МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НЦПИ

ФЕДЕРАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НАУЧНЫЙ ЦЕНТР ПРАВОВОЙ ИНФОРМАЦИИ
ПРИ МИНИСТЕРСТВЕ ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ПРАВОВАЯ ИНФОРМАТИКА

Периодический научный журнал

Выпуск № 1 – 2013

Москва, 2013

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

Правовая информатика. Выпуск 1–2013. — М. : ФБУ НЦПИ при Минюсте России, 2013. — 72 с.

ISSN 1994-1390

«Журнал» «Правовая информатика» является периодическим рецензируемым изданием. Подписка на журнал на 2013 год производится по объединенному каталогу «Пресса России» или письмом в редакцию.
Индекс подписки: 44723
Адрес редакции: 125437, Москва, Михалковская ул, 65, стр.1
Телефон: +7(495)539-23-17, E-mail: pravo360@gmail.com
www.pravo360.ru

ISSN 1994-1390

СОДЕРЖАНИЕ

Морозов Андрей Витальевич

доктор юридических наук, профессор

История правовой информатизации Минюста России на рубеже веков

Аннотация: *в статье автор описывает этапы правовой информатизации Министерства юстиции с последних десятилетий XX века, включая первые годы нынешнего века, и даёт описание ключевых событий и правовых актов.*

Ключевые слова: *право, информационное право, министерство юстиции, информация.*

Реализация практически всех задач, стоящих перед Министерством сегодня, невозможна без применения современных информационных технологий.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая является системообразующим фактором жизни общества. В связи с этим вопрос о правовой информатизации в нашей стране и участии в этом Министерства юстиции приобретает особое значение, поскольку целью правовой информатизации является повышение уровня правовой информированности общества путём всестороннего обеспечения органов государственной власти, должностных лиц и граждан полной и достоверной информацией о действующих в России законодательных и других правовых актах в условиях автоматизации информационных процессов, что является одной из задач, стоящих перед Минюстом России как федеральным органом исполнительной власти.

Вопрос о правовой информатизации в нашей стране был поставлен в 70-х годах в связи с развитием АСУ различных уровней. Правовая основа и механизмы ее реализации, выраженные термином «правовое обеспечение», не вышли за рамки ведомственных актов, нескольких постановлений Совета Министров СССР, аналогичных актов республиканского уровня.

Министерство юстиции СССР одно из первых применило новейшие технологии в области правового информирования, и в 1973 году во ВНИИ советского законодательства (ВНИИСЗ), входящем в структуру Минюста СССР, был создан сначала сектор информационно-поисковых языков, а затем отдел правовой информации, ставший впоследствии основой Научного центра правовой информации (НЦПИ), созданного 25 июня 1975 года решением Правительства СССР.

Актуальной задачей было создание общесоюзной системы правовой информации, состоящей из сетей полностью совместимых и взаимосвязанных автоматизированных информационно-поисковых систем (АИПС) различного уровня. АИПС «Законодательство», созданная в НЦПИ в конце 80-х годов, представляла собой передовую в то время систему, обладавшую развитым программным, техническим, лингвистическим и методическим обеспечением. В этой области проводились соответствующие комплексные научные разработки, и НЦПИ был единственной организацией, которая обеспечивала высшие органы представительной, исполнительной и судебной власти правовой информацией.

С 1991 года начинается активный процесс развития правовой информатизации. При участии Минюста России и НЦПИ (директор – А.И. Иваненко) была разработана Программа правовой информатизации России, утвержденная 24.07.1991 Председателем Комитета по законодательству С.М. Шахраем, в соответствии с которой работы по правовой информатизации

осуществлялись в Администрации Президента Российской Федерации, Аппарате Правительства Российской Федерации, в системах органов Прокуратуры Российской Федерации, Минюста России и МВД России.

С.М. Шахраю принадлежит заслуга закрепления термина «правовая информатизация» в нормативных правовых актах РСФСР и Российской Федерации. Идеи правовой информатизации были развиты и воплощены в создание государственной системы правовой информатизации руководителем Главного Государственно-правового управления Президента Российской Федерации Р.Г. Ореховым, будущими создателями баз данных Консультант Плюс и Гарант Д. Новиковым и Д. Першеевым.

Однако возникшие в этот период разногласия между Министром юстиции Н.В. Федоровым и руководителем ГПУ С.М. Шахраем привели к созданию двух параллельно развивающихся систем правовой информатизации: Минюста и ФАПСИ.

В начале 1991 года в Минюсте СССР был создан отдел внедрения научно-технических средств (начальник отдела – А.В. Морозов) в составе Планово-финансового управления (начальник управления – В.А. Суетов), а в Минюсте РСФСР – сектор правовой информатизации в составе Организационно-контрольного управления (начальник управления – А.С. Абасов).

В 1992 году в сфере правовой информатизации в Российской Федерации были приняты первые ключевые законы Российской Федерации от 23.09.1992 № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных» и от 23.09.1992 № 3526-1 «О правовой охране топологий интегральных микросхем», в разработке которых Минюст принимал активное участие. Наряду с Патентным законом Российской Федерации от 23.09.1992 указанные правовые акты создали основу системы правового регулирования отношений, возникающих при создании, правовой охране и использовании топологий интегральных микросхем, программ для электронных вычислительных машин и баз данных.

В Минюсте России в этот период в составе Организационно-контрольного управления (начальник управления – Е.Г. Чуганов) был создан отдел информатизации, и в соответствии с решением коллегии Минюста России от 24.12.1992 № 16-2 «О мерах по правовой информатизации судов, органов и учреждений Минюста России» в органах юстиции были введены должности специалистов по правовой информатизации.

1993 год занимает особо важное место в развитии правовой информатизации в нашей стране, поскольку была принята Конституция Российской Федерации, в которой закреплены впервые около 30 правовых норм, касающихся термина «информация» и составляющих основу законодательства в данной области. В статье 29 Конституции Российской Федерации провозглашено право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом, являющееся основополагающим в развитии правовой информатизации.

21 июля 1993 года был принят Закон Российской Федерации «О государственной тайне», в котором урегулированы отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. Значительный интерес в этом смысле представляют собой уникальные правовые акты из архивов НЦПИ, например, связанные с захоронением тела В.И. Ленина или до сих пор влияющее на нашу жизнь Постановление Совета Народных Комисаров № 497 от 30 мая 1918 года «О переводе часовой стрелки» на 2 часа вперед.

В результате совместных действий НЦПИ (директор – А.В.Морозов) и НТЦ «Система» ФАПСИ (первый директор – В.М. Хургин) была разработана и Указом Президента Российской Федерации от 28.06.93 № 966 утверждена Концепция правовой информатизации России, где определена задача создания информационно-правовой системы в Российской Федерации, основывающаяся на решении двуединой задачи: информатизации правовой сферы – с одной стороны, и обеспечения правового регулирования общественных отношений в области информатизации – с другой.

Кроме того, в соответствии с Указом Президента Российской Федерации от 19.10.93 № 1665 «Об информационно-правовом сотрудничестве Российской Федерации с государствами-членами Содружества Независимых Государств» Минюсту России совместно с другими заинтересованными федеральными органами исполнительной власти была поручена разработка Концепции создания межгосударственной системы правовой информатизации, одобренная Указом Президента Российской Федерации

от 27.12.1993 № 2293 «Вопросы формирования единого информационно-правового пространства Содружества Независимых Государств».

В соответствии с распоряжением Правительства Российской Федерации от 15.01.1993 № 59-р в НЦПИ при Минюсте России начал создаваться банк ведомственных нормативных актов на базе автоматизированной информационно-поисковой системы «Законодательство». На его аппаратно-программной основе со второй половины 1993 года в Минюсте России начала функционировать распределенная информационно-вычислительная система, объединяющая по каналам связи суды и органы юстиции субъектов Российской Федерации.

Решением коллегии Минюста России от 01.07.93 № 10-3 «О результатах проверки деятельности Научного центра правовой информации (НЦПИ) при Министерстве юстиции Российской Федерации» работа НЦПИ по обеспечению правовой информацией судов, органов и учреждений юстиции Российской Федерации была признана неудовлетворительной, и приказом Министра от 09.08.93 № 65/16-01 было образовано Управление информатизации Министерства юстиции Российской Федерации (начальник управления и директор НЦПИ – А.В. Морозов).

В то время совокупная база данных информационных систем НЦПИ составляла несколько тысяч документов. В 2000-м году Центр уже занимался актуализацией и обработкой базы данных правовых актов, объем которой составлял более 100 тысяч документов. В 2000 году был создан Регистр нормативных правовых актов субъектов Российской Федерации, который сегодня включает около 1 млн. документов. Ранее была начата обработка ведомственных нормативных актов, то есть нормативных актов федеральных органов исполнительной власти, которая продолжается и по сегодняшний день.

29.10.1993 НЦПИ был заключен первый договор на обеспечение пользователей базой данных правовой информации, впоследствии получившей предложенное мной название «ЭТАЛОН». Сейчас это название используют и коллеги из НЦПИ Республики Беларусь.

02.03.1993 утверждено Положение о региональном центре правовой информатизации, в котором предусмотрено образование его в составе органов юстиции.

1994 год ознаменовал собой начало определенного этапа развития в области обмена правовой информацией с государствами-участниками Содружества Независимых Государств, так как 21.10.94 было подписано межгосударственное Соглашение «Об обмене правовой информацией», в соответствии с протоколом, по которому Минюст России является держателем правовых актов для обмена с государствами-участниками СНГ. Указанное Соглашение послужило основой для развития также двусторонних отношений в этой области с государствами-участниками СНГ, а в Минюсте был создан соответствующий отдел.

Решением Координационно-консультативного Комитета Содружества Независимых Государств от 14.07.1994 была утверждена Концепция межгосударственной подсистемы обмена правовой информацией.

Минюст России принимал участие в разработке принятых в 1994 году и, безусловно, важных для развития правовой информатизации федеральных законов: «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» (№ 5-ФЗ от 14.06.94), «Об обязательном экземпляре документов» (№ 77 – ФЗ от 29.12.1994), «О библиотечном деле» (№ 78-ФЗ от 29.12.1994).

В развитии правовой информатизации крайне важным явилось закрепление в Гражданском кодексе Российской Федерации, подготовленном с участием Минюста России и принятым 30 ноября 1994 года, целого ряда гражданско-правовых норм, направленных на развитие информационного законодательства. Огромная заслуга в этом будущего Министра юстиции П.В. Крашенинникова. Так, впервые информация в статье 128 ГК РФ определена в качестве объекта гражданских прав, в статье 139 установлены такие правовые режимы информации, как служебная и коммерческая тайна. В частности, определено, что информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Кроме того, в 1994 году были изданы Указы Президента Российской Федерации № 223 «Об образовании Федеральной комиссии по правовой информатизации при Президенте Российской Федерации» и № 607 «О взаимодействии федеральных органов государствен-

ной власти Российской Федерации в области информационно-правового сотрудничества с органами власти государств-участников Содружества Независимых Государств», утверждена соответствующая Программа.

В соответствии с Указом Президента Российской Федерации от 03.12.1994 № 2147 «О мерах по совершенствованию юридического обеспечения деятельности Президента Российской Федерации» на Минюст России возложена функция генерального заказчика межгосударственной системы правовой информатизации в Российской Федерации.

Для дальнейшего развития правовой информатизации Минюста России важное значение имело постановление Правительства Российской Федерации от 21.10.1994 № 1181 «О мерах по обеспечению взаимодействия органов государственной власти Российской Федерации в области информационно-правового сотрудничества с государствами-участниками Содружества Независимых Государств», которым признано целесообразным использование для обмена созданного в соответствии с Постановлением Правительства Российской Федерации от 08.05.92 № 305 «О государственной регистрации ведомственных нормативных актов» в НЦПИ при Минюсте России банка данных ведомственных нормативных актов для информационно-правового обеспечения деятельности федеральных органов исполнительной власти. Указанным постановлением предписано федеральным органам исполнительной власти обеспечить начиная с 1995 года передачу в НЦПИ издаваемых ими нормативных актов не только на бумажных носителях, но и в машиночитаемой форме по каналам модемной связи.

Вместе с моими коллегами мы разработали Программу информатизации системы юстиции на 1994–1995 годы, которая была утверждена решением коллегии Минюста России от 21.01.1994 № 1-1, также в соответствии с приказом Министра юстиции России от 17.06.1994 № 19-01-90-94 был утвержден порядок обеспечения судов, органов и учреждений юстиции средствами вычислительной техники.

В 1995 году был принят ряд федеральных законов, играющих важную, роль в развитии правовой информатизации в Российской Федерации, в разработке основных положений которых специалисты Минюста России принимали активное участие.

Среди них особое место занимал Федеральный закон «Об информации, информатизации и защите информации», по праву считавшийся базовым в информационной сфере, поскольку в нем были заложены основы правового регулирования отношений во всех основных предметных областях информатизации и в информационной безопасности. Также были приняты федеральные законы «О связи», «О рекламе» и другие.

Указом Президента Российской Федерации от 04.08.1995 № 808 утверждена Президентская программа «Правовая информатизация органов государственной власти Российской Федерации», а разработка президентских программ «Правовая информатизация органов исполнительной власти Российской Федерации» и «Правовая информатизация органов государственной власти субъектов Российской Федерации» была поручена ГПУ, Минюсту России и ФАПСИ.

Постановлением Правительства Российской Федерации от 03.06.1995 № 550 «О дополнительных функциях Министерства юстиции Российской Федерации» на Минюст России было возложено проведение юридической экспертизы правовых актов, принимаемых органами государственной власти субъектов Российской Федерации, а также функции генерального заказчика межгосударственной системы правовой информатизации в Российской Федерации. Минюст России в соответствии с указанным постановлением координирует работу по созданию национальных банков данных, предназначенных для межгосударственного обмена. В целях реализации соглашений, направленных на информационно-правовое сотрудничество, используются базы данных правовых актов, формируемые в Министерстве. Информационные ресурсы Минюста России предоставлены координирующим международный информационно-правовой обмен органам Исполнительного комитета СНГ, Республик Беларусь, Казахстан, Кыргызстан, Узбекистан, Украина. Помимо этого, Минюст России активно участвует в разработке международных договоров и соглашений в сфере информационного и правового сотрудничества.

Для развития правовой информатизации Минюста России исторически важным явилось создание в 1995 году в порядке эксперимента центров правовой информатизации Минюста России в Самарской, Тульской, Владимирской и Ивановской областях.

В мае 1995 года в Египте состоялся Девятый международный конгресс ООН в области предупреждения преступности и уголовного

правосудия и информатизации правовой сферы. В составе делегации Российской Федерации, направленной для участия в работе конгресса, результаты информатизации правовой сферы представляли эксперты России (заместитель Министра юстиции Е.Н. Сидоренко и А.В. Морозов).

Начало 1996 года было омрачено пунктом 10 Указа Президента Российской Федерации № 117 от 29.01.1996, в котором предписывалось внести предложения по реорганизации (читай ликвидации) НЦПИ при Минюсте России, что в принципе ставило под угрозу существования всю систему правовой информатизации Минюста России. Он до сих пор не отменён, хотя многие о нём и не знают. В течение двух месяцев НЦПИ должен был прекратить своё существование и быть переданным в распоряжение Администрации Президента. В интервью начальника отдела ГПУ Президента Российской Федерации Б.В. Гузанова «Российской газете» было заявлено, что в структуре Администрации Президента Российской Федерации будет создан Федеральный центр правовой информации, в который скоро «вольется» НЦПИ Минюста России. Усилиями руководства НЦПИ, руководителей судов и правоохранительных органов удалось сохранить уникальный фонд правовой информации. Председатель Верховного Суда, Председатель Высшего Арбитражного Суда, Генеральный прокурор, Министр юстиции поддержали доводы А.В. Морозова, что НЦПИ как уникальное учреждение должен остаться при Минюсте, обратились с письмами к Руководителю Администрации Президента Российской Федерации А.Б. Чубайсу, и он принял решение оставить НЦПИ в системе Минюста России.

В 1996 году был принят Федеральный закон «Об участии в международном информационном обмене», создающий необходимые условия для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиты интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защиты интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

Правовая информатизация впервые была выделена в качестве самостоятельного направления в деятельности Министерства в постановлении Правительства Российской Федерации от 17.10.96 № 1177 «Об утверждении Концепции реформирования органов и учреждений юстиции Российской Федерации», что имеет, безусловно, историческое значение в развитии правовой информатизации Минюста России.

Ряд приказов Министра юстиции Российской Федерации, изданных в 1996 году, также был направлен на совершенствование работ по правовой информатизации. В частности, приказом Министра от 01.07.1996 № 16-02-455-96 было образовано Управление информатизации и статистики. Кроме того, были изданы приказы от 23.12.1996 № 19-01-189-96 «Об организации автоматизированного учета правовых актов субъектов Российской Федерации», от 09.07.96 № 19-01-104-96 «О совершенствовании порядка проведения в Министерстве юстиции Российской Федерации юридической экспертизы правовых актов субъектов Российской Федерации», подготовленные Управлением информатизации и статистики.

Продолжала развиваться система правовой информатизации Минюста России. В 1996 году было образовано 22 центра правовой информатизации в субъектах Российской Федерации.

В связи с вступлением России в 1996 году в Совет Европы и включением ее информационных ресурсов в информационное пространство европейских государств, одной из важнейших задач правовой информатизации стало налаживание функционирования системы юстиции европейских государств, направленное на обеспечение соблюдения прав и свобод граждан этих государств. Сотрудничество в этой области было обусловлено внедрением в системе юстиции и судебной системе современных информационных технологий.

В 1969 году в качестве рабочего органа Комитета министров Совета Европы был создан Комитет экспертов по информационным технологиям и праву, на котором в 1996 году автор выступал представителем от Российской Федерации. Основными задачами указанного Комитета является выработка комплекса мер, направленных на организацию информационно-правового сотрудничества государств-членов организации. В соответствии с решениями Межведомственной комиссии Российской Федерации по делам Совета Европы эксперты Минюста России являются координаторами и полноправными представителями Российской Федерации в Лиссабонской сети, Европейском суде по правам человека. В связи с этим Правовому департаменту Совета Европы был предоставлен доступ к базам данных правовой информации Минюста России.

Постановлением Правительства Российской Федерации от 24.07.1997 № 930 ФАПСИ и Минюсту России поручено обеспечить создание единой системы информационно-телекоммуникационного обеспечения (отсюда берет начало термин – ЕСИТО) Министерства юстиции, которая представляет собой интегрированную иерархическую трехуровневую систему, открытую для взаимодействия с другими автоматизированными системами в рамках единого информационного пространства органов государственной власти, где в качестве основных компонентов выделяются информационно-телекоммуникационные подсистемы.

В августе 1997 года был образован Департамент правовой систематизации и информации. Продолжалось развитие системы правовой информатизации Минюста России, и в течение 1997 года было образовано еще 16 центров правовой информатизации Министерства юстиции в субъектах Федерации, в апреле 1997 года был создан Главный информационно-аналитический центр Министерства юстиции Российской Федерации. Всего за 1995–1997 гг. вместе с ГИАЦ образовано 44 центра правовой информатизации Минюста России.

Важным событием в деятельности Министерства юстиции в сфере правовой информатизации стал проведенный в июне 1997 года в рамках программы ООН в области предупреждения преступности, уголовного правосудия и информатизации правовой сферы международный семинар в НЦПИ и Твери, в котором среди двухсот участников были эксперты США и Канады, стран Совета Европы и СНГ, ведущие фирмы и специалисты в сфере правовой информатизации. Участники семинара отметили достижения в правовой информатизации Минюста России и результаты, достойные признания на международном уровне.

С 1997 года информационные ресурсы Минюста России стали доступны для пользователей в Интернете (зарегистрирован домен SCLI.RU), доступ на Web-сервер был организован через выделенный высокоскоростной канал.

Созданная система распределенной обработки информации позволяла обрабатывать информацию, поступающую из органов государственной власти. Информация субъектов Российской Федерации обрабатывалась территориальными органами Минюста России или центрами правовой информатизации и передавалась в НЦПИ как центральный узел системы по коммутируемым каналам связи, в том числе с использованием сети Интернет.

В базу данных помещались не только тексты правовых актов, но и все изменяющие их акты, что позволяло при необходимости выявить историю создания и изменений актов. Средства обеспечения информационного поиска, входящие в состав операционной системы ЭВМ, создавали возможность осуществлять подбор информации по разовым запросам пользователей.

Указанный программно-технологический комплекс получил дальнейшее развитие как информационная правовая система «Фонд», первоначально предназначенная для информационно-правового обеспечения деятельности судов, органов и учреждений юстиции. На программные комплексы ЭТАЛОН и ФОНД зарегистрированы авторские права. В 1997 году указанная база стала доступна для широкого круга пользователей. Разделы базы данных охватывают все аспекты, как правового регулирования предпринимательской деятельности, так и вопросы правового статуса личности, защиты прав и свобод человека и гражданина.

В 1998 году в целях реализации положений статьи 15 Конституции Российской Федерации, Указа Президента Российской Федерации от 14.02.1998 № 170 «О мерах по повышению эффективности работы, связанной с формированием Свода законов Российской Федерации», упорядочения законодательства, обеспечения его стабильности, укрепления конституционной законности в Минюсте России (Департамент информатизации – А.В.Морозов, Л.В.Филатова) совместно с ГПУ и органами исполнительной власти проводилась работа по систематизации действующих нормативных правовых актов для включения их в Свод законов Российской Федераций.

Также были изданы приказы Минюста России от 11.08.1998 № 94 «О деятельности учреждений Министерства юстиции Российской Федерации по правовой информатизации» и от 30.09.1998 № 116 «О порядке информационного взаимодействия Министерства внутренних дел Российской Федерации и уголовно-исполнительной системы Министерства юстиции Российской Федерации».

Летом 1998 года состоялся первый семинар руководителей подразделений информатизации учреждений по регистрации прав на недвижимое имущество и сделок с ним. Был разработан и представлен на утверждение проект

концепции автоматизированной информационной системы государственной регистрации прав на недвижимое имущество и сделок с ним (АИС ГРП), одной из основных задач которой является создание и ведение Единого государственного реестра прав на недвижимое имущество и сделок с ним в электронной форме. Разработка и внедрение указанной системы еще в 1999 году могла позволить осуществлять оперативный доступ к достоверной всесторонней информации об объектах недвижимости, правах на недвижимое имущество и сделок с ним, моделирование деловых процессов регистрации недвижимости, устранение существующих пробелов в едином информационном пространстве государства, обеспечивать информационное взаимодействие между учреждениями юстиции по регистрации прав и их филиалами. Однако идеи автономного развития учреждений по регистрации прав не позволили реализоваться этим планам.

В 1999 году Указом Президента Российской Федерации от 02.08.1999 г. № 954 утверждено Положение о Министерстве юстиции Российской Федерации, в соответствии с которым Минюст России:

- предоставляет правовую информацию Президенту Российской Федераций; Правительству Российской Федерации, иным федеральным органам государственной власти;
- участвует в разработке и реализации программ правовой информатизации;
- осуществляет государственный учет нормативных правовых актов субъектов Российской Федерации;
- ведет контрольные экземпляры нормативных правовых актов федеральных органов исполнительной власти, организует деятельность своих территориальных органов по ведению контрольных экземпляров нормативных правовых актов субъектов российской Федерации;
- организует работу по созданию и ведению баз данных правовой информации в сфере юстиции;
- осуществляет обмен правовой информацией с иностранными государствами, координирует деятельность по созданию национальных банков Данных законодательства государств-участников Содружества Независимых Государств;
- обеспечивает сбор и обработку; статистических данных, разработку форм статистической отчетности и документов первичного учета в сфере юстиции;
- ведет реестр коллегий адвокатов.

В сентябре 1999 года под председательством Министра юстиции Ю.Я. Чайки состоялось заседание коллегии Минюста России, посвященное вопросам информатизации Министерства юстиции Российской Федерации. Коллегия одобрила основные положения концепции информатизации и направления развития системы правовой информатизации Минюста России.

Важным шагом в развитии правовой информатизации Минюста стало утверждение приказом Министерства от 21.01.2000 № 10 Концепции информатизации Министерства юстиции Российской Федераций, в которой нашли отражение состав, структура и основные подсистемы системы информатизации Минюста России, проблемы, анализ тенденций развития, а также вопросы обеспечения информационной безопасности. Основной целью развития и совершенствования системы информатизации Минюста России на основе применения современных информационных технологий является эффективное выполнение основных задач, стоящих перед Министерством.

В 2000 году роль информационной сферы в развитии общества возрастает, развитие глобального информационного общества становиться первоочередной задачей. В Окинавской Хартии Глобального информационного Общества, подписанной Президентом Российской Федерации В.В. Путиным и другими главами «восьмерки» 22 июля 2000 г., государства провозглашают следующий принцип: «все люди повсеместно без исключения, должны иметь возможность пользоваться преимуществами глобального информационного общества». Информационно-телекомуникационные технологии становятся жизненно важным фактором развития мировой экономики. Выделены основные направления: электронная коммерция, электронное образование, электронное государство, в том числе электронная юстиция и информационная безопасность.

С 1995 по 2003 автор участвовал в работе Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности. В 1999 году распоряжением Секретаря Совета Безопасности Российской Федерации В.В. Путина был назначен заместителем председателя рабочей комиссии при аппарате Совета Безопасности Российской Феде-

рации по вопросам совершенствования нормативной правовой базы в области обеспечения информационной безопасности.

В качестве основного результата деятельности рабочей комиссии можно отметить разработку «Основных направлений нормативного правового обеспечения информационной безопасности Российской Федерации», одобренных Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности 27 ноября 2001 г. решением № 5.4. и Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г.

Указом Президента Российской Федерации от 10.08.00 № 1486 на Минюст России возложено ведение федерального банка нормативных правовых актов субъектов Российской Федерации – Федерального регистра нормативных правовых актов субъектов Российской Федерации. В НЦПИ была разработана новая технология. Активное участие в этом принял Белгородский центр правовой информатизации (директор – Е.А.Марков).

В соответствии с Положением о порядке ведения федерального регистра нормативных правовых актов субъектов Российской Федерации, утвержденным Постановлением Правительства Российской Федерации от 29.11.2000 № 904, информационно-технологическое обеспечение ведения федерального регистра осуществлялось НЦПИ и центрами правовой информатизации Минюста России в субъектах Российской Федерации.

Приказом Минюста России от 18.09.2000 № 273 был утвержден План мероприятий по реализации Указа Президента Российской Федерации от 10.08.2000 № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации». Из 36 пунктов приказа исполнение 33 было возложено на Департамент правовой информатизации Минюста России. Не получив на реализацию поставленных задач дополнительной штатной численности и бюджетного финансирования, Департамент успешно организовал работу подразделений и учреждений правовой информатизации и разработал методику ведения Федерального регистра, позволившую с 1 января 2001 года территориальным органам Минюста России начать ведение Федерального регистра нормативных актов субъектов Российской Федерации как на бумажном носителе, так и в электронном виде.

В целях унификации банков данных правовой информации, а также обеспечения автоматизированного обмена правовой информацией между федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами Прокуратуры Российской Федерации и органами местного самоуправления Указом Президента Российской Федерации от 15.03.2000 № 511 одобрен классификатор правовых актов.

Созданные в НЦПИ базы данных правовой информации Минюста России основаны на качественной юридической обработке помещаемых в них правовых актов, имеют возможности выявления взаимосвязей и ссылок между документами, создания актуальных редакций, определения нормативности, классификации (рубрикации) правовых актов в соответствии с утвержденным классификатором.

В целях организации участия Российской Федерации в деятельности международной организации уголовной полиции издан приказ Министерства юстиции Российской Федерации, Государственного таможенного комитета Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной пограничной службы Российской Федерации, Федеральной службы налоговой полиции Российской Федерации от 26.06.2000 № 684; 184; 560; 353; 302; 257 «Об утверждении Инструкции об организации информационного обеспечения сотрудничества правоохранительных и иных органов по линии Интерпола».

В 2001 г. Советом Европы приняты, подготовленные с моим участием как представителя России, Рекомендации № 2 государствам-членам Совета Европы относительно устройства и переустройства судебных систем и правовых информационных систем и Рекомендации № 3, в которых предусмотрена обязанность государства обеспечить доступ к правовой информации в электронной форме, к электронным регистрам в правовой области, в том числе и через Интернет, а также автоматизация судебных технологий.

10.01.2002 был принят Федеральный закон «Об электронной цифровой подписи», в разработке которого мы принимали участие, который устанавливает правовую основу для использования электронной цифровой подписи, определяет полномочия органов, удостоверяющих открытые ключи электронной цифровой подписи, а также права, обязанности и ответственность физических и юридических лиц, уча-

ствующих в деятельности, связанной с применением электронной цифровой подписи.

28 января 2002 г. Постановлением Правительства Российской Федерации № 65 утверждена первая подобного рода Федеральная целевая программа «Электронная Россия (2002–2010 годы)». Особенно важно, что целью указанной программы являлось создание условий для развития демократии, повышение эффективности функционирования экономики, государственного управления и местного самоуправления за счет внедрения и массового распространения информационных и коммуникационных технологий, обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширения подготовки специалистов по информационным и коммуникационным технологиям и квалифицированных пользователей.

В 2002 году в Минюсте были приняты правовые акты, регламентирующие использование сети Интернет и предусматривающие создание автоматизированных систем: приказы Минюста России от 20.05.2002 № 130 «О внедрении единой автоматизированной системы «Делопроизводство» в центральном аппарате Министерства юстиции Российской Федерации и территориальных органах от 23.05.2002 № 133 «Об организации работы по созданию и сопровождению Интернет-сайта Министерства юстиции Российской Федерации»; от 04.06.2002 № 148 «О создании автоматизированной информационной системы службы судебных приставов»; от 13.06.2002 № 164 «Об утверждении Временного положения об использовании сети Интернет в центральном аппарате Министерства юстиции Российской Федерации».

К празднованию 200-летнего юбилея Минюста России Департаментом правовой информатизации и научно-технического обеспечения был подготовлен сборник основных нормативных правовых актов о федеральной юстиции.

За прошедшее десятилетие также сделано немало.

С теплотой вспоминаю и благодарю моих коллег Т.А. Полякову, Л.В. Филатову, Ю.А. Бикбулатова, Ю.В. Матвиенко, Л.Е. Маршалко, В.П. Пронина, Е.В. Горбачеву и многих других за годы творческого и продуктивного труда в системе Министерства юстиции на благо нашей Родины и ее народа.

Лазарев Виктор Михайлович
доктор технических наук, профессор
Любимов Алексей Евгеньевич
кандидат технических наук

Предложения по использованию информационно-аналитических систем в информационно-правовом обеспечении органов законодательной и исполнительной власти федерального, регионального и местного уровней

Аннотация: *в статье описан реализованный подход к комплексной обработке неструктурированной – текстовой и аудиовизуальной – информации в целях поддержки принятия решении пользователей правовой информации.*

Ключевые слова: *неструктурированная информация, полнотекстовый поиск, анализ текста, обработка аудиовизуальной информации, моделирование на основе когнитивных карт, поддержка принятия решений.*

Введение

В соответствии с Концепцией информатизации Министерства юстиции Российской Федерации на Министерство юстиции Российской Федерации федеральными законами, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации возложены задачи сбора, обработки, хранения, анализа правовой информации и организации ее использования. При этом основными информационными ресурсами, находящимися в распоряжении Министерства юстиции Российской Федерации и подведомственных ему организаций, являются компьютерные базы данных по различным аспектам права. Кроме того, Минюст России обладает уникальными информационными ресурсами на бумажных носителях – это фонды правовых актов НЦПИ, Минюста России, бывшего Минюста СССР, содержащие около 3,5 млн. документов. Важная роль в использовании этих информационных ресурсов принадлежит Научному центру правовой информации (НЦПИ) при Министерстве юстиции Российской Федерации. Созданная система распределенной обработки правовой информации позволяет обрабатывать в НЦПИ информацию, поступающую из федеральных органов государственной власти, а также органов государственной власти Москвы и Московской области. Правовая информация органов

государственной власти субъектов Российской Федерации обрабатывается территориальными органами Минюста России или центрами правовой информатизации и передается в НЦПИ как в центральный узел системы по коммутируемым каналам связи, в том числе с использованием сети Интернет.

Дальнейшее развитие системы информатизации Минюста России требует создания высокоинтеллектуальных систем, выполняющих не только функции справочно-информационного обслуживания пользователей, но и обеспечивающих эффективную поддержку законотворческой деятельности.Указанные системы должны обеспечивать законотворческую деятельность Минюста России на основе решения следующих задач:

- обработки запросов, заданных в виде свободных наборов терминов или произвольных текстов на естественном языке;
- выделения в полнотекстовой базе данных множества релевантных документов (или их фрагментов) с автоматическим ранжированием текстов по уровню релевантности;
- динамического формирования текстов документов, актуальных на задаваемый пользователем период времени;
- навигации в правовой базе данных не только по заранее установленным гиперссылкам, но и по любому другому признаку,выбираемому пользователем (например, по органам, источникам опубликования позициям общеправового классификатора отраслей права ит.д.).

Информационное пространство, в котором функционируют организации, осуществляющие правовое обеспечение существенно изменилось и имеет следующие особенности:

- неструктурированные данные (тексты, изображения, видео, аудио и пр.) составляют большую часть накопленной информации: их доля может составлять более 95% накопленных данных;
- увеличивается разнообразие и количество технических средств получения, преобразования и представления информации (телевидение, радио, интернет, электронная почта, видео конференцсвязь, сотовая связь, видеозапись и пр.);
- увеличивается количество источников информации (газеты, журналы, телевизионные и радиоканалы, интернет-сайты, форумы, блоги и т.п.);
- скорость распространения неструктурированной информации непрерывно растет;
- современные международные связи и деловое общение, как никогда ранее, предполагают многоязыковость.

Все это приводит к резкому возрастанию роли информационно-аналитических систем при возрастании требований к ним, а именно: сокращаются сроки представления данных эксперту, аналитику; увеличивается количество факторов учитываемых системой; все более важное значение приобретает прогнозирование развития событий в интересах государственных органов.

В связи с этим крайне актуальной является проблема автоматизации процессов обработки неструктурированной информации в информационно-аналитических системах. В настоящей статье описан реализованный подход к комплексной обработке неструктурированной информации в целях поддержки принятия решений.

Предлагается в качестве одного из путей решения этой проблемы рассматривать разработку и внедрение информационно-аналитических систем, позволяющих круглосуточно обрабатывать огромные разнородные информационные потоки путем создания единого информационного пространства и применения интеллектуальных технологий работы с информацией.

Неструктурированная информация: проблемы обработки

Как показали исследования, проведенные ведущими независимыми аналитическими агентствами, объем всей накопленной в мире информации превысил 281 экзабайт (или 281 млрд. гигабайт) [1]. Особого внимания заслуживает тот факт, что более 95 % всей созданной и накопленной в мире информации носит неструктурированный характер, т.е. имеет форму текстов произвольного содержания и аудиовизуальную форму. Неструктурированная информация включает в себя: телефонные разговоры, голосовую почту, электронную почту, текстовые документы, бумажные документы, изображения, веб-страницы, видео и сотни других различных видов и форматов файлов и данных, причем доля информации, представленной в аудиовизуальной форме, стремительно растет.

К сожалению, в настоящее время попытки выгодно использовать этот огромный и стратеги-

ческий ресурс, часто оказывались безуспешными, т.к. у многих организаций, как частных, так и государственных, нет необходимой технологии, чтобы понять и эффективно работать с информацией, которая находится вне упорядоченных баз данных, и тем более, с информацией в аудиовизуальной форме. При этом работа со структурированной информацией остается также крайне важной в деятельности любой организации.

Все это требует наличия информационной инфраструктурной платформы, которая может работать со всеми типами информации, методом, принятым для структурированных баз данных. Аналогично системе управления реляционными базами данных, которая явилась революцией в компьютерном мире в 1960-х годах, эта инновационная платформа должна давать компьютерам возможность обрабатывать не только структурированные данные, но также громадные количества частично структурированной и неструктурированной информации, используя реляционный индекс.

Анализ положений об органах государственной власти (ОГВ) показал, что, как правило, последним, на законодательном уровне, вменяется в обязанность осуществлять мониторинг информационного пространства в сфере своих компетенций, разрабатывать предложения по улучшению тех или иных ситуаций в сфере своих компетенций. Кроме того, специализированные службы органов государственной власти ежедневно занимаются информационным обеспечением рутинной и интеллектуальной деятельности персонала ОГВ.

Анализ официальных документов (Концепция формирования в РФ электронного правительства до 2010 года, Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года, Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов и др.) показал, что существует ряд общих проблем, значительно усложняющих внедрение информационных систем в органах государственной власти. К таким проблемам относятся:

- внутриведомственный характер информационно-коммуникационных технологий в органах государственной власти, препятствующий эффективному межведомственному взаимодействию и повышению качества государственных услуг, предоставляемых гражданам;
- нестандартизированность действующих государственных информационных систем и их недоступность другим органам государственной власти для оперативного использования;
- противоречивость данных, содержащихся в государственных информационных системах;
- использование недокументированных форматов данных, протоколов обмена, иных закрытых информационных технологий и отсутствие единых классификаторов, справочников и схем данных, что ограничивает возможность применения автоматизированных средств поиска и аналитической обработки информации, содержащейся в различных системах, и затрудняет доступ организаций и граждан к государственным информационным системам;
- неавтоматизированность процедур сбора и обработки информации, необходимой для определения и контроля целевых показателей результативности деятельности органов государственной власти.

Кроме того, существуют и объективные тенденции и проблемы, характерные для внешней среды любой современной организации, которые оказывают существенное влияние на то, как организации работают с информацией. Среди них можно отметить тенденцию к приданию электронной информации определенного правового статуса, а также значительное снижение времени, отводимого на подготовку и принятие решений.

Таким образом, можно в общем виде сформулировать основные проблемы, с которыми сталкиваются органы государственной власти при обработке информации:

- необходимость работать с информацией разного типа (структурированная и неструктурированная);
- разнородность источников и форматов данных (телевидение, радио, печатные издания, интернет, базы данных и пр.);
- большие объемы данных;
- необходимость гибко и оперативно настраивать систему на различные задачи в соответствии с меняющейся обстановкой;
- необходимость синхронизации мощностей системы с нарастающими потоками данных (масштабируемости);
- необходимость эффективно анализировать данные в распределенной среде;

- необходимость прогнозирования развития ситуаций, например, по модели «что, если...»;
- необходимость мониторинга открытого информационного пространства (интернет/СМИ);
- необходимость применять максимально стандартизованные решения.

Описание предлагаемого подхода

Решение перечисленных проблем требует использования современных аналитических систем. В статье представлено описание одной из таких систем. Информационно-аналитическая система (ИАС) «Лавина» предназначена для сбора, обработки и консолидации разнородной неструктурированной информации – текстовой и аудиовизуальной – из внутренних и внешних источников (базы данных, интернет, файловые системы, корпоративные информационные системы, телевизионный и радио эфир и др.) и ее автоматической аналитической обработки в режиме, близком к реальному времени.

Применение ИАС «Лавина» позволяет:

- оперативно отслеживать появление новых информационных поводов;
- осуществлять непрерывный мониторинг и анализ развития различных ситуаций;
- оценивать «информационный портрет» персоны, организации, бренда и пр. в СМИ и социальных медиа;
- прогнозировать развитие ситуаций.

Принципиальной особенностью системы «Лавниа» является то, что, во-первых, система способна обрабатывать как текстовую, так и аудиовизуальную информацию и, во-вторых, система поддерживает полный цикл обработки данных, т.е. преобразование данных в информацию и извлечение знаний из информации посредством проведения анализа текста и ситуационного моделирования.

В качестве источников данных для ИАС могут выступать любые известные источники информации (интернет, файловые системы, базы данных, аудио- и видеоканалы). ИАС способна работать как с потоком, так и с файлами практически всех известных форматов. Укрупненная схема работы системы представлена на рис. 1.

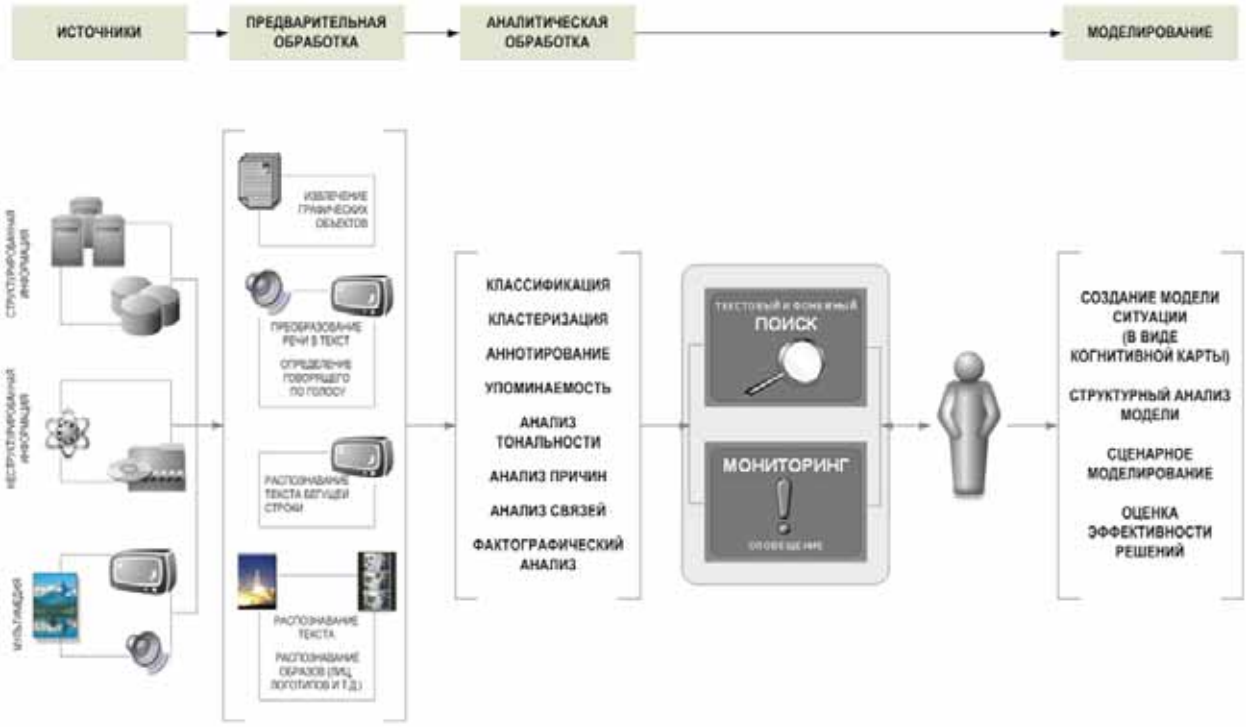

Рис.1. Укрупненная схема работы системы

Каждый входящий файл подвергается предварительной обработке. Речь, содержащаяся в аудиофайлах и звуковых дорожках видеофайлов, преобразовывается в текст, и определяется принадлежность голоса говорящего (диктора). Бегущая строка и титры в видеофайлах преобразовываются в текст. В графических файлах, извлеченных из текста, а также

кадрах, на которые разбиваются видеофайлы, производится поиск и распознавание печатного текста и образов (логотипов, силуэтов и т.п.) и идентификация лиц. Такая информация, так же как и текстовое содержание документов, индексируется и становится доступной для поиска, мониторинга и дальнейшей аналитической обработки. Результаты обработки текстов на примере анализа деятельности госкорпораций представлены на рис.2.

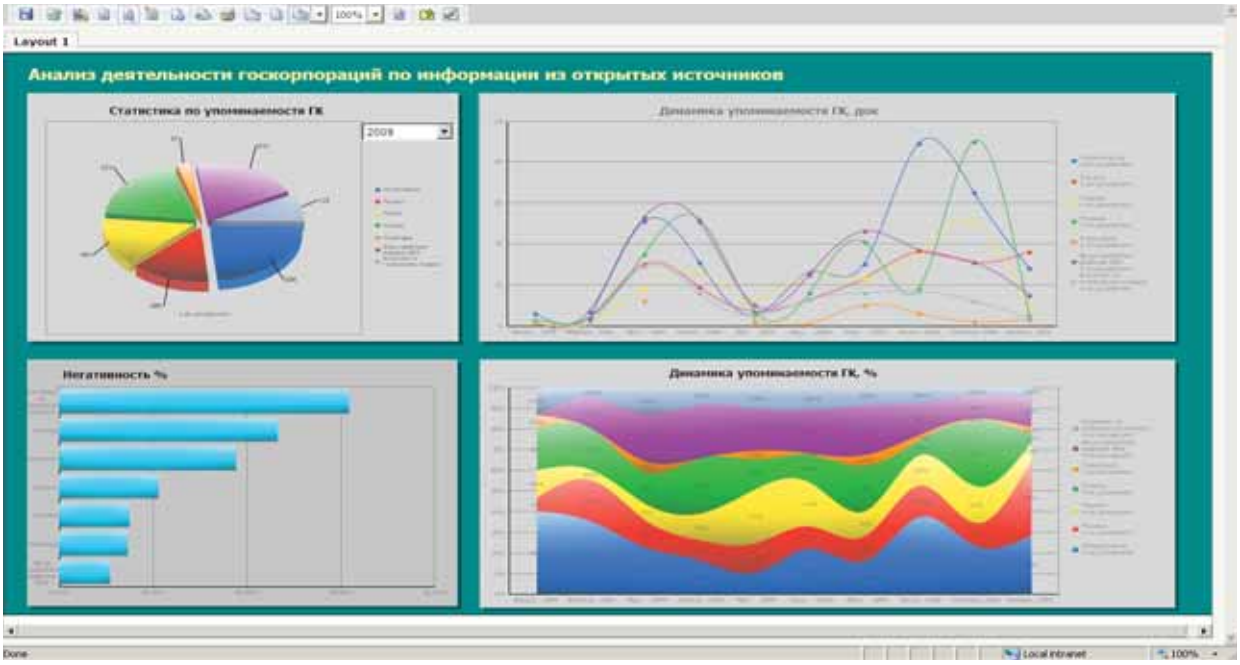

Рис. 2. Результаты аналитической обработки текстов. На примере анализа деятельности госкорпораций

Аналитическая обработка неструктурированной информации заключается в ее:

- классификации;
- кластеризации;
- аннотировании;
- формировании рядов данных по:
  - упоминаемости,
  - основным тенденциям,
  - оценке критики,
  - негативного и позитивного окраса тех или иных объектов, событий
  - и пр.

На основе производимого синтаксического и семантического анализа текстов возможно решения ряда прикладных задач, таких, как: контент-анализ, ивент-анализ, поддержка ситуационного моделирования и пр.

Когнитивное моделирование

При решении задач управления слабоструктурированными объектами (СО) и ситуациями, часто возникают трудности по структурированию и переработке информации, необходимой для подготовки и принятия управленческих решений.

Одной из причин является недостаток информации о состоянии СО в условиях изменяющейся и слабо контролируемой внешней среды. Отсутствие достаточных знаний о системе, относительно которой принимается решение, не является единственной неопределенностью, обусловленной субъективными причинами. Также можно выделить неопределенность целей развития СО и критериев выбора управленческого решения [2]. Как правило, неудовлетворенность текущим состоянием системы осознается субъектом управления, но его представления о причинах и возможных способах изменения ситуации в СО размыты, нечетки и противоречивы. Формализация нечетких представлений – одна из главных задач, которую необходимо решить при разработке моделей и методов поддержки принятия решений в слабоструктурированных ситуациях [3].

Другая трудность связана с тем, что субъекту управления приходится манипулировать качественной информацией в виде гипотез (предположений), интуитивных понятий и смысловых образов. Многочисленные исследования процессов принятия решений подтверждают, что субъекту управления несвойственно мыслить и принимать решения только в коли-

чественных характеристиках. Он мыслит, прежде всего, качественно, и для него поиск решения – это, поиск, в первую очередь, замысла решения, где количественные оценки играют вспомогательную роль [4]. Поэтому «структуры знания в мышлении субъекта (лица, принимающего решения), оказываются важнейшими элементами ситуации, неустранимыми из модели принятия решений».

В практике подготовки и принятия решений класс управленческих задач, связанных с выявлением и диагностированием слабоструктурированных проблем и постановки целей развития СО, слабо поддержан формализованными методами, которые ориентированы на преодоление перечисленных выше трудностей.

Для решения этих задач на практике, как правило, применяются эвристические экспертные методы (мозговой штурм, интервьюирование и т.п.). При этом для структуризации проблемы нередко используется иерархическое представление – в виде дерева. Традиционные теоретические методы концентрируют внимание на процессах выбора альтернативы из фиксированного набора решений, но чаще всего множество альтернатив не может быть представлено эксперту в полном объеме. Поэтому важен не только процесс поиска рационального решения, но и собственно процесс формирования его допустимых вариантов [5].

В качестве формализованного метода, ориентированного на работу с неоднородной информацией (качественной и количественной), с экспертными знаниями, когда исследуемая система, ситуация, проблема не могут быть описаны субъектом управления точно, сегодня все шире применяется когнитивный подход, который позволяет поддержать ранние этапы процесса подготовки и принятия решений – этапы выявления и диагностирования слабоструктурированных проблем и постановки целей развития СО [6].

Типичным классом СО, для решения проблем развития которых целесообразно применение когнитивного моделирования, является социально-экономические системы.

Основные понятия в современном когнитивном моделировании

Ключевые понятия, сложившиеся и широко используемые в рамках когнитивного подхода и его различных школ, в публикациях зачастую не определяются; при этом нередко возникает неоднозначность понимания вплоть до противоречий как из-за различий понимания в разных школах, так и, в некоторых случаях, в рамках одной школы. Авторами статьи предпринята попытка уточнить некоторые основные понятия когнитивного подхода к решению задач анализа и управления СО.

Когнитивное моделирование – это исследование функционирования и развития слабоструктурированных систем и ситуаций посредством построения когнитивной карты СО.

Когнитивная карта [7]отражает субъективные представления (индивидуальные или коллективные) исследуемой проблемы, ситуации, связанной с функционированием и развитием СО. Основными элементами когнитивной карты являются базисные факторы[8] (или просто факторы) и причинно-следственные связи между ними.

Содержательно, *базисные факторы* – это факторы, которые (1) определяют и ограничивают наблюдаемые явления и процессы в СО и окружающей его среде и (2) интерпретированы субъектом управления как существенные, ключевые параметры, признаки этих явлений и процессов.

Метод формирования стратегических проблем развития социально-экономической системы

В общем виде *управление развитием социально-экономической системы*(СЭС) можно представлять как построение стратегии развития системы, которая определяет основные цели и общие направления их достижения, и ее реализацию.

Одним из ключевых этапов построения стратегии управления СЭС является выявление проблем развития системы, оказывающих негативное влияние на достижение стратегических целей управления.

В данном разделе кратко представлен метод формирования стратегии решения слабоструктурированных проблем на основе линейных динамических когнитивных моделей применительно к СЭС.

Задача управления состоит в переводе СЭС в одно из состояний, соответствующих *целевому образу* системы. Динамика изменения факторов когнитивной модели, характеризующих состояние системы в некоторый момент времени, определяется моделью вида (1).

Целевой образ СЭС задает, что необходимо изменить с позиции субъекта управления, и формально представляется как

$C = (X^C, R(X^C))$, (2)

где X^C – подмножество целевых факторов, $X^C \subseteq X$ (X – множество факторов когнитивной модели);

$R(X^C)$ – вектор оценок динамики факторов (ОДФ), определяющий желательные направления изменения целевых факторов.

$$R(x_i^C) = \begin{cases} +1, \text{ если желательно увеличение значения фактора } x_i^c \\ -1, \text{ если желательно уменьшение значения фактора } x_i^c \end{cases}$$

В рамках предлагаемого метода рассматривается коллективный субъект управления–руководство СЭС, принимающее управленческие решения, и его окружение (системные аналитики и эксперты), осуществляющие подготовку решений. На стратегию управления развитием СЭС могут влиять и другие субъекты, которые имеют собственные цели, интересы, представления и установки, определяющие выбор решений по развитию СЭС. В этом случае ту же задачу управления нужно решать с позиции каждого выделенного субъекта.

Стратегия решения проблем развития СЭС состоит из wстратегических шагов, которые задают последовательность изменений состояний системы

$S^0 \rightarrow S^1 \rightarrow S^2 \ldots \rightarrow S^m \rightarrow S^C$,

где S^0 – исходное состояние,

S^C– целевое состояние (соответствующее целевому образу (2),

$S^i \rightarrow S^{i+1}$ – *стратегический шаг*, на котором выявляется проблема и на основе ее анализа на множестве факторов *X* когнитивной модели выделяется подмножество локальных целей (целевых факторов) и подмножество управлений (управляющих факторов), изменение которых приводит к желательному изменению целевых факторов.

Каждый стратегический шаг $S^i \rightarrow S^{i+1}$ включает

- выявление проблемы на базе моделирования саморазвития начального состояния *i*–го шага, в результате которого проблема уточняется в виде P^i – подмножества факторов, изменение которых не соответствует целевому образу;
- диагностирование проблемы путем построения «подграфа причин» и структурно-целевого анализа с целью выделения из P^i подмножества локальных непротиворечивых целевых факторов Y^i и поиска вариантов управлений (подмножеств управляющих факторов) U_j^i, способствующих изменению Y^i в желательном направлении. Непротиворечивость целевых факторов означает, что желательное изменение любого целевого фактора из Y^i не приводит к нежелательному изменению остальных факторов из Y^i;
- моделирование управляемого развития системы, на основании которого формируются различные сценарии.

Заключение

В заключении нам представляется целесообразным сформулировать направления дальнейших исследований. Опыт применения различных моделей и методов на базе когнитивного подхода (в России и за рубежом), повышающийся интерес управленцев-практиков к разработкам в данном направлении показывают целесообразность развития данного подхода в управлении. При этом следует отметить наличие нерешенных (или отчасти решенных) проблем. Выделим некоторые направления исследований, которыми авторы статьи будут заниматься в рамках дальнейшего развития когнитивного подхода в моделировании и управлении.

Разработка *научно-методического обеспечения*. В этом направлении проводятся работы, связанные с разработкой методик выявления типичных рисков из-за человеческого фактора при формировании и формализации знаний о развитии слабоструктурированной системы, ее проблемах, целях развития и стратегиях разрешения проблем, включая формирование системы критериев, ориентированной на достоверность формализации первичных знаний (представлений); разработку принципов и методов, направленных на повышение уровня надежности и точности измерений при построении когнитивных карт и интерпретации результатов.

Разрабатывается подход к формализации первичных представлений о слабоструктурированной проблеме в виде коллективной когнитивной карты с целью обобщения и согласования разных представлений у носителей проблемы, компетентных в различных предметных областях знаний. Решение этой задачи опира-

ется на разработанные методы концептуальной структуризации и критерии и частные технологии формирования и согласования коллективных понятий.

Планируется проведение цикла работ по интеграции когнитивного подхода и методов теории активных систем, поскольку в обоих научных направлениях большое значение отводится исследованию сложных систем, в которых одним из основных элементов являются активные субъекты, существенно влияющие на эффективность управления системой.

Повышение прикладной значимости результатов исследований. Продолжается работа по созданию технологии когнитивного моделирования слабоструктурированных ситуаций и систем с развитым научно-методическим и инструментальным обеспечением для внедрения в практику управленческой деятельности по планированию и управлению развитием социально-экономических систем.

В настоящее время разработан программно-аналитический комплекс, в котором реализованы функции построения когнитивных моделей, структурно-целевого анализа, сценарного моделирования и сравнительной оценки сценариев.

Модульная архитектура разработанного комплекса позволяет наращивать его другими инструментальными средствами решения различных задач управления, а также взаимодействовать с современными информационно-аналитическими системами (например, системами сбора и анализа информации, ERP – системами).

Литература

1. The Expanding Digital Universe. A Forecast of Worldwide Information Growth Through 2010 / D. Reinsel, Ch. Chute, W. Schlichting, et al. – Framingham, MA: IDC, 2007. – 24 p.; The Diverse and Exploding Digital Universe. An Updated Forecast of Worldwide Information Growth Through 2011 / Ch. Chute, A. Manfrediz, S. Minton, et al. – Framingham, MA: IDC, 2008. – 16 p.
2. Диев В.С. Нечеткость в принятии решений // Философия науки. – 1998. – № 1(4). – С. 45–52.;
3. Трахтенгерц Э.А.Субъективность в компьютерной поддержке решений. – М.: СИНТЕГ, 2001. – 256 с.
4. Сергеев В.М. Когнитивные методы в социальных исследованиях // Язык и моделирование социального взаимодействия. – г. Благовещенск: БГК им. И.А. Бодуэна де Куртенэ, 1998. – С. 3–19.
5. Компьютерная поддержка сложных организационно-технических систем / В.В. Борисов, И.А. Бычков, А.В. Дементьев и др. – М.: Горячая линия – Телеком, 2002. – 154 с.;
6. Дёрнер Д. Логика неудачи. Стратегическое мышление в сложных ситуациях. – М.: Смысл, 1997. – 243 с.;
7. Федулов А.С. Нечеткие реляционные когнитивные карты // Теория и системы управления. – 2005. – №1. – С. 120–132.
8. Лазарев В.М., Свиридов А.П. Нейросети инейрокомпьютеры. Монография. – М.: 2011. – 131 с. МИРЭА, 2011.

Атагимова Эльмира Исамудиновна
кандидат юридических наук

Проблемы отрицательного влияния интернета на нравственное воспитание подростков в информационном пространстве и пути решения

Аннотация: *рассматриваются проблемы негативного информационного воздействия интернета на нравственное воспитание подрастающего поколения. Раскрываются поправки принятые Федеральным законом РФ № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет» для решения данной проблемы.*

Ключевые слова: *Интернет, нравственно-правовое воспитание, подрастающее поколение, негативное влияние, Федеральный закон РФ, поправки.*

Internet (Интернет) – всемирная информационная компьютерная сеть. Самая большая в мире совокупность разнотипных компьютерных сетей. Объединяет миллионы компьютеров, баз данных, файлов и людей. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (WorldWideWeb, WWW) и множества других систем (протоколов) передачи данных. Интернет-аудитория в России ежегодно увеличивается. Пользователей интернета, по данным Всероссийского центра изучения общественного мнения (ВЦИОМ)РФ на начало 2012 года (Инициативный всероссийский опрос ВЦИОМ проведён 31 марта – 1 апреля 2012 г.) , 70 млн. чел (всё население РФ – 143 млн. чел.). По этому показателю Россия вышла на первое место в Европе и на шестое место в мире. Рост числа пользователей интернета в России будет продолжаться и далее. Согласно результатам исследования «Российского рынка интернет-торговли: товары 2012», проведенного агентством РБК.research, весной 2013 года уровень проникновения интернета составит 63,6%, а в 2018 году он превысит отметку в 80% [1].Это при том, что не учитывается самая юная возрастная категория веб-пользователей. По данным Госкомстата России, Всероссийского центра изучения общественного мнения, в России насчитывается около 8-10 млн. пользователей Интернета в возрасте до 14 лет [2]. И показатель контактов с нежелательным содержимым сайтов (порносайты, сайты об азартных играх, с ресурсами о насилии, алкоголе и наркотиках) с каждым днем возрастает. Юных пользователей – детей выходящих в сеть самостоятельно подстерегают такие ресурсы, которые пропагандируют насилие, издевательств подростков друг над другом (особенно школьное видео) и животными. Немало сайтов, связанных с ненавистническим контентом, «ВКонтакте» есть группы ненависти к реальному ребенку. Жертвы иногда создают свои группы ненависти к обидчикам. Так плетется паутина вражды. Появляются тысячи сайтов, которые призывают причинить себе боль и вред. Каждый четвертый ребенок заходит на сайты о диетах, а учитывая, что это в основном девочки, то каждая вторая из них пытается это использовать. Суммарно получается, что каждый второй заходит на один из подобных сайтов. Международные специалисты США и Европы пришли к выводу о недостаточности и даже малоэффективности при таком характере угроз и рисков технологических и запретительных средств защиты[3].

Беспокойство вызывает то, что негативное влияние интернета угрожает и психическому состоянию ребенка. Интернет, подобно другим СМИ, стал существенным фактором воспитания. Особенно опасным видится формирование личности путем идентификации себя с конкретной позицией или определенным способом поведения. Ребенок старается подражать распространенным образцам. Как получатель информации он поддается давлению и может легко стать жертвой всяких мошенников и создателей рекламы. Ребенок получает сообщения, не относясь к ним критически, и не осознает, что имеет дело с игрой видимостей. Благодаря тому, что дети получают неограниченный контакт с пространством, которое может обеспечить им интересное содержание и развлечения на все свободное время и отсутствие ограничений может иметь плачевные последствия. Необходимо помнить, что Интернет, как средство передачи информации, которое может вводить в зависимость и влиять на психику, является одновременно и пространством деятельности преступников. Ребенок легко может стать жертвой педофилии. Благодаря наивности детей, преступники легко получают порнографические материалы. Чаще всего несовершеннолетние пользователи попадают на опасные странички случайно. Многочисленные всплывающие окна, неверно истолкованные поисковиком запросы, ссылки в социальных сетях – все это приводит ребенка на сайты небезопасного содержания, связанные с негативным контентом, киберхулиганством, домогательствами, виртуальными контактами с кибермошенниками, наркодилерами, экстремистами, педофилами, сутенерами и порнографами [4]. Значительное большинство подобных преступлений остаются скрытыми от родителей, правоохранительных органов и общества. «Виртуальную» личность весьма трудно привлечь к ответственности за противоправные деяния, совершаемые в сети. Работая в чате, пользователь сети может представиться кем угодно, создать любой собственный образ какой ему угодно, менять свою внешность [5].

Особого внимания заслуживает широкое распространение электронных игр среди подростков. Авторы компьютерных игр стараются показать как можно более реальный игровой мир. Во многих компьютерных играх игра со смертью идет постоянно. Герой игры постоянно приближается к смерти, постоянно играет с ней и обманывает ее. У героя «компьютерной реальности» нет своего внутреннего мира он не испытывает ни страха, ни угрызений совести. Ребенок, сидя часами за монитором, учится разрушать. Поэтому созидательных навыков и бережного отношения к своей жизни, а тем более к чужой у него не формируется. То, что ещё вчера считалось преступлением, в играх сегодня является нормальным явлением. Искажению и разрушению подвергается не только действительность, но и мораль.

Еще в 60-е годы западные психологи (А. Бандура и др.) [6] доказали, что демонстрация сцен насилия по телевидению способствует проявлениям агрессивного поведения и искаженному восприятию действительности, делает наблюдателей безразличными к насилию в будущем, усиливает чувство опасности, враждебности и тревоги у человека. При этом человек переходит от непосредственного познания окружающего мира, к познанию мира воображаемого, виртуального, считая ЕГО реальностью. А ведь граница между фантазией и реальностью, которую способны различить даже не все взрослые, тем более расплывчата для ребёнка. Сейчас эта ситуация еще больше усугубляется при создании виртуальных миров.

Согласимся с Владимиром Путиным, который в рамках послания ФС РФ заявил, «Надо признать, уважаемые друзья, влияние школы на формирование детей и подростков в последние годы ослабло. У неё появились сильные конкуренты: интернет, электронные СМИ» [7].

Таким образом, в условиях быстрого распространения информационных технологий важнейшей проблемой становиться процесс формирования у подрастающего поколения, морально нравственных ориентиров, позволяющих определить, что такое хорошо и что такое плохо.

Защита детей от агрессивного негативного воздействия интернета это одна из наиболее важных и актуальных проблем для государства. В связи с этим, для защиты детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности был принят Федеральный закон № 139-ФЗ от 28 июля 2012 года (в прошлом Законопроект № 89417-6) – Федеральный закон Российской Федерации «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в

сети Интернет». Этот закон внёс в другие федеральные законы ряд положений, предполагающих фильтрацию интернет-сайтов по системе чёрного списка и блокировку запрещённых интернет-ресурсов. Федеральный закон направлен на совершенствование механизма, обеспечивающего защиту детей от информации, способной причинить вред их здоровью и (или) развитию, и предусматривает внесение изменений в федеральные законы «О защите детей от информации, причиняющей вред их здоровью и развитию», «О связи» и «Об информации, информационных технологиях и защите информации»[8]. Федеральным законом уточняется порядок размещения производителями и (или) распространителями информационной продукции, способной причинить вред здоровью и (или) развитию детей, знака и (или) текстового сообщения об ограничении её распространения среди детей соответствующей возрастной группы. В законе более подробно регламентируются способы маркировки контента. Так, согласно поправкам обозначение категории информационной продукции знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения информационной продукции среди детей осуществляется с соблюдением требований данного Федерального закона ее производителем и (или) распространителем следующим образом:

1) применительно к категории информационной продукции для детей, не достигших возраста шести лет, – в виде цифры «0» и знака «плюс»;
2) применительно к категории информационной продукции для детей, достигших возраста шести лет, – в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шести лет»;
3) применительно к категории информационной продукции для детей, достигших возраста двенадцати лет, – в виде цифры «12» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 12 лет»;
4) применительно к категории информационной продукции для детей, достигших возраста шестнадцати лет, – в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 16 лет»;
5) применительно к категории информационной продукции, запрещенной для детей, – в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей».

Федеральным законом частично изменяется порядок проведения экспертизы информационной продукции, право инициирования которой будет предоставлено юридическим лицам, индивидуальным предпринимателям, общественным объединениям и гражданам без предварительного обращения в уполномоченный федеральный орган исполнительной власти [7]. Конкретизируются особенности распространения информации посредством информационно-телекоммуникационных сетей, в том числе в сети «Интернет», в местах, доступных для детей. А именно, предусматривается, что доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», в местах, доступных для детей, предоставляется лицом, организующим доступ к сети «Интернет» в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Поправки в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вносят следующие изменения: в целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, в Федеральный закон добавляется новая статья 151 предусматривающая создание единой автоматизированной системы «Единый реестр доменных имён, универсальных указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено федеральными законами».

Основаниями для включения сведений в реестр, согласно ч. 5 статьи 151 являются:

1. решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти в отношении распространяемых посредством сети «Интернет» материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений; информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

2. вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено [8].

В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр владелец сайта в сети «Интернет» обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети «Интернет» провайдер хостинга обязан ограничить доступ к такому сайту в сети «Интернет» в течение суток.

Тот факт, что на одном IP-адресе могут находиться несколько сайтов с разными доменными именами, законом не учитывается.

В Кодекс Российской Федерации об административных правонарушениях вносятся положения об ответственности за неприменение в местах, доступных для детей, операторами связи, оказывающими телематические услуги связи, либо администрацией таких мест при осуществлении доступа к информации, распространяемой через Интернет, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Поправки в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» поясняют, что ограничение и возобновление доступа к информации, распространяемой через Интернет, регулируется Федеральным законом «Об информации, информационных технологиях и о защите информации».

Изменения в ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» вступили в силу 30 июля, в день публикации. 1 ноября 2012 года вступили в силу положения, касающиеся единого реестра доменных имен и URL-адресов, содержащих запрещённую к распространению информацию. Был создан Единый реестр запрещённых сайтов.

Надеемся, что данные поправки к закону реализуют себя в российском законодательстве в полном объеме, и помогут в формировании гармоничной и психологически устойчивой личности каждого ребенка, бережному и грамотному воспитанию детей на идеях добра и справедливости.

Литература

1. Интернет РФ: Главные новости и события, статистика Рунета. Главные новости декабря 2012. http://www.bizhit.ru
2. Интернет и дети. http://schuc1231.mskobr.ru http://schuc1231.mskobr.ru/novosti/materialy_po_bezopa snosti_igternet
3. Дети интернет-поколения России: новая реальность? http://maxpark.com
4. Пристанская. О.В. Начальник отдела по обеспечению деятельности Уполномоченного при Президенте Российской Федерации по правам ребенка.Рекомендации по проведению уроков медиабезопасности школьников. http://nsportal.ru
5. Танимов О.В. Проблемы виртуальной личности в сети Интернет. Мониторинг правоприменения. № 4 – 2012. – М.: ФБУ НЦПИ при Минюсте России, 2012.
6. Кузьмин Н.Н. Некоторые аспекты влияния компьютерных технологий на нравственно-правовое воспитание подростка .http://hghltd.yandex.net/
7. http://президент.рф
8. Электронный фонд правовой и нормативно-технической документации. http://docs.cntd.ru



Загородников Сергей Николаевич

доктор биологических наук, кандидат технических наук, профессор

Максимов Денис Алексеевич

Петрова Любовь Петровна

Безопасность экономической информации в рыночной среде

Аннотация: *рассматриваются положения отдельных нормативных актов, обеспечивающих правовое регулирование защиты информации, циркулирующей в сфере экономических отношений.*

Ключевые слова: *безопасность, информационный, экономический, нормативный, акт.*

Необходимым фактором для принятия каких-либо решений является наличие актуальной и достоверной информации, определяющей диапазон возможных действий, лица, принимающего решение. Мы живем в эпоху информатики, и любая фирма, которая игнорирует процессы организации, упорядочения и охраны необходимой для бизнеса и его развития актуальной и достоверной информации, подвергает себя риску быть разоренной или вытесненной с рынка. В любом решении, которое принимается в бизнесе, присутствует риск. Поэтому необходимо принимать меры для обеспечения того, чтобы информация, от которой зависит развитие бизнеса, а также само благополучное существование фирмы, не была похищена, искажена или уничтожена, чтобы специалисты и руководители фирмы получали по интересующим их проблемам актуальные и неискаженные сведения.

С развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называют веком энергетики, то наступивший XXI – веком информатики. Информация в практической деятельности проявляется во множестве аспектов — вот только некоторые из таких способов проявления:

- во-первых, производство информации как таковой — это производственная отрасль, т.е. вид экономической деятельности;
- во-вторых, информация является фактором производства, один из фундаментальных ресурсов любой экономической системы;
- в-третьих, информация является объектом купли-продажи, т.е. выступает в качестве товара;
- в-четвертых, некоторая часть информации является общественным благом, потребляемым всеми членами общества;
- в-пятых, информация — это элемент рыночного механизма, который наряду с ценой и полезностью влияет на определение оптимального и равновесного состояний экономической системы;

- в-шестых, информация в современных условиях становится одним из наиболее важных факторов в конкурентной борьбе;
- в-седьмых, информация становится важнейшим средством деловых и правительственных кругов, используемым при принятии решений и формировании общественного мнения [1].

Возрастание роли информации во всех сферах функционирования общества, в жизни и работе каждого человека ставит вопросы о создании эффективной системы информационной безопасности. «Информационная безопасность – это состояние защищённости информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния. (Википедия-Internet). Согласно определению ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности» информационная безопасность включает в себя «все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки (п. 2.14)».

Информационная безопасность является важной частью общей безопасности бизнеса, использующей организационно-правовые, административные, инженерно-технические, воспитательные и иные меры, позволяющей снизить до минимальных размеров риск дезорганизации работы или полного уничтожения бизнеса.

Зачастую под обеспечением информационной безопасности понимается только физическая охрана вычислительных средств, оргтехники, носителей информации. Такие способы пригодны, как правило, только при противостоянии криминалу. Между тем, вступая в рыночные отношения, любая организация сталкивается с острой конкурентной борьбой, существующей на любом цивилизованном рынке. И эта борьба таит в себе немало опасностей для предприятия. Если компания достигла каких-либо успехов в своём бизнесе, можно не сомневаться в том, что она вызывает немалый интерес со стороны компаний-конкурентов. Любая информация о работе фирмы будет привлекать повышенное внимание с их стороны. Поэтому защита информации становится важнейшей частью современной системы безопасности бизнеса. Как правило, подходы к решению данной проблемы сводятся к созданию правил, определяющих для работы с отдельными видами информации режим повышенной секретности, а также уделяющих основное внимание защите информации от несанкционированного доступа (НСД). Методами решения данной задачи обычно служат простое ограничение использования тех или иных информационных технологий (ИТ) (например, Интернета или электронной почты) или их полный запрет. Для коммерческих организаций такой подход неудобен, а зачастую и просто неприемлем — бизнес не может эффективно работать без интенсивной поддержки ИТ и активного взаимодействия с клиентами и партнерами. Для коммерческих организаций актуальна не только защита информации от НСД, но и обеспечение безопасности информации и установленного функционирования ИТ. Под обеспечением безопасности информации обычно понимается сохранение ее конфиденциальности, целостности и доступности. Необходимость обеспечения установленного функционирования ИТ организации тесно связана с более общей задачей обеспечения непрерывности ее бизнеса. Таким образом, обеспечение информационной безопасности в коммерческих организациях имеет значительную специфику, и традиционные методы защиты информации от НСД не покрывают всех аспектов данной задачи [2].

Решение проблем информационной безопасности на практике осуществляется по различным направлениям. Одним из таких направлений является правовое регулирование. В научном плане развитие законодательства по информационной безопасности идет, в частности, по линии систематизации соответствующих норм. Настоящая работа представляется авторами как фрагмент решения проблемы комплексного обеспечения информационной безопасности в конкурентной борьбе.

Для получения или добывания каких-либо сведений, представляющих определенный интерес и характеризующих деятельность конкурентов, клиентов или партнеров, для того, чтобы убедиться в том, что деловой партнер действительно в состоянии выполнить свои договорные обязательства, и, как говорят, вас «не кинет», используются средства промышленного шпионажа (или, по другому, конкурентной разведки). Правовой основой сбора информации о партнерах, конкурентах и иных лицах являются Закон Российской Федерации «О частной детективной и охранной деятельности»

№ 2487 от 11 марта 1992 года (в последней редакции от 03.12.2011 № 389-ФЗ), другие законы и правовые акты Российской Федерации. В соответствии со статьей 1 указанного выше закона «частная детективная и охранная деятельность определяется как оказание на возмездной договорной основе услуг физическим и юридическим лицам, имеющими специальное разрешение (лицензию) органов внутренних дел организациями и индивидуальными предпринимателями в целях защиты законных прав и интересов своих клиентов (в ред. ФЗ от 22.12.2008 № 272-ФЗ)». Подобная деятельность может осуществляться предприятиями, имеющими специальное разрешение (лицензию) органов внутренних дел Российской Федерации.

Уточним, что охраняются и защищаются с правовой точки зрения не сама информация, а права на нее; что различают тайну как вид конфиденциальной информации и режим тайны как вид правового режима охраны прав и законных интересов субъектов в отношении этой информации.

Поскольку каждая тайна выступает в виде прямых ограничений при реализации информационных прав и свобод человека и гражданина, то их правовое регулирование в соответствии с конституцией РФ возможно только через федеральные конституционные и федеральные законы.

В случае промышленного шпионажа субъектом (т.е. стороной, которая осуществляет активные действия) является отдельный предприниматель, фирма, т.е. физическое или юридическое лицо. Промышленный, или бизнес-шпионаж, обычно преследует две цели: а) проверить благонадежность делового партнера; б) – вытеснить или уничтожить конкурента. Для достижения названных целей необходима информация. В первом случае минимальная задача такова: необходимо убедиться, что деловой партнер действительно не подведет. Во втором случае о конкуренте желательно знать все: источники поставок товара, готовящиеся контракты, финансовое состояние, методы работы фирмы и постоянные деловые связи, – в общем, все то, что определяет экономическое положение фирмы-конкурента. Получив необходимую информацию, ее анализируют и определяют возможность вступления в деловые отношения с партнером (если цель – убедиться в благонадежности партнера) или определяют способ воздействия на конкурента, например, перехват поставок или контрактов, переманивание наиболее ценных специалистов, передача конфиденциальной информации, содержащей негативные характеристики конкурента, в правоохранительные органы. Легальный бизнес-шпионаж включает в себя такие методы, как анализ прессы, рекламных публикаций и т.д. Простой анализ рекламы позволяет оценить прибыль фирмы-конкурента с точностью до 10-15%, наружное видеонаблюдение за офисом позволяет оценить число сотрудников, их материальное положение, привычки, дает возможность выяснить круг лиц, входящих в высшее звено организации.

Интерпол следующим образом характеризует промышленный шпионаж:

«Это приобретение любым обманным путем интеллектуальной собственности, принадлежащей какому-либо юридическому лицу, которая была создана или законно приобретена этим юридическим лицом с целью произвести что-то, что имеет или может иметь промышленную ценность и, в более широком плане, ценность для национальной экономики» [4].

Законом предусмотрено два вида частной детективной и охранной деятельности: сыск и охрана.

В целях сыска разрешается предоставление следующих видов услуг:

1) сбор сведений по гражданским делам на договорной основе с участниками процесса;
2) изучение рынка, сбор информации для дедовых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;
3) установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;
4) выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;
5) поиск без вести пропавших граждан;
6) поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества;

В целях охраны предоставляются следующие услуги:

1) защита жизни и здоровья граждан;
2) охрана имущества собственников, в том числе при его транспортировке;

3) проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации;

4) консультирование и подготовка рекомендаций клиентам по вопросам правомерной защиты от противоправных посягательств;

5) обеспечение порядка в местах проведения массовых мероприятий.

Указанные выше услуги, что особо подчеркивается в Законе, могут оказывать лишь физические или юридические лица, имеющие статус частного детектива, частного детективного предприятия или объединения, частного охранника или частного охранного предприятия либо охранно-сыскного подразделения. Физические и юридические лица, не имеющие такого статуса, не вправе оказывать сыскные и охранные услуги.

Частным детективом признается гражданин Российской Федерации, получивший в установленном порядке лицензию на частную сыскную деятельность и выполняющий перечисленные в законе сыскные услуги. Совмещение этой деятельности с государственной службой не допускается [3].

Лицензия на работу в качестве частного детектива выдается органом внутренних дел в течение месяца со дня подачи заявления гражданином, претендующим на ее получение, сроком на 3 года.

В законе указаны ограничения на выдачу лицензии. Лицензии не выдаются:

1) гражданам, не достигшим 21 года;

2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;

3) гражданам, имеющим судимость за совершение умышленного преступления;

4) гражданам, которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);

5) гражданам, уволенным с государственной службы, из судебных, прокурорских и иных правоохранительных органов по компрометирующим их основаниям;

6) бывшим работникам правоохранительных органов, осуществлявшим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год;

7) гражданам, не представившим необходимые документы.

Если гражданин не согласен с отказом в выдаче лицензии, он может обратиться в вышестоящий орган внутренних дел или в суд. Частным детективам запрещается:

1) скрывать от правоохранительных органов ставшие им известными факты готовящихся или совершенных преступлений;

2) выдавать себя за сотрудников правоохранительных органов;

3) собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;

4) осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;

5) прибегать к действиям, посягающим на права и свободы граждан;

6) совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;

7) фальсифицировать материалы или вводить в заблуждение клиента;

8) разглашать собранную информацию, использовать ее в каких-либо целях вопреки интересам своего клиента или в интересах третьих лиц;

9) передавать свою лицензию для использования ее другими лицами.

Проведение сыскных действий, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища, влечет за собой установленную законом ответственность.

Промышленный шпионаж может быть открытым (легальным) или закрытым (в этом случае используются незаконные методы получения информации). Нелегальный бизнес-шпионаж включает в себя, во-первых, агентурный метод получения информации и, во-вторых, различные технические методы получения информации (например, перехват телефонных переговоров, аудиоинформации, почтовых и электронных сообщений). При использовании агентурного метода получения информации возможны два направления деятельности: а) вербовка, б) внедрение в организацию своего человека. Оба способа имеют свои преимущества. В любой коммерческой структуре есть вторые или третьи лица, которые по своим знаниям и опыту приближаются к уровню высшего звена и кото-

рые способны самостоятельно вести свою игру. Результатом вербовки может быть то, что выгодные заказы пойдут «налево», т.е., в частности и тем лицам, которые организовали бизнес-шпионаж в свою пользу. Если принять, что конечной целью промышленного шпионажа является уничтожение фирмы-конкурента, то вариант с внедрением имеет существенные преимущества, т.к. доверие к своему человеку, конечно же, больше. Объектами агентурной разработки могут быть не только, скажем, вторые или третьи лица фирмы-конкурента, но и любые сотрудники любого, даже самого низшего, звена, которым вполне по силам осуществить скрытую установку подслушивающей аппаратуры, которая в обиходе носит название «жучки» и т.д. Для установки такой аппаратуры необходимо от нескольких секунд до двух-трех минут, а для установки аппаратуры, перехватывающей телефонные сообщения, вообще не нужно проникать в офис, так как достаточно найти телефониста, который согласится найти искомый телефонный кабель. Отметим, что по закону производство и сбыт такой техники преследуется в уголовном порядке и наказывается длительным сроком.

Распространенным способом получения конфиденциальной информации является незаконный доступ в информационные системы или компьютерный шпионаж, который преследует, как правило, экономические цели. Преступления этой категории чаще всего совершаются для получения следующей информации: программ обработки данных, результатов научных исследований, конструкторской документации и калькуляции, сведений о стратегии сбыта продукции и списков клиентов конкурирующих фирм, административных данных, сведений о планах и о технологии производства. Наиболее распространенная в настоящее время форма компьютерных преступлений – деятельность хакеров, владельцев персональных компьютеров, незаконно проникающих в информационные сети. Хакеры – это квалифицированные и изобретательные программисты, занимающиеся разными видами компьютерных махинаций, начиная с нарушений запретов на доступ к компьютерам в совокупности с их несанкционированным использованием, вплоть до хищения секретных сведений.

Съём информации с компьютера может осуществляться многими способами:

- хищение носителей информации;
- копирование программной информации с носителей;
- чтение оставленных без присмотра распечаток программ;
- чтение информации с экрана посторонним лицом (во время отображения ее законным пользователем или при его отсутствии);
- подключение к компьютеру специальных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений (известно, что с помощью направленной антенны такой перехват возможен в отношении аппаратуры в металлическом корпусе на расстояниях до 200 метров, а в пластмассовом – до одного километра);
- несанкционированный доступ программ к информации, либо расшифровка программной зашифрованной информации. Последний способ называется «электронным грабежом».

Существует ряд характерных черт преступлений, связанных с использованием ЭВМ, которые усложняют расследование и предъявление обвинения по ним. Помимо юридических трудностей возникают и другие проблемы, с которыми может столкнуться следствие. Среди них:

- сложность обнаружения преступлений, связанных с использованием ЭВМ;
- большая дальность действия современных средств связи делает возможным внесение незаконных изменений в компьютерную информацию с помощью дистанционных терминалов либо закодированных телефонных сигналов практически из любого района;
- затруднения в понимании порядка работы ЭВМ в технологически сложных случаях;
- информация преступного характера, заложенная в память и служащая доказательством для обвинения, может быть ликвидирована почти мгновенно;
- обычные методы финансовой ревизии в случае этих преступлений не применимы, т.к. для передачи информации используются электронные импульсы, а не финансовые документы.

Что может сделать с вашей информацией злоумышленник?

Во-первых, просто ее прочитать (и использовать затем вам во вред), что называется нарушением конфиденциальности информации. Во-вторых, изменить содержимое или присвоить себе авторство сообщения, что является наруше-

нием целостности информации. Классический пример нарушения целостности — добавление лишнего нуля в платежном документе, а это совершенно недопустимо. Способов защититься также два: шифрование информации, которое поможет скрыть ее от чересчур любопытных, и применение электронной подписи (ЭП), которая не позволит что-либо изменить «по дороге» в письме или пересылаемом документе и даст возможность точно установить, кто именно является автором пришедшего сообщения.

Одним из средств защиты данных от несанкционированного доступа является их шифрование. Математическая дисциплина, изучающая алгоритмы шифрования текстов, называется криптографией. Цель криптографической системы заключается в том, чтобы зашифровать осмысленный исходный текст (также называемый открытым текстом), получив в результате совершенно бессмысленный на взгляд шифрованный текст (криптограмму). Получатель, которому он предназначен, должен быть способен расшифровать (говорят также «дешифровать») эту криптограмму, восстановив, таким образом, соответствующий ему открытый текст. При этом противник должен быть неспособен раскрыть исходный текст. Существует важное отличие между расшифрованием и раскрытием шифрованного текста. Раскрытием системы шифрования (криптосистемы) называется результат работы, приводящий к возможности эффективного раскрытия любого, зашифрованного с помощью данной криптосистемы, открытого текста. Степень неспособности криптосистемы к раскрытию называется ее стойкостью.

Все методы шифровки можно разделить на две группы: шифры с секретным ключом и шифры с открытым ключом. Первые характеризуются наличием некоторой информации (секретного ключа), обладание которой даёт возможность как шифровать, так и расшифровывать сообщения. Поэтому они именуются также одноключевыми. Шифры с открытым ключом подразумевают наличие двух ключей – открытого и закрытого; один используется для шифровки, другой для расшифровки сообщений. Эти шифры называют также двухключевыми.

Шифры с секретным ключом подразумевают наличие некой информации (ключа), обладание которой позволяет как зашифровать, так и расшифровать сообщение. С одной стороны, такая схема имеет те недостатки, что необходимо кроме открытого канала для передачи шифрограммы наличие также секретного канала для передачи ключа, а кроме того, при утечке информации о ключе, невозможно доказать, от кого из двух корреспондентов произошла утечка.

Шифры с открытым ключом подразумевают наличие двух ключей – открытого и закрытого; один используется для шифровки, другой для расшифровки сообщений. Открытый ключ публикуется – доводится до сведения всех желающих, секретный же ключ хранится у его владельца и является залогом секретности сообщений. Суть метода в том, что зашифрованное при помощи секретного ключа может быть расшифровано лишь при помощи открытого и наоборот. Ключи эти генерируются парами и имеют однозначное соответствие друг другу. Причём из одного ключа невозможно вычислить другой. Характерной особенностью шифров этого типа, выгодно отличающих их от шифров с секретным ключом, является то, что секретный ключ здесь известен лишь одному человеку, в то время как в первой схеме он должен быть известен по крайней мере двоим. Это даёт такие преимущества: не требуется защищённый канал для пересылки секретного ключа, вся связь осуществляется по открытому каналу; «что знают двое, знает свинья» – наличие единственной копии ключа уменьшает возможности его утраты и позволяет установить чёткую персональную ответственность за сохранение тайны; наличие двух ключей позволяет использовать данную шифровальную систему в двух режимах – секретная связь и цифровая подпись.

Одним из лучших используемых в настоящее время симметричных алгоритмов является отечественный стандарт шифрования ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Этот алгоритм является обязательным для применения в государственных организациях России, а также в негосударственных, но обменивающихся с ними конфиденциальной информацией. Основной особенностью Российского стандарта является высокая стойкость криптографического алгоритма. Она основывается на использовании 256-битного ключа. Алгоритмы симметричного шифрования обеспечивают высокую скорость шифрования и простоту аппаратной и программной реализации. Однако зависимость числа ключей от числа абонентов является квадратичной, что при большом количестве пользователей делает неэффективной работу службы

генерации ключей из-за низкой скорости обработки огромного количества информации.

В криптосистемах с открытым ключом не требуется передача секретного ключа между абонентами, участвующими в обмене защищаемой информацией. Суть разработанного подхода заключается в том, что в обмене защищаемыми документами каждый абонент использует пару взаимосвязанных ключей – открытый и секретный. Отправитель подписываемого документа передает получателю открытый ключ. Он может это сделать любым несекретным способом или поместить ключ в общедоступный справочник. При помощи открытого ключа получатель проверяет подлинность получаемой информации. Секретный ключ, при помощи которого подписывалась информация, хранится в тайне от всех. Таким образом, решаются две проблемы: нет нужды в секретной доставке ключа (так как при помощи открытого ключа нельзя расшифровать сообщения, которые зашифрованы для этого открытого ключа, и, следовательно, перехватывать открытый ключ нет смысла); отсутствует также квадратичная зависимость числа ключей от числа пользователей, так как – для N пользователей требуется 2N ключей.

Сообщение, зашифрованное при помощи открытого ключа какого-либо абонента, может быть расшифровано только им самим, поскольку только он обладает секретным ключом. Таким образом, чтобы послать закрытое сообщение, вы должны взять открытый ключ получателя и зашифровать сообщение на нём. После этого даже вы сами не сможете его расшифровать.

Все государства уделяют пристальное внимание вопросам криптографии. Наблюдаются постоянные попытки наложить некие рамки, запреты и прочие ограничения на производство, использование и экспорт криптографических средств. В России лицензируется ввоз и вывоз средств защиты информации, в частности, криптографических средств, согласно Указу Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (в ред. Указа Президента РФ от 25.07.2000 г. № 1358).

Объясняется такая политика теми особенностями, которые имеет криптография в плане её доступности для использования и трудности преодоления. Криптографическая защита относительно дёшева, а средства её преодоления либо очень дороги, либо вообще не существуют. Один человек с персональным компьютером может успешно противопоставить свою защиту любым государственным структурам.

Криптография, в отличие от мер физической защиты, обладает тем уникальным свойством, что при правильном выборе метода затраты на обеспечение защиты информации много меньше затрат на преодоление этой защиты. То есть, обыкновенный гражданин может себе позволить такую крепкую защиту, которую не в силах преодолеть государство со всей его финансовой и технической мощью.

В современных системах с высокими требованиями к защищенности информации для шифрования используются методы, основанные на аналитических преобразованиях текста. Смысл этих методов заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Можно, например, использовать правило умножения матрицы на вектор, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны сохраняться в тайне), а символами умножаемого вектора последовательно служат символы шифруемого текста. Расшифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве основы берется матрица, обратная той, с помощью которой осуществляется закрытие, а в качестве вектора – сомножителя – соответствующее количество символов закрытого текста. Данный метод легко реализуется программными средствами.

Электронные документы – это документы, созданные электронными средствами в виде текстовых или графических файлов. Электронные документы способны найти широкое применение в коммерческих и управленческих процессах лишь при условии, что достоверность содержащейся в них информации не вызывает сомнений.

Процесс обмена электронными документами существенным образом отличается от обычной формы обмена документами на бумажных носителях. При широком внедрении в деловую и административную практику обмена электронными документами необходимо решить проблему подтверждения подлинности содержащейся в них информации и ее соответствия смыслу волеизъявления человека. Технически эта проблема решается путем использования средств

ЭЦП. 10 января 2002 г. был принят ФЗ № 1-ФЗ «Об электронной цифровой подписи» (в редакции от 8 ноября 2007г. № 258-ФЗ), который закладывает основы решения проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными документами, при соблюдении которых электронная цифровая подпись признается юридически равнозначной собственноручной подписи человека в документе на бумажном носителе.

Статья 3 этого закона устанавливает, что «электронный документ – документ, в котором информация представлена в электронно-цифровой форме».

ЭЦП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющей идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе. С помощью ЭЦП гарантируется авторство (поступление информации из достоверного источника), неотказуемость (аналог собственноручной подписи)

Федеральный Закон «Об электронной цифровой подписи» определяет условия использования ЭЦП в электронных документах органами государственной власти и государственными организациями, а также юридическими и физическими лицами, при соблюдении которых:

- средства создания подписи признаются надежными;
- сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены;
- предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам;
- соблюдаются правовые нормы, содержащие требования к письменной форме документа;
- сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства;
- обеспечивается охрана персональной информации.

Определены требования к сертификату ключа подписи, выдаваемому удостоверяющим центром для обеспечения возможности подтверждения подлинности ЭЦП. Устанавливается состав сведений, содержащихся в сертификате ключа подписи, срок и порядок его хранения, а также порядок ведения реестров сертификатов.

Согласно статье 6 данного Закона сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя, отчество владельца сертификата ключа подписи или псевдоним владельца;
- открытый ключ электронной цифровой подписи;
- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Для шифрования ЭЦП используется ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Это российский стандарт, описывающий алгоритмы формирования и проверки электронной подписи. Принят и введён в действие Постановлением Госстандарта России от 12 сентября 2001 года.

Исходя из статьи 160 Гражданского кодекса Российской Федерации на информацию, заверенную ЭЦП, распространяются все традиционные процессуальные функции собственноручной подписи, в том числе, удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства.

Согласно статьи 3 закона об ЭЦП «подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном дан-

ной электронной цифровой подписью электронном документе».

Защита информации в сфере современных технологий информационного обмена предусматривает четыре уровня:

Предотвращение – только авторизованный персонал имеет доступ к информации и технологии.

Обнаружение – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

Ограничение – уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению.

Восстановление – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Меры защиты – это меры, вводимые руководством, для обеспечения безопасности информации – административные руководящие документы (приказы, положения, инструкции), аппаратные устройства или дополнительные программы – основной целью которых является предотвратить преступления и злоупотребления, не позволив им произойти. Меры защиты могут также выполнять функцию ограничения, уменьшая размер ущерба от преступления.

В заключение отметим основные факторы или события, содействующие или сопутствующие компьютерным преступлениям:

- неавторизованное использование компьютерного времени
- неавторизованные попытки доступа к файлам данных
- кражи частей компьютеров
- кражи программ
- физическое разрушение оборудования
- уничтожение данных или программ
- неавторизованное владение съемными носителями информации или распечатками.

Литература

1. Копылов В.А., Информационное право. Вопросы тории и практики. М,, «Юристъ», 2003.
2. Степанов Е.А., Корнеев И.К., Информационная безопасность и защита информации, М., «Инфра-М», 2001.
3. Загородников С.Н., Шмелев А.А., Основы информационного права, М., «Академический проект», 2005.
4. Шаваев А.Г., Криминологическая безопасность негосударственных объектов экономики, М., «Инфра-М», 1995.
5. Шиверский А.А., Защита информации: проблемы теории и практики, М., «Юристъ», 1996.
6. Костров А.В., Основы информационного менеджмента. М., «Финансы и статистика», 2003.

Коваленко Егор Владимирович

Макаренко Дмитрий Григорьевич

Дистанционное оказание юридических услуг населению как развитие государственных юридических бюро

Аннотация: *предлагается новый подход к оказанию населению бесплатных юридических услуг через создание сети дистанционных центров на современной технологической платформе и показываются существенные достоинства такого развития услуг вместо развиваемых сейчас государственных юридических бюро.*

Показывается, что с помощью современных технологий реально обеспечить консультациями всю Россию сравнительно недорого для государства, создав в каждом федеральном округе консультационные юридические бюро – Всероссийские бюро справедливости (жалоб).

Ключевые слова: *дистанционный доступ, IP-телефония, программное обеспечение, юридические консультации.*

В российской действительности сложилось положение, что гражданам некуда жаловаться на бездействие или неправовые действия чиновников на местах.

В советские времена существовал закон, обязывающий письменно (и устанавливающий ответственность должностных лиц за неисполнение) реагировать на обращения граждан в любое государственное учреждение; таким образом, у гражданина появлялись документы, с которыми можно было далее искать справедливости.

Сейчас об адекватной ответственности должностных лиц ничего не слышно.

Общество постоянно сталкивается с тем, что многие позитивные начинания власти при их реализации торпедируются на местах, компрометируются ненадлежащим исполнением чиновниками низового и среднего уровня. Например, под давлением высшей власти России создаются сайты государственных услуг. Казалось бы, народ должен радоваться – ведь в России Интернет есть повсеместно. Однако пользоваться услугами сайтов госуслуг весьма затруднительно – при том, что на их разработку затрачиваются космические суммы, сайты неудобны, медленны, структура запутана. При их использовании запрашивается масса ненужной для оказания услуги информации. Даже к врачам, нам, специалистам в области оказания дистанционных услуг, записаться непросто. Сайты не унифицированы, однотипные государственные учреждения имеют совершенно различные по структуре сайты, имена сайтов выбираются произвольно – в отличие от западных стран. На каких-то сайтах запрашивается СНИЛС (кстати, 90% граждан не могут сказать, что означает эта аббревиатура – на самой карточке написано «Страховое свидетельство» – ярчайший пример неуважения чиновничеством своих граждан), на сайте налоговиков надо вводить паспортные данные, еще есть ИНН – как будто бы за более чем 20 лет современной России нельзя было придти к единому идентификационному номеру. Например, сайты всех госучреждений Германии имеют имена с единой структурой, найти любое ведомство или университет легко. Складывается впечатление, что в деле создания сайтов госус-

луг и вообще сайтов государственных учреждений мы имеем дело с саботажем чиновников – не перевелись же в России специалисты, ведь сайты коммерческих структур (созданные российскими специалистами за значительно меньшие деньги) гораздо удобнее и работают быстрее.

Для снижения напряжения в обществе на самом деле надо сделать не так уж и много – объективно материальное положение российских граждан за последние годы существенно выросло. Однако в обществе бытует ощущение несправедливости, а средства массовой информации публикуют в основном негативную информацию, развивая чувство безысходности.

Сейчас жаловаться некуда, а советы обратиться в суд население воспринимает как издевку. При наших размерах и дорогах страны в больницу добраться проблематично, что уж говорить о других, менее важных для гражданина госучреждениях.

В то же время опыт фирмы «Национальная юридическая служба» [1] показывает, что 70% юридических и житейских проблем решается при первом обращении, 20% требуют более глубоких консультаций и лишь 10% требуют судебного решения. Так что советы по каждому поводу идти в суд народ справедливо считает издевательством.

В правосознании значительной части граждан закрепилось недоверие к государственным и муниципальным служащим, представителям различных государственных и общественных структур.

В 2004 г Министерство юстиции [2] представило В.В.Путину свои предложения о создании системы оказания государственной правовой помощи малообеспеченным гражданам, и в итоге Правительством Российской Федерации было издано постановление от 22.08.2005 № 534 «О проведении эксперимента по созданию государственной системы оказания бесплатной юридической помощи малоимущим гражданам».

Технологическое системы оказания бесплатной юридической помощи малоимущим гражданам было традиционным: в нескольких крупных городах открыли государственные юридические бюро.

Постепенно бюро создавались при всемерной поддержке Министерства Юстиции России и к 2010 году финансирование этой работы достигло 69,6 миллиона рублей, которые проконсультировали 41900 обращений граждан в 2010 году, и лишь 1400 обращений получили сопровождение в судебном производстве [2].

Однако юридические бюро в крупных городах малоэффективны, а в малых населенных пунктах бюро не создашь.

Тем не менее, в рамках отдельного региона или федерального округа, при применении дистанционных технологий возможно создание регионального независимого центра жалоб, или бюро справедливости, как его назвали авторы [3], при тех же затратах, что и на финансирование государственных юридических бюро, но с охватом всего населения региона и по значительно более широкому кругу вопросов, волнующих граждан.

Авторы статьи [4] многие годы работали в Германии, где по заказу страховой компании создали систему круглосуточной помощи русскоязычным гражданам Германии; вернувшись в Россию, была создана коммерческая фирма круглосуточной юридической помощи и консьерж-услуг для некоторых категорий клиентов, для чего были разработаны специальные технологические процедуры и специальное программное обеспечение, сценарии оказания услуг, сформирован необходимый аппаратный комплекс.

В структуре Министерства юстиции существует Научный центр правовой информации – первая в СССР научно-практическая организация, профессионально работающая с правовой информацией. НЦПИ располагает мощным вычислительным комплексом оборудования, квалифицированными юридическими кадрами, необходимыми площадями. В НЦПИ с 2011 года развернут телефонный центр обслуживания в рамках программы развития госуслуг – то есть получен некоторый позитивный опыт оказания юридической помощи населению.

Было бы полезно в рамках развития частно-государственного партнерства в 2013 году НЦПИ и ООО «Национальная юридическая служба» на базе региональных подразделений Министерства юстиции или отделений НЦПИ внедрить в нескольких регионах страны центры дистанционного оказания услуг с финансированием этих работ из региональных бюджетов или, на первом этапе, Министерства юстиции России. Такое внедрение с учетом имеющегося опыта работы в ООО «Национальная юридическая служба» и партнерства с НЦПИ возможно осуществить в несколько недель после принятия решения, причем на местах не требуется ничего, кроме помещения 50-80 м (в расчете на регион 2 миллиона человек) и дежурных юристов со зна-

нием местного языка (для кавказских регионов), так как специальные средства, созданные в ООО «Амулекс», позволяют переадресовать в считанные мгновения, которые обратившийся гражданин даже не заметит, к специализированному на данной проблеме юристу в НЦПИ или ином месте. Комплекс средств позволяет обратиться гражданину как по телефону (бесплатно), так и по SKYPE или по e-mail. Годовое функционирование системы для региона 2 миллиона человек обойдется около 7 миллионов рублей.

В первую очередь, такие центры справедливости было бы целесообразно внедрять в проблемных регионах – например, в Дагестане, в отдаленных районах Севера и Сибири, на Дальнем Востоке, в Карелии.

Нам представляется, что предлагаемые центры дистанционного обслуживания весьма полезны также тем главам регионов, которые намерены участвовать в выборах, или при необходимости с небольшими затратами произвести опрос населения по некоторым, важным для региона вопросам.

Социальное напряжение в регионах, где будут созданы центры дистанционного обслуживании, существенно уменьшится: ведь человеку часто помогает даже не решение мучающей его проблемы, а возможность ее обсудить с компетентным специалистом. Как свидетельствует наш опыт, в процессе изложения жалобы нередко человек сам находит ее решения: ему не хватает часто поддержки. Затраты же на дистанционное обслуживание обращений граждан составляют около 200 руб. против 1641 руб. [2] в существующих государственных юридических бюро.

Литература

1. www.amulex.ru Сайт ООО «Национальная юридическая служба»
2. Залуцкая И.А. Создание и деятельность государственных юридических бюро. Журнал «Мониторинг правоприменения», №3, 2012, с.7-15
3. Макаренко Г.И., Михалевич В.В. Дистанционное оказание юридических услуг населению через создание Всероссийского бюро справедливости. В журнале «Мониторинг правоприменения», №4-2012, стр.4-9.
4. Макаренко Г.И., Макаренко Д.Г. Организация «скорой» юридической помощи населению. В журнале «Правовой мониторинг», Выпуск № 10, НЦПИ, 2009 г, с.30-32. См. на сайте http://www.scli.ru/upload/monitoring/PM_N10.pdf

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

Булгакова Елена Валерьевна
кандидат юридических наук, доцент

Селезнёва Елизавета Алексеевна
кандидат юридических наук

Информационная безопасность защитника (адвоката). Организационно-правовой аспект

Аннотация: *в настоящей статье выявлены правовые и организационные проблемы обеспечения информационной безопасности защитника (адвоката). В статье приведены меры по уменьшению рисков, связанных с утечкой информации, которая стала известна защитнику (адвокату) при выполнении им своих профессиональных обязанностей.*

Ключевые слова: *информационная безопасность адвоката, адвокатская тайна, электронное правосудие.*

Модернизация юридической деятельности в свете проводимых правовых реформ, внедрения инноваций (информационных технологий) в эту сферу, создавших предпосылки к переходу от традиционных форм отправления правосудия к системе «Электронного правосудия» – сложный, многоэтапный процесс, требующий переосмысления и применения комплексных подходов в решении, возникающих при этом проблем правового, организационного, технического характера. В поддержку вышеуказанных глобальных перемен, были приняты ряд важных нормативных правовых актов[1], Министерством юстиции Российской Федерации разработан стратегически важный Проект федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации» (в части установления правового режима электронного документа и обеспечения его юридической значимости в деятельности органов судебной власти, прокуратуры и нотариата, в том числе при оказании государственных услуг в электронном виде) [2], созданы платформы единых информационно-телекоммуникационных систем (ЕИТКС), государственных автоматизированных систем (ГАС), таких как ГАС «Правосудие» [3] и др., обеспечивающих информационное электронное взаимодействие между участниками «Электронного правосудия». Принципы, положенные в основу работы «Электронного правосудия» позволили сделать этот процесс более открытым, прозрачным, доступным для граждан. Тем не менее, возникающие проблемы при функционировании этой системы – свидетельство недостаточности принимаемых мер, отсутствия комплексных, упорядоченных решений в реализации организационного, правового, технического элементов обеспечения эффективной работы «Электронного правосудия».

Одной из актуальных проблем, стоящих перед «Электронным правосудием» является обеспечение информационной безопасности участников данного процесса, информационной безопасности профильных автоматизированных информационно-телекоммуникационных систем, защиты информации, циркулирующей в них. В настоящее время система информационного взаимодействия участников «Электронного правосудия» уже внедрена, хотя отдельные ее блоки находятся на стадии разработки и, к сожалению, многие проблемы, в частности информационной безопасности, приходится решать, что называется «на ходу», напрямую столкнувшись с реальными угрозами безопасности. Обозначим наиболее значимые причины такого положения:

- проблемы подготовки и переподготовки, недостаточное количество специалистов в области обеспечения информационной безопасности в прикладных сферах, в частности – юриспруденции;
- значительные пробелы в существующей законодательной базе по вопросам обеспечения

информационной безопасности участников «Электронного правосудия», АИС, защите информации;

- в недостаточной мере используются наработки зарубежных стран, таких как США, Франция, Великобритания и др., имеющих значительный опыт в вопросах законодательного регулирования и правоприменительной практики по вопросам информационной безопасности «Электронного правосудия;
- отсутствие комплексного методологического подхода в обеспечении информационной безопасности участников «Электронного правосудия», в рамках их информационного взаимодействия;
- несовершенство, а порой и отсутствие инструкций по обеспечению информационной безопасности участников «Электронного правосудия»;
- отсутствие методики оценки эффективности мер по обеспечению информационной безопасности участников «Электронного правосудия»;
- трудности перехода к единой системе стандартов по обеспечению информационной безопасности АИС, используемых в сфере «Электронного правосудия»;
- система информационного взаимодействия участников «Электронного правосудия» носит сложный характер, представляя собой многоуровневую, распределенную систему организационного управления и др.

Для устранения имеющихся пробелов было проведено комплексное исследование организационно-правовых, технических вопросов обеспечения информационной безопасности участников уголовного процесса в системе «Электронного правосудия». Эффективность принимаемых мер по обеспечению информационной безопасности работы системы «Электронного правосудия» была проанализирована при помощи специально разработанного программного комплекса: «Комплексное обеспечение информационной безопасности участников уголовного процесса» [4], протестированного в правоохранительных органах Волгоградской области (ГСУ ГУ МВД России по Волгоградской области) и адвокатских образованиях г. Волгоград, г. Москва, республики Коми, г. Сыктывкар. На рис. 1 изображена архитектура программного комплекса по оценке мер адекватности и эффективности политики безопасности функционирования «Электронного правосудия», а на рис. 2 приведена экранная копия.

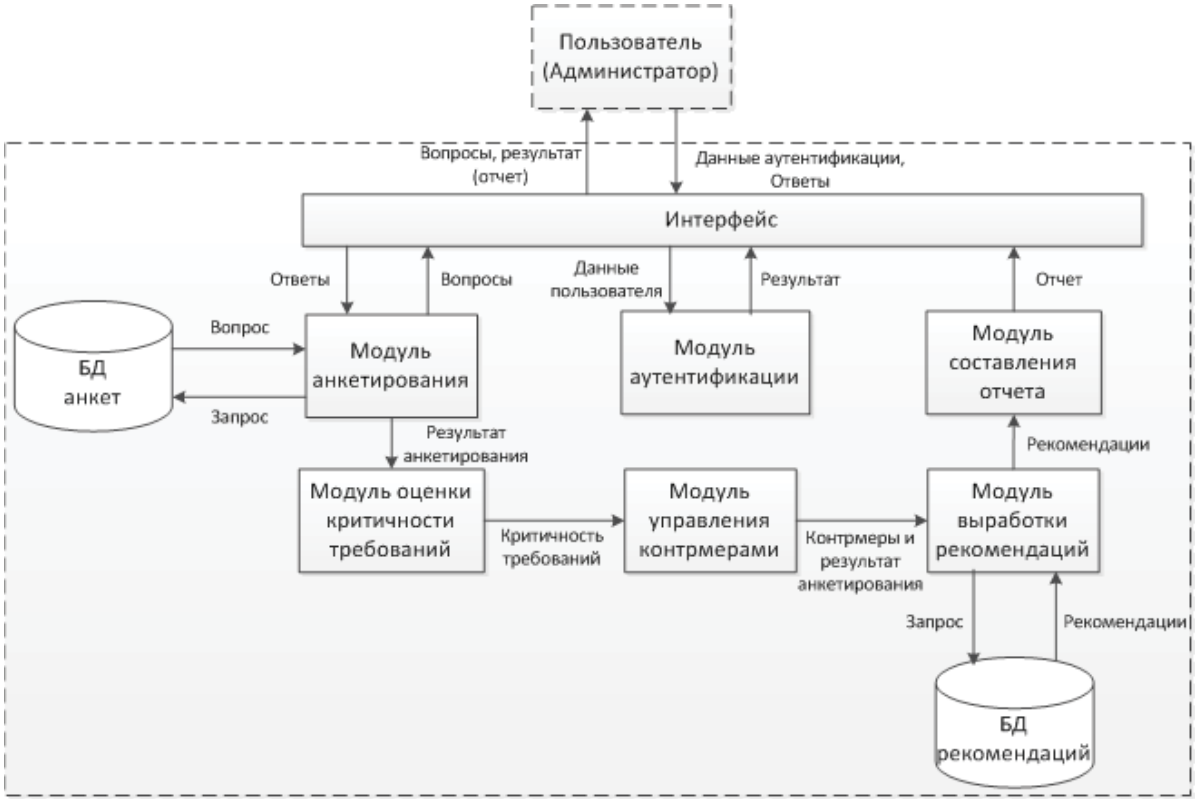

Рис.1. Архитектура программного комплекса по оценке мер адекватности и эффективности политики безопасности функционирования «Электронного правосудия»

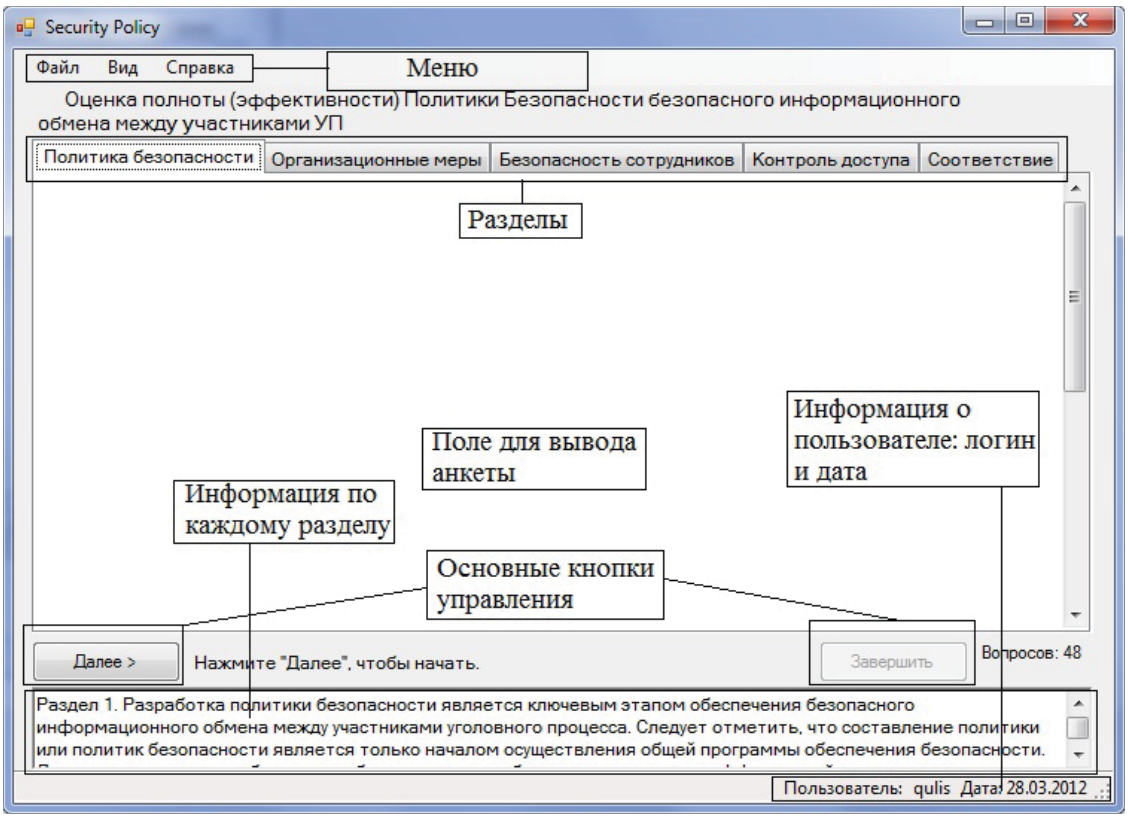

Рис. 2. Головной интерфейс. Экранная копия

При этом следует отметить, что меры направленные на обеспечение защищенности системы «Электронного правосудия» носят в основном технический характер и направлены на обеспечение информационной безопасности АИС, а вопросы обеспечения информационной безопасности отдельных ее участников обеспечиваются частично или не обеспечиваются ни на одном из уровней.

Согласно проведенному исследованию, наиболее тревожная ситуация по вопросу обеспечения информационной безопасности сложилась в деятельности защитника (адвоката). На рис. 3, в таблице 1 приведены результаты анкетирования отдельных пользователей системы «Электронного правосудия» по соблюдению мер информационной безопасности.

Таблица 1.

Пример тестирования программного комплекса.
Результаты тестирования отдельных пользователей системы «Электронного правосудия»

Подразделения / **Элементы ПБ**	ГСУ ГУ МВД	ГУ МВД	Адвокатская контора КОНСУЛ
Правовой	60 / 10 / 23 (93)	62 / 12 / 21 (94)	59 / 20 / 11 (90)
Организационный	43 / 24 / 12 (79)	48 / 14 / 23 (85)	39 / 21 / 13 (73)
Инженерно-технический	29 / 21 / 11 (61)	32 / 23 / 12 (67)	21 / 12 / 9 (42)
Программно-аппартаный	38 / 24 / 12 (74)	45 / 15 / 22 (79)	31 / 11 / 14 (56)
Криптографический	28 / 16 / 15 (49)	31 / 19 / 11 (61)	18 / 8 / 13 (39)

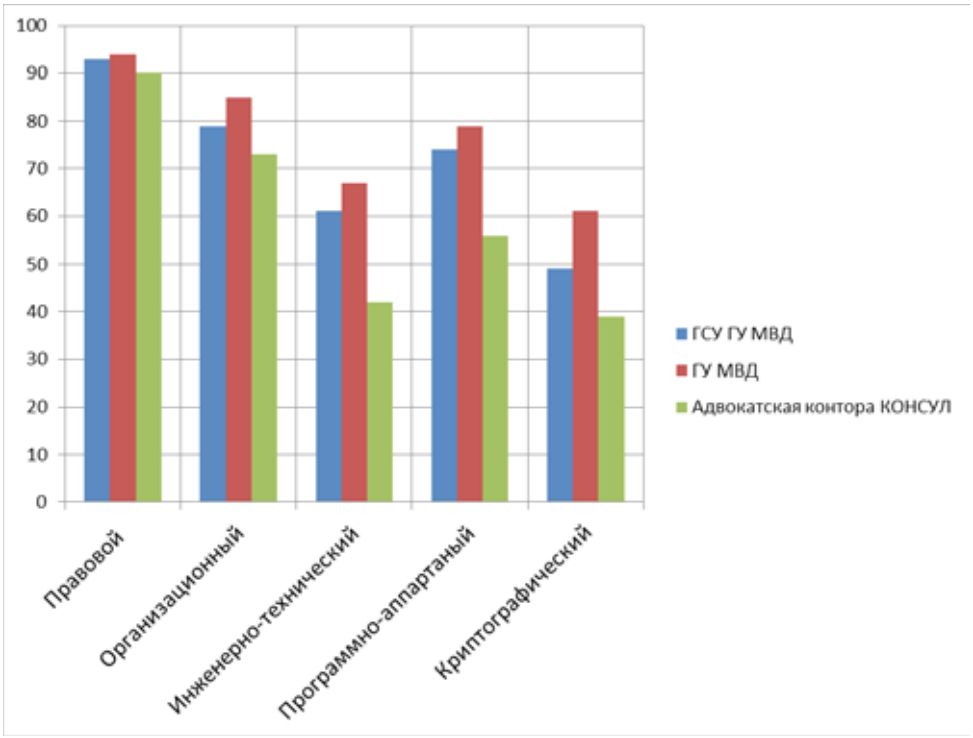

Рис. 3. Диаграмма по результатам работы программного комплекса. Пример тестирования: Адвокатская контора КОНСУЛ в республике Коми, г. Сыктывкар; ГСУ ГУ МВД России по Волгоградской области; ГУ МВД России по Волгоградской области

Вопрос обеспечения информационной безопасности защитника (адвоката) на данный момент остается практически без внимания, несмотря на высокие риски, связанные с профессиональной деятельностью. Указом Президента РФ от 06.03.1997 № 188 к сведениям, составляющим конфиденциальную информацию, доступ к которой ограничен в соответствии с Конституцией РФ и федеральными законами являются: врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров и др.

Защитник (адвокат) обязан сохранять «адвокатскую тайну» [5]; в процессе расследования приходится сталкиваться с государственной тайной, тайной переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, тайной усыновления и т. д.; не разглашать данные предварительного расследования. К сведениям, образующим тайну предварительного расследования, относятся: 1) сведения, относящиеся к работникам правоохранительных органов и иным участникам уголовного процесса; 2) информация о следственных версиях, тактике проведения следственных действий, мерах безопасности, применяемых в отношении участников расследования; 3) сведения о личности, местожительстве и других идентифицирующих признаках участников расследования; 4) сведения о мерах обеспечения безопасности участников расследования; сведения, отражающие стратегию и тактику расследования, в том числе о планировании расследования и следственных версиях; 5) сведения о взаимодействии между следователем и работниками оперативных подразделений; 6) доказательства по уголовному делу, а также результаты анализа доказательственной информации; может знакомиться с материалами уголовных дел и фиксировать их с использованием технических средств, делать копии, и др.

В вопросе о соблюдении адвокатской тайны, режима конфиденциальности следует упомянуть кодекс профессиональной этики адвоката[6], принятый Всероссийским съездом адвокатов 31.01.2003 г., в котором в частности в статье 6 говорится: «...доверия к адвокату не может быть без уверенности в сохранении профессиональной тайны. Профессиональная тайна адвоката обеспечивает иммунитет доверителя, предоставленный последнему Конституцией Российской Федерации. Соблюдение профессиональной тайны является безусловным приоритетом деятельности адвоката. Срок хранения тайны не ограничен во времени. Адвокат не может быть освобожден от обязанности хранить профессиональную тайну никем,

кроме доверителя. Без согласия доверителя адвокат вправе использовать сообщенные ему доверителем сведения в объеме, который адвокат считает разумно необходимым для обоснования своей позиции при рассмотрении гражданского спора между ним и доверителем или для своей защиты по возбужденному против него дисциплинарному производству или уголовному делу. Правила сохранения профессиональной тайны распространяются на: факт обращения к адвокату, включая имена и названия доверителей; все доказательства и документы, собранные адвокатом в ходе подготовки к делу; сведения, полученные адвокатом от доверителей; информацию о доверителе, ставшую известной адвокату в процессе оказания юридической помощи; содержание правовых советов, данных непосредственно доверителю или ему предназначенных; все адвокатское производство по делу; условия соглашения об оказании юридической помощи, включая денежные расчеты между адвокатом и доверителем; любые другие сведения, связанные с оказанием адвокатом юридической помощи. В целях сохранения профессиональной тайны адвокат должен вести делопроизводство отдельно от материалов и документов, принадлежащих доверителю. Материалы, входящие в состав адвокатского производства по делу, а также переписка адвоката с доверителем, должны быть ясным и недвусмысленным образом обозначены как принадлежащие адвокату или исходящие от него. Правила сохранения профессиональной тайны распространяются на помощников и стажеров адвоката, а также иных сотрудников адвокатских образований[7].

Таким образом, адвокат не может оказывать результативную профессиональную помощь клиенту до тех пор, пока между ними не будет достигнуто полное взаимопонимание. В то же время клиент должен чувствовать абсолютную уверенность и возможность действовать исходя из того, что вопросы, обсуждаемые с адвокатом, и предоставленная им адвокату информация будут сохранены как конфиденциальные, без каких-либо на то специальных требований или условий со стороны клиента.

Этическое правило конфиденциальное и должно применяться безотносительно к тому факту, что другие лица могут владеть такой же информацией.

Основным правилом является следующее: адвокат не должен раскрывать имя лица, которому он предоставляет консультацию или которое его приглашает для выполнения поручения до тех пор, пока это не потребуется исходя из сути решаемой проблемы (вопроса).

Адвокат должен сохранять конфиденциальность по отношению к любому клиенту, независимо от того является ли клиент постоянным или обращается за оказанием разовой помощи. Эта обязанность продолжает существовать и после прекращения взаимоотношений по юридическим вопросам и не ограничивается моментом прекращения оказания правовой помощи клиенту, независимо от того какие между клиентом и адвокатом возникли разногласия» [8].

Не имея правовых гарантий в сфере информационной безопасности защитника (адвоката), не проработанности организационно-технических мер по защите сведений, ставших ему известных в рамках своих профессиональных обязанностей возможны ситуации непреднамеренного (неумышленные действия) разглашения информации, что может самым негативным способом сказаться на интересах подзащитного, следствия. Так, например защитник (адвокат) сфотографировав и перебросив на флэш карту материалы уголовного дела, которые ему были предоставлены для ознакомления, может ее потерять или при последующем использовании флэш карта может быть подвергнута вирусной атаке и информация может быть передана третьим лицам, искажена, уничтожена и др. Да, и внешние злоумышленники действуют в отношении адвокатов, с целью получения информации незаконными методами создавая угрозы не только информационной безопасности, но и жизни[9].

Исходя из прав и обязанностей защитника (адвоката) и учитывая широкий круг информационного взаимодействия с иными участниками «Электронного правосудия», продемонстрированный на рис. 4 следует включить данную фигуру в общую политику безопасности и разработать правовую, организационно-техническую базу для ее интеграции в систему обеспечения информационной безопасности «Электронного правосудия».

Список угроз информационной безопасности защитника (адвоката) постоянно растет. Стоит отметить, что после внедрения системы «Электронного правосудия» уровень возможных угроз не снизился, при этом возникли новые угрозы, сопряженные с использованием новых технических средств хранения и обработки данных, каналов передачи данных, несанкционированного доступа к информации и др.

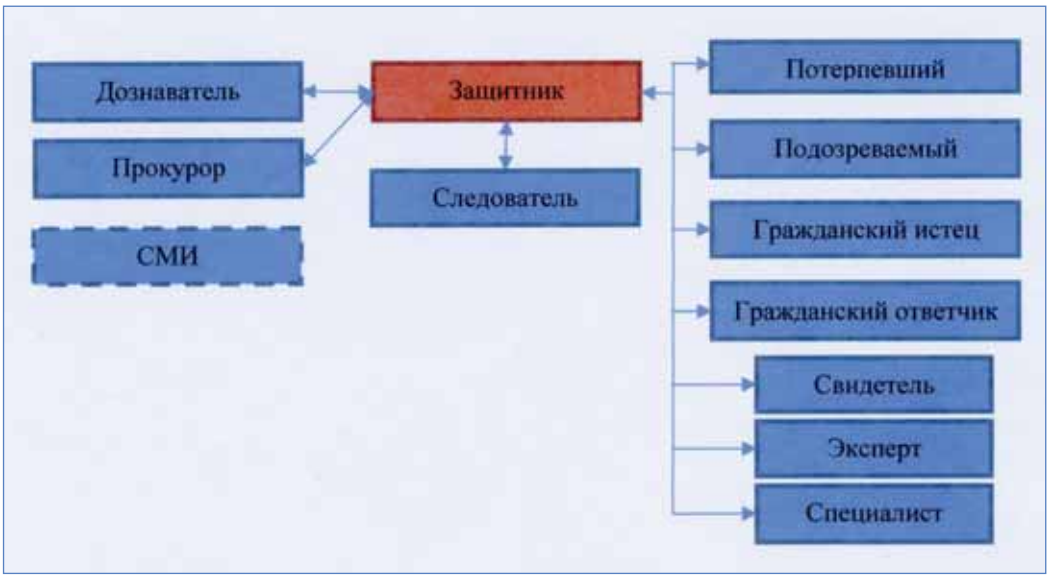

Рис. 4. Неполная схема информационного взаимодействия защитника (адвоката) с другими участниками системы «Электронного правосудия»

Для обеспечения защиты информации, которой оперирует защитник (адвокат) в электронной информационной среде, с учетом выявленных угроз безопасности, следует применять следующие средства:

- межсетевые экраны;
- антивирусная защита;
- системы обнаружения вторжений;
- криптографическая защита;
- зашита от утечек по технических каналам;
- применение электронно – цифровой подписи;
- мониторинг и управление ПБ серверов и АРМ.

Так как, информационное взаимодействие участников «Электронного правосудия», осуществляется посредством использования специализированных ЕИТКС, ГАС, АИС, АИПС и др., то безопасность обмена данными между участниками зависит от их защищенности и правил (регламентации) работы с информацией в соответствии с политикой безопасности.

В результате исследования нами были выделены основные направления и меры по совершенствованию политики безопасности информационного взаимодействия защитника (адвоката) с иными участниками «Электронного правосудия»:

- создание защищенного АРМ защитника (адвоката) и обеспечение, соблюдение режима доступа к ресурсам «Электронного правосудия». Согласно категориям пользователей системы отнести защитника (адвоката) к внутреннему пользователю. Разработать механизм идентификации и аутентификации при работе с системами «Электронного правосудия»;
- разработка инструкций по соблюдению мер информационной безопасности. Обучение защитников (адвокатов);
- ответственность за нарушения установленного порядка пользования ресурсами;
- правовая, организационно-техническая регламентация использования ресурсов «Электронного правосудия» участниками;
- защита речевой информации;
- контроль эффективности обеспечения информационной безопасности участников «Электронного правосудия».

Таким образом, для обеспечения информационной безопасности участников «Электронного правосудия» должны в полной мере выполнятся все регламенты и правила политики безопасности, в свою очередь она должна быть полной, непротиворечивой, подвергаться постоянному обновлению.

Благодаря разработанной системе оценки эффективности соблюдения политики безопасности системы информационного взаимодействия участников «Электронного правосудия», посредством непрерывного мониторинга стало возможным своевременное обнаружение угроз безопасности, принятия адекватных мер защиты, что в значительной мере позволило минимизировать соответствующие риски. На основе проведенных исследований были разработаны методические рекомендации по соблюдению ре-

жима информационной безопасности для судей, прокуроров, следователей, защитников (адвокатов), экспертов, специалистов, оперативных работников и других участников, сотрудников пресс-служб. Разработан и внедрен в правоохранительные органы, адвокатские образования программный комплекс по оценке эффективности мер по обеспечению безопасности отдельных участников «Электронного правосудия».

Таким образом, эффективность работы «Электронного правосудия» зависит, в том числе, и от развития соответствующей законодательной базы, теоретических основ и практических рекомендаций по комплексному обеспечению информационной безопасности участников «Электронного правосудия», и используемых в профессиональной деятельности автоматизированных систем. Внедрение специализированного программного комплекса по оценке полноты и адекватности политики безопасности системы «Электронного правосудия», возможности которого рассмотрены в настоящей статье, несет в себе обучающую функцию, контролирует уровень знания участниками системы мер по обеспечению информационной безопасности и позволяет осуществлять непрерывный мониторинг информационной безопасности системы, обеспечивая стабильность ее работы.

Литература

1. Государственная программа Российской Федерации «Информационное общество» (2011 – 2020 годы), утвержденная Распоряжением Правительства Российской Федерации от 20.10.2010 № 1815-р.; «Об электронной подписи»: Федеральный закон от 06.04.2011 № 63-ФЗ // Российская газета. – 2011. – 8 апреля; «Стратегия национальной безопасности Российской Федерации до 2020 года», утвержденная Указом Президента РФ от 12.05.2009 № 537; Федеральная целевая программа «Развитие судебной системы России»; от 22.12.2008 № 262 – ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»; от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»; «Об утверждении правил делопроизводства в федеральных органах исполнительной власти»: постановление Правительства РФ от 15.06.2009 № 477 // РГ. – 2009. – 24 июня.; «Концепция использования информационных технологий в деятельности федеральных органов государственной власти», одобренная распоряжением Правительства Российской Федерации от 27 сентября 2004 г. № 1244-р.; «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. – 2006. – № 31 (Ч. 1). – Ст. 3448.; «Положение о системе межведомственного электронного документооборота», утвержденное постановлением Правительства Российской Федерации от 22 сентября 2009 г. № 754 и др.
2. Министерство юстиции Российской Федерации: http://www.minjust.ru/. Дата обращения к ресурсу 25.10.2012 г.
3. Федеральное государственное унитарное предприятие «Научно-исследовательский институт «Восход»». Головное предприятие Минкомсвязи России в области разработки и внедрения инфокоммуникационных систем государственного и специального назначения http://www.voskhod.ru/index.php Государственная автоматизированная система «Правосудие» — это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и управлений (отделов) Судебного департамента при Верховном Суде Российской Федерации. Дата обращения к ресурсу 10.11.2012 г.; Министерство внутренних дел Российской Федерации: http://www.mvd.ru/mvd/structure/unit/inspector/publications/show_47503. Реализация проекта «Создание ЕИТКС ОВД» позволит создать единое информационное пространство ОВД, обеспечит требуемый уровень их информационных ресурсов, даст возможность практическим работникам на всех уровнях управления органов внутренних дел незамедлительно получать требуемую информацию. Дата обращение к ресурсу 12.10.2012 г.
4. Булгакова Е.В., Гордеев В.Н. Государственное свидетельство регистрации программ ЭВМ № 2012616760.
5. Общим для всех видов конфиденциальных сведений является тот факт, что свободный доступ к ним ограничен в силу предписаний федерального законодательства, в частности Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации», принятым Государственной Думой РФ 26 апреля 2002 года (с изменениями и дополнениями от 28.10.2003 г. № 134ФЗ, от

20.12.2004 г. № 163ФЗ). Адвокатской тайне посвящена ст. 8 Закона, которая наиболее полно отражает содержание этого понятия.

6. Кодекс профессиональной этики адвоката (принят Всероссийским съездом адвокатов 31.01.2003) (в ред. от 05.04.2007) // Справочная правовая система Консультант плюс.
7. Там же. Ст. 5.
8. Барщевский М.Ю. Адвокатская этика. 19 июня 2008 года, четверг. http://www.pro-zakon.com/node/516. Дата обращения к ресурсу 12.11.2012.г.
9. Убийства адвокатов России, причинение телесных повреждений, к сожалению, не редкость. В центре Москвы преступник на глазах у свидетелей расстрелял адвоката Станислава Юрьевича Маркелова. Вспомним убийства адвокатов М. Я. Евлоева, Е.Б. Замосквичева, С.Р. Жалинова, И.В. Розенберга, К.Б. Деева, Е.В Яцык, И.В. Максимовой, Д.Д. Штейнберга, Д.Ю. Соболева и др. См.: Научные публикации адвокатов коллегии – безопасность адвоката. http://www.trunov.com/content.php?act=showcont&id=3489. Сайт коллегии адвокатов г. Москвы «Трунов, Айвар и пар-

Кубанков Александр Николаевич
доктор военных наук, профессор

Содержание учебной дисциплины «Система обеспечения информационной безопасности России»

Аннотация: *рассмотрена структура и содержание новой учебной дисциплины «Система обеспечения информационной безопасности России». Обосновано включение в нее разделов, посвященных концептуально-правовой и организационной основе обеспечения информационной безопасности России. Приведено содержание тем учебной дисциплины.*

Ключевые слова: *магистратура, информационная безопасность страны, концептуально-правовая основа информационной безопасности, организационная основа информационной безопасности.*

Учебным планом магистерской программы «Правовое обеспечение информационной безопасности» в РПА Минюста России в 3-м семестре предусмотрена учебная дисциплина по выбору магистранта «Система обеспечения информационной безопасности России» объемом 1 зачетная единица (36 академических часов) [1, 2]. Бюджет времени делится на 12 часов аудиторных занятий и 24 часа самостоятельной работы. В качестве промежуточной аттестации предусмотрен зачет.

Изучение магистерских программ [3, 4], связанных с информационным правом и правовой информатикой, показало следующее.Подобной самостоятельной дисциплины в учебных планах нет. Вопросы, связанные с системой обеспечения информационной безопасности России, затрагиваются в различных учебных дисциплинах. Общим является то, что на изучение этих вопросов отводится не более 2 – 4 часов. Таким образом, перед разработчиком данной учебной дисциплины встала задача обоснования ее содержания и методики.

Согласно доктринальным документам [5] системаобеспечения информационной безопасности России есть совокупность концептуально-правовой, организационной, экономической и технологическойсоставляющих. С учетом необходимости формирования стандартных компетенций, специализации, а также содержания других учебных дисциплин разработчик пришел к выводу, что учебная дисциплина «Система обеспечения информационной безопасности России» прежде всего должна отражать вопросы концептуально-правовой и организационной составляющих этой системы. Поэтому предложена следующая структура курса:

вводное занятие;

раздел 1 «Концептуально-правовая основа информационной безопасности России»;

раздел 2 «Организационная основа информационной безопасности России»;

зачёт.

На вводном занятии до магистрантов доводятся требования государственного образовательного стандарта высшего профессионального образования к подготовке магистров по направлению «Юриспруденция», касающиеся учебной дисциплины «Система обеспечения информационной безопасности России». Кроме того доводятся:

структура, особенности изучаемой дисциплины и ее актуальность в современном мире; цели учебной дисциплины; формы контроля успеваемости студентов по учебной дисциплине; порядок работы студента на лекциях, семинарах; организация самостоятельной работы; порядок подготовки и защиты рефератов.

1 раздел состоит из двух тем:

тема 1 «Доктрина информационной безопасности России»;

тема 2«Правовое обеспечение информационной безопасности России».

По теме 1 изучаются понятие информационной безопасности страны; интересы личности, общества и государства в информационной сфере; угрозы информационной безопасности страны и их источники; задачи и методы обеспечения информационной безопасности страны.

Тема 2 охватывает следующие вопросы: правовые регулирование, обеспечение и защита интересов личности и общества в информационной сфере; правовое регулирование в области информационного обеспечения государственной политики; правовое обеспечение индустрии информации и современных информационных технологий в стране; правовое обеспечение безопасности инфокоммуникаций; международно-правовое регулирование в области информационной безопасности.

2 раздел состоит из трёх тем:

тема 3 «Состав системы обеспечения информационной безопасности России и функции её элементов»;

тема 4 «Функции руководителя государства по управлению информационной безопасностью России. Совещательные и консультативные органы»;

тема 5 «Полномочияорганов исполнительной власти по обеспечению информационной безопасности России».

По теме 3 изучаются: принцип разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в системе обеспечения информационной безопасности государства; элементы системы обеспечения информационной безопасности России: Президент, Федеральное собрание, Правительство, Совет безопасности, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом и Правительством, органы исполнительной власти субъектов федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством участие в решении задач обеспечения информационной безопасности России.

Тема 4 охватывает следующие вопросы: конституционные полномочия Президента России; определение приоритетных направлений государственной политики в области обеспечения информационной безопасности России; формирование, реорганизация, упразднение подчиненных президенту органов и сил по обеспечению информационной безопасности России и руководство ими; санкционирование действий по обеспечению информационной безопасности России; работа Совета безопасности по выявлению и оценке угроз информационной безопасности, подготовке проектов решений Президента для предотвращения таких угроз, разработке предложений в области обеспечения информационной безопасности, координации деятельности органов и сил по обеспечению информационной безопасности, контролю реализации решений Президента; функции межведомственных и государственных комиссий.

Тема 5 включает изучение полномочий МВД, МИД, Минобороны, Минкомсвязи, Минюста, ФСБ, ФСО в вопросах обеспечения информационной безопасности России.

По мнению автора предложенное содержание новой учебной дисциплины «Система обеспечения информационной безопасности России» соответствует его наименованию и гармонично сочетается с содержанием других дисциплин, предусмотренных учебным планом.

Литература

1. Официальный сайт РПА Минюста России: http://rpa-mu.ru/magistratura/magisterskie-programmyi/infobezopas
2. Морозов А.В. Структура и содержание магистерской программы «Правовое обеспечение информационной безопасности»// Правовая информатика. – 2012, № 2. – С. 41,...,46.
3. Официальный сайт НИУ «ВШЭ»: http://pravo.hse.ru/legal_info/concept
4. Официальный сайт НИЯУ «МИФИ»: http://www.mephi.ru/obrdeyat/graduate/#mag
5. Доктрина информационной безопасности Российской Федерации. – 2000.

Рустикова Галина Сергеевна
Орлов Владимир Игоревич

Предоставление бесплатной юридической помощи на основе портала Юстиция

Аннотация: *Рассматривается возможность использования ресурсов портала «Юстиция» для оказания бесплатной юридической помощи и правового просвещения населения.*

Ключевые слова: *бесплатная юридическая помощь, правовое просвещение населения, информационное общество.*

На заседании коллегии Минюста России по теме «О состоянии системы оказания бесплатной юридической помощи в Российской Федерации», состоявшегося в Минюсте России 23 ноября 2012 г., Министр юстиции Российской Федерации А.В. Коновалов, в своем выступлении отметил, что наличие доступа населения к квалифицированной юридической помощи не менее важно, чем к качественным медицинским услугам. Это очевидно.

Немало людей нуждается в квалифицированной юридической помощи, но в силу тех или иных обстоятельств, например, недостаток времени или денежных средств, они не могут обратиться за платной помощью. В этом случае, большинство либо обращаются за советами к друзьям, либо покупают юридическую литературу, либо ищут ответы на интересующие их вопросы на просторах Интернета, что влечет за собой потерю огромного количества времени и сил, и, зачастую, уводит от правильного решения проблемы. Задавая вопросы на различных форумах или знакомым и друзьям вряд ли можно получить помощь именно компетентного в этих вопросах специалиста. К тому же, по данным последних социологических опросов, 60 процентов населения остро нуждаются не только в информации о принимаемых в стране законах и их разъяснении, но и в элементарной справочной информации: о местонахождении судебных, законодательных и исполнительных органов, порядке обращения в них, получения консультаций [1].

В соответствии с пунктом 4 статьи 28 федерального закона от 21.11.2011 № 324-ФЗ «О бесплатной юридической помощи в Российской Федерации», правовое информирование и правовое просвещение населения может осуществляться юридическими клиниками образовательных учреждений высшего профессионального образования и негосударственными центрами бесплатной юридической помощи[2].

В настоящий момент Центр правовой помощи ФГБОУ ВПО «Российская правовая академия Министерства Юстиции Российской Федерации» (далее Академия) оказывает бесплат-

ную юридическую помощь населению по вопросам различных отраслей права. Прием граждан осуществляется преподавателями и студентами старших курсов Академии. Участие студентов Академии позволяет проводить их обучение практическим навыкам под руководством опытных юристов, прививает стажерам такие важнейшие для юриста качества, как стремление служить обществу и защищать права человека.

Объединив возможности портала «Юстиция» и опыт ведущих ученых, совмещающих свою научную деятельность с педагогической, можно осуществлять комплексную работу по повышению уровня правовой культуры граждан, включая уровень осведомленности и юридической грамотности[3], для формирования правосознания граждан.

На наш взгляд, для наиболее оптимального и быстрого решения этой проблемы, следует интегрировать несколько источников получения необходимой информации: образовательные ресурсы, размещенные на портале «Юстиция» (в том числе видеолекции); видеоуроки по использованию справочных правовых систем; ссылки на соответствующие Интернет-ресурсы (базы данных справочных правовых систем (БД СПС)); а так же информацию о работе Центра правовой помощи (ЦПП), с возможностью задавать вопросы непосредственно на форуме портала или общаясь с преподавателями Академии по телефону, указанному на сайте или через видеоконференцию.

В настоящий момент часть из перечисленных выше возможностей уже внедрена. Остальное будет реализовано на портале «Юстиция» в самое ближайшее время.

При создании портала «Юстиция» использовались современные технологии создания медиа-ресурсов в сети Интернет с использованием, так называемых, технологий Web 2.0, что позволило создать многофункциональный интернет-портал «Юстиция» с возможностью общения в режиме видеоконференции.

Комплекс является мультиплатформенным, что позволяет вести работу не только с персонального компьютера, но и используя современные технические устройства с доступом к информационно-телекоммуникационной сети «Интернет» такие как смартфоны (сотовые телефоны), планшетные компьютеры и пр.

Портал «Юстиция» интегрирован с наиболее популярными социальными сетями Twitter и Facebook, что позволяет объединить пользователям свои аккаунты из разных социальных сетей в единую систему с комплексом дистанционного образования для повышения эффективности процесса обучения путем увеличения функциональных возможностей и полной автоматизации рассылки материалов обучаемым с помощью личных сообщений в этих сетях.

Главная страница портала «Юстиция» состоит из четырех разделов: «Мониторинг правоприменения», «Правовое просвещение», «Наука» и «Образование», которые в свою очередь разделены на подразделы.

Мониторинг правоприменения	**Правовое просвещение**	**Наука**	**Образование**
Законодательство	Бесплатная юридическая помощь	Ведущие ученые	Бакалавры и специалисты
Правовой анализ	Вопросы граждан	Конференции и публикации	Магистры
Законопроектная инициатива	Патриотическое воспитание	Диссертации	Повышение квалификации

Раздел «Мониторинг правоприменения» предназначен для того, чтобы помочь пользователям портала оценить положения действующего законодательства, ознакомиться с официальными и неофициальными толкованиями права, быть в курсе законопроектной деятельности государственных органов и общественного обсуждения нормативно-правовых актов, а так же выявить проблемы отечественного законодательства.

Подраздел «Законодательство» позволяет получать доступ к Интернет-версиям информационно-правовых справочных систем Эталон Плюс, Кодекс, Консультант Плюс и Гарант.

Подраздел «Правовой анализ» посвящен проблемам применения наиболее актуальных

нормативно-правовых актов, изучению судебной практики и вопросам совершенствования законодательства. Для более качественного анализа в подавляющем большинстве случаев предоставляется возможность непосредственно с сайта обращаться к контексту документа, и прослеживать его взаимосвязи с другими источниками права и иными явлениями социальной действительности.

Подраздел «Законопроектная инициатива» знакомит пользователя портала «Юстиция» с деятельностью палат Федерального Собрания РФ по принятию законов, а так же с работой исполнительных органов государственной власти в сфере законотворческой инициативы. Из этого подраздела можно получить доступ к ресурсам, на которых проходит общественное обсуждение нормативно-правовых актов, и к тематическим интернет-форумам, посвященным нормотворческому процессу в нашей стране. В данном разделе можно ознакомиться с деятельностью Минюста России по выдаче заключений о соответствии законопроектов Конституции Российской Федерации, федеральному законодательству, правилам юридической техники.

Раздел «Правовое просвещение» портала «Юстиция» в первую очередь ориентирован на широкий круг пользователей с целью передачи им необходимых юридических знаний, укрепления правосознания и преодоления правового нигилизма, формирования специальных навыков и способностей отстоять свои законные интересы. Материалы этого раздела подготавливаются профессиональными юристами в содружестве с общественными организациями и другими специалистами – педагогами, психологами, сотрудниками библиотек, журналистами, госслужащими.

Ответы на вопросы по различным отраслям права, задаваемые в первую очередь обычными гражданами, консультации, услуги по составлению исков и заявлений, а также полезные юридические советы предоставляются в подразделе «Бесплатная юридическая помощь». Информация представлена как в документальном, так и в видео формате. Все данные систематизированы для удобства пользования в соответствии с выработанным классификатором, что облегчает работу с архивами и позволяет получить полный и исчерпывающий ответ на интересующий вопрос. Данный подраздел может быть полезен так же практикующим юристам, и тем, кто только изучает юриспруденцию, т.к. в нем собраны видеоматериалы, отражающие взгляды ветеранов юстиции, ведущих ученых, наиболее опытных лекторов и практикующих юристов на современные социально-экономические и правовые проблемы. В этом подразделе в дальнейшем планируется проводить онлайн консультации граждан совместно с Центром правовой помощи ФГБОУ ВПО «Российская правовая академия Министерства Юстиции Российской Федерации»[4].

Подраздел «Вопросы пользователей» представляет собой сборник ответов на типовые вопросы пользователей портала, касающиеся функционирования Интернет-ресурса. Все ответы поддерживаются в актуальном состоянии. Так же существует форма, предназначенная для ответов на индивидуальные вопросы пользователей, если на данные вопросы нет ответов среди типовых. Кроме того, задавать вопросы можно по электронной почте, отправляя письмо с адреса, на который зарегистрирован аккаунт пользователя, или через социальные сети.

В подразделе «Патриотическое воспитание» собраны и постоянно пополняются видеоматериалы, посвященные ветеранам юстиции.

Доступ к дистанционному образовательному комплексу осуществляется через раздел «Образование» портала «Юстиция». Подразделы «Бакалавры и специалисты», «Магистратура» и «Повышение квалификации» предназначены для студентов и слушателей, обучающихся дистанционно, и содержат электронные учебно-методические комплексы, которые предоставляют в их распоряжение обширные информационно-справочные материалы по профилю подготовки, а также возможность эффективной оценки уровня освоения пройденного материала.

Доступные темы в курсе открываются путём однократного нажатия на активную ссылку. После этого пользователь будете перемещен на страницу, где отобразится электронный учебно-методический комплекс по дисциплине, состоящий из электронных учебно-методических материалов, электронного учебного пособия, комплекта видеолекций по курсу и электронной системы тестирования.

Учебные материалы содержат гиперссылки на нормативно-правовую базу. Пользователю системы предоставляется возможность ознакомиться с «Глоссарием» и получить дополнительную «Справочную информацию» при нажатии на соответствующую ссылку.

Для удобства пользования предоставляется возможность открыть «Справочное руководство», в котором содержится описание комплекса дистанционного обучения и представ-

лена информация об общих правилах работы с данным интерактивным продуктом.

Результаты тестирования показывают качество освоения соответствующего курса.

Особое место в ходе дистанционного обучения уделяется видеолекциям, однако использование этого ресурса требует наличия у пользователя доступа в информационно телекоммуникационную сеть Интернет, скорости которого должно хватать на воспроизведение материала. При отсутствии такового, пользователю дистанционного образовательного комплекса предоставляется доступ к материалам в текстовом виде.

В системе дистанционного обучения предусмотрен отдельный модуль для общения с преподавателем дистанционных курсов, для этого потребуется перейти на вкладку «Общение». В этом же разделе обучаемые имеют возможность обмениваться сообщениями между собой посредством «Форума» или же в личных «Блогах». Общение с преподавателем возможно так же путем обращения к специальным формам в ходе ознакомления с учебно-методическими и лекционными материалами или из подраздела «Наука».

Применение в учебном процессе видеоматериалов позволяет сочетать мультимедийные возможности современных информационных систем и традиционные педагогические технологии, что разрешает многие проблемы развивающего, личностно-ориентированного обучения, дифференциации, гуманизации, формирования индивидуальной образовательной перспективы учащихся.

Включение в видеоматериалы необходимого количества практических примеров в виде аудио и видеозаписей, использование цветных фотографий высокого разрешения, анимации, интерактивных курсов и т.д., позволяют в динамичной форме вооружить слушателей знаниями, ранее не доступными для восприятия на аудиторных занятиях, а также значительно сокращают материальные затраты на организацию обучения. Проведение занятий с использованием видеоматериалов – один из путей повышения эффективности образовательного процесса на основе реализации принципов дистанционных образовательных технологий в обучении.

Раздел «Наука» главной страницы портала «Юстиция» состоит из трех подразделов. В первом из них, который назван «Ведущие ученые», размещены персональные сведения об ученых и специалистах, деятельность которых связана с изучаемыми курсами. Данный подраздел имеет перекрестные связи с другими ресурсами портала позволяющий быстро просмотреть учебные материалы, подготовленные конкретным лицом и размещенные на портале, а так же ознакомиться с текстами его исследований и научных статей, а при наличии возможности – отправить личное сообщение по электронной прочте или через ресурсы социальных сетей.

Подразделы «Конференции и публикации» и «Диссертации» позволяют пользователям портала получить полнотекстовый доступ к диссертациям, авторефератам, материалам круглых столов и конференций по изучаемым проблемам, что позволяет их использовать для цитирования в научных, исследовательских, полемических, критических и информационных целях.

Создание интернет-портала «Юстиция» является своевременным и актуальным, т.к. существует острая необходимость вести комплексную работу по повышению уровня правовой культуры граждан, включая уровень осведомленности и юридической грамотности, для формирования правосознания граждан. Работа по правовому просвещению населения позволит нашей стране не только поднять уровень правосознания граждан, но и решить актуальные вопросы подъёма экономики и гармонизации общественных отношений.

Литература

1. Центр правового просвещения как форма повышения правовой культуры граждан [Электронный ресурс] : Информационные материалы просветительских организаций/ портал «Просветительство». – Режим доступа к порталу: http://www.prosvetitelstvo.ru/library/articles/?SHOWALL_1=1.
2. Российская газета, 2011, 21 ноября.
3. Российская газета, 2011, 14 июля. Основы государственной политики Российской Федерации в сфере развития правовой грамотности и правосознания граждан.
4. http://rpa-mu.ru/cpp.

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

Остроушко Александр Владимирович
кандидат юридических наук, доцент

К вопросу о правовом регулировании оборота электронной подписи

Аннотация: *в статье рассмотрены проблемы построения системы межведомственного электронного документооборота в нашей стране, выявлен ряд проблем препятствующих эффективному электронному взаимодействию между государственными органами. Обоснована необходимость принятия законодательных мер для защиты от неправомерного использования электронной подписи.*

Ключевые слова: *информационное общество, электронная подпись, электронное правительство, электронный документооборот, эффективность исполнения государственной программы.*

Общемировая тенденция внедрение информационных технологий в деятельность государственных органов приводит к тому, электронные документы начинают постепенно вытеснять документы на традиционных носителях. В Российской Федерации, вслед за ведущими странами, выработана своя стратегия внедрения электронного документооборота в работу государственных органов. Основным показателем хода реализации и оценки эффективности выполнения государственной программы является доля электронного документооборота между органами государственной власти в общем объеме межведомственного документооборота.

В 2002 г. Постановлением Правительства Российской Федерации от 28 января 2002 г. N 65 была утверждена Федеральная целевая программа «Электронная Россия (2002 – 2010 годы)», в течение 2005 – 2010 гг. в соответствии с третьим этапом реализации Программы предполагалось довести долю электронного документооборота в общем объеме документооборота до 65% внутри ведомств и до 40% в межведомственном документообороте.Эти высокие показатели не были выполнены и по состоянию на конец 2010 года эффективность исполнения программы оценивалась как низкая: в полной мере электронный документооборот между государственными органами, а также электронные коммуникации между государственными органами и гражданами так и не функционировали. Эффективность государственного управления в России за счет внедрения безбумажного документооборота за эти годы практически не изменилась, поэтому финансирование программы было продолжено и на основании Приказа Минэкономразвития РФ от 21.12.2010 N 664 «Об утверждении формы соглашения между Министерством экономического развития Российской Федерации и высшим исполнительным органом государственной власти субъекта Российской Федерации о предоставлении субсидии из федерального бюджета бюджетам субъектов Российской Федерации в рамках реализации Федеральной целевой программы «Электронная Россия (2002 –2010 годы)»[6].

Действующая на текущий момент Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)» содержит несколько иные показатели (индикаторы) выполнения государственной программы, так в 2010 году доля электронного документооборота между органами государственной власти в общем объеме межведомственного документооборота должна была составить всего 10 процентов, в 2011 году – 15 процентов и в 2014 году возрасти до 70 процентов. Годовой отчет о ходе реализации и оценке эффективности государственной программы Российской Федерации «Информационное общество (2011 – 2020 годы)» за 2011 год не содержит данных о доле электронного документооборота между органами государственной власти в об-

щем объеме документооборота[7], хотя данный индикатор является одним из отчетных.

Сказанное выше позволяет сделать вывод, что внедрение электронного документооборота в нашей стране затормаживается рядом системных проблем. Одной из них является наличие определенных трудностей при внедрении электронной подписи.

Разрабатывая отечественное законодательство об электронной подписи, требуется учитывать ряд международных актов: Директива Европейского союза «Об общих условиях использования электронных подписей» (Directiveon a CommunityFrameworkforelectronicsignatures.OfficicalJournal L013, 19.01.2000, p. 0012-0020), Модельный закон «Об электронной цифровой подписи», принятый Межпарламентской Ассамблеей стран – участниц СНГ, Модельный закон Комиссии ООН по международному торговому праву ЮНСИТРАЛ (UNCITRAL – UnitedNationsCommissiononInternationalTradeLaw) «Об электронной торговле», разработанный в 1996 г. и рекомендованный ООН в качестве базового документа для национальных законодательств, принятые ООН в 1997 г. разработанные ЮНСИТРАЛ Единообразные правила по электронной подписи [14, с. 224-255] и ряд других.

К настоящему времени утвержден ряд нормативных документов: во-первых, Стратегия развития информационного общества в Российской Федерации, утвержденная поручением Президента Российской Федерации от 7 февраля 2008 г. N Пр-212 [8]. Во-вторых, Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденная распоряжением Правительства Российской Федерации от 17 ноября 2008 г. N 1662-р [3]. В-третьих, План мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности, утвержденный распоряжением Правительства Российской Федерации от 12 февраля 2011 г. № 176-р [4].

На решение задач правового регламентирования электронного документооборота, в частности, направлен Федеральный закон Российской Федерации № 63-ФЗ «Об электронной подписи», принятый 6 апреля 2011 г. [2], который вступил в силу 8 апреля 2011 г. При этом согласно ч. 2 ст. 20 нового закона Федеральный закон от 10 января 2002 года N 1-ФЗ «Об электронной цифровой подписи» утратит силу только с 1 июля 2013 года из-за задержек утверждения Минкомсвязью порядка прохождения удостоверяющими центрами аккредитации по правилам Федерального закона Российской Федерации № 63-ФЗ «Об электронной подписи».

Согласно п.1 ст. 2 ФЗ «Об электронной подписи» электронная подпись – это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[2]. На практике электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной таковой у документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью, либо удостоверенного уполномоченным органом или лицом (нотариусом). Электронную подпись получает лицо, а удостоверяет подпись один из удостоверяющих центров, и человек может действовать как от своего имени, так и от имени организации в рамках полномочий.

Например, если гражданин, как должностное лицо организации, имеет право на подпись документов без доверенности, это можно делать и с использованием электронной подписи [11].

Услуги, оказываемые с помощью электронной подписи достаточно распространены, например, в интернете есть спецоператоры связи, которые, по сути,оказывают удостоверяющие (нотариальные) услуги. С помощью электронной подписи можно заказать выписку из единого государственного реестра юридических лиц и совершить ряд иных юридически значимых действий.

Считаем, что новый Закон по правовым характеристикам приравнивает бумажный документ к электронному, например, согласно ч. 3 ст. 11 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» электронный документ, электронное сообщение, подписанные электронной цифровой подписью или иным аналогом собственноручной подписи, признаются равнозначными документу, подписанному собственноручной подписью.

При этом по ч. 4 статьи – в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронны-

ми сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами [1].

Таким образом, можно прогнозировать за электронной подписью – будущее, однако, на наш взгляд, уже сейчас законодателю необходимо обратить внимание на усиление правовой охраны ее оборота. Так, специалисты по информационным технологиям, в частности – Е.Н. Филенко, отмечают, что внедрение электронной подписи идет медленнее, чем ожидалось, так как существует ряд сдерживающих факторов:

- несмотря на широкое внедрение информационных технологий, не предполагается переводить в электронный вид наиболее важные документы – документы на недвижимость, свидетельства о рождении и т.п.;
- невостребованность технологии ЭП для документов электронной почты, так как применение этой технологии может привлечь нежелательное внимание со стороны хакеров, госслужб, борющихся с терроризмом, и т.п.;
- проблемы, связанные с использованием ЭП, такие, как подделка ЭП, незаконное получение и использование сертификатов ЭП, передача ЭП другому лицу в нарушение установленных правил;
- отсутствие необходимости применения ЭП в закрытых информационных системах, в которых высокий уровень защиты и контроля и так обеспечивается;
- отсутствие необходимой инфраструктуры в виде удостоверяющих центров и центров сертификации[12, с.156].

Филенко Е.Н. прав, что электронная подпись, как и любое другое средство автоматизации делопроизводственных процессов, способно принести немалую пользу при правильном использовании, но в каждом конкретном случае необходимо анализировать выгоды от использования электронной подписи и риски, связанные с ее применением[13].

В этой связи следует учитывать, что давно существует и широко используется криптоанализ –анализ возможностей подделки электронной подписи. Попытку сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».

Гольдвассер, Микали и Ривест описывают следующие модели атак, которые актуальны и в настоящее время: атака с использованием открытого ключа (криптоаналитик обладает только открытым ключом); атака на основе известных сообщений, а противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им; адаптивная атака на основе выбранных сообщений (криптоаналитик может получить подписи электронных документов, которые он выбирает сам).

В научной литературе описывается классификация возможных результатов атак: полный взлом цифровой подписи; получение закрытого ключа, что означает полный взлом алгоритма; универсальная подделка цифровой подписи; нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа; выборочная подделка цифровой подписи; возможность подделывать подписи для документов, выбранных криптоаналитиком; экзистенциальная подделка цифровой подписи; возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком.

При этом некоторые авторы говорят о возможности социальных атак, направленных не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами, где злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа, либо может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи, либо подменить открытый ключ владельца на свой собственный, выдавая себя за него[10, с. 178].

В целом за два последних десятилетия резко возросло число открытых работ по криптоанализу, который становится одной из наиболее активно развивающихся областей информационных исследований. Появился целый арсенал математических методов, представляющих интерес для криптоаналитика. Кроме того, повышение производительности вычислительной техники сделало возможными такие типы атак, которые раньше были неосуществимы.

Ряд специалистов считает, что подделать электронную подпись невозможно – это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, со-

храняет актуальность[9]. Однако лавинообразный рост производительности вычислительных средств ставит этот вывод под сомнение, дополнительная защита от подделки может, на наш взгляд, обеспечиваться сертификацией удостоверяющим центром открытого ключа подписи.

Однако оборот и контроль за обращением цифровой подписи будут осуществлять физические лица, которые должны делать это, несомненно, добросовестно. К сожалению, практика показывает, что это не всегда так, уполномоченные лица нередко совершают противоправные деяния. Поэтому с целью сохранения конфиденциальности владельцев электронной подписи, защиты от ее неправомерного использования требуется принять соответствующие законодательные меры, возможно, сформулировать новую норму в уголовный кодекс. Проблема в том, что УК РФ на сегодняшний день не говорит об электронной подписи как о предмете преступления, хотя последствия ее незаконного оборота обладают серьезной общественной опасностью.

Литература

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.
2. Об электронной подписи : Федеральный закон Российской Федерации от № 63-ФЗ // Российская газета. 2011. 8 апр.
3. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года : Распоряжение Правительства Российской Федерации от 17 ноября 2008 г. N 1662-р СЗ РФ. 2008. № 47. Ст. 5489.
4. План мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности : Распоряжение Правительства Российской Федерации от 12 февраля 2011 г. № 176-р // СЗ РФ. 2011. № 8. Ст. 1151.
5. Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)» // Российская газета. 2010. 16 нояб.
6. Федеральная целеваяпрограмма «Электронная Россия (2002 – 2010 годы) // Документ опубликован не был: Доступ из системы КонсультанатПлюс.
7. Годовой отчет о ходе реализации и оценке эффективности государственной программы Российской Федерации «Информационное общество (2011 – 2020 годы)» URL : http://minsvyaz.ru/ru/doc/?id_4=764 [по состоянию на 20.01.2013 г.].
8. Стратегия развития информационного общества в Российской Федерации, утвержденная поручением Президента Российской Федерации от 7 февраля 2008 г. N Пр-212 // Российская газета. 2008.16 фев.
9. Авдошин С., Савельева А. Криптоанализ: вчера, сегодня, завтра // URL: http://www.osp.ru/os/2009/03/8120956/.
10. Венбо Мао. Современная криптография. / под редакцией Клюшиной Д.А. М. : Издательский дом Вильямс, 2005. С. 768.
11. Диденко П. Электронная цифровая подпись – 2015 // URL: http://lenta.ru/articles/2010/08/02/digising.
12. Загнетко А. Несколько соображений о судьбе ЭЦП в России // Connect. 2005. № 5. С. 156.
13. Филенко Е.Н. Проблемы использования электронной цифровой подписи // Трудовое право. 2007. № 11.
14. Draft Uniform Rules on Electronic Signatures A/CN.9/WG.IV/WP.84. Official Records of the General Assembly, Fifty-fifth Session, Supplement N 17 (A/55/17), paras. 224-255.

References

1. On Information, Information Technologies and Protection of Information: The Federal Law of 27.07.2006 № 149-FZ / / NW. 2006. № 31 (1 pm). Art. 3448.
2. Electronic Signature: The Federal Law of the Russian Federation № 63-FZ / / RossiyskayaGazeta. 2011. April 8.
3. The concept of long-term socio-economic development of the Russian Federation for the period up to 2020: Government of the Russian Federation on November 17, 2008 N 1662-P NW. 2008. № 47. Art. 5489.
4. The action plan for the transition of federal bodies of executive power in the paperless with the internal organization: Government of the Russian Federation of February 12, 2011 № 176-p / / NW. 2011. Number 8. Art. 1151.
5. The State Program of the Russian Federation, «The Information Society (2011 – 2020 years)» // RossiyskayaGazeta. 2010. 16 Nov..

6. Federal Target Program «Electronic Russia (2002 – 2010 years) // The document has not been published: Access the system KonsultanatPlyus.
7. Annual report on the implementation and evaluation of the national program of the Russian Federation, «The Information Society (2011 – 2020 years)» URL: http://minsvyaz.ru/ru/doc/?id_4=764 [as of 20.01.2013 was] .
8. The strategy of development of the information society in the Russian Federation, approved by order of the President of the Russian Federation dated February 7, 2008 Avenue N-212 // RossiyskayaGazeta. February 2008.16.
9. Avdoshin S., A. Savelyev Cryptanalysis: Yesterday, Today, Tomorrow // URL: http://www.osp.ru/os/2009/03/8120956/.
10. Venbo Mao. Modern cryptography. / Edited by DA Klyushin M. Williams Publishing House, 2005. S. 768.
11. Didenko P. Digital signature – 2015 / / URL: http://lenta.ru/articles/2010/08/02/digising.
12. Zagnetko A few thoughts on the fate of EDS in Russia / / Connect. 2005. Number 5. S. 156.
13. Filenko EN Problems of using digital signature // Employment Law. 2007. Number 11.
14. Draft Uniform Rules on Electronic Signatures A/CN.9/WG.IV/WP.84. Official Records of the General Assembly, Fifty-fifth Session, Supplement N 17 (A/55/17), paras. 224-255.

Махноносов Эдуард Викторович

Линьков Григорий Сергеевич

Формирование единого информационного пространства нотариата в Российской Федерации

Аннотация: *в статье рассматриваются вопросы формирования единого информационного пространства, обеспечивающего повышение эффективности всех видов нотариальной деятельности в Российской Федерации за счет применения современных информационно-телекоммуникационных технологий.*

Ключевые слова: *информационное общество, информационное пространство, нотариальный документооборот, электронный нотариальный архив.*

На современном этапе развития информационного общества в Российской Федерации использование информационно-коммуникационных технологий в нотариальной деятельности является необходимым условием обеспечения соответствия нотариальной защиты конституционных прав граждан и юридических лиц потребностям государства и общества.

Учитывая происходящие сегодня в мире процессы глобализации, вступление России в ВТО, изменение социально-экономических условий в государстве, развитие правовых институтов не вызывает сомнения, что совершенствование и правовое регулирование нотариальной деятельности нуждается в глубоком научном переосмыслении, выработки новых подходов с учетом современных реалий нашей жизни и особенно развития информационного общества в России.

Принципы формирования единого информационного пространства в Российской Федерации предопределяют, что правоотношения в сфере нотариального документооборота, электронного нотариального архива, порядка совершения нотариальных действий (при совершении которых предъявляются электронные документы) должны быть урегулированы на федеральном уровне, а не на уровне субъектов Федерации и это связано как с обеспечением государственных гарантий конституционных прав человека и гражданина в информационной сфере, так и экономической составляющей.

В условиях развития электронного взаимодействия, формирования электронного правительства, новых подходов к обеспечению юридической значимости электронных документов, что исключительно важно для реформирования нотариата, особого внимания заслуживает вопрос о том, как должны соотносится правовые нормы с техническими принципами обеспечения электронного взаимодействия не только внутри нотариального сообщества, но и с внешними информационными системами, прежде всего информационными системами органов государственной власти Российской Федерации и судами.

Основной целью формирования единого информационного пространства небюджетного

нотариата в Российской Федерации является создание современной формы организации деятельности нотариусов и нотариальных палат, обеспечивающей повышение эффективности всех видов этой деятельности за счет применения современных информационно-телекоммуникационных технологий.

При этом данная цель неразрывно связана с общими целями института нотариата, такими как:

- улучшение качества нотариального обслуживания населения;
- увеличение количества совершаемых нотариальных действий;
- повышение эффективности работы нотариусов и нотариальных палат;
- обеспечение единства нотариальной практики;
- повышение уровня защиты прав и законных интересов граждан и организаций при обращении к нотариусам за совершением нотариальных действий и использовании нотариально удостоверенных документов;
- обеспечение дополнительной защиты профессиональной деятельности и прав нотариусов при совершении ими нотариальных действий и выполнении ими других обязанностей, возложенных на них законом.

Безусловно, использование современных информационно-телекоммуникационных технологий дает принципиально новые и недоступные ранее возможности, позволяющие поднять нотариат на более высокую ступень развития и обеспечить ему достойное место среди других правовых институтов государства.

16 мая 2009 года Собранием представителей нотариальных палат субъектов Российской Федерации была утверждена Концепция информатизации небюджетного нотариата Российской Федерации. [3]Тем самым была создана концептуальная правовая основа обеспечения системного подхода к решению задач в сфере информатизации нотариальной деятельности.

С учетом выработанного системного подхода и принципов обеспечения совместимости и преемственности технических и программных решений для информатизации внебюджетного нотариата наиболее приоритетными сегодня являются следующие задачи:

- создание и развитие собственной информационной инфраструктуры (корпоративной сети), обеспечивающей внедрение и использование информационных технологий;
- создание информационных ресурсов и систем, обеспечивающих актуальность и достоверность обработки информации (сбор, хранение, передача и использование);
- обеспечение информационной безопасности на основе применения комплекса специальных мер и средств (криптографических, программно-технических, организационных и других);
- формирование нормативно-правовой базы и принятие комплекса организационных мероприятий, обеспечивающих обязательное использование создаваемых информационных ресурсов нотариусами;
- создание единого электронного реестра завещаний и наследственных дел;
- повышение квалификации нотариусов и сотрудников нотариальных палат, как пользователей создаваемых информационных систем;
- эффективное формирование и использование создаваемых информационных ресурсов;
- использование информационных технологий для повышения информированности населения о возможностях, предоставляемых институтом нотариата и преимуществах использования нотариальной формы документов;
- организация online-сервисов, повышающих удобство граждан при их обращении к нотариусам (справочники, ответы на вопросы, запись на прием и подача документов в электронном виде и т.д.);
- формирование нормативно-правовой базы, обеспечивающей внедрение внутреннего электронного документооборота внебюджетного нотариата и постепенная замена им традиционного бумажного документооборота;
- использование сертифицированной электронно-цифровой подписи для обеспечения юридической значимости электронных документов;
- интеграция внутренних информационных ресурсов с информационными системами федеральных органов государственной власти и постепенный переход на взаимодействие с ними в электронной форме;
- реализация принципа «единого окна» при обращении граждан за счет организации юридически значимого информационного обмена с другими органами и организациями;
- создание единого электронного реестра нотариальных действий и ведение электронного архива нотариальных документов;

- формирование нормативно-правовой базы, обеспечивающей появление новых видов нотариальных действий, связанных с электронными документами;
- интеграция внутренних информационных ресурсов с международными информационными системами, решение вопросов трансграничного информационного обмена с нотариатами других стран.

Изменения, внесенные Федеральным законом от 2 октября 2012 года № 166-ФЗ «О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации» [2] в Основы законодательства Российской Федерации о нотариате [1] предусматривают введение в 2014 году ряда электронных реестров нотариальных действий в Единой информационной системе нотариата Российской Федерации.

В настоящее время в стадии завершения формирования находится ядро IT инфраструктуры, обеспечивающее активное использование нотариусами информационных технологий в своей деятельности, созданы предпосылки для совершенствования и расширения сферы деятельности нотариата на основе применения новых информационных технологий.

Так, в рамках проекта электронной регистрации нотариусами передано в Федеральную налоговую службу более 20 тысяч пакетов документов в электронной форме, подписанных электронной подписью для совершения регистрационных действий в отношении юридических лиц.

Следует отметить, что с созданием в 2006 году Единой информационной системы нотариата России (далее – ЕИС) и дальнейшем ее развитием были устранены значительные различия между нотариусами субъектов Российской Федерации по использованию информационных и коммуникационных технологий в своей деятельности. Применение электронной подписи сегодня позволяет нотариусу участвовать через ЕИС в электронном документообороте с органами государственной власти. Электронная подпись используется также и для электронного документооборота со Сбербанком России. Соглашением, заключенным Федеральной нотариальной палатой и ОАО Сбербанк России, Фондом «Центр инноваций» организована передача заявлений в Сбербанк о розыске вкладов в связи с ведением нотариусом наследственного дела в электронной форме с электронной подписью нотариуса.

Введенная в эксплуатацию в ЕИС система удаленного перевыпуска сертификатов электронной подписи позволяет в настоящее время производить регламентные действия по перевыпуску электронной подписи непосредственно с рабочего места нотариуса без дополнительных материальных затрат с его стороны.

Формирование первой очереди соответствующего современным требованиям Центра обработки данных на федеральном уровне (перераспределение нагрузки) позволяет оптимизировать IT-ресурсы в нотариальных конторах. Тем самым необходимый функционал ЕИС может быть использован нотариусом без приобретения дорогостоящего оборудования, что немаловажно для малочисленных нотариальных палат и нотариусов, осуществляющих свою деятельность в дотационных нотариальных округах.

Важно, что наличие комплексных программ внедрения информационных и коммуникационных технологий исключает дублирование разработки типовых программных решений, несовместимость программно-технических решений, невозможность обмена данными между различными информационными системами, и, как следствие, исключает несистемные расходы на такие технологии как со стороны Федеральной нотариальной палаты, нотариальных палат субъектов Российской Федерации, так и нотариусов.

В соответствии с заключенным осенью 2011 года Федеральной нотариальной палатой и Министерством связи и массовых коммуникаций Российской Федерации Соглашением об организации электронного взаимодействия с органами государственной власти с использованием Системы межведомственного электронного взаимодействия была проведена, согласно установленным требованиям, установка предоставленного Минкомсвязи России серверного оборудования. В настоящий момент при помощи Системы межведомственного электронного взаимодействия отрабатывается взаимодействие с Росреестром по получению выписок из ЕГРП по запросам нотариусов, формируемым в ЕИС нотариата России.

Кроме того, необходимо отметить также положительный эффект применения информационных технологий в нотариальной деятельности по следующим направлениям:

- нотариус имеет возможность оперативной проверки информации, которая предоставляется ему обратившимся к нему гражданином, посредством получения необходимой инфор-

мации из стороннего источника – соответствующего электронного государственного реестра. Это позволяет выявить недостоверную информацию, и даже поддельные документы, что повышает уровень безопасности как самого нотариуса (он несет имущественную ответственность за результаты своего труда), так и участников правоотношений. В настоящее время в ЕИС реализован сервис получения выписок из Единого государственного реестра юридических лиц;

- использование нотариусами и сотрудниками нотариальных контор автоматизированных рабочих мест снижает вероятность допущения ошибки при составлении нотариального документа, уменьшает время его изготовления. Соответственно при этом сокращается и время ожидания граждан в процессе совершения нотариального действия;
- нотариатом создаются и используются информационные ресурсы и сервисы, направленные на сокращение временных и финансовых затрат граждан, решающие частично или полностью задачи «одного окна»;
- информационные ресурсы нотариата используются в деятельности органов государственной власти и организаций;
- проводится работа по подготовке изменений и дополнений в нормативные правовые акты в связи с применением нотариусами в своей деятельности информационных технологий.

Представляется особенно актуальным вопрос, связанный с законодательным закреплением нового вида нотариальных действий, который неизбежно будет применяться при использовании электронных документов, активно использоваться в нотариальной деятельности, это – удостоверение тождественности электронного документа документу на бумажном носителе и, соответственно, удостоверения тождественности документа на бумажном носителе электронному документу. В связи с этим необходимо решение вопроса применительно к нотариальным действиям с электронными документами о необходимости нормативного правового регулирования использования средств визуализации электронного документа. При этом нормативно-правовое регулирование может осуществляться посредством издания подзаконного нормативного правового акта федерального органа исполнительной власти, уполномоченного в данной сфере, что позволит, по нашему мнению, более оперативно вносить в него изменения в условиях внедрения новых средств визуализации, что несомненно важно, учитывая динамику развития современных информационных технологий.

В целях повышения квалификации нотариусов и сотрудников нотариальных палат субъектов Российской Федерации проводятся специализированные циклы лекций о применении информационных технологий как на курсах аккредитованных Федеральной нотариальной палатой ВУЗов, так и на региональном уровне.

На основании проведенного анализа имеющейся сегодня практики, а также обозначенных направлений применения информационных технологий в нотариальной деятельности можно сделать следующие выводы:

- нотариальным сообществом России сформирован системный подход к решению задач в сфере информатизации нотариальной деятельности, в том числе по созданию и дальнейшему развитию соответствующей современной информационной инфраструктуры нотариата, отвечающий установленным требованиям, на всей территории Российской Федерации;
- проводится активная работа по организации электронного взаимодействия с органами государственной власти, возможности осуществления юридически значимых действий в электронном виде, в том числе обеспечивающих оказание органами власти государственных услуг в электронном виде;
- осуществляется планомерная работа по формированию навыков использования информационных технологий среди нотариусов и сотрудников нотариальных палат субъектов Российской Федерации;
- созданная инфраструктура и запланированное ее дальнейшее развитие соответствуют положениям разрабатываемых проектов нормативных правовых актов, а также учитывают основные тенденции развития правоотношений в информационной сфере.

Вместе с тем в качестве существующих сегодня проблем и сдерживающих факторов развития информационных технологий в нотариальной деятельности в целях получения наиболее оптимальных результатов следует отметить наличие проблем организации широкополосного доступа в Интернет для конечных пользователей ЕИС; отсутствие правового регулирования нотариальной деятельности в сфере электронного документооборота, совершения нотариальных действий с электронными документами, а также

недостаточную актуальность баз данных, формируемых на основе сведений поступающих от нотариусов, что пока не позволяет оптимально использовать проверочные сервисы.

На устранение указанных сдерживающих факторов, как организационного, так и правового характера, включая и вопросы правового обеспечения информационной безопасности, касающиеся обеспечения юридической значимости электронных документов в настоящее время должны быть направлены усилия нотариального сообщества, поскольку от этого в информационном обществе в значительной степени зависит повышение качества нотариальной защиты прав граждан и юридических лиц.

Литература

1. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 года N 4462-1 (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 10, ст. 357; Собрание законодательства Российской Федерации, 2003, N 50, ст. 4855; 2004, N 27, ст. 2711; N 35, ст. 3607; N 45, ст. 4377; 2005, N 27, ст. 2717; 2006, N 27, ст. 2881; 2007, N 1, ст. 21; N 27, ст. 3213; N 41, ст. 4845; N 43, ст. 5084; 2008, N 52, ст. 6236; 2009, N 1, ст. 14, 20; N 29, ст. 3642; 2010, N 28, ст. 3554; 2011, N 49, ст. 7064; N 50, ст. 7347; 2012, N 27, ст. 3587).
2. Федеральный закон от 02.10.2012 N 166-ФЗ «О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации» // «Российская газета», № 230, 05.10.2012г.
3. Концепция информатизации небюджетного нотариата Российской Федерации, утвержденная 16 мая 2009 г. Собранием представителей нотариальных палат субъектов Российской Федерации (Протокол №21) // www.fciit.ru

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

Семенова Екатерина Игоревна

Сравнительно-правовой анализ законодательства стран СНГ по вопросам проведения антикоррупционной экспертизы нормативных правовых актов и их проектов

Аннотация: *рассматриваются особенности проведения антикоррупционной экспертизы нормативных правовых актов и их проектов в странах СНГ. Дана классификация стран по уровню развития антикоррупционной экспертизы в национальном законодательстве.*

Ключевые слова: *антикоррупционная экспертиза, правовые акты, законодательство стран СНГ, коррупциогенный фактор, методика, правила, коррупционные риски, проверка на коррупциогенность.*

В большинстве европейских стран порядок и правила оценки проектов правовых актов на коррупциогенность специально не регулируются ни в регламентах парламентов, ни в постановлениях правительства, ни тем более в актах правоохранительных органов. В ряде стран (Испания, Португалия, Польша) в регламентах упоминается лишь возможность юридической экспертизы. Так, в ч. 3 ст. 34 Регламента польского Сейма предусмотрена возможность направления проекта на экспертизу, если в пояснительной записке нет упоминания о проведении таковой в период подготовки проекта к рассмотрению в Сейме. В рамках этой экспертизы может быть полностью или частично проведена и оценка проекта на коррупциогенность [1]. В подтверждение вышесказанного приведем следующее заявление эксперта Совета Европы Саймона Годдарда (Великобритания) на круглом столе в Государственной Думе в июне 2008 г.: «В Великобритании ничего подобного не существует, нет ничего такого, о чем Вы рассказывали в области оценки рисков при разработке законодательства. Скажу так — даже названия такого нет. Но все же существуют процессы, которые, как мы надеемся, и нам помогают идентифицировать риски коррупции» [2].

Данное обстоятельство объясняется тем, что антикоррупционная экспертиза нормативных правовых актов и их проектов (далее – антикоррупционная экспертиза) проводится в странах с высоким уровнем коррупции с целью устранения и предотвращения первичных причин ее проявления. Именно поэтому, антикоррупционная экспертиза получила развитие в странах постсоветского пространства – страны СНГ и Прибалтики, ряде бывших социалистических стран Европы, а также в странах третьего мира в Азии и Африке. Россия в 2011 году по уровню восприятия коррупции оказалась на 143 месте из 183 возможных. Соседями России по рейтингу стали Азербайджан, Беларусь. Немногим лучше дела обстоят в Молдове – 112 место, Казахстане – 120 место и Армении – 129 место. Украина и Таджикистан занимают 152 место, Киргизия — 164 место, а Туркменистан и Узбекистан поделили 177 строчку рейтинга [3].

Изучение вопроса формирования института антикоррупционной экспертизы в странах СНГ с целью перенимания опыта в данной области представляется интересным по нескольким причинам. Во-первых, как уже было отмечено выше в странах СНГ, в том числе и в России, высокий уровень коррупции и одним из способов противодействия данному явлению выступает антикоррупционная экспертиза. Во-вторых, развитие правовых систем данных стран основывалось на законодательстве и юридической практике бывшего СССР, а, следовательно, эти государства имеют схожие правовые проблемы

во многом являющиеся причинами возникновения коррупционных рисков. В-третьих, странами-участниками Межпарламентской ассамблеи стран СНГ принимались модельные законы, регламентирующие вопросы антикоррупционной экспертизы [4], которые хотя и имеют форму рекомендаций, однако же свидетельствуют об общности интересов союзных стран в борьбе с коррупционными проявлениями в нормативных правовых актах и их проектах.

Рассмотрение вопроса становления антикоррупционной экспертизы в странах СНГ показало, что хотя в этих государствах и идет активное формирование данного института, однако этот процесс неравномерен, что можно объяснить особенностями развития национальных правовых систем и наличием внутриполитических проблем в этих государствах. В частности об этом свидетельствуют мониторинговые отчеты об антикоррупционной деятельности, предоставляемые странами для Организации экономического сотрудничества и развития (далее — ОЭСР) в рамках Стамбульского плана действий по борьбе с коррупцией [5]. Системный анализ данных мониторинга и законодательства стран СНГ позволяет выделить три группы стран по уровню развития антикоррупционной экспертизы в национальном законодательстве. К первой группе относятся государства, которые только формируют институт антикоррупционной экспертизы («на стадии становления») — Азербайджан, Таджикистан, Украина, Армения. Ко второй группе — страны, которые восполняют пробелы правового регулирования антикоррупционной экспертизы («развивающиеся») — Узбекистан и Киргизия. Третья же включает государства, которые оттачивают механизм проведения экспертизы, стремясь сделать антикоррупционную экспертизу наиболее эффективной мерой противодействия коррупции («развитые») — Казахстан, Молдова. Основываясь на анализе законодательства стран СНГ по вопросам антикоррупционной экспертизы и вышеуказанных мониторинговых отчетах для ОЭСР дадим краткую характеристику каждой из указанных групп.

Итак, для государств СНГ находящихся на стадии становления характерны следующие особенности правового регулирования антикоррупционной экспертизы:

1. Закрепление в различных актах необходимости проведения такой экспертизы

В Таджикистане необходимость проверки действующих правовых актов на коррупциогенность отмечается в Стратегии по борьбе с коррупцией на период 2008-2012 гг., в указе Президента Республики Таджикистан № 864 «О дополнительных мерах по борьбе с коррупцией» и постановлении Правительства от 2 сентября 2010 г. «Об утверждении Плана мероприятий по обеспечению исполнения дополнительных мер по усилению противодействия коррупции в Республике Таджикистан на 2010 – 2012 годы» [6].

В Национальной антикоррупционной стратегии Украины на 2011 – 2015 годы, утвержденной указом от 21 октября 2011 года № 1001, предусмотрено усовершенствование антикоррупционной экспертизы путем внедрения многоступенчатой методики оценки коррупционных рисков в законодательстве. Так же одним из мероприятий Государственной программы по предотвращению и противодействию коррупции на 2011 – 2015 годы, утверждённой постановлением Кабинета Министров Украины от 28 ноября 2011 года № 1240 является обеспечение доступа общественности для ознакомления к проектам нормативно-правовых актов, усовершенствование механизма организации проведения общественной антикоррупционной экспертизы проектов нормативно-правовых актов.

2. Наличие актов формально закрепляющих данный институт в системе национального права

Так, Конституционный закон Азербайджанской Республики «О нормативных юридических актах» от 17 февраля 2011 г. [7] лишь фиксирует антикоррупционную экспертизу, на ряду с правовой и лингвистической экспертизами, как один из видов проводимых экспертиз нормативных правовых актов в этой стране. Других актов, регламентирующих объекты, субъекты, сроки проведения антикоррупционной экспертизы в Азербайджане нет.

Общее требование о проведении антикоррупционной экспертизы правовых актов было введено в 2009 году Постановлением Правительства Республики Армения от 22 октября 2009 г. №1205-Н «Об оценке регулирующего воздействия антикоррупционных нормативных правовых актов». В соответствии с данным постановлением, все законы, упомянутые в статье 27.1 закона РА «О правовых актах», подлежат антикоррупционной экспертизе. Как объяснили экспертам группы мониторинга во время их визита в страну, такая экспертиза проводится в отношении всех законов, а также некоторых подзаконных актов [8].

На сегодняшний день подготовлен и прошел согласование проект Закона Республики

Таджикистан «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов». Законопроект предусматривает базовую (внутриведомственную), внешнюю и независимую антикоррупционную оценку проекта нормативного правового акта. В законопроекте обозначены объекты, принципы проведения экспертизы, предусмотрены статьи об актах реагирования и иных документах, в которых отражаются результаты антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов, и возможности институтов гражданского общества и граждан в порядке, предусмотренном нормативными правовыми актами Республики Таджикистан проводить за счет собственных средств независимую антикоррупционную оценку нормативных правовых актов и проектов нормативных правовых актов. Пока что этот акт все еще не принят и согласно Государственной программе по реализации Концепции прогнозного развития законодательства Республики Таджикистан в сфере государственного устройства, право-защиты, обороны и безопасности на 2012-2015 годы № 97, утвержденной от 1 марта 2012 года [9], предусматривается принятие указанного закона в течении 3 лет (в период с 2012 по 2015 год).

На данный момент вопросы проведения антикоррупционной экспертизы на Украине определяются всего лишь одной статьей — статьей 15 Закона Украины от 7 апреля 2011 года №3206-VI «О принципах предотвращения и противодействия коррупции» [10], которой закреплено, что субъектом, уполномоченным проводить экспертизу является Министерство Юстиции Украины, а к объектам обязательной антикоррупционной экспертизы отнесены проекты законов Украины, актов Президента Украины, других нормативно-правовых актов, разрабатываемых Кабинетом Министров Украина, министерствами, другими центральными органами исполнительной власти. Так же возможно проведение общественной антикоррупционной экспертизы проектов нормативно-правовых актов, проводимой за счет физических лиц, объединений граждан, юридических лиц или других источников, не запрещенных законодательством.

3. Отсутствие методики, порядка и сроков проведения антикоррупционной экспертизы

В приложениях к указанному Конституционному закону Азербайджанской Республики «О нормативных юридических актах» содержится «Список факторов, составляющих угрозу злоупотреблений для нормативных актов (и проектов нормативных актов)». Таким образом, фактически отсутствует методика проведения экспертизы (а лишь простое перечисление коррупциогенных факторов) и детальный порядок проведения экспертизы.

Поправками в указанный выше Закон Украины от 7 апреля 2011 года №3206-VI «О принципах предотвращения и противодействия коррупции», были отменены порядок [11] и методология [12] проведения антикоррупционной экспертизы. Согласно статье 15 данного закона порядок и методология проведения антикоррупционной экспертизы проектов нормативно-правовых актов и порядок обнародования ее результатов определяются Министерством юстиции Украины. Однако такие акты так и не были приняты.

Государственная программа по реализации Концепции прогнозного развития законодательства Республики Таджикистан в сфере государственного устройства, правозащиты, обороны и безопасности на 2012-2015 годы, утвержденная в марте 2012 года, предусматривает принятие упрощенной методики антикоррупционной экспертизы.

Согласно мониторинговому отчету в Армении экспертизу проводит специальный орган Министерства юстиции – Агентство экспертизы правовых актов. Методология проведения экспертизы основана на применении 9 специальных критериев, направленных на снижение рисков коррупции. По результатам проведения антикоррупционной экспертизы нормативных правовых актов составляются соответствующие отчеты, не имеющие обязательной силы, и вопрос правовых последствий несоблюдения содержащихся в них положений законом «О правовых актах» не регулируется. Вероятно, отчеты о результатах антикоррупционной экспертизы играют примерно ту же роль, что и любые комментарии к проекту соответствующего правового акта со стороны любого другого компетентного органа в процессе межведомственных консультаций. Отчет направляют автору проекта, который, с учетом содержащихся в нем рекомендаций, вносит в проект необходимые поправки [13].

У развивающихся стран имеются акты, регулирующие проведение антикоррупционной экспертизы, в которых определены субъекты, объекты, сроки проведения экспертизы, в том числе есть методика с достаточным количеством коррупциогенных факторов для предотвращения коррупциогенных правонарушений. В Узбекистане и Киргизии делаются попытки детали-

зации порядка проведения антикоррупционной экспертизы, а также нарабатывается практика ее проведения. Однако, в этих государствах объектом данной экспертизы являются только проекты нормативных правовых актов.

В соответствии с Постановлением Президента от 23 августа 2011 г. № ПП-1602 «О мерах по дальнейшему совершенствованию деятельности Министерства юстиции Республики Узбекистан» Министерству юстиции поручено проведение обязательной экспертизы законопроектов на предмет выявления в них коррупционных рисков. В Узбекистане была утверждена Приказом Министра юстиции от 20 октября 2011 г. №106 методика, которая должна применяться ко всем проектам нормативно-правовых актов, разрабатываемым Кабинетом министров, Парламентом, Президентом, а также органами местного уровня. Она включает в себя набор коррупциогенных факторов, включая краткую характеристику каждого фактора.

На основании проведенного анализа составляется соответствующее заключение, имеющее характер рекомендации. Это заключение может содержать описание последствий, которые возникнут, если выявленные коррупционные риски не будут устранены. На основании заключения осуществляется разработка конкретных предложений, которые передаются в соответствующие органы, и были инициированы многие изменения в законодательстве. Например, в Кодексе об административной ответственности было уточнено положение о штрафах за нарушения правил дорожного движения, вопрос освобождения от административной ответственности был передан в компетенцию судов, более четко прописаны положения об электронных налоговых декларациях и других документах, о службе «единого окна» при декларировании доходов и т.д. [14].

Согласно статье 20 Закона Кыргызской Республики «О нормативных правовых актах Кыргызской Республики» от 20 июля 2009 года № 241 проекты нормативных правовых актов по вопросам обеспечения конституционных прав, свобод и обязанностей граждан; правового статуса общественных объединений, средств массовой информации; государственного бюджета, налоговой системы; экологической безопасности; борьбы с правонарушениями; введения новых видов государственного регулирования предпринимательской деятельности должны подлежать правовой, правозащитной, гендерной, экологической, антикоррупционной и иной научной экспертизе (в зависимости от правоотношений, на регулирование которых направлен проект нормативного правового акта) [15]. Инструкция о порядке проведения правовой, правозащитной, гендерной, экологической, антикоррупционной экспертиз проектов подзаконных актов №319 от 08.12.2010г. закрепляет понятия, принципы, задачи, общий порядок проведения указанных экспертиз. Этот нормативный правой акт является прототипом столь желаемого в российском научном сообществе закона «Об экспертной деятельности» [16], «Об экспертизе нормативных правовых актов» [17]. Названная Инструкция представляет собой одновременно методику и правила проведения антикоррупционной экспертизы – перечислены коррупциогенные факторы с раскрытием их состава, регламентирован процесс проведения антикоррупционной экспертизы, в том числе инструкция содержит требования, предъявляемые к пакету документов, предоставляемых для проведения экспертизы, а также к структуре и оформлению экспертного заключения.

Основными отличными признаками «развитых» стран (Республика Молдова, Казахстан) являются качественная экспертиза, действительно способная предотвращать коррупционные риски, и отточенный механизм ее проведения. В этих странах антикоррупционная экспертиза является эффективной мерой противодействия коррупции. Республика Молдова и Казахстан проводят обязательную антикоррупционную экспертизу, как нормативных правовых актов, так и их проектов. Более того в Молдавии проводится экспертиза проектов о внесении изменений, дополнений или о признании нормативных правовых актов утративших силу.

В этих странах уже не решаются проблемы апробации методики и внедрения порядка проведения антикоррупционной экспертизы. Это объясняется тем, что процесс проведения антикоррупционной экспертизы был начат в этих странах достаточно рано по сравнению с другими государствами — в 2006 году.

Задачами проведения антикоррупционной экспертизы являются не только выявление и устранение коррупциогенных рисков, но и общая оценка последствий принятия проекта нормативного правового акта (проекта) в части возможности совершения коррупционных правонарушений, определение возможной эффективности борьбы с коррупционными правонарушениями. В Казахстане также предусматривается выработ-

ка рекомендаций по включению в текст превентивных антикоррупционных норм [18].

Для обеспечения специализации экспертов в Республике Молдова выделяются области в которых проводится антикоррупционная экспертиза, а именно:

1. конституционное и административное право, юстиция и внутренние дела, права и свободы человека;
2. экономика и торговля;
3. бюджет и финансы;
4. просвещение и образование, культура, культы и СМИ;
5. законодательство о труде, социальном обеспечении, защите здоровья и семьи [19].

В развитых странах детально проработаны акты, регулирующие порядок и методику проведения антикоррупционной экспертизы с раскрытием составляющих коррупциогенных факторов. Разработанная методика выявления коррупциогенных факторов в Молдове в совокупности с сформированной практикой проведения антикоррупционной экспертизы [20] явилась для многих стран основой для написания национальных методик.

В том числе при проведении антикоррупционной экспертизы используются как общетеоретические и специальные познания, так и сведения о практике применения законодательства и подзаконных актов. Так, например, учитываются результаты социологических исследований по вопросам сложившейся коррупционной практики и действующих коррупционных схем, статистические данные, материалы научно-практических конференций, семинаров, совещаний, проводимых по проблемам действующего законодательства, обращения граждан в государственные органы, судебная и правоприменительная практика.

По результатам экспертизы составляется экспертное заключение, к которому могут быть приложены выписки из законодательных актов; примеры конкретных случаев коррупции, которые были совершены или могут быть совершены в связи с принятием проекта законодательного или иного нормативного акта; выписки из международных договоров и другие необходимые документы; примеры судебной практики.

Однако стоит отметить особенности регулирования антикоррупционной экспертизы в этих странах, которые можно оценить как с положительной стороны, так и с отрицательной стороны.

Так, в Республике Казахстан проводится обязательная научная антикоррупционная экспертиза проектов законов. Данная экспертиза осуществляется научными учреждениями, услуги которых закупаются на основании тендеров и оплачиваются республиканским бюджетом. Таким образом, проведение тендера обеспечивает прозрачность в выборе субъекта, уполномоченного проводить антикоррупционную экспертизу. Данные научные учреждения определяются ежегодно и часто меняются, что, по мнению ОЭСР, снижает эффективность антикоррупционной экспертизы, поскольку опыт работы, накопленный в предыдущих научных организациях, может не быть использован в последующих. ОЭСР считает, что «возложение обязанности проведения антикоррупционной экспертизы на государственный орган позволяет наилучшим образом использовать накопленный опыт, обеспечить единство практики, подготовку квалифицированных экспертов. Кроме того, экспертиза переходит из разряда научной в разряд официальной, что меняет ее статус и повышает требования к учету ее результатов» [21].

В Молдавии закреплен большой перечень коррупциогенных факторов (более 20 коррупциогенных факторов), называемый «условной классификацией элементов коррупциогенности». Разработчики Методики полагают, что создать закрытый перечень просто невозможно и что в этом направлении экспертиза всегда будет совершенствовать свои методологические разработки. Тем более что коррупция возникает не только в результате плохо проработанных и неудачно сформулированных законов, но и сама может стать ключевым фактором в процессе законотворчества [22]. С другой стороны не понятно кем и как должны фиксироваться новые виды коррупциогенных факторов. Таким образом, открытый перечень может служить основой для широкого толкования понятий, вложенных в формулировку коррупциогенных факторов, в результате чего может быть написано ошибочное экспертное заключение.

Выше сказанное в своей совокупности свидетельствует о том, что правовое регулирование вопросов антикоррупционной экспертизы в странах СНГ не лишено недостатков. Хотя ОЭСР сформулировало рекомендации, направленные на устранение выявленных замечаний, для каждой страны СНГ, но все же анализ данных рекомендаций позволяет сделать вывод о том, что некоторые предложения являются общими, в частности следующие:

- ввести проведение антикоррупционной экспертизы действующих правовых актов;
- ввести обязательную антикоррупционную экспертизу;
- предусмотреть специальные процедуры в случая обнаружения в проекте коррупциогенных норм, например, обязанность разработчика проекта учесть замечания, в случае невнесения соответствующих изменений обосновать свой отказ и приложить заключение экспертизы к проекту акта для его подачи на рассмотрение органа, уполномоченного принимать такой акт;
- ввести требование публиковать результаты антикоррупционной экспертизы проектов актов, что значительно повысило бы прозрачность процесса принятия решений, укрепило доверие к органам государственной власти, способствовало бы повышению информированности общества о коррупции и коррупциогенных правовых нормах, а также позволило бы гражданскому обществу лучшим образом контролировать деятельность властей.

Сравнительно—правовой анализ законодательства стран СНГ и России по вопросам проведения и организации антикоррупционной экспертизы (приложение № 1) позволяет сделать вывод, что наша страна может быть отнесена ко второй группе стран — к «развивающимся». России необходимы существенные изменения в законодательстве, регулирующем антикоррупционную экспертизу для того, чтобы попасть в ряды «ведущих стран». В настоящее время необходимо соотнести накопленный отечественный опыт с опытом стран СНГ по вопросам проведения антикоррупционной экспертизы для того, чтобы выявить какие конкретно приемы могут быть имплементированы в российское законодательство. Более того, такой гибкий подход позволит определить смогут ли данные новации эффективно работать в рамках нашей правовой системы.

Литература

1. См.: Правовые акты: антикоррупционный анализ / отв. ред. В.Н.Найденко, Ю.А.Тихомиров, Т.Я.Хабриева. М., 2009.
2. Стенограмма круглого стола на тему: «Практика применения и перспективы развития законодательства России, стран Восточной Европы и Азии, регламентирующего вопросы антикоррупционной экспертизы законодательных актов и их проектов». Госдума, 24-25 июня 2008 г. С. 78.
3. Данные Международной неправительственной организации Transparency International http://cpi.transparency.org/cpi2011/results/
4. Модельный закон «Основы законодательства об антикоррупционной политике», принятый Межпарламентской Ассамблеей государств-участников СНГ Постановлением N 22-15 // Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2004. N 33. С. 225 – 260., Модельный закон «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов», утвержденный постановлением № 37-12 от 17.05.2012 г. МПА СНГ // СПС «Консультант плюс»
5. Подробнее об этом: http://www.oecd.org/corruption/acn/istanbulactionplan/
6. http://anticorruption.tj/en/about-anti-corruption/anti-corruption-national-strategy
7. http://base.spinform.ru/show_doc.fwx?rgn=33085
8. http://www.oecd.org/corruption/acn/48965498.pdf
9. http://mmk.tj/ru/Government-programs/programs/security
10. http://base.spinform.ru/show_doc.fwx?rgn=45268
11. Порядок проведения антикоррупционной экспертизы проектов нормативно-правовых актов, утвержден постановлением Кабинета Министров Украины от 16 сентября 2009 года №1057 (не действует)
12. Постановление Кабинета Министров Украины от 8 декабря 2009 года №1346 «Об утверждении Методологии проведения антикоррупционной экспертизы проектов нормативно-правовых актов» (не действует)
13. http://www.oecd.org/corruption/acn/48965498.pdf
14. http://www.oecd.org/corruption/acn/49882461.pdf
15. http://minjust.gov.kg/?page_id=258
16. Миронов А.Н. Экспертиза проектов нормативных правовых актов федеральными органами исполнительной власти // Административное право и процесс. 2012. N 2. С. 32 – 38; Нестеров А.В. Экспертная деятельность // http://www.

hse.ru/data/2012/10/08/1247168533/ExpertisaProektovNPA.doc

17. Короткова О.А. Экспертиза законопроектов и законодательных актов: теоретико—правовой аспект: Автореферат Дисс. ... канд. Юрид. Наук. М., 2010; Тихомиров Ю.А. О теории правового регулирования: сравнительный анализ // Журнал российского права. 2009. № 12. С. 8.; Сборник материалов межригионального научно—практического семинара по проблемам мониторинга законодательства и правоприменительной практики в субъектах Российской Федерации / Московская городская дума, М., 2008 С. 64
18. Пункт 2 Методических рекомендаций по проведению антикоррупционной экспертизы нормативных правовых актов и их проектов, одобренных на 2-м заседании Межведомственной комиссии по вопросам совершенствования действующего законодательства в части противодействия коррупции 17 сентября 2007 года // http://www.csr.ru/meropriatia?id=20&view=velvetto_event
19. Пункт 5 положения об организации процесса проведения антикоррупционной экспертизы проектов законодательных и нормативных актов, утвержденного постановлением Правительства Республики Молдова № 977 от 23. 08. 2006 http://www.csr.ru/meropriatia?id=20&view=velvetto_event
20. http://www.csr.ru/meropriatia?id=20&view=velvetto_event
21. http://www.oecd.org/countries/kazakhstan/48908356.pdf
22. Правовые акты: антикоррупционный анализ: научно-практическое пособие / И.С. Власов, А.А. Колесник, Т.О. Кошаева и др.; отв. ред. В.Н. Найденко, Ю.А. Тихомиров, Т.Я. Хабриева. М.: КОНТРАКТ, Волтерс Клувер. С. 170

Рецензент: **Куракин Алексей Валентинович**,
доктор юридических наук, профессор

Приложение № 1

Сравнительно—правовой анализ законодательства стран СНГ и России по вопросам проведения и организации антикоррупционной экспертизы

Страны	Нормативные правовые акты закрепляющие антикоррупционную экспертизу	Нормативные правовые акты регулирующие антикоррупционную экспертизу	методика	объект	Субъекты проведения государственной антикоррупционную экспертизу	Учет правоприменительной практики	Обязательность проведения
Азербайджан	+	—	—	Проекты нормативных правовых актов	Различные государственные органы	—	+
Армения	+	+	+	нормативные правовые акты и их проекты	Государственный орган при Министерстве юстиции	—	+
Казахстан	+	+	+	Проекты нормативных правовых актов	**Проводится научная экспертиза** Научные учреждения на основе конкурсов и тендеров	+	+
Киргизия	+	+	В виде инструкции	Проекты нормативных правовых актов	Парламент, независимые эксперты, организации гражданского общества	—	+
Молдова	+	+	+	Проекты нормативных правовых актов	государственный научный центр	+	+
Российская Федерация	+	+	+	нормативные правовые акты и их проекты	Разные государственные органы, независимые эксперты, организации гражданского общества	+	+
Таджикистан	+	— (есть проект закона)	—	нормативные правовые акты и их проекты	Разные государственные органы	—	—
Узбекистан	+	+	+	Проекты нормативных правовых актов	Министерство юстиции	—	+
Украина	+	—	—	Проекты нормативных правовых актов	Министерство юстиции	—	+

Сведения об авторах

АТАГИМОВА Эльмира Исамудиновна – ведущий юрисконсульт юридического отдела Федерального бюджетного учреждения «Научный центр правовой информации при Министерстве юстиции Российской Федерации», кандидат юридических наук, г. Москва
E-mail: atagimova75@mail.ru

БУЛГАКОВА Елена Валерьевна – доцент кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, кандидат юридических наук, г. Москва.
E-mail: Koordinator-proekta@mail.ru.

ЗАГОРОДНИКОВ Сергей Николаевич – профессор кафедры «Математические методы в экономике» Российского экономического университета им. Г.В. Плеханова, доктор биологических наук, кандидат технических наук, г. Москва.
E-mail: T_zagorodnikova@rambler.ru

КУБАНКОВ Александр Николаевич – профессор кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, заслуженный работник связи России, доктор военных наук, профессор, г. Москва.
E-mail: kan9991@gmail.com

КОВАЛЕНКО Егор Владимирович – управляющий партнер ООО «Национальная юридическая служба», г.Москва
E-mail: kovalenko@amulex.ru

ЛАЗАРЕВ Виктор Михайлович – главный научный сотрудник ЗАО Научно-технический центр «Поиск-ИТ», доктор технических наук, профессор, г. Москва.
E-mail: V_lazarev@poisk-it.ru

ЛИНЬКОВ Григорий Сергеевич – главный специалист правового обеспечения Фонда «Центр инноваций и информационных технологий, магистр университета МГИМО, г. Москва.
E-mail:glinkov@fciit.ru

ЛЮБИМОВ Алексей Евгеньевич – генеральный директор ЗАО Научно-технический центр «Поиск-ИТ», кандидат технических наук, г. Москва.
E-mail: www.poisk-it.ru

МАКАРЕНКО Дмитрий Григорьевич – генеральный директор ООО «Национальная юридическая служба», г.Москва.
E-mail: makarenko@amulex.ru

МАКСИМОВ Денис Алексеевич – ассистент кафедры «Математические методы в экономике» Российского экономического университета им. Г.В. Плеханова, г. Москва.
E-mail: Loony86@mail.ru

МАХНОНОСОВ Эдуард Викторович – директор Фонда «Центр инноваций и информационных технологий», советник Президента Федеральной нотариальной палаты, соискатель кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, г. Москва.
E-mail:director@fciit.ru

МОРОЗОВ Андрей Витальевич – заведующий кафедрой информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, доктор юридических наук, профессор, г. Москва.
E-mail: av_morozov@list.ru

ОРЛОВ Владимир Игоревич – аспирант кафедры №48 «Компьютерное право» Национального исследовательского ядерного университета «МИФИ», г. Москва
E-mail: orlow13@mail.ru

ОСТРОУШКО Александр Владимирович – доцент кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, кандидат юридических наук, доцент, г. Москва.
E-mail: ostroushko@mail.ru

ПЕТРОВА Любовь Петровна – доцент кафедры «Математические методы в экономике» Российского экономического университета им. Г.В. Плеханова, г. Москва.
E-mail: Kafedra_mme@mail.ru

РУСТИКОВА Галина Сергеевна – преподаватель кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации, г. Москва.
E-mail: rustikova-gs@list.ru

СЕЛЕЗНЁВА Елизавета Алексеевна – адвокат, Юридический институт Московского государственного университета путей сообщения, кандидат юридических наук, г. Москва.
E-mail: Sellisa@yandexd.ru

СЕМЕНОВА Екатерина Игоревна – младший научный сотрудник Научно-исследовательского института Российской правовой академии Министерства Юстиции Российской Федерации, г. Москва.
E-mail: semenova_ek@list.ru

Abstract and keywords

A.V. Morozov

History of legal informatization of the Ministry of Justice of Russia at the turn of the century

Abstract: *In the article the author describes the stages of legal informatization of the Ministry of Justice of Russia from the last decades of the 20th century to the beginning of this century and presents an account of key events and legal acts.*

Keywords: *law, information technology law (IT law), Ministry of Justice, information*

V.M. Lazarev, A.E. Lubimov

Proposals on using information analysis systems in providing legal information for legislative and executive authorities at the federal, regional and local levels

Abstract: *The article describes an implemented approach to integrated processing of unstructured (textual and audio-visual) data serving the purpose of supporting decision making by legal information users.*

Keywords: *unstructured information, full-text search, text analytics, processing of audio-visual information, modelling on the basis of cognitive maps, support of decision-making.*

E. I. Atagimova

Problems concerning negative influence of Internet information on moral education of juveniles in the information space and means for solving them

Abstract: *Problems concerning negative influence of Internet information on moral education of juveniles are examined in the article. Clarifications are given on the amendments to Federal Law No. 139-FZ of the 28th of July 2012 "On Modifications to the "Federal Law on Protecting Children from Information Harmful to Their Health and Development" and to Certain Legislative Acts of the Russian Federation on the Issues of Restricting Access to Unlawful Information in the Internet" that have been passed in order to solve this problem.*

Keywords: *Internet, legal and moral education, rising generation, negative influence, Federal Law of the Russian Federation, amendments.*

S.N. Zagorodnikov, D.A. Maksimov, L.P. Petrova

Economic information security in the market environment

Abstract: *Provisions of different normative acts that ensure legal regulation of information protection in the field of economic relations are considered.*

Keywords: *security, information, economic, normative act.*

E.V. Kovalenko, D.G. Makarenko

Remote provision of legal services to population as the development of the system of public legal aid offices

Abstract: *A new approach to the provision of free legal services to population through setting-up a network of remote centres on a modern technology platform is proposed. Considerable advantages of this way of development of services over the currently developed system of public legal aid offices are demonstrated.*

It is demonstrated that modern technologies can help to provide legal consultations over all of Russia at a comparatively low cost for the government by way of setting-up consultative legal aid offices — All-Russian Offices for Justice (Complaints).

Keywords: *remote access, IP telephony, software, legal consultations.*

E.V. Bulgakova, E.A. Selezneva

Information security of defence lawyers (advocates). Organizational and legal aspects

Abstract: *In this article, legal and organizational problems of ensuring information security of defence lawyers (advocates) are brought to light. The article lists measures needed to reduce risks related to leaks of information that became known to the defence lawyer (advocate) in discharging his professional duties.*

Keywords: *information security of defence lawyers (advocates), client-attorney privilege, e-justice.*

A.N. Kubankov

Content of the academic discipline "System for ensuring Russia's information security"

Abstract: *The structure and content of the new academic discipline "System for ensuring Russia's information security" are examined in the article. A justification is given for including sections on the legal conceptual and organizational background for ensuring Russia's information security in the curriculum of the subject. The content of topics of the academic discipline is given.*

Keywords: *Master's programme, information security of the country, legal conceptual background for ensuring information security, organizational background for ensuring information security.*

G.S. Rustikova, V.I. Orlov

Granting free legal assistance through the "Yustitsia" ('Justice') portal

Abstract: *Opportunities for using the resources of the "Yustitsia" ('Justice') portal for granting free legal assistance to the population and promoting its legal awareness are examined.*

Keywords: *free legal assistance, legal awareness of the population, information society.*

A.V. Ostroushko

On the issue of legal regulation of the use of digital signature

Abstract: *The article considers problems in creating a system of inter-agency e-document flow in our country. A number of problems hindering efficient electronic interaction between public authorities are brought to light. A justification is given for the need of taking legislative measures for the protection against unlawful use of digital signature.*

Keywords: *information society, digital signature, electronic government, e-document flow, efficiency of government programme implementation.*

E.V. Makhnonosov, G.S. Linkov

Building a single information space for the notary system in the Russian Federation

Abstract: *The article considers issues of building a single information space for ensuring the increase in efficiency of all types of notary activities in the Russian Federation by means of using modern information and telecommunication technologies.*

Keywords: *information society, information space, notary document flow, electronic notarial archive.*

E.I. Semenova

Comparative legal analysis of the legislation of the Commonwealth of Independent States on issues of anti-corruption expert monitoring of normative legal acts and their drafts

Abstract: *Particularities of anti-corruption expert monitoring of normative legal acts and their drafts in the countries of the Commonwealth of Independent States are examined. A classification of the countries according to the level of development of anti-corruption expert monitoring in their national legislations is given.*

Keywords: *anti-corruption monitoring, legal acts, legislation of the Commonwealth of Independent States, corruption-generating factor, methodology, rules, corruption risks, checking for corruption-generating properties, OECD.*