых актов, договоров, регламентов, стандартов, внутренних положений и инструкций организатора учёта и регистраторов, иных документов, предписывающих ведение учёта, определяющих процедуры ведения учёта и формы ведения учёта;
- организационных структур организатора учёта и регистраторов;
- средств, обеспечивающих ведение учёта, включая средства делопроизводства, инженерно-техническое оборудование и информационно-коммуникационные компьютерные приложения, реализующие логику учёта, а также исходные тексты, системную и пользовательскую документацию этих компьютерных приложений.

Электронный учёт – учет, данные которого могут существовать и быть использованы (в том числе для определения прав и обязанностей лиц и иных правовых последствий учётных событий) исключительно в электронной форме.

Государственный учёт – учёт, организатором которого выступают органы государственной власти и управления. Под государственным учётом информационных ресурсов понимается упорядоченное осуществление органами власти или уполномоченными ими организациями, структурными подразделениями и должностными лицами, сбора в электронной форме сведений о лицах, объектах, процессах и/или явлениях различной природы, а также обеспечивающих её обработку информационных технологиях и технических средствах, и их систематизация.

Федеральные органы исполнительной власти обеспечивают в соответствии с установленной сферой деятельности сбор данных для обязательной государственной регистрации:

Кадастровый учёт – государственный учёт, предметом которого являются исключительно объекты, сбор данных для которых не связан с обязанностью каких-либо лиц предоставлять эти данные.

К числу важнейших систем государственного учёта относятся [8]:

- Паспортная система.
- Система записи актов гражданского состояния.
- Система регистрации юридических лиц, индивидуальных предпринимателей, налогоплательщиков.

- Система регистрации прав на недвижимое имущество.
- Система правовой информации.

Система правовой информации, содержащая учётные данные о нормативных правовых актах, конечно, включает в себя также и многие данные вышеперечисленных систем.

В сфере государственной регистрации прав на недвижимость и государственного кадастрового учёта недвижимости предоставляются следующие виды государственных услуг:

- государственная регистрация прав, ограничений (обременений) прав на недвижимость и сделок с ней;
- государственный кадастровый учёт объектов недвижимости;
- предоставление сведений из государственного кадастра недвижимости и Единого государственного реестра прав на недвижимое имущество и сделок с ним.

Учётные системы федеральных органов исполнительной власти (регистры, реестры, классификаторы, номенклатуры) являются федеральными информационными ресурсами. На это прямо указано во многих нормативных правовых актах[9].

Выше подчёркивалось значение многих видов учётных систем, это, прежде всего, реестры, учётные данные которых приобретают юридическую значимость при их включении в учётную систему. К таким учетным системам (информационным ресурсам) относятся, например, государственный реестр нормативных правовых актов федеральных органов исполнительной власти, который ведется Минюстом России в соответствии с Положением о Министерстве юстиции Российской Федерации, утвержденным Указом Президента РФ от 13.10.2004 № 1313. Назовём также другие органы государственной власти, которые создают соответствующие учётные системы, например:

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций формирует реестр зарегистрированных средств массовой информации и реестра лицензий на телевизионное вещание, радиовещание [10];

Федеральная служба по труду и занятости в соответствии с Постановлением Правительства от 30.06.2004 № 324 ведет в установленном порядке регистры получателей государственных услуг в сфере занятости населения [11];

Федеральное медико-биологическое агентство – регистр работников, занятых на работах с химическим оружием, радиационно-эпидемиологический регистр работников обслуживаемых организаций и населения обслуживаемых территорий [12];

Министерство здравоохранения и социального развития Российской Федерации – реестр курортного фонда Российской Федерации, реестр лекарственных средств для медицинского применения; реестр исследователей, проводящих (проводивших) клинические исследования лекарственных препаратов для медицинского применения [13].

Формирование учетных систем в электронном виде включает электронное взаимодействие на самых разных уровнях. Это взаимоотношения между государственными службами и гражданами, между государством и частными компаниями, государственными организациями и их сотрудниками, а также между различными государственными органами и уровнями государственного управления. В целях такого взаимодействия федеральных органов исполнительной власти для реализации задачи по предоставлению государственных услуг и исполнению государственных функций в электронном формате принято Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» [14].

Система электронного взаимодействия представляет собой федеральную государственную информационную систему, включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам, в том числе учетным системам, сведения об истории движения в системе взаимодействия электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме.

Целью создания этой информационной системы является технологическое обеспечение информационного взаимодействия при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме.

Основными функциями единой системы межведомственного электронного взаимодействия являются:

а) обеспечение передачи запросов, иных документов и сведений, необходимых для получения государственных и муниципальных услуг и поданных заявителями через единый портал, в подключенные к системе взаимодействия информационные системы органов и организаций, обязанных предоставить испрашиваемые государственные (муниципальные) услуги;

б) обеспечение обмена электронными сообщениями между органами и организациями, информационные системы которых подключены к системе взаимодействия, при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций;

в) обеспечение передачи на единый портал запросов, иных документов и сведений, обработанных в информационных системах органов и организаций, а также информации о ходе выполнения запросов о предоставлении государственных или муниципальных услуг и результатах их предоставления.

Задача перевода в электронный вид государственной учётной деятельности, определяемая государственной программой Российской Федерации «Информационное общество (2011–2020 годы)», должна быть обеспечена необходимым правовым регулированием. В настоящее время эта деятельность не рассматривается как самостоятельный объект законодательного регулирования. Отсутствует нормативно закреплённый состав требований к процедурам формирования, ведения, обработки и хранения юридически значимой информации. Вместе с тем действующее информационное законодательство (имеется в виду вся система нормативных правовых актов) достаточно полно обеспечивает ведение таких информационно-учётных систем, как регистры и реестры нормативных правовых актов.

В соответствии с распоряжением Правительства Российской Федерации от 27.12.2011 № 2387-р «О Концепции создания и развития государственной информационной системы учёта информационных систем, разрабатываемых и приобретаемых за счет средств бюджетов бюджетной системы Российской Федерации» была представлена концепция создания информационной системы учёта всех информационных систем в стране.

Основными направлениями создания и развития системы учёта информационных систем являются:

- обеспечение единства (комплексности) принципов создания, внедрения и эксплуатации информационных систем на всех уровнях государственного управления;
- повышение эффективности использования информационных технологий государственными органами;
- раскрытие информации об использовании информационных систем государственными органами.

На сегодняшний день все меньше и меньше сведений государства фиксируется ручкой на бумаге. Однако официально учёт сведений, используемых для осуществления многочисленных функций государственного управления, ведётся в бумажном виде, при этом реально «бумажный вид» готовится с использованием информационных технологий.

Законодательные нормы должны сделать возможным ведение учёта действительно в электронной форме. Кроме этого, законодательство должно предписать изменение статуса существующих и использующих сегодня так называемых «информационных» систем сбора и хранения данных, превратив их в системы достоверного и официального учета в электронной форме.

Использование ИКТ позволит распространить средства обеспечения достоверности данных учета практически на все виды учёта, существующие в стране.

Ведение учёта должно быть закреплены законодательно, должны быть известны и закреплены в нормативной правовой базе цели и правовые последствия внесения в государственные учётные системы тех или иных данных. Вся совокупность входящих в учётную систему договоров, стандартов, внутренних положений и инструкций, компьютерных программ, обеспечивающих ведение государственного учёта, должна вводиться в действие и корректироваться с соблюдением публичной процедуры, аналогичной процедуре введения в действие и корректировки таких компонентов учётной системы, как нормативные правовые акты.

Литература.

1. Электронное правительство // Твоя война; www.warweb.ru.
2. Васькова М.Г. Электронное государство: проблемы правового регулирования // Информационное право. 2009. № 4.

3. См. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. – 2010. – № 31. – Ст. 4179.
4. См. Постановление Правительства РФ от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» // СЗ РФ. – 2011. – № 44. – Ст. – 6274.
5. СЗ РФ. – 2010. – № 46. – Ст. 6026. 2011. – № 22. – Ст. 3173; № 51. – Ст. 7543; 2012. № 4. Ст. 514.
6. СЗ РФ. – 2006. – № 18. – Ст. 2055.
7. СЗ РФ. – 2009. – № 37. – Ст. 4416.
8. Автор не ставил своей задачей осветить все информационно-учетные системы органов государственной власти. Понятно, что это невозможно, в силу многочисленности их функций
9. См., например, Федеральный закон от 08.08.2001 № 129 (ред. от 01.04.2012) «О государственной регистрации юридических лиц и индивидуальных предпринимателей» // СЗ РФ. – 2001. – № 33 (часть 1). – Ст. – 3431.
10. Постановление Правительства РФ от 26.01.2012 № 24 «О государственной информационной системе в области средств массовой информации» // СЗ РФ. – 2012. – № 6. – Ст. 669.
11. СЗ РФ. – 2004. – № 28. – Ст. 2901.
12. Постановление Правительства РФ от 11.04.2005 № 206 «О Федеральном медико-биологическом агентстве// СЗ РФ. – 2005. – № 16. – Ст. 1456.
13. Постановление Правительства РФ от 30.06.2004 № 321 «Об утверждении Положение о Министерстве здравоохранения и социального развития Российской Федерации// СЗ РФ. – 2004. – № 28. – Ст. 2898.
14. СЗ РФ. – 2010. – № 38. Ст. 4823.

Бекетнова Юлия Михайловна
Крылов Григорий Олегович,
доктор физико-математических наук, кандидат юридических наук
Фомин Ярослав Алексеевич,
доктор технических наук

Выявление рисков нарушения финансовой и информационной безопасности

Аннотация: *рассматривается проблема распознавания субъектов финансовой и информационной безопасности. В статье приведен пример диагностики организаций на предмет выявления рисков нарушения финансовой и информационной безопасности.*

Ключевые слова: *оценка рисков, информационная безопасность, распознавание образов.*

Введение

Теория распознавания образов [1] широко применяется при решениии задач сканирования, диагностики, радиоразведки, квалификации правонарушений и в других областях. Представляет интерес примение этой теории в задачах финансовой и информационной безопасности.

Актуальность работы. Решение задачи оценки субъектов финансовой и информационной безопасности в интересах своевременного выявления рисков правонарушений является одним из приоритетных направлений исследований проблем финансовой и информационной безопасности. Ниже приведен пример статистического оценивания благонадежности организаций на основе теории распознавания образов.

В соответствии с теорией распознавания образов выбираются соответственно m1 лучших и m2 худших организаций. Лучшими в рамках настоящего исследования будем считать организации – члены Российского союза промышленников и предпринимателей, худшими – организации, ликвидированные по решению арбитражных судов. Для определенности выберем по пять организаций из каждой группы, которые будем оценивать по следующим признакам: количество филиалов и дочерних компаний; количество организаций, имеющих номер телефона, указанный в документах исследуемой компании; количество организаций, в которых руководитель совмещает должность руководителя и учредителя; количество компаний, которыми руководит директор исследуемой организации (см. таблицу)

№	Признак	Организации – члены Российского союза промышленников и предпринимателей S1					Организации, ликвидированные по решению суда S2				
		$X_1^{(1)}$	$X_2^{(1)}$	$X_3^{(1)}$	$X_4^{(1)}$	$X_5^{(1)}$	$X_1^{(2)}$	$X_2^{(2)}$	$X_3^{(2)}$	$X_4^{(2)}$	$X_5^{(2)}$
1	Количество филиалов и дочерних компаний	2	6	0	11	17	0	0	0	0	0
2	Количество организаций, имеющих номер телефона, указанный в документах исследуемой компании	54	1	1	1	1	1	1	1	1	1
3	Количество организаций, в которых руководитель совмещает должность руководителя и учредителя	1	0	0	2	0	4	1	19	8	8
4	Количество компаний, которыми руководит директор исследуемой организации	4	3	2	4	2	6	2	20	8	12

Рассмотрим вначале признаковое пространство, состоящее из первых трех признаков.

Для групп предприятий S_1 и S_2 составим векторы средних (соответственно a_1 и a_2), а также их разность (a_1-a_2) и сумму (a_1+a_2):

$$a_1 = \frac{1}{m1}\sum_{i=1}^{m1} x_i^{(1)} = \begin{bmatrix} 7{,}2 \\ 11{,}6 \\ 0{,}6 \end{bmatrix},$$

$$a_2 = \frac{1}{m2}\sum_{i=1}^{m2} x_i^{(2)} = \begin{bmatrix} 0 \\ 1 \\ 8 \end{bmatrix},$$

$$a_1 - a_2 = \begin{bmatrix} 7{,}2 \\ 10{,}6 \\ -7{,}4 \end{bmatrix}, \quad a_1 + a_2 = \begin{bmatrix} 7{,}2 \\ 12{,}6 \\ 8{,}6 \end{bmatrix}.$$

Вычислим ковариационные матрицы M_1 и M_2, где m_1 и m_2 количество организаций – членов Российского союза промышленников и предпринимателей и организаций, ликвидированных по решению суда соответственно (здесь $m_1 = m_2 = 5$).

Ковариационная матрица m_1 имеет вид:

$$M_1 = \frac{1}{m1-1}\sum_{i=1}^{m1} (X_i^{(1)} - a_1)(X_i^{(1)} - a_1)^T \quad (1)$$

$$M_1 = \begin{pmatrix} 47{,}7 & -68{,}9 & 0{,}6 \\ -68{,}9 & 561{,}8 & 5{,}3 \\ 0{,}6 & 5{,}3 & 0{,}8 \end{pmatrix}.$$

Ковариационная матрица M_2 имеет вид:

$$M_2 = \frac{1}{m2-1}\sum_{i=1}^{m2} (X_i^{(2)} - a_2)(X_i^{(2)} - a_2)^T. \quad (2)$$

$$M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 46{,}5 \end{pmatrix}.$$

Найдем общую ковариационную матрицу M

$$M = \frac{1}{m1+m2-2} * (m_1 M_1 + m_2 M_2)$$

$$M = \begin{pmatrix} 29{,}813 & -43{,}063 & 0{,}375 \\ -43{,}063 & 351{,}125 & 3{,}313 \\ 0{,}375 & 3{,}313 & 29{,}563 \end{pmatrix} \quad (3)$$

и обратную ковариационную матрицу M^{-1}

$$M^{-1} = \begin{pmatrix} 0{,}041 & 5{,}014 * 10^{-3} & -1{,}079 * 10^{-3} \\ 5{,}014 * 10^{-3} & 3{,}467 * 10^{-3} & -4{,}521 * 10^{-4} \\ -1{,}079 * 10^{-3} & -4{,}521 * 10^{-4} & 0{,}034 \end{pmatrix}$$

Для определения достоверности D_3 вычислим расстояние Махалонобиса

$$d_3^2 = \frac{1}{2} * (a_1 - a_2)^T * M^{-1} * (a_1 - a_2)$$

$d_3^2 = 2{,}6569$, $d_3 = 1{,}63$.

Найдем σ_1 и σ_2, где $m_1 = m_2 = 5$, а значение n для упрощения вычислений выберем минимальным n=1

$$\sigma_1^2 = \frac{1}{m_1} + \frac{1}{m_2}; \; \sigma_1^2 = \frac{1}{m_1} + \frac{1}{m_2} + \frac{4}{n}; \quad (4)$$

$\sigma_1 = 0{,}632$; $\sigma_2 = 2{,}121$.

Найдем вероятности ошибок распознавания $\alpha_3 = \beta_3$ по формуле

$$\alpha_3 = \beta_3 = F\left(-\frac{d_3}{\sigma_2}\right) + \left(\frac{\sigma_2}{d_3\sqrt{2\pi}}\right) * \exp\left(-\frac{d_3^2}{2\sigma_2^2}\right) *$$

$$* \left[\left(\frac{\sigma_2^2}{\sigma_2^2 - \sigma_1^2}\right)^{\frac{p-1}{2}} - 1\right],$$

где F(z) – табулированный интеграл вероятности.

Достоверность распознавания равна

$D_3 = 1 - \alpha_3 = 1 - \beta_3 = 0{,}73$.

Поскольку достоверность распознавания D3 при трех признаках оказывается недостаточно высокой, добавим еще один показатель (№4) – количество компаний, которыми руководит директор исследуемой организации.

Для групп предприятий S_1 и S_2 составим векторы средних (соответственно a_1 и a_2), а также их разность (a_1-a_2) и сумму (a_1+a_2)

$$a_1 = \frac{1}{m1}\sum_{i=1}^{m1} x_i^{(1)} = \begin{bmatrix} 7{,}2 \\ 11{,}6 \\ 0{,}6 \\ 3 \end{bmatrix},$$

$$a_2 = \frac{1}{m2}\sum_{i=1}^{m2} x_i^{(2)} = \begin{bmatrix} 0 \\ 1 \\ 8 \\ 9{,}6 \end{bmatrix}.$$

и вычислим ковариационные матрицы: M1 и M2 по формулам (1) и (2):

$$M_1=\begin{pmatrix} 47,7 & -68,9 & 0,6 & -1 \\ -68,9 & 561,8 & 5,3 & 13,25 \\ 0,6 & 5,3 & 0,8 & 0,75 \\ -1 & 13,25 & 0,75 & 1 \end{pmatrix},$$

$$M_2=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 46,5 & 45,5 \\ 0 & 0 & 45,5 & 46,8 \end{pmatrix}.$$

Найдем общую ковариационную матрицу M по формуле (3):

$$M=\begin{pmatrix} 29,813 & -43,063 & 0,375 & -0,625 \\ -43,063 & 351,125 & 3,313 & 8,281 \\ 0,375 & 3,313 & 29,563 & 28,906 \\ -0,625 & 8,281 & 28,906 & 29,875 \end{pmatrix}$$

и обратную ковариационную матрицу M^{-1}

$$M^{-1}=\begin{pmatrix} 0,041 & 0,00489 & -0,011 & 0,009905 \\ 0,00489 & 0,003569 & 0,007521 & -0,008164 \\ -0,011 & 0,007521 & 0,656 & -0,637 \\ 0,009905 & -0,008164 & -0,637 & 0,653 \end{pmatrix}$$

Для определения достоверности D_4 вычислим расстояние Махалонобиса:

$$d_4^2 = \frac{1}{2}*(a_1-a_2)^T*M^{-1}*(a_1-a_2),$$

d_4=1,666.

Значения σ_1 и σ_2 совпадают с (4), т.к. $m_1 = m_2 = 5$ и $n = 1$ не изменяются.

Вероятность ошибок распознавания $\alpha_4=\beta_4$ вычисляются по формуле

$$\alpha_4=\beta_4=F\left(-\frac{d_4}{\sigma_2}\right) + \left(\frac{\sigma_2}{d_4\sqrt{2\pi}}\right)*\exp\left(-\frac{d_4^2}{2\sigma_2^2}\right)*$$

$$*\left[\left(\frac{\sigma_2^2}{\sigma_2^2-\sigma_1^2}\right)^{\frac{p-1}{2}} - 1\right],$$

$D_4= 1- \alpha_4 = 1- \beta_4 = 0,73$.

Поскольку достоверность распознавания D3 при трех признаках оказывается недостаточно высокой, добавим еще один показатель (№4) – количество компаний, которыми руководит директор исследуемой организации.

Для групп предприятий S_1 и S_2 составим векторы средних (соответственно a_1 и a_2), а также их разность (a_1-a_2) и сумму (a_1+a_2)

$$a_1 = \frac{1}{m1}\sum_{i=1}^{m1} x_i^{(1)}=\begin{bmatrix} 7,2 \\ 11,6 \\ 0,6 \\ 3 \end{bmatrix},$$

$$a_2 = \frac{1}{m2}\sum_{i=1}^{m2} x_i^{(2)}=\begin{bmatrix} 0 \\ 1 \\ 8 \\ 9,6 \end{bmatrix}.$$

и вычислим ковариационные матрицы: M_1 и M_2 по формулам (1) и (2):

$$M_1=\begin{pmatrix} 47,7 & -68,9 & 0,6 & -1 \\ -68,9 & 561,8 & 5,3 & 13,25 \\ 0,6 & 5,3 & 0,8 & 0,75 \\ -1 & 13,25 & 0,75 & 1 \end{pmatrix},$$

$$M_2=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 46,5 & 45,5 \\ 0 & 0 & 45,5 & 46,8 \end{pmatrix}.$$

Найдем общую ковариационную матрицу M по формуле (3):

$$M=\begin{pmatrix} 29,813 & -43,063 & 0,375 & -0,625 \\ -43,063 & 351,125 & 3,313 & 8,281 \\ 0,375 & 3,313 & 29,563 & 28,906 \\ -0,625 & 8,281 & 28,906 & 29,875 \end{pmatrix}$$

и обратную ковариационную матрицу M^{-1}

$$M^{-1}=\begin{pmatrix} 0,041 & 0,00489 & -0,011 & 0,009905 \\ 0,00489 & 0,003569 & 0,007521 & -0,008164 \\ -0,011 & 0,007521 & 0,656 & -0,637 \\ 0,009905 & -0,008164 & -0,637 & 0,653 \end{pmatrix}$$

Для определения достоверности D_4 вычислим расстояние Махалонобиса:

$$d_4^2 = \frac{1}{2}*(a_1-a_2)^T*M^{-1}*(a_1-a_2),$$

d_4=1,666.

Значения σ_1 и σ_2 совпадают с (4), т.к. $m_1 = m_2 = 5$ и $n = 1$ не изменяются.

Вероятность ошибок распознавания $\alpha_4=\beta_4$ вычисляются по формуле

$\alpha_4=\beta_4=F(-\frac{d_4}{\sigma_2}) + (\frac{\sigma_2}{d_4\sqrt{2\pi}})*\exp(-\frac{d_4^2}{2\sigma_2^2})*$

$*\left[\left(\frac{\sigma_2^2}{\sigma_2^2-\sigma_1^2}\right)^{\frac{p-1}{2}} - 1\right]$,

$D_4= 1- \alpha_4 = 1- \beta_4 = 0{,}73$.

Для установления оптимальной размерности p признакового пространства вычислим отношение расстояний Махалонобиса d_4^2 (при p = 4) и d_3^2 (при p = 3).

$\frac{d_4^2}{d_3^2} = 1{,}045 < \sqrt{p} = \sqrt{4} = 2$.

Т.к. $\frac{d_4^2}{d_3^2} = 1{,}045 < \sqrt{p} = \sqrt{4} = 2$, то оптимальная размерность признакового пространства p = 4.

Вычислим теперь обобщенный показатель благонадежности организации $\ln L$ при n = 1.

$\ln L = \frac{1}{2}*(a_1-a_2)^T*M^{-1}[2\,X_i - (a_1 + a_2)]$,

$\frac{1}{2}*(a_1-a_2)^T*M^{-1} = (0{,}18\ \ 0{,}036\ -0{,}324\ 0{,}197)$.

Организация №1

№	Признак	Значение признака
1	Количество филиалов и дочерних компаний	120
2	Количество организаций, имеющих номер телефона, указанный в документах исследуемой компании	1
3	Количество организаций, в которых руководитель совмещает должность руководителя и учредителя	0
4	Количество компаний, которыми руководит директор исследуемой организации	1

X_i	X_1
$2\,X_i - (a_1 + a_2)$	232,8
	-6,6
	-12,6
	1,706
$\ln L$	46,187

Организация №2

№	Признак	Значение признака
1	Количество филиалов и дочерних компаний	0
2	Количество организаций, имеющих номер телефона, указанный в документах исследуемой компании	1
3	Количество организаций, в которых руководитель совмещает должность руководителя и учредителя	45
4	Количество компаний, которыми руководит директор исследуемой организации	35

X_i	X_1
$2\,X_i - (a_1 + a_2)$	-7,2
	-6,6
	77,4
	69,706
$\ln L$	-12,884

Таким образом, можно утверждать, что Организация №1 является благонадежной, а Организация №2 – неблагонадежной.

Выводы: Применение теории распознавания образов при анализе признакового пространства организаций позволяет получить новые количественные оценки финансовой и информационной безопасности

Чеботарева Анна Александровна,
кандидат юридических наук

Механизмы электронной демократии: возможности и проблемы их реализации в Российской Федерации

Аннотация: *рассматривается понятие и сущность электронной демократии, анализируются механизмы электронной демократии, предусмотренные Проектом Концепции развития в Российской Федерации механизмов электронной демократии до 2020 года.*

Ключевые слова: *электронная демократия, электронное правительство, электронное государство, электронное голосование, цифровое неравенство, информационная безопасность.*

Наряду с построением правового, конституционного, социального государства провозглашаемая сегодня важнейшая задача – построение государства электронного.

Как соотносятся между собой понятия «электронное правительство» и «электронное государство»? В российской правовой литературе английский термин E-Government получил несколько переводов. Чаще он переводится как «электронное правительство». Такой перевод допустим, но он сужает понятие, по существу сводя вопрос только к исполнительной власти. Термин «электронное государство» не только больше соответствует английскому эквиваленту, но и подчеркивает, что речь идет обо всех трех ветвях власти – законодательной, исполнительной и судебной[a].

Сегодня возможно лишь констатировать недостаточный уровень информированности общества, конкретного человека(о законотворчестве, госуслугах, обо всех процессах, происходящих во властных структурах, являясь сдерживающим фактором развития принципа открытости власти).

Электронное государство – это, прежде всего, как справедливо отмечает в своих работах И.Л. Бачило[b], социальное государство, в свою очередь социальное государство в определенной части является сервисным государством, то есть предоставляющим услуги. При этом нужно иметь в виду, что только сервисные задачи и работа в этом направлении не исчерпывают функций государственных и муниципальных органов в области социальной сферы. Это, пожалуй, конечный итог каждой социальной функции – предоставить условия для граждан и организаций реализовать свои социальные и иные права.

Необходимо отметить, что современная Россия переживает один из наиболее сложных этапов информатизации – процесс адаптации и коренной перестройки государства на пути к его «электронной версии». И в этом процессе далеко не последняя роль должна отводиться полноценному обеспечению прав и свобод человека. Действительно, «во всех подходах к понятию электронного государства прослеживается его негативная черта – ориентация на общеуниверсальное представление о личности и человеке, отсутствие индивидуальных особенностей при совершении каких – либо юридических действий. Развитые информационно – коммуникационные технологии могут явиться мощным инструментом подавления населения и стать предпосылкой возникновения антидемократического режима. Поэтому законодательство переживающего становление электронного государства должно содержать гарантии пресечения противоправного вмешательства в жизнь и сознание людей в определенных интересах, а также быть готово к информационным изменениям и отражать основные вопросы его функционирования»[c].

Проиллюстрируем сказанное на примере концепции развития в России электронной демократии. Одна из задач электронной демократии сегодня – максимально полно привлечь граждан к участию в принятии решений госу-

дарственной властью. Госвласть вызывает к себе шквал критики, поскольку люди видят ее неэффективность, но при этом власть сегодня закрыта от прямого общения с гражданами.

И в этом смысле механизмы электронной демократии могут оказаться актуальными и эффективными. И что самое важное – они могут изменить взаимоотношения власти и граждан в сторону позитивного партнерства, обоюдной ответственности!

Обсуждаемый сегодня проект Концепции развития в Российской Федерации механизмов электронной демократии до 2020 года[d] является как никогда своевременным и необходимым.

Именно сегодня «наряду с тем, что в большинстве сфер деятельности государства происходят позитивные изменения в реализации реформ, развитие информационной организации государства объективно переживает сложный период. В результате информационная сфера, ее ресурсы, в том числе и их защищенность, отстают в развитии от других институтов современного российского общества. Данное обстоятельство негативно сказывается не только на информационной организации государства, но и на состоянии информационной безопасности России, информационной безопасности личности и всего общества в целом. Не вызывает сомнений, что процесс внедрения инструментов электронной демократии в реалии современной России неизбежен и необратим.

Под *электронной демократией* понимается такая форма организации общественно-политической деятельности граждан, которая обеспечивает за счет широкого применения информационно-коммуникационных технологий качественно новый уровень взаимодействия граждан друг с другом, с органами государственной власти, органами местного самоуправления, общественными организациями и коммерческими структурами

Единая система электронной демократии Российской Федерации (ЕСЭД) представляет собой единую общероссийскую информационно-коммуникационную платформу (единую «точку входа») и специальный программно-аппаратный комплекс, обеспечивающий ведение на официальных интернет-ресурсах органов власти разделов электронной демократии, состоящих из взаимосвязанных наборов функциональных блоков, поддерживаемых в части администрирования органами власти, а в части контентного наполнения совместно органами власти, гражданами и организациями.

Безусловно, «самым активным и часто уязвимым субъектом в эпоху перемен, а информатизация, цифровизация и сетевая жизнь информационной среды – это не что иное, как революция в развитии социума, остается человек, индивид, гражданин. И понять, что изменяется по воздействием информационно-технологических факторов чрезвычайно важно»[e].

К числу механизмов электронной демократии относятся:

- электронное голосование (голосование по мобильному телефону, интернет-выборы и т.д.);
- механизмы сетевой коммуникации граждан и коллективного обсуждения социально значимых проблем и вопросов общественно-политической тематики в режиме on-line;
- механизмы формирования онлайн-сообществ, включая механизмы планирования и реализации гражданских инициатив и проектов коллективных действий;
- механизмы сетевой коммуникации граждан с органами власти, включая инструменты воздействия на принятие решений и гражданский контроль за деятельностью органов власти;
- механизмы общественного онлайн-управления на муниципальном уровне.

Охарактеризуем каждый из механизмов.

1. Механизм электронного голосования.

Понятие «электронного голосования» отечественный законодатель определил в Федеральном законе Российской Федерации от 12 июня 2002 г. N 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»[f]. Это голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса средств автоматизации ГАС «Выборы». В свою очередь, под электронным бюллетенем понимается бюллетень, подготовленный программно-техническими средствами в электронном виде, применяемый при проведении электронного голосования.

2. Механизмы сетевой коммуникации граждан и коллективного обсуждения социально значимых проблем и вопросов общественно-политической тематики в режиме on-line.

До появления специализированных средств сетевого общения удаленная коммуникация по принципу многих со многими была крайне затруднена и практически невозможна. Так называемые технологии Web позволили ор-

ганизовывать массовые обсуждения с множеством независимых участников, территориально отдаленных друг от друга, в режиме реального времени. Сегодня нет необходимости собирать людей в каком-то замкнутом физическом пространстве с целью коллективного обсуждения каких-либо вопросов. Такое обсуждение можно с успехом организовать на специализированных интернет-ресурсах (форумы, интернет-конференции, вебинары, скайп-сессии и т.п.), на площадке практически любой социальной сети, а также в блогах. При этом упрощается коммуникация с труднодоступными аудиториями (территориально, инвалидами, в силу других причин). На ряде порталов в период предвыборных агитаций этот механизм получает воплощение в проектах «Интернет-дебаты».

3. Механизмы формирования онлайн-сообществ, включая механизмы планирования и реализации гражданских инициатив и проектов коллективных действий.

Коллективное обсуждение социально значимых проблем, а также формирование консолидированных позиций часто способствует тому, что в интернет-среде начинают складываться так называемые «сетевые сообщества» (онлайн-комьюнити), представленные в пространстве интернета и определяемые как группы людей, объединенные какими-либо общими интересами или проблемами, общающиеся между собой посредством интернет-ресурсов и/или мобильной связи с целью обсуждения различных общественных и политических вопросов и проблем. В ряде случаев такая форма общения может выступать своеобразным аналогом объединений граждан, собраний граждан, уличных пикетов, митингов, шествий или демонстраций. Обманутые дольщики, борцы с точечной застройкой или защитники окружающей среды фиксируют результаты своей работы на фото, аудио- или видео-носители. При этом современные цифровые технологии позволяют в считанные минуты отправлять такие изображения и записи на огромные расстояния, размещать их в общедоступных социальных медиа (блогах, форумах и социальных сетях), где эти материалы становятся достоянием общественности, а нередко и предметом судебных разбирательств. Публичное осуждение всё ещё продолжает оставаться механизмом действенной борьбы с различного рода недугами современной системы общественных отношений. Публичность позволяет более эффективно бороться с бюрократизмом и коррупцией в политической сфере. Однако в большинстве случаев неформальные публикации на форумах и в блогах не доходят до ответственных лиц: у публикаций на форумах и в блогах нет никакого официального статуса, законодательство не обязывает чиновников реагировать на такие публикации, и не всегда органы государственной власти имеют возможность своевременно узнавать о наличии таких публикаций. Более того, сегодня в среде госуправления принято считать такие публикации маргинальными в полном объеме и не заслуживающими объективного внимания и диалога.

К примеру интернет-комьюнити можно отнести форумчанинов новостных порталов.

Придание общественной огласки социально значимым проблемам является не единственным инструментом влияния на принятие необходимых общественно-политических решений. Онлайн-сообщества также используются их участниками как удобное средство планирования и организации реальных мероприятий. Большую популярность получили так называемые флеш-мобы, а также акции недовольства граждан, которые, к сожалению, в ряде случаев перерастают в массовые беспорядки и погромы. К примеру, акции «маршей миллионов».

4. Механизмы сетевой коммуникации граждан с органами власти, включая инструменты воздействия на принятие решений и гражданский контроль за деятельностью органов власти.

Речь о реальном, а не декларативном влиянии граждан на процесс общественно-политического управления. Одним из таких механизмов является формирование коллективных позиций в формате электронных обращений в уполномоченные организации, прежде всего, в органы государственной власти и местного самоуправления.

Коллективные обращения выражают консолидированное мнение пользователей по существу обсуждаемых вопросов. Консолидированное мнение – это полезный результат сетевого общения, один из важнейших элементов, на которых базируется электронная демократия.

В теории коллективных действий разработано множество моделей принятия коллективных решений. Одной из самых распространенных моделей является модель, при которой в среде коллектива выделяется некая малая– инициативная или рабочая – группа. Малая группа готовит проект коллективного решения и выкладывает его для открытого комментирования и общественной экспертизы. После сбора комментариев, предложений и оценок, а также

анализа содержания дискуссий, которые развернулись на интернет-ресурсе по существу данного проекта, рабочая группа дорабатывает проект коллективного решения, вносит в него правки. Далее может начаться повторное обсуждение проекта либо данный проект принимается за окончательный и высылается в ответственные организации. Также в отношении проекта коллективного решения может вводиться процедура голосования с применением модели относительного или квалифицированного большинства. Сервисы системы электронной демократии позволяют объединять множество поступающих заявлений от населения в коллективные обращения, что существенно экономит трудозатраты органов государственной власти и органов местного самоуправления по работе с обращениями граждан и организаций.

Важнейшим инструментом гражданского влияния и контроля за деятельностью органов власти являются оценочные процедуры. К разновидностям таких процедур в рамках систем электронной демократии следует отнести онлайн-опросы, онлайн-оценки, онлайн-рейтинги, онлайн-экспертизы и др. Пользователи системы электронной демократии коллективно оценивают деятельность органов власти, формируя тем самым некую консолидированную оценку. Оценочным процедурам могут подвергаться как общие вопросы эффективности работы того или иного органа власти, а также отдельные должностные лица, конкретные нормативно-правовые акты, планы действий, финансовые документы, ответы органов власти на обращения и запросы граждан и организаций и др.

Наибольшую популярность получили сегодня опросы в социальных медиа, где каждый участник того или иного онлайн-сообщества может организовать публичный опрос на любую тему, в том числе связанную с проблемами территории проживания.

5. Механизмы общественного онлайн-управления на муниципальном уровне.

Механизмы общественного онлайн-управления в отличие от механизмов общественного онлайн-обсуждения и контроля за деятельностью органов власти не получили на данный момент широкого распространения и реализации в формате специализированных интернет-ресурсов электронной демократии. Граждане в целях общественного онлайн-управления используют преимущественно площадки городских интернет-форумов, социальные сети, а также узкоспециализированные интернет-ресурсы, которые направлены на решение проблем определенной тематики для ограниченного круга лиц.

В российской действительности, говорить об общественном онлайн-управлении, тем более на муниципальном уровне, пока, к сожалению, рано.

Безусловно, «плюсов» в применяемых технологиях электронного голосования больше, чем достаточно. Тем не менее, возможных проблем тоже немало. Так – и это подчеркивается проектом Концепции – электронные технологии могут быть использованы и в качестве средств фальсификации результатов голосования; кроме того, не исключены серьезные сбои в функционировании автоматизированных комплексов, обеспечивающих электронное голосование. Поэтому крайне важно в рамках внедрения электронного голосования разрабатывать не только процедуры голосования, подсчета голосов, но и процедуры контроля данных процессов, а также процедуры верификации результатов голосования. И, безусловно, важнейшей проблемой электронного голосования продолжает оставаться проблема цифровой идентификации граждан, являющихся пользователями систем электронной демократии. Во многом данная проблема является главным препятствием на пути повсеместного внедрения механизмов электронного голосования на уровне выборов субъектов государственной и муниципальной власти. Эта проблема – не только проблема электронного голосования: идентификация гражданина при общении с органами власти – одна из наиболее сложных, требующих своего четкого решения проблема e-government[g].

В вопросе развития механизмов электронной демократии у большинства регионов России – еще все впереди. Создать эффективную систему электронной демократии возможно только при условии четкой правовой поддержки, закрепляющей за всеми участниками электронного взаимодействия, включая граждан и их объединения, не только права, но и ответственность. При этом должны быть соблюдены такие конституционные права граждан как право на свободу слова и свободу собраний, неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений, свободный поиск, получение, передачу, производство и распространение информации любым законным способом.

Сегодня существуют серьезные препятствия на пути развития механизмов электронной демократии в современной России.

В первую очередь, это касается процедур двустороннего взаимодействия граждан с органами власти по общественно-политическим вопросам. Механизм обращений и запросов граждан и организаций в органы власти в электронном виде не получил широкого распространения в силу отсутствия необходимых и достаточных процедур, которые бы юридически гарантировали и практически обеспечивали полное равенство данных обращений и процедур перед их физическими аналогами.

Следующей важнейшей проблемой являются вопросы идентификации и аутентификации участников информационного взаимодействия, в том числе в части практической реализации.

Сохраняется цифровое неравенство между федеральным центром, субъектами Российской Федерации и муниципалитетами. Проникновение интернета протекает неравномерно, качество доступа к данному ресурсу в масштабах страны находится ещё на недостаточном уровне.

К негативным факторам следует отнести также и отсутствие эффективных инструментов популяризации механизмов электронной демократии среди населения. Без массового информирования граждан о широких возможностях механизмов электронной демократии невозможно сформировать среду доверия к данным механизмам.

К вопросу об информационной безопасности. Очень важным аспектом является наличие в проекте Концепции развития в Российской Федерации механизмов электронной демократии отдельного пункта, посвященного вопросам обеспечения безопасности, защищенности и других требований, предъявляемых к системам электронной демократии.

В частности, Концепцией предусмотрено, что информационная безопасность единой системы электронной демократии (ЕСЭД) должна обеспечиваться за счет реализации многоуровневой системы безопасности и контроля, выполняющей следующие задачи:

- обеспечение целостности информации;
- обеспечение защиты программных и технических средств, используемых для сбора, передачи и обработки информации от утечки и разрушающего воздействия.

При этом основными направлениями создания комплексной защиты информации являются:

- организационно-режимные меры защиты;
- защита информации от утечки по каналам побочных электромагнитных излучений и наводок;
- защита от вирусных атак;
- обеспечение достоверности и подлинности информации при хранении и передаче сообщений в рамках ЕСЭД;
- защита информации от несанкционированного доступа[h].

Литература.

1. Право на доступ к информации. Доступ к открытой информации / Отв. ред. И.Ю. Богдановская. – М.: Юстицинформ, 2009. – С. 222.
2 Бачило И.Л. Государство социальное или сервисное? (информационно-правовой аспект) // Право. Журнал высшей школы экономики. – 2010. – № 1. – С. 7.
3 Васькова М.Г. Электронное государство: проблемы правового регулирования // Информационное право. – 2009. – № 4. – С. 24.
4 Единый портал электронной демократии // Режим доступа: http://e-democratia.ru/s/blog/msg?textId=10292940
5. Бачило И.Л. Правовые вопросы социальных и демократических процессов в информационном обществе России // Информационное общество: проблемы развития законодательства: Сб. науч. работ. – М.: ИГП РАН, ЮРКОМПАНИ, 2012. – С. 11.
6. Собрание законодательства Российской Федерации от 17 июня 2002 г. N 24 ст. 2253
7. См. об этом: Чеботарева А.А. Человек и электронное государство. Право на информационную безопасность. – Чита: ЧитГУ, 2011. – С. 27.
8. Единый портал электронной демократии // Режим доступа: http://e-democratia.ru/s/blog/msg?textId=10292940

Шамков Николай Степанович

Организационно-правовые проблемы внедрения системы электронного документооборота (СЭД) в органах государственного управления по материалам федеральной службы судебных приставов

Аннотация: *рассматривается понятие и сущность электронной демократии, анализируются механизмы электронной демократии, предусмотренные Проектом Концепции развития в Российской Федерации механизмов электронной демократии до 2020 года.*

Ключевые слова: *электронная демократия, электронное правительство, электронное государство, электронное голосование, цифровое неравенство, информационная безопасность.*

Современный период развития России отмечен активным и повсеместным проникновением электронных технологий в быт ее граждан, в деятельность средств массовой информации, общественных организаций, хозяйствующих субъектов и государственных органов.

Если для отдельного человека данные технологии – это технические средства, позволяющие оперативно получать широкий спектр информационных услуг, то для органов государственной власти – не только инструмент повышения эффективности делопроизводства, но и, как представляется, побудитель внедрения научных основ в организацию самого управления как необходимого условия успешной и всеобъемлющей автоматизации управленческих процессов.

Практика внедрения систем электронного делопроизводства и документооборота показывает, что чем шире использован принцип научности, рациональности в организации системы управления, тем больше возможностей для автоматизации деловых процессов в данной системе.

Развитие службы судебных приставов в современной России можно подразделить на два этапа:

- 1997 – 2004 г.г. – этап создания и развития службы в системе Министерства юстиции Российской Федерации.
- 2005 – 2012 г.г. – этап создания и развития в качестве самостоятельного федерального органа исполнительной власти – Федеральной службы судебных приставов, подведомственной Министерству юстиции Российской Федерации.

Служба судебных приставов, созданная в системе органов Министерства юстиции Российской Федерации, возглавляется заместителем министра юстиции Российской Федерации – главным судебным приставом Российской Федерации.

Основной особенностью службы в системе Минюста России является централизованная система управления, обеспеченная закрепленными в законе полномочиями главного судебного пристава Российской Федерации по назначению на должность и освобождению главных судебных приставов субъектов Российской Федерации, установлению штатов и структуры службы, осуществлению финансового и материально – технического обеспечения.

По своему правовому положению Федеральная служба судебных приставов занимает особое место среди федеральных органов исполнительной власти в силу, прежде всего, наделенных законодательством полномочиями по обеспечению установленного порядка деятельности судов с возможным применением огнестрельного оружия и специальных средств, обеспечению принудительного исполнения судебных актов и актов других уполномоченных органов, произ-

водству дознания, розыска должника, его имущества, розыск ребенка самостоятельно или с привлечением органов внутренних дел.

Основное отличие Службы от других государственных органов, как представляется, заключается в процессуальном характере функций отдельных должностных лиц, прямо закрепленных в законодательстве.

К таким должностным лицам относятся: директор Федеральной службы судебных приставов – главный судебный пристав Российской Федерации, руководители управлений Федеральной службы судебных приставов по субъектам Российской Федерации – главные судебные приставы субъектов Российской Федерации, начальники отделов судебных приставов – старшие судебные приставы и их заместители, а также судебные приставы-исполнители.

С одной стороны, служба судебных приставов представляет собой федеральный орган исполнительной власти и на него распространяются все полномочия органа государственного управления в установленной сфере, с другой – это орган по осуществлению прямо указанных в законе процессуальных функций принудительного исполнения, обеспечиваемых должностными лицами, наделенными процессуальной самостоятельностью.

Как субъект управления по отношению к объекту управления – территориальным органам, служба (ее центральный аппарат) осуществляет общие обеспечивающие управленческие функции, такие как анализ, планирование, координирование, организация, распорядительство и контроль исполнения.

Вместе с тем, наряду с обеспечивающими управленческими функциями главный судебный пристав Российской Федерации (его заместители), в необходимых случаях, в силу возложенных на него полномочий как непосредственно, так и через главных судебных приставов субъектов Российской Федерации, осуществляет управление самим процессом принудительного исполнения.

Двойственность функций управления, осуществляемого аппаратом службы судебных приставов, а также отдельными должностными лицами, наделенными законом процессуальными полномочиями, нашло свое отражение в организации и осуществлении делопроизводства, как технологии документационного обеспечения управления.

С учетом поставленных при внедрении СЭД целей, увязанных с широтой охвата автоматизацией технологических процессов работы с документами, подлежащих внедрению в ФССП России, программные средства условно подразделены на несколько уровней:

- система электронного делопроизводства;
- система электронного документооборота.

В основу подразделения СЭД на уровни положены признаки, закрепленные в определениях ключевых понятий «делопроизводство» и «документооборот», содержащиеся в ГОСТе Р 51141-98 «делопроизводство и архивное дело термины и определения».

Так, согласно ГОСТу Р 51141-98 делопроизводство – отрасль деятельности, обеспечивающая документирование и организацию работы с официальными документами; документооборот – движение документов в организации с момента их создания или получения до завершения исполнения или отправления.

Поскольку реальное комплектование штатами Федеральной службы судебных приставов началось в январе 2005 г. обеспечение документирования являлось на данном этапе основной задачей вновь созданного управления делопроизводства.

В период с января по март 2005 г. управление делопроизводства обеспечивало своевременную регистрацию входящей (исходящей) документации, доведение документов до соответствующих руководителей и исполнителей, контроль исполнения документов в сроки, установленные руководством службы, а также своевременную отправку корреспонденции.

В указанный период регистрация входящих и исходящих документов осуществлялась двумя работниками управления делопроизводства в электронном журнале с минимальным составом реквизитов.

С учетом наметившейся в рассматриваемый период устойчивой тенденции роста объема поступающей в службу корреспонденции (более 1 тыс. в месяц) возникла настоятельная необходимость в создании технической возможности регистрации входящих и исходящих документов одновременно с рабочих мест в количестве не менее 5 единиц.

Чрезмерный объем внутреннего документооборота, в основном, обусловлен письменными обращениями одних управлений в другие с просьбой «высказать» свои предложения и замеча-

ния на тот или иной проект документа по вопросам, входящим в их собственную компетенцию.

Свежим примером такого обращения может служить письмо Управления государственной службы и кадров от 12.02.2009 06-222вн с просьбой внести предложения о праздновании 23 февраля.

Другим источником излишней переписки являются, например, письменные запросы ОКУ отчетов структурных подразделений о выполнении ими поручений руководства ФССП России об участии в работе оперативных совещаний, в то время как в протоколах данных совещаний, находящихся в ОКУ, содержится информация о всех присутствовавших на этих совещаниях сотрудниках.

Взаимодействие управлений между собой, основанное на переписке, как представляется, характеризуется следующими негативными факторами:

1. Нарушением требований нормативных правовых актов.

Указанное взаимодействие противоречит положению пункта 1.17 Типового регламента внутренней организации федеральных органов исполнительной власти, утвержденного постановлением Правительства Российской Федерации от 28.07.2005 № 452, не предусматривающего ведение начальникам управлений федеральных служб переписки с иными структурными подразделениями этого же органа.

2. Влечет за собой дополнительные затраты служебного времени на подготовку писем, их подписание, регистрацию и отправку адресату, затраты на бумагу, другие расходные материалы.
3. Снижение уровня оперативности и результативности взаимодействия, основанного на переписке.

Зачастую ответы даются в последнюю очередь (по объективным причинам). Качество проработки вопросов не всегда осуществляется на должном уровне, поскольку чаще всего они даются по вопросам, не входящим в их компетенцию, а, следовательно, подготавливаются лицами, глубоко не знающими предмет и объективно незаинтересованными в его изучении.

4. Снижение уровня персональной ответственности структурных подразделений за решение возложенных на них задач.
5. Отсутствие мотивации у работников к выполнению дополнительных задач, не входящих в предмет их ведения, ввиду объективной потребности специалиста в более глубоком познании предмета своей деятельности.

Кроме того, на отсутствие мотивации может влиять также отсутствие системы учета и объективной оценки данной работы по установленным показателям.

С учетом происходящих в настоящее время кризисных явлений в финансовой сфере, а также принятого руководством страны курса на инновационный путь развития экономики и совершенствования государственного аппарата, Управление делопроизводства подготовило предложения по минимизации документооборота в центральном аппарате Службы, основанные как на активном использовании системы электронного документооборота, так и на совершенствовании механизмов осуществления организационно-контрольных функций.

Поиск путей минимизации документооборота для достижения целей повышения эффективности и результативности деятельности центрального аппарата привел к выводу о том, что проблема сокращения внутренней переписки путем использования только одних электронных технологий без оптимизации действующих в Службе механизмов осуществления управленческих функций трудно разрешима, поскольку, как представляется, простая замена бумажного носителя на электронный может повысить оперативность взаимодействия структурных подразделений, однако не сможет оказать существенного влияния ни на сокращение объема документооборота (в том числе электронного), ни на высвобождение работников от излишних затрат служебного времени, являющихся основными показателями повышения эффективности системы управления.

По истечении 6 месяцев с момента внедрения СЭДД автором исследованы следующие аспекты:

- влияние СЭДД на эффективность деятельности службы;
- влияние СЭДД на эффективность осуществления управленческих функций;
- влияние практики управления на использование возможностей СЭДД;
- проблемы в использовании возможностей СЭДД
- факторы, препятствующие широкому использованию СЭДД в управленческой деятельности.

Изучение влияния СЭДД на эффективность деятельности службы выявило следующее:

- сокращение затрат служебного времени делопроизводителей на документирование;
- ускорение информационных потоков;
- сокращение непроизводительных затрат рабочего времени исполнителей;

С технологической точки зрения внедрение СЭДД способствовало обеспечить:

- систематизацию учета и хранения документов;
- оперативный доступ к документам и отчетной информации;
- эффективное управление процессами движения и обработки документов.

2. Невозможность использования данных статистического отчета для комплексного анализа ситуации ввиду отсутствия целостного учета объекта обжалования и жалоб (с использованием взаимообусловленных показателей).

Действующий формат статистической отчетности направлен на решение задач, связанных исключительно с обобщением данных.

Данный вывод находит подтверждение в том, что из 90 поручений, содержащихся в решениях двух коллегий, проведенных в 2008 г. (от 25.03.2008 № 193, от 08.09.2008 № 404) 30 поручений дано территориальным органам о проведении дополнительного анализа.

Применительно к работе с обращениями граждан и организаций данная система статистического наблюдения может обеспечить:

- обобщение данных по структуре тематик обращений, их повторности; обоснованности, своевременности дачи ответов, составу заявителей;
- сравнение показателей между территориальными органами службы;
- сравнение показателей отчетного периода с показателями других периодов.

В ходе изучения организации учета обращений, их рассмотрения, а также результативности деятельности в данной сфере были выявлены следующие факторы, негативно влияющие как на эффективность деятельности в указанной сфере, так и на возможность эффективного применения электронных технологий в части автоматизации деловых процессов.

К числу данных факторов можно отнести следующее:

1. Большой объем служебного времени, затрачиваемый коллективами отделов судебных приставов (судебными приставами-исполнителями) на выполнение работ по составлению ведомственной статистической отчетности с количеством показателей (6 659 ежемесячно – на период исследования), значительно превышающих потребности ФССП России в их практическом использовании в изучении эффективности деятельности территориальных органов.

Рассматриваемая ведомственная статистическая отчетность не в полной мере соответствует принципам официального статистического учета, а именно: принципу использования научно обоснованной методологии, принципу рационального выбора источников информации, принципу снижения нагрузки на респондентов и принципу согласованности действий субъектов учета, предусмотренным в статье 4 Федерального закона от 29 ноября 2007 года № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации».

2. Неотлаженность системы учета обращений по их видам (предложение, заявление, жалоба), предусмотренным в Федеральном законе от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Используемая система учета не позволяет наиболее полно выявлять количественные и качественные характеристики предложений (рекомендации по совершенствованию законов, нормативных правовых актов, деятельности Службы), заявлений (просьб граждан в реализации их прав, сообщения о нарушении законов, о недостатках в Службе, критика Службы), жалоб (просьб граждан о восстановлении и защите их нарушенных прав).

3. Осуществление учета обращений, а также их анализа в отрыве от состояния объекта обжалования (исполнительного производства).

Отсутствие целостного подхода к осуществлению контроля за обеспечением исполнительного производства и рассмотрению жалоб, поступающих в связи с этими исполнительными производствами, препятствует налаживанию сквозного контроля за осуществлением исполнительных производств на каждой стадии, в том числе за обжалованием действий по ним.

По этой же причине проблематичным является осуществление контроля за реализацией (фактическим удовлетворением) требований по вопросам исполнительного производства, содержащихся в жалобах, признанных обоснованными.

Информация с мест свидетельствует, что не каждая жалоба, признанная аппаратом территориального органа, центральным аппаратом службы обоснованной, реально удовлетворяется судебными приставами-исполнителями. Указанные обстоятельства зачастую порождают повторные обращения по жалобам, признанным обоснованными.

По результатам анализа системы статистического наблюдения, а также осуществляемой на ее основе системы управления территориальными органами руководству службы были внесены следующие предложения:

- создать единый формат показателей для комплексного анализа ситуации в территориальных органах;
- функции анализа, планирования, координирования, организации, распорядительства и контроля исполнения возложить на конкретное структурное подразделение службы.

Кроме факторов, относящихся к ведомственным недостаткам организационного характера, выявлены проблемы правового регулирования как в сфере официального статистического учета, так и в сфере государственного управления.

Так, изучение Федерального закона от 29 ноября 2007 года № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» показало, что закрепленные в статье 4 такие принципы официального статистического учета и системы государственной статистики как научная обоснованность, применение научно обоснованной официальной статистической методологии, рациональный выбор источников, применение единых стандартов при использовании информационных технологий и общероссийских классификаторов технико-экономической и социальной информации для создания и эксплуатации системы государственной статистики в целях ее совместимости с другими государственными информационными системами в тексте закона не конкретизированы.

Состоящий из 9 статей закон, предусматривает:

- цель и предмет регулирования (ст.1);
- основные понятия, используемые в законе (ст.2);
- правовое регулирование официального статистического учета и системы государственной статистики (ст.3);
- принципы официального статистического учета и системы государственной статистики (ст.4);
- порядок осуществления официального статистического учета (ст.5);
- виды и формы статистического наблюдения (ст.6);
- формирование официальной статистической методологии (ст.7);
- порядок предоставления первичных статистических данных и административных данных субъектам официального статистического учета (ст.8);
- гарантии защиты первичных статистических данных, содержащихся в формах федерального статистического наблюдения (ст.9).

Закрепленные в законе принципы статистического учета и системы статистики, в том числе научной обоснованности, научно обоснованной методологии, единых стандартов при использовании информационных технологий, не вошли в перечень основных понятий, предусмотренной в статье 3 закона.

Как видно из текста закона, правовые нормы, которые содержали бы требования к порядку осуществления статистического учета исходя из закрепленных в законе принципов (статья 4), отсутствуют.

Основные итоги и результаты изучения проблем внедрения системы электронного документооборота можно сформулировать в следующих положениях.

1. Потенциал электронных технологий по автоматизации деловых процессов не исчерпывается современными потребностями в автоматизации системы управления.

Сфера применения системы электронного документооборота ограничивается преимущественно документированием и ускорением информационных потоков.

2. Уровень правового регулирования технологий и процессов государственного управления является одним из основных препятствий к внедрению единой автоматизированной системы управления (АСУ).

Основные управленческие функции законодательно не закреплены, требования к ним не определены.

Отсутствие императивных норм по осуществлению управленческих функций в определенных параметрах создает условия необяза-

тельности их использования в управленческой деятельности.

3. Предпосылкой успешного внедрения АСУ может служить синхронизация законодательства в сфере информатизации и государственного управления.

Что информационное право развивается разработки ученых в сфере организации управления в государственном аппарате законодательно не закреплены, в то время как в информационном праве, например, закреплено развернутое понятие «электронная подпись».

Литература.

1. Федеральный закон от 21 июля 1997 г. № 118-ФЗ «О судебных приставах».
2. Федеральный закон от 21 июля 1997 г. № 119-ФЗ «Об исполнительном производстве».
3. Федеральный закон от 2 октября 2007 года № 229-ФЗ «Об исполнительном производстве».
4. Федеральный закон от 22.07.2008 № 132-ФЗ «О внесении изменения в статью 22 Федерального закона «О судебных приставах».
5. Федеральный закон от 11.07.2011 № 196-ФЗ «О внесении изменений в Федеральный закон «Об исполнительном производстве» и статью 8 Федерального закона «О судебных приставах».
6. Федеральный закон от 06.12.2011 № 410-ФЗ (ред. от 25.06.2012) «О внесении изменений в Федеральный закон «О судебных приставах» и отдельные законодательные акты Российской Федерации».
7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
8. Федеральный закон от 27 июля 2006 года N 149-ФЗ “Об информации, информационных технологиях и о защите информации” (Собрание законодательства Российской Федерации, 2006, № 31 (часть I), ст. 3448).
9. Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (Собрание законодательства Российской Федерации, 2006, № 19, ст. 2060.
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31 (1 ч.), ст. 3451; 2009, № 48, ст. 5716; 2009, № 52, (1 ч.), ст. 6439).
11. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (Собрание законодательства Российской Федерации, 2009, № 7, ст. 776).
12. Указ Президента Российской Федерации от 13 октября 2004 года N 1313 «Вопросы Министерства юстиции Российской Федерации».
13. Указ Президента Российской Федерации от 13 октября 2004 года N 1316 «Вопросы Федеральной службы судебных приставов».
14. Указ Президента Российской Федерации от 2 мая 1996 г. № 638 «О порядке подготовки проектов указов, распоряжений Президента Российской Федерации, предусматривающих принятие постановлений, распоряжений Правительства Российской Федерации» (Собрание законодательства Российской Федерации, 1996, № 19, ст. 2257).
15. Постановление Правительства Российской Федерации от 3 ноября 1994 г.
16. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (Собрание законодательства Российской Федерации, 2005, № 30 (ч. II), ст. 3165).
17. Постановление Правительства Российской Федерации от 27 декабря 1995 г. № 1268 «Об упорядочении изготовления, использования, хранения и уничтожения печатей и бланков с воспроизведением Государственного герба Российской Федерации» (Собрание законодательства Российской Федерации, 1996, № 2, ст. 123; 2001 № 24, ст. 2461; 2006, № 52, ст. 5587).
18. Постановление Правительства Российской Федерации от 13 августа 1997 г. № 1009 «Об утверждении Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации» (Собрание законодательства Российской Федерации, 1997, № 33, ст. 3895; 1997, № 50, ст. 5689;1998 , № 47, ст. 5771; 1999, № 8, ст. 1026; 2006, № 29, ст. 3251; 2009, № 2, ст. 240; 2009, № 12, ст. 1443; 2010, № 9, ст. 964).
19. Постановление Правительства Российской Федерации от 01 июня 2004 г. № 260 «О Регламенте Правительства Российской Федерации и Положении об Аппарате Правительства Российской Федерации» (Собрание законодательства Российской Федерации, 2004, № 23, ст. 2313; 2006, № 23, ст. 2514; 2006, № 29,

ст. 3251; 2007, № 32, ст. 4150; 2008, № 14, ст. 1413; 2008, № 21, ст. 2459; 2008, № 49, ст. 5833; 2009, № 11, ст. 1302; 2009, № 12, ст. 1443; 2009, № 19, ст. 2346; 2009, № 36, ст. 4358; 2009, № 49 (2 ч.), ст. 5970; 2009, № 49 (2 ч.), ст. 5971; 2009, № 52 (2 ч.), ст. 6609).

20. Постановление Правительства Российской Федерации от 19 января 2005 г. № 30 «О типовом регламенте взаимодействия федеральных органов исполнительной власти» (Собрание законодательства Российской Федерации, 2005, № 4 ст. 305; 2005, № 47, ст. 4933; 2007, № 43, ст. 5202; 2008, № 9, ст. 852; 2008, № 14, ст. 1413; 2009, № 12, ст. 1429; 2009, № 25, ст. 3060; 2009, № 41, ст. 4790; 2009, № 49 (2 ч.), ст. 5970).

21. Постановление Правительства Российской Федерации от 28 июля 2005 г. № 452 «О типовом регламенте внутренней организации федеральных органов исполнительной власти» (Собрание законодательства Российской Федерации, 2005, № 31, ст. 3233; 2007, № 43, ст. 5202; 2008, № 9, ст. 852; 2008, № 14, ст. 1413; 2008, № 46, ст. 5337; 2009, № 12, ст. 1443; 2009, № 19, ст. 2346; 2009, № 25, ст. 3060; 2009, № 47, ст. 5675; 2009, № 49 (2 ч.), ст. 5970; 2010, № 9, ст. 964).

22. Постановление Правительства Российской Федерации от 15 июня 2009 г. № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти» (Собрание законодательства Российской Федерации 2009, № 25, ст. 3060).

23. Постановление Правительства Российской Федерации от 22 сентября 2009 г. № 754 «Об утверждении Положения о системе межведомственного электронного документооборота» (Собрание законодательства Российской Федерации, 2009, № 39, ст. 4614).

24. Постановление Правительства Российской Федерации от 20 февраля 2010 г. № 72 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием федерального закона «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов» (Собрание законодательства Российской Федерации, 2010, № 9, ст. 964).

25. Постановление Правительства Российской Федерации от 26 февраля 2010 г. № 96 «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов» (Собрание законодательства Российской Федерации, 2010, № 10, ст. 1084).

26. Морозов А.В. Концепция информатизации Министерства юстиции Российской Федерации, 1999.

27. Баранников А.Ф. Теория организации: Учебник – М.: ЮНИТИ-ДАНА, 2004.

28. Смирнов Э.А. Теория организации: Учебное пособие – М.: ИНФРА-М, 2006

29. Авторский коллектив РАГС. Делопроизводство в системе государственного управления. Учебно-практическое пособие – М.: РАГС, 2001.

30. Ярков В.В. Комментарий к Федеральному закону «Об исполнительном производстве» (постатейный) и к Федеральному закону «О судебных приставах», М.: ЮРИСТЪ, 1999.

31. Рогожин М.Ю. Документационное обеспечение управления: Учебно – практическое пособие – М.: ТК Велби, Изд-во Проспект, 2006.

32. Подлесных В.И. Теория организации, Бизнес-пресса,2003.

рецензент: ***Морозов Андрей Витальевич,***
доктор юридических наук, профессор

Сведения об авторах

АРУТЮНОВА Лусине Борисовна – Российская правовая академия Министерства юстиции Российской Федерации, соискатель.

E-mail: l.arutyunova@bk.ru

БЕКЕТНОВА Юлия Михайловна – Национальный исследовательский ядерный университет «МИФИ», аспирант кафедры финансового мониторинга.

E-mail: beketnova@mail.ru

БЕЛЯВСКИЙ Алексей Анатольевич – адвокат гильдии российских адвокатов.

E-mail: bons007@mail.ru

БОЙЧЕНКО Игнат Сергеевич – Российская правовая академия Министерства юстиции Российской федерации, аспирант.

E-mail: xshadozx@ya.ru

ГОБРУСЕНКО Константин Иванович – кандидат юридических наук, Федеральная служба финансового мониторинга, заместитель начальника управления по противодействию отмыванию доходов.

E-mail: nik122@yandex.ru,

ЕВСТИФЕЕВА Наталья Александровна – Национальный исследовательский ядерный университет «МИФИ», старший преподаватель кафедры финансового мониторинга.

E-mail: naftita@mail.ru

ИВАНОВА Анна Юрьевна – начальник Управления договорно-правовой работы Научного центра правовой информации при Министерстве юстиции Российской Федерации.

E-mail: Anna.Ivanova@scli.ru

КОМЕНДАНТОВА Елена Владимировна – Российская правовая академия Министерства юстиции Российской Федерации, соискатель.

E-mail: komendantovae@bk.ru.

КОНОВАЛОВА Юлия Викторовна – Федеральная служба финансового мониторинга, ведущий специалист – эксперт международного управления.

E-mail:UVKonovalova@mail.ru

КРЫЛОВ Григорий Олегович – доктор физико-математических наук, кандидат юридических наук, Российская правовая академия Министерства юстиции Российской Федерации, профессор кафедры информационного права, информатики и математики.

E-mail: op50@mail.ru,

МИХАЛЕВИЧ Владимир Владимирович – заместитель директора Научного центра правовой информации при Министерстве юстиции Российской Федерации.

E-mail: vladimir.mikhalevich@scli.ru

МОРОЗОВ Антон Андреевич – Национальный исследовательский ядерный университет «МИФИ», аспирант.

E-mail: morozov.aa.1988@rambler.ru

Сведения об авторах

НИКИТИНА Виктория Леонидовна – Национальный исследовательский ядерный университет «МИФИ», Москва, заместитель заведующего кафедрой кибербезопасности, магистрант кафедры информационной безопасности банковских систем.

E-mail: VLNikitina@mephi.ru

РЯБКОВ Виктор Ефимович – Национальный исследовательский ядерный университет «МИФИ», заместитель заведующего кафедрой финансового мониторинга.

E-mail: VERyabkov@mephi.ru

ФИЛАТОВА Людмила Васильевна – кандидат юридических наук, старший научный сотрудник, профессор кафедры информационного права, информатики и математики, Российская правовая академия Министерства юстиции Российской Федерации.

E-mail: lv_filatova@mail.ru

ФОМИН Ярослав Алексеевич – доктор технических наук, Национальный исследовательский ядерный университет «МИФИ», профессор кафедры финансового мониторинга.

E-mail: naftita@mail.ru

ЧЕБОТАРЕВА Анна Александровна – кандидат юридических наук, доцент, Московсковский областной гуманитарный институт, заведующий кафедрой государственно-правовых дисциплин.

E-mail: anna_galitskaya@mail.ru

ШАМКОВ Николай Степанович – Российская правовая академия Министерства юстиции Российской Федерации, соискатель.

E-mail: nshamkov@inbox.ru

Annotations and key words

Belyavsky A. A., Komendantova E. V.

Organizational and legal systemlaw enforcement, anti-delinquencyin the information area of the Russian Federation

Annotation: *Examines the key issues of information law enforcement agencies in connection with changes in the current legislation of the Russian Federation. Shown that information security law making and law enforcement – a priority for the near future.*

Keywords: *information security, information, information sector, law enforcement, public information, information of the offense.*

Boychenko I. S.

Topical issues of development of information society

Annotation: *In this article reviews the legislation in the sphere of provision of government services as well as electronic cooperation between the government and citizens, and state departments. Propose measures to improve the interaction of the information society institutions.*

Keywords: *society, legislation, information, state, service, cooperate.*

Gobrusenko K.I, . Konovalova J. V.

Topical issues of the organization of information security analytical units Rosfinmonitoring

Annotation: *We consider the organization of information management analytical units Rosfinmonitoring in the interest of combating legalization (laundering) of proceeds from crime and terrorist financing.*

Keywords: *countering the legalization (laundering) of money, information resources, analytical units Rosfinmonitoring, automation of information processes, financial investigation.*

Evstifeeva N. A., Krylov G. O., Ryabkov V. E.

Feature space for analysis reputational risks of credit institutions as agents of financial and information security

Annotation: *The problem of analysis of credit institutions as agents of financial and information security. The paper presents the characteristics of feature space for reputation assessment of credit institutions.*

Keywords: *risk assessment, information security, pattern recognition.*

Ivanova A. Y.

Organizational and legal methods of protection of intellectual property on the created software

Annotation: *Discusses the problems of protection of copyright for software.*

Key words: *software, computer program, database, software, means of protection of copyright rights.*

Krylov G. O.

The problems of information security at the money transfer National Payment System

Annotation: *The problems of information security in the national payment system, after Russia joins the World Trade Organization*

Keywords: *World Trade Organization, the transfer of funds, information security*

Morozov A. A., Arutyunova L. B.
Formation of a unified space of a significant legal electronic interaction

Annotation: *This article provides details on problems of formation of unified legal space of a significant electronic interaction as well as to overcome these problems.*

Keywords: *law, information security, information technology, public functions.*

Nikitina V. L.
Monitoring problem universal electronic cards in the national payment system

Annotation: *The problems of monitoring universal electronic cards in the national payment system, after Russia joins the World Trade Organization.*

Keywords: *World Trade Organization, the national payment system in Russia, universal electronic cards, monitoring.*

Gobrusenko K. I., Ryabkov V. E.

Legal issues of information support analytical units Rosfinmonitoring

Annotation: *The legal issues of information support analytical units Rosfinmonitoring for tackling the legalization (laundering) of proceeds from crime and terrorist financing.*

Keywords: *countering the legalization (laundering) of information technology, the presumption of openness of information, electronic documents.*

Filatova L. V., Mikhalevich V. V.
Legal information and accounting systems of the federal bodies of executive power in the "electronic government"

Annotation: *Article focuses on the structure and purpose of the information and legal accounting systems executive in "e-government", as well highlight the principles of the organization of such systems.*

Keywords: *information, informational law, law, the state, the electronic state.*

Beketnova J. M., Krylov G. O., Fomin Y. A.
Identification of risks and violations of financial security

Annotation: *The problem of the recognition of financial entities and information security. This article is an example of diagnosis of organizations to identify risks violations of financial and information security.*

Keywords: *risk assessment, information security, pattern recognition.*

Chebotareva A. A.
Mechanisms of electronic democracy: possibilities and problems of their realization in the Russian Federation

Annotation: *The concept and essence of electronic democracy is considered, the mechanisms of electronic democracy provided by the Draft of the Concept of development in the Russian Federation of mechanisms of electronic democracy till 2020 are analyzed.*

Keywords: *electronic democracy, electronic government, electronic state, electronic vote, digital inequality, information security.*

Shamkov N. S.
Organizational and legal problems of implementing electronic document management systems

in public administration based on the Federal Bailiff Service

Annotation: *This article explores problem of implementing the electronic document management systems to the bailiffs with the features due to its ongoing mandate to enforce judgments.*

Keywords: *law, government, electronic document management, bailiffs.*