

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ



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

ПРАВОВАЯ ИНФОРМАТИКА

Периодический научный журнал

№ 2 – 2014

Москва, 2014

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

Правовая информатика. №2–2014. — М. : ФБУ НЦПИ при Минюсте России, 2014. — 64 с.
ISSN 1994-1404

Издается с 1996 года

Редакционная коллегия

Сергин М.Ю.	Главный редактор, доктор технических наук, профессор
Атагимова Э.И.	ответственный секретарь, кандидат юридических наук
Горбачева Е.В.	
Макаренко Г.И.	
Матвиенко Ю.В.	кандидат медицинских наук
Танимов О.В.	кандидат юридических наук, доцент

Редакционный совет

Морозов А.В.	Председатель Совета, доктор юридических наук, профессор
Абдусаламов Р.А.	кандидат педагогических наук, доцент
Астанин В.В.	доктор юридических наук, профессор
Батурин Ю.М.	доктор юридических наук, профессор
Горбачева Е.В.	
Макаренко Г.И.	
Марков А.С.	кандидат технических наук, доцент
Матвиенко Ю.В.	кандидат медицинских наук
Павленко П.А.	
Полякова Т.А.	доктор юридических наук, профессор
Рассолов И.М.	доктор юридических наук, профессор
Севостьянов В.Л.	кандидат технических наук
Сергин М.Ю.	доктор технических наук, профессор
Федичев А.В.	кандидат технических наук, доцент
Филатова Л.В.	кандидат юридических наук, старший научный сотрудник
Шихнабиева Т.Ш.	доктор педагогических наук, профессор

Иностранные члены Редакционного совета

Курбанов Г.С.	доктор юридических наук, профессор (Азербайджанская Республика)
Шаршун В.А.	кандидат юридических наук (Республика Беларусь)

**Журнал «Правовая информатика» является периодическим рецензируемым изданием, выходит 4 раза в год.
Подписка на журнал 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)539-23-63, E-mail: pravo360@gmail.com

www.pravo360.ru

СОДЕРЖАНИЕ

Чхутиашвили Лела Васильевна

Банковские информационные технологии в рыночных условиях хозяйствования. 4

Цирлов Валентин Леонидович

Правовые вопросы безопасности киберпространства в системе отечественных нормативных документов 9

Атагимова Эльмира Исамудиновна, Рамазанова Ирина Маиловна

Некоторые аспекты законодательного уровня обеспечения информационной безопасности в Российской Федерации. 14

Шахалов Игорь Юрьевич, Райкова Наталья Олеговна

К вопросу об интегрировании систем менеджмента качества и информационной безопасности 20

Шихнабиева Тамара Шихгасановна

О некоторых подходах к модернизации образовательных систем с использованием интеллектуальных методов и моделей 27

Макаренко Татьяна Николаевна, Сарапкина Елена Николаевна

Актуальные вопросы систематизации правовых актов 32

Магдилова Лариса Владимировна

Особенности формирования информационно-правового пространства органов государственной власти в Республике Дагестан: правовой аспект 39

Танимов Олег Владимирович, Богатова Марина Константиновна

Обеспечение информационной безопасности при управлении крупными городами. 44

Фадеева Наталья Анатольевна

Повышение квалификации специалистов по ведению регистров нормативных правовых актов в ФБУ НЦПИ при Минюсте России 50

Сведения об авторах 56

Abstract and keywords 57



**Чхутиашвили
Лела Васильевна**
кандидат экономических
наук, доцент

Банковские информационные технологии в рыночных условиях хозяйствования

Аннотация: Статья посвящена банковским технологиям в современных рыночных условиях хозяйствования. Банки могут разрабатывать и внедрять новые виды услуг, основанные на информационных технологиях, с применением новейших методик кодировки данных, «умных» сетей и других средств безопасности. Внедрение таких услуг требует создания партнерских отношений между банками, предоставляющими услуги, телекоммуникационными организациями и самими предпринимателями.

Ключевые слова: информационное общество, банковская система, технология, бизнес, коммерческие банки, банковские переводы.

Переход человечества к информационному обществу характеризуется сменой индустриального технологического базиса на информационный, на смену сырью и энергии приходят информационные технологии – технологическая основа информационной индустрии, важнейшим ресурсом которой являются информация и знания.

Одним из направлений информационной экономики является сетевая экономика или Интернет-экономика (виртуальная экономика). Развитие информационных и телекоммуникационных технологий сформировали среду для экономической деятельности в Интернет, а коммерциализация Интернета привела к изменениям способов ведения бизнеса и появлению электронного рынка, основанного на принципах сетевой экономики.

Благодаря развитию информационных технологий, электронной и компьютерной техники коммерческие банки проникают на удаленные территории, завоевывают новых клиентов.

Предпосылкой внедрения технологий дистанционного обслуживания клиентов является, например, широкое распространение мобильных телефонов – индивидуальных средств связи, благодаря которым по желанию клиентов может осуществляться контроль и маркетинг счета.

Обеспечение доступа к платежному сервису через Интернет – обязательный элемент для качественного обслуживания наиболее привлекательных для банка клиентов – физических лиц, являющихся представителями среднего класса.

Мобильный банк – это новый сегмент банковского бизнеса, который быстро развива-

ется и становится сферой использования передовых схем и технологий оказания и продвижения услуг. В России эксперименты в этой области уже перешли в практическую плоскость, мобильные расчеты стали элементами продуктового ряда банков. Так, Банк Проектного Финансирования принял участие в масштабном проекте, благодаря которому клиентам могут поступать SMS-сообщения об операциях по карточному счету, оплате услуг операторов мобильной связи со счета, есть возможность и заблокировать в случае необходимости свою карту. Ключевым компонентом в этой технологии является приложение, которое располагается на SIM-карте, оно позволяет использовать мобильный телефон не только как средство осуществления платежей, но и как устройство для генерации динамических паролей. Это значит, что пароли могут меняться и создавать полную защиту от несанкционированного доступа, оставаясь известными только владельцу мобильного телефона.

Разработчики информационных технологий пошли дальше – сегодня платежная система «Рапида» предлагает продукт «SMS-платежи», который не требует подобной замены. Расчетные услуги банков переходят в цифровой формат. Все больше и больше клиентов начинают пользоваться банковскими онлайн-услугами и системами электронных платежей, так как они имеют ряд привлекательных качеств: скорость, эффективность и удобство в использовании. Ожидается, что подавляющее большинство безналичных платежей будет осуществляться в электронном виде.

Среди многих видов электронных расчетов одним из самых перспективных для банков

является электронная оплата счетов. Активный онлайн-клиент значительно прибыльнее оффлайн-клиента, а активный клиент системы электронной оплаты счетов – прибыльнее онлайн-клиента. Крупные банки могут сэкономить, если их клиенты будут активно оплачивать счета в режиме реального времени. Быстрые и простые в использовании услуги оплаты счетов онлайн весьма выгодны банкам, так как у клиентов повышается уровень удовлетворенности обслуживанием и увеличивается степень лояльности к обслуживающим их банкам.

Необходим перевод этой операции на штрих-кодovou основу, когда на выставляемые счета будет в современном виде заноситься информация, что удобно и для организации, которая оказала гражданину услугу, и для банка. Штрих-кодovая технология обработки счетов позволяет достичь важных результатов в работе с клиентами:

- › сократить время обслуживания клиентов за счет автоматизации ввода всей необходимой информации с платежных документов;
- › радикально сократить количество ошибок при вводе информации о платеже;
- › ускорить процесс перечисления денег на счета организации-получателя;
- › использовать электронные каналы связи для взаимодействия с получателями платежей;
- › увеличить рост производительности сотрудников отделений и филиалов;
- › в целом улучшить качество обслуживания клиентов.

Другое направление, также показавшее хорошие результаты в обработке коммунальных платежей – создание расчетных (биллинговых) центров для учета и контроля оплаты платежей, которые представляют собой организации, консолидирующие информацию, поступающую от организаций-поставщиков услуг по счетам, выставленным абонентам, для оплаты предоставленных услуг. В создании таких организаций, участвующих в приеме платежей, заинтересованы и органы государственной власти, поскольку таким образом формируется база данных о плательщиках.

Банки могут разрабатывать и внедрять новые виды услуг, основанные на информационных технологиях, с применением новейших методик кодировки данных, «умных» сетей и других средств безопасности. Внедрение таких услуг потребует создания партнерских отношений между предоставляющими услуги банками, телекоммуникационными организациями и са-

мыми предпринимателями. К таким услугам относятся, в частности, следующие:

круглосуточные системы перевода денег, которые устанавливают в точках продаж. Такие системы могут уменьшить время совершения сделок до примерно 10–15 секунд даже в часы пик. Результатом их использования должны стать уменьшение очередей, увеличение удовлетворенности клиентов торговых предприятий и соответственно повышение их лояльности;

услуги, характеризующиеся большим объемом передаваемых данных, такие, как возможности электронной подписи, создание электронных графических изображений, чеков, создание резервных копий данных и т. д.

Спрос на услуги, предоставляемые с помощью беспроводной связи, огромен. Банки могут использовать преимущества такого высокого спроса, расширив существующую сетевую инфраструктуру, необходимую для обеспечения беспроводных услуг, чтобы позволить своим клиентам:

- › заказывать товары в режиме онлайн и оплачивать их с помощью беспроводных устройств;
- › заказывать, оплачивать и получать информацию и другие нематериальные ценности с помощью беспроводных устройств;
- › использовать автоматизированные кассовые аппараты для самостоятельной оплаты товаров в магазинах;
- › оплачивать покупки на автоматизированных кассовых аппаратах с помощью беспроводных устройств;
- › использовать беспроводные устройства для автоматической оплаты транспортного налога (без остановки автомобиля).

Используются обычные каналы передачи сообщений в процессинговый центр платежной системы, при этом используется общий для ведущих операторов SMS-номер. Персональный платежный сервис сохраняет историю платежей. Клиент банка может в любое время найти полную информацию по всем платежам, которые когда-либо были им выполнены, а также использовать уже выполненные платежи в качестве образцов для формирования новых. Клиент способен наиболее часто производимые им платежи выделить в специальный раздел и для удобства пользования ими пронумеровать их, указать расписание их исполнения.

Успешно применяется банками еще одна технология – «Персона-банк». Разработчик этой технологии, компания «РФК», предоставляет с ее помощью возможность обслуживания банка-

ми физических лиц через Интернет. При этом от клиента требуется минимум навыков общения с компьютером. Система содержит все необходимые клиенту функции: рублевые и валютные переводы, информацию по проводкам (выписки, остатки по счетам), вклады, кредиты, периодические платежи, работу с карт-счетами и т.д.

Среди достоинств системы выделяются следующие:

- простой интерфейс, который доступен пользователю-неспециалисту;
- наличие шлюзов для интеграции со скоринговыми системами, что позволяет автоматизировать процесс принятия решений о выдаче кредита;
- возможность просмотреть хронику погашения кредита;
- возможность авторизации платежей с помощью SMS-сообщений;
- возможность автоматического информирования клиента о произведенных платежах с помощью SMS, а также предварительного информирования о следующих платежах, просроченных сроках погашения кредита и платежах по процентам;
- возможность входить в систему с любого компьютера.

В России переводы физических лиц относятся к одной из наиболее массовых услуг, этот рынок очень динамично развивается. Собственная расчетная система, позволяющая переводить средства в самые отдаленные города и поселки страны, позволяет коммерческим банкам осуществлять все виды денежных переводов в рублях и иностранной валюте: перевод средств со вкладов или наличными в пределах самой системы банка, в том числе срочные переводы в течение суток, переводы сумм со вклада в другую кредитную организацию на территории или за пределы территории России, переводы наличной иностранной валюты без открытия счета за пределы Российской Федерации.

Упорядочение денежного обращения через Интернет имело в виду деятельность нескольких объектов потенциального риска, которые обрели в схеме защиты особый контур:

- клиент банка, который вступает с кредитно-финансовой организацией в отношения дистанционного обслуживания и совершает действия со своим счетом;
- компания-провайдер, услугами которой пользуется клиент и через аппаратно-программные средства которой проходят потоки данных от клиента к банку и обратно, из-

за чего есть вероятность утраты, искажения, разглашения, подмены данных;

- аппаратно-программные средства собственно банка, в число которых входят маршрутизаторы, брандмауэры, серверы и т.д., на основе которых построена автоматизированная банковская система;
- компании-провайдеры процессинговых услуг для банка, которые оказывают банку помощь в работе с данными, например в обслуживании серверных кластеров, в хранении данных и т. д.

При внедрении технологии интернет-банкинга необходимо обеспечить:

- полную функциональность, предполагавшуюся при проектировании и предлагавшуюся клиентам;
- непрерывность работы системы дистанционного банковского обслуживания;
- соблюдение всех требований для выполнения банковских операций;
- защиту банковской и клиентской информации от несанкционированного доступа;
- контроль над функционированием системы.

Будущее платежной системы в долгосрочной перспективе будет во многом зависеть от технологий, которые в данное время находятся в стадии разработки. Применение компьютерных систем, управляемых человеческим голосом, существенно упростит операции, совершаемые по Интернету и по телефону. Биометрические технологии повысят уровень безопасности операций, совершаемых как физическими, так и юридическими лицами. Новые технологии дадут пользователям возможность отслеживать товары в режиме реального времени на всем протяжении цепи поставок.

Появление технологий интернет-банкинга, WAP-телефонии, GSM- и SMS-банкинга для владельцев мобильных телефонов, теле-банкинга и т. д. ставит вопрос о необходимости новой оценки не просто компьютеризации банка, а его новой роли, которая предопределяет перевод значительных объемов финансовых операций в реальную сферу.

Таким образом, в последней четверти XX века человечество вступило в новую стадию своего развития – стадию построения информационного общества. Известно, что в основе его построения лежат свои специфические технологии, производственно-технологические системы и производственные отношения. Для информационного общества эту роль, прежде всего, играют информационные технологии, инноваци-

онные системы и инновационная организация различных сфер человеческой деятельности. Ее конечным результатом должно стать создание новой формы организации экономики – инновационной экономики.

Инновационная экономика – это экономика общества, основанная на знаниях, инновациях, на доброжелательном восприятии новых идей, новых машин, систем и технологий, на готовности их практической реализации в различных сферах человеческой деятельности. Она выделяет особую роль знаний и инноваций, прежде всего, знаний научных.

Инновационность в качестве важнейшей черты новой экономики проявляется, прежде всего, в способности трансформировать знания в создание новых продуктов и услуг. Также нововведения включают в себя выявление и удовлетворение нужд потребителей, улучшение в маркетинге, распределении и услугах. В ближайшие годы главным двигателем экономического роста будут отрасли хозяйства и сферы деятельности, основанные на нововведениях.

Процесс информатизации общества помимо положительных последствий имеет и ряд отрицательных сторон. Так, объединение компьютеров в глобальные сети дало возможность большому количеству людей приобщиться к огромному массиву накопленной в мире информации и тут же породило проблемы с охраной интеллектуальной собственности, помещаемой и хранящейся в ней [1].

Преступные группы и сообщества начали активно использовать в своей деятельности информационные технологии. Для достижения целей прежде всего корыстных преступники стали активно применять компьютеры и специальную технику, создавать системы конспирации и скрытой связи в рамках системного подхода при планировании своих действий [2].

Негативным последствием информатизации общества является появление компьютерной преступности. Под компьютерным преступлением стали понимать предусмотренные общественно-опасные деяния, совершаемые с использованием средств компьютерной техники.

Экономические компьютерные преступления совершаются по корыстным мотивам и включают компьютерное мошенничество, кражу программ (компьютерное пиратство), кражу услуг и машинного времени, экономический шпионаж.

Информация превратилась в мощное средство конкурентной борьбы. Чем больше информации собрано, выверено, просеяно, тем бо-

лее плодотворными будут принимаемые решения по сравнению с конкурентами.

К сожалению, незаконный съём информации остановить практически невозможно, поскольку в ответ на защитные меры разрабатываются все новые программные и аппаратные средства электронного шпионажа.

Организации-жертвы компьютерных преступлений неохотно сообщают об этом в правоохранительные органы. Принимая решения, жертва компьютерного преступления руководствуется одним из факторов: компьютерный преступник не рассматривается как типичный уголовный преступник; расследование компьютерных преступлений является делом весьма дорогостоящим; будучи разоблаченными, компьютерные преступники в большинстве случаев отделяются легкими наказаниями; законодательство не всегда применимо к компьютерным преступлениям, что приводит к серьезным затруднениям при правильной их квалификации; правоохранительные органы не склонны относить многие из компьютерных правонарушений к категории преступлений и, соответственно, отказывают в возбуждении уголовного дела; раскрытие компьютерных преступлений сопряжено, как правило, с открытием финансовых, коммерческих и других служебных тайн, которые могут стать достоянием гласности во время судебного рассмотрения дел [3].

Электронная охота за информацией стала повседневным явлением и приобрела глобальный характер. Мировое сообщество до сих пор в должной мере не осознало ее масштабы и негативные последствия для государств, организаций, людей. Поэтому основная задача заключается в том, чтобы всесторонне оценить их, глубоко понять и вывести на уровень проблемы с последующей разработкой системы комплексных мер по предотвращению и нейтрализации. Одновременно следует предусмотреть специальные меры по организации личной информационной безопасности людей.

Законодательство при всей его динамике не успевает за темпом жизни, в связи с чем всегда образуются области отношений, которые не урегулированы правом или урегулированы на недостаточно должном уровне.

Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Интернет является информационно-телекоммуникационной сетью. Законодатель воспринимает Интернет просто как некое устрой-

ство, при помощи которого осуществляется обмен данными между респондентами. Однако правовой статус Интернет-пространства видится гораздо более сложным и значимым. Соответственно и легальное отражение Интернета представляется недостаточным, способствующим развитию порочных деструктивных практик со стороны недобросовестных пользователей и способствует злоупотреблениям правом. Определенность в этом вопросе сегодня крайне необходима и должна способствовать противодействию данным негативным явлениям.

Для правового регулирования виртуального пространства целесообразно не ограничиваться изданием отдельного закона, а эффективно внести соответствующие изменения в уже существующие нормативные акты, признав тем самым наличие нового важного сегмента обще-

ственной жизни, требующего внимания и регламентации. Только комплексный подход позволит эффективно бороться с неконституционным правомиспользованием в сети.

Литература

1. Батурин Ю. М. Информация общества, право и человек // Влияние научно-технического прогресса на юридическую жизнь. – М.: Юридическая литература, 1988. – 356 с.
2. Крылов В. В. Информационные компьютерные преступления. – М.: Издательская группа ИНФРА М-НОРМА, 1997. – 276 с.
3. Информатика для юристов: Учебник / О. Э. Згадай, С. Я. Казанцев, Л. А. Казанцева; Под ред. С. Я. Казанцева. – М.: Мастерство, 2001. – 256 с.





**Цирлов
Валентин
Леонидович**

кандидат технических
наук, доцент

Правовые вопросы безопасности киберпространства в системе отечественных нормативных документов

***Аннотация:** Работа посвящена нормативно-правовым аспектам безопасности киберпространства. Дан обзор нового международного стандарта ISO/IEC 27032. Подробно рассмотрены руководящие принципы и механизмы безопасности киберпространства. Проведен анализ возможности использования стандарта в индустрии информационной безопасности.*

***Ключевые слова:** безопасность, киберпространство, руководящие принципы, стандарты, нормативный документ*

Международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (ISO/IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity) был разработан подкомитетом SC 27 «Информационные методы обеспечения безопасности» технического комитета ISO/ТС «Информационные технологии» почти два года назад, однако на сегодняшний день он практически не известен отечественным специалистам [1]. В то же время, с учетом того факта, что разрабатываемая сейчас «Концепция стратегии кибербезопасности Российской Федерации» [2] вызывает широкую общественную дискуссию, имеет смысл рассмотреть вопрос о целесообразности использования данного стандарта в отечественной практике.

Под **киберпространством** (*cyberspace*) в стандарте понимается комплексная среда, возникающая в результате взаимодействия людей, программного обеспечения и удаленных сервисов с использованием информационных и телекоммуникационных технологий. Принципиально важным при этом является вопрос взаимодействия между различными организациями, обеспечивающими существование киберпространства как единого целого: по мнению разработчиков стандарта, тот факт, что каждая из организаций решает вопросы обеспечения информационной безопасности самостоятельно, создает предпосылки для реализации принципиально новых угроз информационной безопасности. Именно обеспечение конфиденциальности, целостности и доступности информации в киберпространстве с учетом угроз такого рода и понимается под кибербезопасностью. Нетрудно заметить, что данное в стандарте определение кибербезопасности весьма отличается от применяемых в области международных правовых отношений [3-11].

Таким образом, **кибербезопасность** (*cybersecurity*) реализуется на стыке следующих трех компонентов системы обеспечения информационной безопасности (рис. 1):

- безопасность приложений;
- сетевая безопасность;
- безопасность сети Интернет.

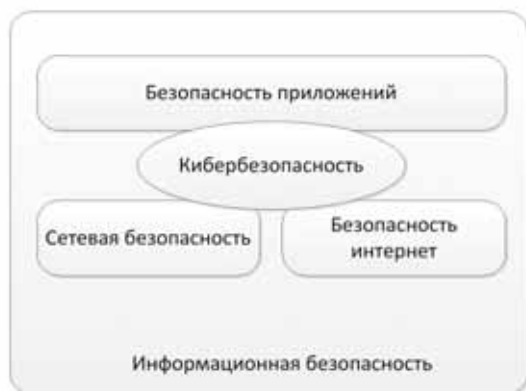


Рис. 1

Выделяются две основных категории участников информационного взаимодействия (рис. 2): провайдеры и потребители.



Рис. 2

Провайдеры могут предоставлять доступ как к среде информационного взаимодействия, так и к тем или иным сервисам. В качестве потребителей могут выступать физические лица и организации.

По сути, в содержательной части стандарт представляет собой набор рекомендаций для провайдеров и потребителей по обеспечению кибербезопасности. Если для физических лиц рекомендации сводятся в основном к выполнению рекомендаций провайдеров, то провайдеры должны реализовывать полноценную систему управления информационной безопасностью в соответствии с требованиями стандарта ISO/IEC 27001 [12]. Подчеркивается важность анализа рисков и управления рисками согласно ISO/IEC 27005 [13].

Механизмы безопасности, предлагаемые для киберпространства, представлены в Таблице 1.

Наибольший интерес представляет раздел стандарта, посвященный рекомендациям по организации совместного использования

информации, а также взаимодействия множества провайдеров и потребителей в киберпространстве. С точки зрения информационного взаимодействия в стандарте выделяются два типа участников: **организации, предоставляющие информацию** (IPO – Information Providing Organisation), и **организации, получающие информацию** (IRO – Information Receiving Organisation). Структурная схема подходов, предлагаемых для обеспечения безопасного взаимодействия, приведена на рис. 3.



Рис. 3

Так, например, в качестве требований по организации бизнес-процессов предлагаются классификация и категорирование информации, подписание соглашений о неразглашении, использование стандартов и организация эффективного планирования деятельности, связанной с совместным использованием информации. В качестве основных технических механизмов предлагаются стандартизация форматов данных, визуализация данных, использование криптографических механизмов и защищенных систем информационного обмена, подчеркивается необходимость тестирования технических средств. Общий порядок организации защищенного информационного взаимодействия предлагается строить в рамках схемы, приведенной на рис. 4.

Заключение

Нетрудно видеть, что стандарт во многом является интерпретацией традиционных подходов к построению систем управления информационной безопасности с акцентом на организацию защищенного информационного взаимодействия. При этом рекомендации по организации такого взаимодействия носят достаточно несистемный характер, что, на наш взгляд, и является основной причиной малой распростра-

Таблица 1

Категории	Механизмы безопасности
Безопасность приложений	Информирование потребителей о реализуемых провайдером подходах к обеспечению безопасности
	Защита сессий веб-приложений
	Контроль корректности вводимых данных
	Безопасность скриптов (прежде всего, в целях защиты от CSS-атак)
	Аудит кода и независимое тестирование приложений
	Подтверждение подлинности провайдера для потребителей
Защита серверов	Корректное конфигурирование серверов
	Реализация системы управления конфигурацией
	Реализация механизмов мониторинга и аудита
	Защита от вредоносного программного обеспечения
	Регулярное сканирование и анализ защищенности сетевых сервисов
Защита конечных пользователей	Корректное конфигурирование и обеспечение защиты операционных систем
	Корректное конфигурирование и обеспечение защиты прикладного программного обеспечения
	Защита от вредоносного программного обеспечения
	Защита от фишинга
	Использование стандартных механизмов безопасности веб-браузеров
	Использование персональных межсетевых экранов и систем обнаружения вторжений
	Использование автоматических обновлений программного обеспечения
Защита от атак, связанных с использованием методов социальной инженерии	Разработка и внедрение политик безопасности
	Категорирование и классификация информации
	Обучение и повышение осведомленности пользователей
	Тестирование сотрудников
	Использование технических механизмов, в первую очередь идентификации и аутентификации

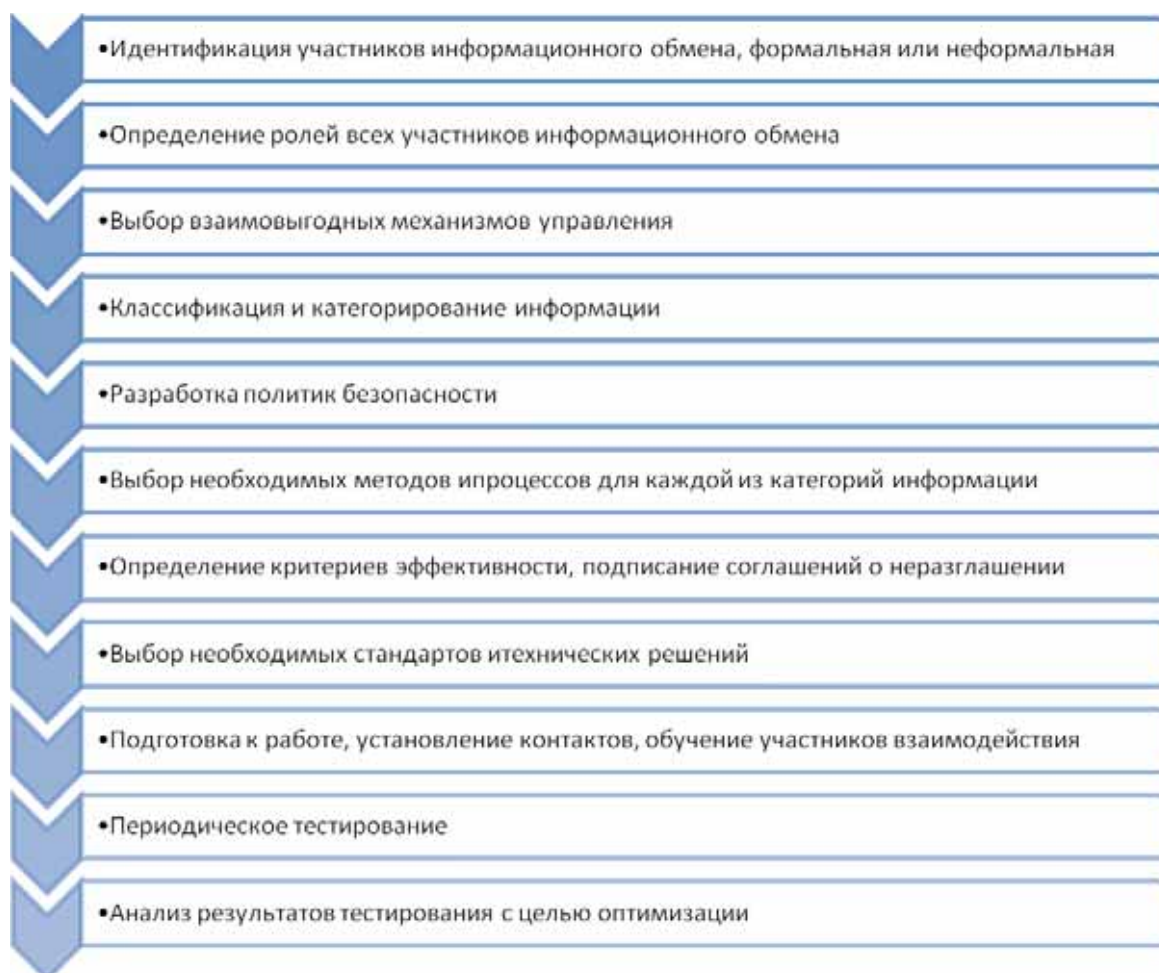


Рис. 4

ненности данного стандарта в индустрии информационной безопасности [14].

Безусловно, отдельные положения стандарта вполне могут быть использованы при разработке «Концепции стратегии кибербезопасности Российской Федерации» и последующих нормативных и методических документов, однако принятие аутентичного перевода ISO/IEC 27032 в качестве стандарта ГОСТ Р, на наш взгляд, вряд ли целесообразно.

Литература

1. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28–35.
2. Гаттаров Р. У. Концепция стратегии кибербезопасности // Вопросы кибербезопасности. 2014. № 1(2). С. 2–4.
3. Безкорвайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
4. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1 (1). С. 2–9.
5. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) // Вопросы кибербезопасности. 2014. № 1 (2). С. 5–12.
6. Гольчевский Ю. В., Некрасов А. Н. К вопросу о кибербезопасности интернет-пользователей // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 235–261.
7. Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Информационное право. 2013. № 5. С. 10–13.
8. Зубарев И. В., Жидков И. В., Кадушкин И. В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1 (1). С. 10–16.

9. Капто А. С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. № 7. С. 616.
10. Карцхия А. А. Кибербезопасность и интеллектуальная собственность (Часть 1) // Вопросы кибербезопасности. 2014. № 1 (2). С. 61–66.
11. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13–21.
12. Шахалов И. Ю., Дорофеев А. В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4–14.
13. Марков А. С., Цирлов В. Л. Управление рисками – нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63–67.
14. Матвеев В. А., Цирлов В. Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1 (1). С. 61–64.





**Атагимова
Эльмира
Исамудиновна**
кандидат юридических наук

Некоторые аспекты законодательного уровня обеспечения информационной безопасности в Российской Федерации

***Аннотация:** в статье рассматриваются некоторые аспекты законодательного регулирования в сфере информационной безопасности России. Освящены наиболее значимые нормативные правовые акты в рассматриваемой области.*

***Ключевые слова:** законодательство, закон, информация, безопасность, информатизация, персональные данные, интернет, защита, технологии.*



**Рамазанова
Ирина Маиловна**
кандидат педагогических
наук, доцент

В 21 веке развитие человечества сопровождается ростом объема накопленных знаний и сведений. Мы являемся свидетелями существенного повышения роли и места информации в жизни личности, общества, государства. За минувшее десятилетие произошел информационный взрыв. Информация сегодня превратилась в мощный реально ощутимый ресурс, имеющий даже большую ценность, чем природные финансовые, трудовые и иные ресурсы. Информация стала товаром, который продается и покупается.

Информационно-коммуникационные технологии, с каждым днем все больше проникая в различные сферы жизни общества, стали важнейшим фактором, влияющим на его развитие, а информатизация всех сфер человеческой деятельности выступает сегодня как важнейшая задача социального развития общества. С учетом бурного развития информационно-коммуникационных технологий углубляется зависимость человека и общества в целом от компьютерных и информационных систем, постоянно увеличивается число пользователей.

Информатизация открыла возможности для реализации одного из прав человека – право на доступ к широкому спектру информации, касающейся деятельности общества (при ограничениях доступа только к особым категориям информации, регламентированных соответствующими правовыми актами). Но нельзя не отметить, что информационные технологии, создавая условия для реализации права гражданина на доступ к информации, одновременно формируют среду, облегчающую нарушение другого его права – право на личную жизнь. Такая проблема, как проблема защиты информации от постороннего доступа и нежелательного воздействия, приобретает сегодня большое значение, так как это касается каждого человека. Фиксация персональных данных стала более доступной для всех заинтересованных в них государственных и негосударственных организаций, что открывает возможность вмешательства в личную жизнь граждан. При использовании технических средств связи информация подвергается воздействию случайных процессов (неисправностям и сбоям оборудования, ошибкам операторов и т. д.), которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки для доступа к ней посторонних лиц. Этому способствует

- › увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью средств вычислительной техники,
- › создание единых баз данных различного назначения и расширение круга пользователей, имеющих доступ к ресурсам вычислительной системы и находящимся в ней массивам данных,
- › автоматизация межмашинного обмена информацией, в т. ч. и на больших расстояниях. Человечество развивается по пути удобства. Создается огромное количество социальных сетей. Облачные технологии позволяют сохранять терабайты информации. Все это приводит к увеличению числа пользователей современного Интернета (свыше 2 миллиардов человек). В России, по разным оценкам, пользуются Интернетом около 60 млн. человек, а к концу 2014 года ожидается, что численность Интернет-пользователей составит около 80 млн. человек [1, с. 7]. Это способствует неуклонному росту числа компьютерных преступлений, также увеличиваются масштабы компьютерных злоупотреблений.

Таким образом, законодательное регулирование защиты информации, а также создание механизма, позволяющего согласовать сам процесс разработки законов с реалиями и прогрессом информационных технологий, давно является объективной необходимостью.

Анализируя законодательство Российской Федерации в области информационной безопасности, стоит отметить, что государственное звучание понятие «информационная безопасность» приобрело в 1989 г., когда по решению Президиума Верховного Совета СССР была создана рабочая комиссия по совершенствованию системы национальной безопасности [2, с. 208]. Большую роль в разработке проблематики информационной безопасности сыграл В. Н. Лопатин, который в 1989–1990 г. возглавляет рабочую группу, отвечающую за вопросы информационной безопасности в составе Комиссии по совершенствованию системы национальной безопасности. По предложениям группы, для более четкого определения предметной области законодательства в сфере обеспечения информационной безопасности предлагалось выделить 3 подгруппы объектов защиты [2, с. 207].

К ним относились:

1. защита информации и прав на нее (включая право на доступ к информации, право на тайну, права на объекты интеллектуальной собственности);

2. защита человека и общества от воздействия «вредной» информации;
3. защита информационных систем и прав на них (в том числе прав и интересов государства по сохранению единого информационного пространства в стране) [3, с. 480].

По предложениям этой комиссии был подготовлен и принят в 1992 г. Закон Российской Федерации «О безопасности» от 5 марта 1992 г. № 24446-1 [4]. Закон закрепил правовые основы обеспечения безопасности личности, общества и государства, определил систему безопасности и ее функции, установил порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

В Законе закреплено определение безопасности как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз», а под жизненно важными интересами понимается совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Названы основные объекты безопасности: это личность – ее права и свободы; общество его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная целостность [4]. Данный Закон действовал до 29 декабря 2010 г. с последующими дополнениями и изменениями. Он был отменен Федеральным законом «О безопасности» от 28.12.2010 г. № 390-ФЗ.

С дальнейшим развитием процессов информатизации научное развитие проблемы информационной безопасности продолжает углубляться. Система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности представлена в разработанной Концепции по национальной безопасности [5]. Основные направления обеспечения информационной безопасности Российской Федерации представлены в Доктрине информационной безопасности Российской Федерации [6], которая послужила основой для:

- › формирования государственной политики в области обеспечения информационной безопасности Российской Федерации,
- › подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации

Федерации и разработки целевых программ обеспечения информационной безопасности Российской Федерации. Далее основные направления обеспечения национальной безопасности Российской Федерации до 2020 года были освещены в Указе Президента Российской Федерации «О стратегии национальной безопасности Российской Федерации до 2020 года» от 12.05.2009 № 537. Данная стратегия является базовым документом по планированию развития системы обеспечения национальной безопасности Российской Федерации, в которой излагаются порядок действий и меры по обеспечению национальной безопасности. Она является основой для конструктивного взаимодействия органов государственной власти, организаций и общественных объединений для защиты национальных интересов Российской Федерации и обеспечения безопасности личности, общества и государства [7].

Переходя к рассмотрению непосредственно понятия «информационная безопасность», необходимо отметить сложность данного явления, что обуславливает многообразие подходов к формулировке понятия «информационная безопасность» [8].

В определении понятия «информационная безопасность», предложенным профессором В. Н. Лопатиным, говорится, что под информационной безопасностью следует понимать состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз [9, с. 79].

В Федеральном Законе от 04.07.96 № 85-ФЗ «Об участии в Международном информационном обмене» информационная безопасность определялась как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [10].

В своем докладе от 10 июля 2010 года № А/55/140 Генеральный секретарь ООН отметил, что информационная безопасность – это состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств как целостность, объективность, доступность и конфиденциальность [11]. Несмотря на то, что в данном определении находят свое отражение два аспекта информационной безопасно-

сти, в связи с тем, что эти аспекты не выделены четко, применение этого определения «информационной безопасности» может привести к некоторым трудностям [12].

В объединенной доктрине США «Информационные операции», определение информационной безопасности отражает только один аспект обеспечения информационной безопасности, а именно второй, связанный со средствами обработки информации. В соответствии с этим определением, информационная безопасность представляет собой защиту и оборону информации и информационных систем от несанкционированного доступа или модификации информации, находящейся в процессе хранения, обработки или передачи, а также от прекращения функционирования системы для санкционированных пользователей. Информационная безопасность включает меры, необходимые для обнаружения, документирования и ответа на эти угрозы [13].

Согласимся с мнением В. Н. Лопатина, что сформулированное им определение понятия информационной безопасности более соответствует логике Закона «О безопасности» и содержанию Концепции национальной безопасности [14].

Интересы государства в плане обеспечения конфиденциальности информации отражены в Законе «О государственной тайне» от 21.07.1993 № 5485-1 [15], который регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. В нем государственная тайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Закон определяет исчерпывающий перечень сведений, отнесенных к государственной тайне. Перечень подразделяется на 4 группы:

1. сведения в военной области;
2. сведения в области экономики, науки и техники;
3. сведения в области внешней политики и экономики;
4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении ко-

торых принято решение о применении мер государственной защиты.

Закон также закрепляет принципы отнесения сведений к государственной тайне, определяет порядок засекречивания относящихся к государственной тайне сведений и их рассекречивания, порядок распоряжения сведениями, составляющими государственную тайну, указывает органы защиты государственной тайны.

Одним из важнейших законодательных актов, положившим начало формированию общей системы нормативно-правовых актов, регулирующих процессы информатизации общества, явился Федеральный закон «Об информации, информатизации и защите информации» 1995 г. [16]. В Законе были определены такие понятия как «информация» – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; Закон ввел впервые в правовую лексику такое понятие как «информатизация» – это организационный, социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов, закрепил определение терминов «документированная информация» (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать, и «конфиденциальная информация» – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

В целом закон 1995 г. создал основу для упорядочения отношений в информационной сфере, а также послужил основой для последующего развития информационного законодательства. Этот закон действовал на протяжении более десяти лет и был заменен в 2006 г. Федеральным законом «Об информации, информационных технологиях и защите информации» [17]. На сегодняшний день Закон 2006 г. является одним из основополагающих российских законов, посвященных вопросам информационной безопасности. Настоящий закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;

- обеспечении защиты информации.

Статья 16 Закона «Об информации, информационных технологиях и защите информации» полностью посвящена защите информации (цитируем ее полностью):

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
 - 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
 - 2) соблюдение конфиденциальности информации ограниченного доступа;
 - 3) реализацию права на доступ к информации.
2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.
4. Владелец информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
 - 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
 - 2) своевременное обнаружение фактов несанкционированного доступа к информации;
 - 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
 - 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
 - 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
 - 6) постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обе-

спечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

В процитированной статье фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации.

Принятие Федерального Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» направлено на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации, а также на воплощение в жизнь международных обязательств Российской Федерации, взятых на себя при ратификации Конвенции Совета Европы о защите личности при обращении с персональными данными от 28 января 1981 года [18]. В этой связи не случайно, что в качестве основополагающих принципов обработки персональных данных законодатель декларирует соответствие способа обработки и объема обрабатываемых данных законным целям, определенным оператором до начала обработки, а также недопустимость объединения баз данных информационных систем персональных данных, созданных для несовместимых между собой целей.

Большое практическое и теоретическое значение имеет определение в комментируемом Законе понятия «персональные данные», под которыми понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). К таким данным относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы. Кроме того, законодателем установлены некоторые особые виды персональных данных, в отношении которых действуют повышенные меры защиты от несанк-

ционированной обработки и распространения. Это информация касается расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни физического лица, а также биометрические персональные данные – сведения, характеризующие физиологические особенности человека (ст. 10 и 11 Закона).

Данный закон устанавливает порядок доступа к персональным данным граждан (физических лиц) и призван обеспечить эффективную защиту прав и свобод человека и гражданина в соответствии с основными правами и свободами, провозглашенными Конституцией РФ.

Согласно ст. 17 Конституции РФ, в России признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права. Ст. 23 и 24 Конституции РФ устанавливают, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. При этом сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. На органы государственной власти и органы местного самоуправления, их должностных лиц возлагается обязанность обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

В современном мире почти каждый желающий может найти в Интернете информацию о персональных данных граждан. При этом свои персональные данные граждане раскрывают зачастую сами, например, оформляя покупку товара с доставкой на дом, регистрируясь на веб-сайте. Но далеко не всегда лица, получающие такую информацию, добросовестно сохраняют ее. Во всем мире стремятся защищать персональные данные на уровне государства, принимая законы, регулирующие порядок сбора, хранения и использования сведений о гражданах страны. Обеспечивая защиту персональных данных, РФ укрепляет правовую защищенность и безопасность личности и создает благоприятную обстановку для всестороннего развития граждан и общества в целом. Кроме того, по мнению многих российских экспертов в области права, одной из целей принятия комментируемого

Закона явилась необходимость устранения некоторых барьеров в торговле со странами Евросоюза, т. к. согласно Директиве Евросоюза персональные данные могут передаваться только в страны, обеспечивающие такой же уровень защиты, как и в Европе. Поэтому положения комментируемого Закона отчасти повторяют положения европейского законодательства в данной сфере [19].

Литература

1. Доменные имена. – М.: Российская государственная академия интеллектуальной собственности, 2013.
2. Сергиенко Л.А. История формирования информационного права в СССР и Российской Федерации 1960-2000 гг. Монография. – М.: ЮРКОМПАНИ, 2013.
3. Концепция развития законодательства в сфере обеспечения информационной безопасности. Изд. Государственной Думы РФ. М., 1998. С. 158. Цитир. по учебнику: И. Л. Бачило, В. Н. Лопатин, М. А. Федотов «Информационное право». Изд. СПб. Юрид. Цент пресс, 2001.
4. Закон РФ от 05.03.1992 № 2446-1 (ред. от 26.06.2008) «О безопасности». (Документ утратил силу в связи с принятием Федерального закона «О безопасности» от 28.12.2010 № 390-ФЗ).
5. Указ Президента РФ от 17.12.1997 № 1300 (ред. от 10.01.2000) «Об утверждении Концепции национальной безопасности Российской Федерации» (Документ утратил силу с 12 мая 2009 года в связи с изданием Указа Президента РФ «О стратегии национальной безопасности Российской Федерации до 2020 года» от 12.05.2009 № 537).
6. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895).
7. Указ Президента Российской Федерации «О стратегии национальной безопасности Российской Федерации до 2020 года» от 12.05.2009 № 537.
8. Днепровский А. Г. Правовые проблемы нового международного информационного порядка. – М.: Наука, 1989.
9. Лопатин В. Н. «Информационная безопасность России: Человек. Общество. Государство». – СПб.: Фонд «Университет», 2000.
10. Федеральный закон от 04.07.1996 № 85-ФЗ (ред. от 29.06.2004) «Об участии в международном информационном обмене». (Документ утратил силу в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ).
11. Документ ООН A/55/140. С. 4.
12. Ермишина Е. В. Международный обмен информацией: правовые аспекты. – М.: Международный. отношения, 1988.
13. Joint Doctrine for Information operations. Jom Pub 3-13. 9 October 1998. P. GL-7.
14. Лопатин В. Н. Реальность – основа концепции информационной безопасности России // PC Week/RE. 1999, № 12.
15. Закон РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013) «О государственной тайне».
16. Федеральный закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003) «Об информации, информатизации и защите информации». (Документ утратил силу в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ).
17. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.02.2014).
18. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
19. [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/>, свободный (загрузка).





**Шахалов
Игорь Юрьевич**

К вопросу об интегрировании систем менеджмента качества и информационной безопасности

***Аннотация:** рассмотрены международные стандарты ИСО 27001 и ИСО 9001. Проведен анализ сходств и различий системы менеджмента качества и системы менеджмента информационной безопасности. Показана возможность интегрирования системы менеджмента качества и системы менеджмента информационной безопасности. Приведены основные этапы построения и внедрения интегрированной системы менеджмента информационной безопасности. Показаны преимущества интегрированного подхода.*

***Ключевые слова:** системы менеджмента, информационная безопасность, интегрированные системы менеджмента, СМИБ, СМК, ИСО 27001.*



**Райкова
Наталья Олеговна**

Введение

В современном мире с появлением распространенных и удобных технических устройств обозначилась довольно остро проблема защиты информации. Наряду с выпуском качественной продукции или оказанием услуг предприятиям и организациям важно сохранять нужную информацию в тайне от конкурентов, чтобы оставаться на выгодных позициях на рынке. В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки.

Таким образом, лидерами на рынке становятся организации, придерживающиеся лучших мировых практик, содержащих требования, руководства по внедрению систем управления бизнес-процессами организации. Лучшими стандартами по разработке, внедрению, мониторингу и улучшению таких систем являются документы Международной Организации по стандартизации (ISO). Особое внимание необходимо уделить стандартам серий ISO 900х и ISO 2700х, в которых собраны лучшие практики по внедрению системы менеджмента качества (СМК) и системы менеджмента информационной безопасности (СМИБ) [1, 2].

Система менеджмента качества, внедренная в соответствии с требованиями стандарта ISO 9001, давно признана неотъемлемым атрибутом успешной компании, производящей высококачественную продукцию или оказывающей услуги высокого класса. Сегодня наличие сертификата соответствия является одновременно эффективным маркетинговым решением и механизмом контроля процессов производства [3]. Аудит СМК является развитым направлением бизнеса.

Ежедневно усиливается зависимость успешной деятельности компании от корпоративной системы защиты информации. Это объясняется увеличением объема жизненно важных данных, обрабатываемых в корпоративной информационной системе. Информационные системы усложняются, растет и число уязвимостей, обнаруживаемых в них. Аудит СМИБ позволяет оценить текущее состояние безопасности функционирования корпоративной информационной системы,

оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы компании [4-6].

Так как стандарт ISO 9001 давно занял лидирующее положение по количеству сертификатов в мире, а стандарт ISO 27001 показывает тенденцию к возрастанию сертификации системы менеджмента информационной безопасности, целесообразно рассмотреть возможное взаимодействие и интеграцию СМК и СМИБ.

Интегрирование стандартов

На первый взгляд, менеджмент качества и информационная безопасность – совершенно различные области. Однако на практике они тесно связаны и образуют одно целое (Рисунок 1). Удовлетворение потребностей клиентов, составляющее объективную цель качества, с каждым годом все больше зависит от доступности информационных технологий и от безопасности данных, для поддержания которых и используется стандарт ISO 27001. С другой стороны, стандарт ISO 9001 точно соответствует корпоративным целям организации, помогая обеспечивать менеджмент информационной безопасности. Благодаря комплексному подходу ISO 27001 может быть эффективно интегрирован в существующие СМК или осуществляться вместе с СМК.

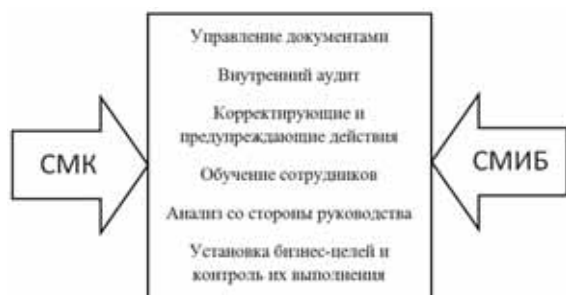


Рис. 1. Сферы взаимодействия и схожести СМК и СМИБ

Более 27 200 организаций самых различных отраслей в более чем 100 странах мира сертифицированы на соответствие ISO 9001:2008 по управлению качеством. В зависимости от рынка и требований законодательства, многие организации все чаще вынуждены иметь дело с ИБ. В этой связи, интеграция системы управления предлагает реальные возможности. Комплексный подход также интересен для компаний, которые не использовали любой процесс управления до сих пор. Стандарты ИСО качества (ISO 9001), охраны окружающей среды (ISO 14000), информационной безопасно-

сти (ISO 27001) и управления ИТ-услугами (ISO 20000) имеют аналогичную структуру и процессный подход. Это дает синергию, которая окупается: на практике интегрированная система менеджмента на текущую эксплуатацию экономит от 20 до 30 процентов от общего объема расходов на оптимизацию системы, проверок и ревизий [7-9].

Стандарты информационной безопасности и управления качеством направлены на постоянное совершенствование в соответствии с моделью Plan-Do-Check-Act (PDCA, «планирование – осуществление – проверка – действие»), известной как «цикл Деминга» (см. рис. 2) [10,11]. Кроме того, они похожи по своей структуре, как показано в таблице соответствия в приложении С стандарта ISO 27001. В обоих стандартах определены понятия процессного подхода, области действия, требования к системе и документации, а также административная ответственность. В обоих случаях структура заканчивается внутренним аудитом, анализом со стороны руководства и улучшением системы. В этом обе системы взаимодействуют. Например, ISO 9001 требует управления несоответствующей продукцией. Аналогично, в стандарте ISO 27001 существует требование по управлению инцидентами для устранения сбоев.



Рис. 2. Цикл Деминга

Различия между стандартами полезно дополняют друг друга, что решительно способствует повышению делового успеха. Например, ISO 9001 требует определения корпоративных целей, ориентированности на клиента и измеримости, в какой степени цели и задачи выполнены. Это три вопроса, которые не находятся в центре интересов ISO 27001. В свою очередь, этот стандарт придает первостепенное значение управлению рисками для поддержания непрерывности бизнеса и предлагает подробную помощь в реализации СМИБ. По сравнению

с этим, ISO 9001 является в большей степени теоретическим стандартом.

ISO 27001 – стандарт не только для ИТ

Многие считают, что стандарт ISO 27001 предназначен только для ИТ-процессов, однако на самом деле это не так. Основополагающим пунктом по внедрению СМИБ стандарта ISO 27001 служит определение активов [12].

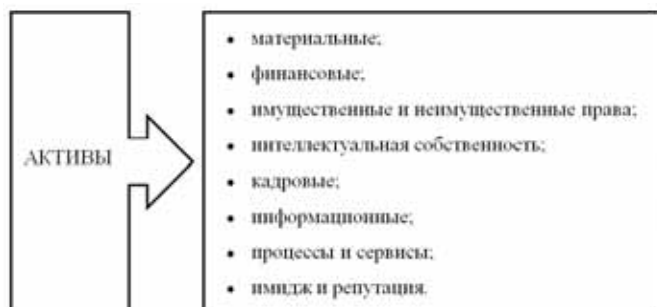


Рис. 3. Виды активов

Под активом понимается все, что представляет для компании ценность (Рисунок 3). То есть активом могут быть: человеческие ресурсы, инфраструктура, инструменты, оборудование, средства коммуникации, службы и любые другие активы, включая услуги по поставке закупаемой продукции. Исходя из процессов, компания определяет, какие у нее есть активы и какие активы задействованы в критичных процессах, производит оценку ценности активов. И уже только после этого производится оценка рисков по всем ценным активам. Таким образом, СМИБ предназначена не только для цифровой информации, которая обрабатывается в автоматизированной системе. Например, некоторые из наиболее критичных процессов связаны

с хранением печатных копий информации, что также учтено в ISO 27001. СМИБ охватывает все способы, с помощью которых может храниться важная информация в вашей компании: начиная от того, как ваши электронные письма защищены, заканчивая тем, где в здании хранятся личные дела сотрудников.

Поэтому огромное заблуждение считать, что раз стандарт направлен на построение системы менеджмента информационной безопасности, то это может относиться только к данным, хранящимся в компьютере. Даже в наш цифровой век все еще много информации отражено на бумажных носителях, которые тоже должны быть надежно защищены.

ISO 9001 не может удовлетворять потребностям компании в ИБ, поскольку он узко направлен на качество продукции. Поэтому очень важно внедрять в компании ISO 27001. На первый взгляд специалисту может показаться, что оба стандарта очень общие, и не имеют конкретики. Однако это не так: в стандарте ISO 27001 описан практически каждый шаг по внедрению и контролю функционирования СМИБ (Рисунок 4).

Основные этапы построения системы менеджмента информационной безопасности

Основные этапы построения СМИБ проиллюстрированы на рисунке 4 [1]. Рассмотрим их подробнее.

Этап 1. Подготовка планов мероприятий. На данном этапе специалисты осуществляют сбор организационно-распорядительных документов (ОРД) и других рабочих материалов,



Рис. 4. Этапы построения СМИБ

касающихся построения и функционирования информационных систем компании, планируемых к использованию механизмов и средств обеспечения ИБ. Кроме того, составляются, согласуются и утверждаются у руководства компании планы мероприятий по этапам работ.

Этап 2. Проверка на соответствие ISO/IEC 27001:2005. Интервьюирование и анкетирование менеджеров и сотрудников подразделений. Анализ СМИБ компании на соответствие требованиям стандарта ISO/IEC 27001:2005.

Этап 3. Анализ нормативных и организационно-распорядительных документов, опирающихся на организационную структуру компании. По его результатам определяется защищаемая область действия (ОД) и разрабатывается эскиз политики ИБ компании.

Этап 4. Анализ и оценка рисков ИБ. Разработка методики по управлению рисками компании и их анализу. Анализ информационных ресурсов компании, в первую очередь ЛВС, с целью выявления угроз и уязвимостей защищаемых активов ОД. Инвентаризация активов. Проведение консультаций для специалистов компании и оценка соответствия фактического и необходимого уровня безопасности. Расчет рисков, определение текущего и допустимого уровня риска для каждого конкретного актива. Ранжирование рисков, выбор комплексов мероприятий по их снижению и расчет теоретической эффективности внедрения [13].

Этап 5. Разработка и реализация планов мероприятий по ИБ. Разработка положения о применимости контролей в соответствии с ISO/IEC 27001:2005. Разработка плана учета и устранения рисков. Подготовка отчетов для руководителя компании.

Этап 6. Разработка нормативных и ОРД. Разработка и утверждение окончательной политики ИБ и соответствующих ей положений (частных политик). Разработка стандартов, процедур и инструкций, обеспечивающих нормальное функционирование и эксплуатацию СМИБ компании.

Этап 7. Внедрение комплексных мероприятий по снижению рисков ИБ и оценка их эффективности в соответствии с утвержденным руководством планом обработки и устранения рисков.

Этап 8. Обучение персонала. Разработка планов мероприятий и внедрение программ по обучению и повышению компетенции сотрудников компании с целью эффективного донесения принципов ИБ до всех сотрудников и

в первую очередь тех, кто работает в структурных подразделениях, обеспечивающих ключевые бизнес-процессы.

Этап 9. Формирование отчетности. Систематизация результатов обследования и подготовка отчетности. Представление результатов работ для руководителей компании. Подготовка документов к лицензированию на соответствие ISO/IEC 27001:2005 и передача их в сертифицирующую организацию.

Этап 10. Анализ и оценка результатов внедрения СМИБ на основании методики, оценивающей надежность функционирования СМИБ компании. Разработка рекомендаций по совершенствованию системы управления ИБ компании.

Анализируя каждый этап внедрения СМИБ, можно сказать, что ISO 27001 имеет четкую структуру и требования, которые позволят выстроить работающую систему, в которой будет взаимодействие на всех нужных уровнях. Но нельзя забывать, что основное отличие СМИБ и СМК в том, что первая система сосредоточена на информационной безопасности.

Важность информационной безопасности в современном мире

Сегодняшний бизнес не может существовать без информационных технологий. Известно, что около 70% мирового совокупного национального продукта зависят тем или иным образом от информации, хранящейся в информационных системах. Повсеместное внедрение компьютеров создало не только известные удобства, но и проблемы, наиболее серьезной из которых является проблема информационной безопасности [14].

Руководители компаний должны осознавать важность информационной безопасности, научиться прогнозировать тенденции в этой области и управлять ими. В этом им может помочь внедрение СМИБ, которая по своей структуре имеет потенциал к развитию, прозрачность управления, гибкость к любым изменениям. Наряду с элементами управления для компьютеров и компьютерных сетей стандарт ISO 27001 уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, нормативным требованиям, в то же время отдельные технические вопросы детализированы в других стандартах серии

ИСО 27000 [1, 13, 15-17]. Преимуществ внедрения в компанию СМИБ очень много, часть из них представлена на рис. 5.



Рис. 5. Преимущества внедрения системы менеджмента информационной безопасности

Следует указать на преимущества ISO 27001:

Демонстрация компетентности безопасности. ISO 27001 представляет собой практическое руководство для организации, которое помогает сформулировать требования безопасности для обеспечения требуемого уровня защищенности и выполнения конкретных целей безопасности. Особенно важно организациям быть компетентными в четырех областях управления безопасностью, включая: определение и оценку активов компании, оценку рисков и определения критериев приема риска, управление и принятие этих пунктов, и постоянное улучшение общей программы безопасности организации.

Обеспечение уверенности клиентов. ISO 27001 обеспечивает независимое доказательство того, что программы корпоративного управления поддерживаются лучшими, передовыми, международными практиками. Сертификация на соответствие ISO 27001 обеспечивает спокойствие корпорациям, стремящимся продемонстрировать добросовестность клиентам, акционерам и потенциальным партнерам, а главное, показать, что в компании успешно реализована надежная система менеджмента информационной безопасности. Для многих серьезно регулируемых отраслей, таких как финансы или Интернет-услуги, выбор поставщика может

быть ограничен теми организациями, которые уже сертифицированы по ISO 27001.

Более эффективное использование ресурсов. Благодаря использованию процессного подхода возможна оптимизация процессов, происходящих в компании. Что влечет за собой уменьшение использования ресурсов, например, времени.

Постоянное улучшение. СМИБ использует PCDA модель, что позволяет регулярно проверять состояние всей системы, проводить анализ и совершенствовать систему управления [7].

1. Имидж, бренд. Сертификация на соответствие ISO 27001 открывает перед компанией широкие возможности: выход на международный уровень, новые партнерства, большее количество клиентов, новые контракты, успех в тендерах. Наличие СМИБ в компании – это показатель высокого уровня развития.
2. Гибкость СМИБ. Независимо от изменений процессов, новых технологий, основа структуры СМИБ остается действенной. СМИБ достаточно легко подстраивается под нововведения, путем модернизации существующих и внедрения новых контрмер.
3. Масштабируемость внедрения стандарта. Так как ISO 27001 предполагает определение области действия, это позволяет сертифицировать лишь часть процессов. Можно начать внедрять СМИБ в наиболее значимую для компании ОД, а уже позже расширять.
4. Аудит. Многие российские компании воспринимают аудиторские работы как катастрофу. ISO 27001 показывает международный подход к проведению аудитов: прежде всего заинтересованность компании в том, чтобы действительно соответствовать стандартам, а не делать сертификацию кое-как, лишь «для галочки».
5. Регулярные внутренние или внешние аудиты позволяют исправлять нарушения, совершенствовать СМИБ, значительно снизить риски. В первую очередь, это нужно компании для собственного спокойствия, что у них все в порядке и риски убытков минимизированы. А уже второстепенно – сертификат соответствия, который подтверждает для партнеров или клиентов, что этой компании можно доверять.
6. Прозрачность управления. Использование стандарта ISO 27001 дает достаточно четкие инструкции по созданию управления, а

также требования к документации, которая должна быть в компании. Проблема многих компаний в том, что существующие документы для определенных отделов просто не читаются, ибо разобраться, что и кому предназначается, зачастую невозможно из-за запутанности системы документации. Иерархичность уровней документации, от политики информационной безопасности до описания определенных процедур, делает использование существующих правил, регламентов и прочего намного легче. Также внедрение СМИБ предполагает обучение персонала: проведение семинаров, рассылок, вывешивание предупреждающих плакатов, что значительно повышает осведомленность об ИБ среди обычных служащих.

Вывод

В заключение следует отметить, что в современном бизнесе неотъемлемость базовой системы менеджмента качества, выстроенной в соответствии с требованиями стандарта ISO 9001, и завоевывающей позиции системы менеджмента информационной безопасности очевидна.

Сегодня лидером рынка станут компании, которые отслеживают не только показатели качества продукции и услуг, но и уровни конфиденциальности, целостности и доступности информации о них. Также немаловажным фактором успеха является прогнозирование и оценка рисков, что требует грамотного подхода и использования лучших международных практик. Совместное внедрение и сертификация систем менеджмента качества и информационной безопасности поможет решить широкий спектр задач для любой отрасли промышленности или торговли, что в свою очередь приведет к качественному повышению уровня оказываемых услуг.

Литература

1. Дорофеев А. В., Шахалов И. Ю. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4–14.
2. Чашкин В. Н. Управление информационной безопасностью как элемент системы управления информационно-технологической деятельностью организации // Безопасность информационных технологий. 2009. № 1. С. 123–124.
3. Горячев В. В. Новый ГОСТ на СМК. Основные отличия от ГОСТ РВ 15.002–2003 // Методы менеджмента качества. 2013. № 7. С. 18–23.
4. Доценко С. П., Пшенецкий С. П. Подход к построению модели систем менеджмента информационной безопасности // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2009. № 53. С. 47–56.
5. Каменев А. В., Загоритко Е. В. Модель системы менеджмента информационной безопасности на предприятии (в организации) // Интеллект. Инновации. Инвестиции. 2013. № 1. С. 111–114.
6. Соловьев А. М. Нормативно-методическая база в области обеспечения информационной безопасности // Экономика, статистика и информатика. Вестник УМО. 2012. № 1. С. 174–181.
7. Козин И. Ф., Лившиц И. И. Информационная безопасность. Интеграция международных стандартов в систему информационной безопасности России // Информатизация и связь. 2010. № 1. С. 50–55.
8. Колодин В. С. Сертификация интегрированных систем менеджмента // Вестник Иркутского государственного технического университета. 2010. Т. 41. № 1. С. 44–48.
9. Меркушова Н. И., Науменко Ю. А., Меркушова Ю. А. Интегрированные системы менеджмента: предпосылки создания на российских предприятиях // Молодой ученый. 2013. № 12 (59). С. 327–331.
10. Воропаева В. Я., Щербов И. Л., Хаустова Е. Д. Управление информационной безопасностью информационно-телекоммуникационных систем на базе модели «Plan-Do-Check-Act» // Наукові праці Донецького національного технічного університету. Серія: “Обчислювальна техніка та автоматизація”. 2013. № 2 (25). С. 104–110.
11. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67–73.
12. Шпер В. Л. О стандарте ISO/IEC 27001 // Методы менеджмента качества. 2008. № 3. С. 60–61.
13. Марков А. С., Цирлов В. Л. Управление рисками – нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63–67.
14. Матвеев В. А., Цирлов В. Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федера-

- ции в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С. 61–64.
15. Барабанов А. В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). С. 37–41.
16. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28–35.
17. Храмцовская Н. Что нужно знать руководителю об информационной безопасности // Кадровик. 2009. № 4. С. 061–072.





Шихнабиева

Тамара

Шихгасановна

доктор педагогических
наук, профессор

О некоторых подходах к модернизации образовательных систем с использованием интеллектуальных методов и моделей

Аннотация: для эффективного функционирования информационных систем, используемых в образовании, необходимо решить ряд проблем, связанных с представлением, обработкой и использованием знаний. Для доступа и эффективного использования знаний необходима их классификация и структуризация. В работе предложены некоторые подходы к совершенствованию и разработке обучающих систем на основе достижений системного анализа, кибернетики, синергетики.

Ключевые слова: образовательные технологии, дистанционное обучение, семантическая сеть, адаптивная семантическая модель, автоматизированная обучающая система.

Известно, что информатизация общества – это социальный процесс, который обеспечивает активное использование постепенно расширяющегося интеллектуального потенциала общества с применением средств информационных и коммуникационных технологий.

Следует отметить, что методы обучения и развития, социальные и профессиональные требования, связанные с построением развитого общества, в значительной степени зависят от уровня использования информационных и коммуникационных технологий в образовательном процессе.

Современные информационные технологии и стремительное расширение разнообразия сетевых образовательных услуг вызвали поток инноваций по реорганизации существующих образовательных систем всех уровней образования. Как следствие, меняется характер и динамика взаимодействия между учащимися и учителями. Это существенным образом влияет на выбор методов, форм и технологий обучения.

В сегодняшней практике сложилось определенное противоречие: стало очевидным, что получение знаний по базовому курсу информатики недостаточно для современного учителя. Информационные и коммуникационные технологии развиваются гораздо быстрее, чем возможности их использования в образовательных целях. Для разрешения сложившейся проблемной ситуации необходимо организовать непрерывное использование информационных и коммуникационных технологий при преподавании

смежных дисциплин, а также непрерывное повышение квалификации специалистов в области информатики.

Обучение с использованием информационных ресурсов Интернет и Интранет является катализатором в становлении новой, прогрессивной теории преподавания и учения, ориентированной на развитие личности учащегося, способного реализовывать свои собственные, в том числе и образовательные проекты и стремящегося к самоусовершенствованию на протяжении всей жизни.

Новые механизмы передачи информации оказали существенное влияние на все стороны образовательной системы. Как следствие, возникает острая необходимость в анализе особенностей применения закономерностей общей теории обучения – дидактики в условиях широкого использования информационных технологий и распределенных в пространстве и времени процессов сетевого обучения.

Функции преподавателя и учащегося в образовательной информационной среде также претерпевают коренные изменения по сравнению с традиционной учебной средой. В учебных средах с использованием информационных и коммуникационных технологий учащийся работает в собственном темпе и без постоянного непосредственного контакта с преподавателем. В данном случае преподаватель из основного носителя и транслятора знаний превращается в советника и консультанта учащегося. Препо-

даватель управляет процессом обучения, имея в своем распоряжении мощный инструмент – компьютер, с его возможностями доставки, хранения, обработки всех видов информации, для демонстрации учебной информации, тренировки и самоконтроля. Учащийся, в свою очередь, получает мощное технологическое средство поддержки самостоятельного интеллектуального труда и доступа к информационной среде, не ограниченного пространством и способом передачи. Учащемуся становятся доступными знания о содержании и методе обучения, которые до сих пор были прерогативой преподавателя.

Интенсивная работа в условиях информационного комфорта активизирует познавательную деятельность учащихся и усиливает творческие компоненты труда преподавателя. Средства информационных и коммуникационных технологий в обучении освобождают преподавателя от множества функций, ставших рутинными в его повседневной деятельности.

Однако для оптимизации использования новых широких возможностей информационной среды настоятельно требуются теоретическое осмысление и технологическая поддержка решения ряда практических задач, связанных с организацией учебного процесса. В связи с этим одной из актуальнейших дидактических задач становится задача эффективного использования информационных и коммуникационных технологий для управления учебным процессом со стороны самого учащегося. Реализация именно такой методической идеи представляется сегодня наиболее перспективной в контексте мировой и отечественной практики обучения.

Следует отметить, что общая задача оптимизации процесса обучения на практике сводится к ряду частных подзадач. Среди них прежде всего следует назвать:

- уточнение тезауруса образовательной информационной среды,
- разработку методик личностно-ориентированных технологий сетевого обучения,
- оценку дидактической эффективности и оптимизацию структуры и формы учебно-методических материалов,
- отработку методик и технологических средств управления учебным процессом, и др.

Проблемы создания эффективных систем обучения, поиска новых педагогических приемов и средств преподавания, особо обострились в последние десятилетия XX века после появления в массовом количестве персональных компьютеров, электронной почты и сети Интер-

нет. Средства информационных и коммуникационных технологий значительно увеличили объем доступной информации, качество и скорость работы с ней по сравнению с предшествующим периодом. Вместе с тем, цифровые технологии породили ряд проблем поиска нужной информации за «разумное время» в громадных базах данных современных информационных систем [1], что делает почти невозможным их использование в учебном процессе без предварительных настроек, создания специальных фильтров и систем поиска нужной информации для учебных и образовательных задач. Проблемы в современном образовательном процессе носят глобальный характер, т. к. в настоящее время нет ни одной развитой страны мира, которая бы не пыталась поставить перед собой задачи изменения системы образования с целью повышения ее эффективности.

Для реализации задач, стоящих перед современным образованием, нужна эффективная, гибкая, модульная система, базирующаяся на наиболее передовых технологиях и средствах обучения.

Одним из актуальных направлений исследований обучения с использованием информационных и коммуникационных технологий является анализ стиля обучения пользователя. Каждый стиль обучения накладывает условия на вид, структуру, форму и методы компоновки учебного материала. Иными словами, необходима личностная ориентированность представляемого учебного материала, что позволяет существенно повысить мотивацию и эффективность процесса обучения. В данном случае образовательная информационная среда адаптируется к каждому пользователю, обучающемуся в ней.

Отличительная черта современного этапа – поиск педагогами-исследователями способов применения формальных методов для описания процесса обучения с использованием аппаратов системного анализа, кибернетики, синергетики, с учетом, развитием и расширением понятий, принципов и достижений дидактики.

Процесс обучения с использованием информационных и коммуникационных технологий является одним из видов информирования, основой которого является семантический диалог [2]. В нашей работе мы рассматриваем обучение с использованием информационных и коммуникационных технологий как информационную семантическую систему, а учебный материал, подлежащий усвоению, – как семантическую информацию. Для рассматриваемой

системы возникает необходимость решения проблемы формализации семантического диалога, обеспечивающая повышение эффективности ее функционирования.

Для успешного решения указанной проблемы необходимо решить две задачи: формализация процесса информирования и формализация семантической информации.

Формализация семантической информации предполагает решение одной из важных задач теории информационных семантических систем, а также искусственного интеллекта – представление знаний. В нашей работе учебный материал представлен в виде адаптивных семантических моделей (АСМ), в вершинах которых находятся понятия предметной области, а дуги означают различные связи между ними [3]. В виде адаптивных семантических моделей представлен непосредственно и сам процесс обучения.

Предлагаемый нами подход основан на структуре человеческих знаний, принципах разработки систем искусственного интеллекта и информационных семантических систем, которым является процесс обучения. Он объединяет процедурный и декларативный подход к представлению знаний, базируется на теории семантических сетей и продукционных правил.

Преимуществом семантических сетей как модели представления знаний и непосредственно самого процесса обучения является наглядность описания предметной области, гибкость, адаптивность к цели обучаемого. Однако свойство наглядности с увеличением размеров и усложнением связей базы знаний предметной области теряется. Кроме того, возникают значительные сложности по обработке различного рода исключений. Для преодоления указанных проблем используют метод иерархического описания сетей (выделение на них локальных подсетей, расположенных на разных уровнях).

Такой подход к организации знаний при разработке обучающих информатике интеллектуальных систем позволяет значительно сократить время обучения и уменьшить объем памяти, занимаемой базой знаний и данных.

Модель в виде иерархической семантической сети, являясь логической структурой изучаемой предметной области, показывает также последовательность изложения учебного материала, что важно для молодых учителей.

На основе установленных типов понятий и видов связей можно построить модель рассматриваемой предметной области в виде многоуровневой адаптивной семантической сети. Сле-

дует отметить, что процесс подобной структуризации знаний достаточно трудоемкий. Однако это наглядная и более выразительная модель, отображающая логическую структуру учебного материала, которая позволяет одновременно видеть все понятия и их взаимосвязи по изучаемой теме, что имеет немаловажное значение для систем обучения на основе информационных и коммуникационных технологий.

Известно, что обучающие технологии традиционно используются в системе образования в качестве средства передачи информации и обучения. В процессе обучения учащиеся постигают смысл сообщений, хранящихся в компьютерах, и «взаимодействуют» с обучающей технологией. При таком использовании компьютера мышление обучаемых ограничивается и контролируется обучающей системой. Отсюда следует, что необходимо расширить возможности компьютера в плане представления информации. При создании адаптивно-семантической модели учебного материала обучаемые используют персональный компьютер в качестве инструмента представления своих знаний.

Использование компьютера в качестве инструмента построения знаний вовлекает обучаемых в процесс формирования знаний, что способствует их пониманию и усвоению, а не только воспроизведению в памяти того, что получено от преподавателя.

Отметим также, что выразительность и образность семантических сетей является важным их преимуществом, позволяющим легче выявить и показать логические отношения в учебном материале.

Если при обычной методике обучения еще можно обойтись рассмотрением только глобальных структур, то при обучении с использованием информационных и коммуникационных технологий связь и последовательность элементов учебного материала оказывается стержневой проблемой. Использование адаптивных семантических моделей в качестве инструмента построения структуры знаний позволяет передать взаимодействие с компьютером в ведение самих обучаемых, что дает им возможность самостоятельно представлять и выражать свои знания. В процессе создания адаптивных семантических моделей обучаемые должны анализировать структуры своих собственных знаний, что помогает им включать новые знания в структуры уже имеющихся знаний. Результатом такого процесса является эффективное использование приобретенных знаний.

Итак, представление учебного процесса в виде адаптивных семантических моделей позволяет обеспечивать

- › индивидуальный темп обучения при реализации обратной связи;
- › деятельностный подход при выборе решения задачи с учетом учебных ситуаций;
- › связь новых понятий с существующими понятиями и представлениями, что улучшает понимание;
- › осуществление глубокой обработки знаний, что повышает способность применять знания в новых ситуациях.

Приведенные выше сведения, соображения и рекомендации позволили систематизировать и обобщить основные методологические положения по представлению и контролю знаний в обучающих системах с использованием адаптивных семантических моделей.

1. Для представления и контроля знаний в системах обучения в качестве основных обеспечивающих эти задачи моделей целесообразно использовать адаптивные семантические модели, учитывая их возможности по более адекватному описанию взаимодействия различных понятий и разделов учебных дисциплин и их адаптацию к быстрому изменению содержания этих дисциплин и уровню знаний обучаемых.
2. Адаптивные семантические модели обеспечивают глубокую структуризацию изучаемых понятий и явлений предметной области, которая может быть представлена наглядно в виде сложных иерархических моделей, способных идентифицировать знания обучаемых и их способности, в полной мере использовать достижения современных систем искусственного интеллекта.
3. Основными этапами структуризации знаний при разработке адаптивных семантических моделей в большинстве случаев можно считать:
 - › определение входных и выходных данных;
 - › составление словаря терминов;
 - › выявление объектов и понятий;
 - › выявление связей между понятиями;
 - › выявление метапонятий и детализация понятий;
 - › построение пирамид знаний;
 - › определение отношений между понятиями;
 - › определение стратегии принятия решений.
4. При построении пирамид знаний должны использоваться наглядные материалы: рисунки, схемы, диаграммы, графики и др.; уровни пирамиды знаний чаще всего возникают в сознании обучаемых в виде наглядных образов.

5. Одним из основных методов структуризации знаний является психосемантика, которая позволяет исследовать структуры сознания через реконструкцию индивидуальной системы знаний, выявляя категориальные структуры сознания экспертов.
6. В связи с тем, что свойство наглядности адаптивных семантических моделей при использовании многомерных баз знаний и усложнением связей между ее объектами теряется, целесообразно использовать многоуровневые адаптивные семантические модели, в которых понятия и объекты предметной области располагаются на нескольких уровнях.
7. Основными источниками содержательной информации для образовательных АСМ должны являться:
 - › государственные образовательные стандарты;
 - › типовые (примерные) учебные планы;
 - › рекомендуемая Минобрнауки России учебная и учебно-методическая литература;
 - › материалы научно-методических, научно-практических конференций и выставок, обеспечивающих опережающее обучение студентов.
8. Разработку образовательных АСМ по конкретным учебным дисциплинам рекомендуется проводить в следующей последовательности:
 - › классификация понятий в предметной области;
 - › выделение общих свойств и признаков, присущих каждому уровню понятий;
 - › выделение отличительных признаков каждого уровня понятий;
 - › установление связей между понятиями, относящимися к одному уровню;
 - › выделение межуровневых и межпредметных связей.
9. Контроль знаний обучаемых на основе АСМ должен предполагать смысловую обработку их ответов и сравнение знаний обучаемых с данными образовательной адаптивной семантической модели, при этом может использоваться сеть запроса учебной информации и обеспечивается активизация учебной деятельности студентов и повышение объективности контроля их знаний.
10. Процедура синтеза тестов для контроля знаний обучаемых должна обеспечивать максимально возможную информацию о предметной области в ответах обучаемых при минимально возможном числе тестов.

Литература

1. Шуклин Д. Е. Cerebrum: Сетевая объектно-ориентированная система управления базой знаний. / [Электронный ресурс]. – Режим доступа: <http://www.shuklin.com/ai/ht/ru/cerebrum/>, свободный (загрузка).
2. Соломатин Н. М. Информационные семантические системы. М. : Высшая школа, 1989. – 179 с.
3. Шихнабиева Т. Ш., Ахмадова Г. Ф. Об использовании адаптивных семантических моделей в экспертных системах экологического мониторинга // Научно-технический журнал «Мониторинг: наука и технологии», № 2, 2010. – С.61–67.





**Макаренко
Татьяна
Николаевна**



**Сарапкина
Елена Николаевна**

Актуальные вопросы систематизации правовых актов

***Аннотация:** рассматриваются вопросы сохранения, распространения и поиска правовой информации. Затрагиваются проблемы систематизации, классификации и официального опубликования правовых актов.*

***Ключевые слова:** систематизация законодательства, автоматизированные информационные поисковые системы, классификация правовых актов, электронное опубликование, официальные электронные источники опубликования.*

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, которая является системообразующим фактором жизни общества.

Право затрагивает интересы всех индивидов и всех социальных групп, охватывает все их действия и поступки, а правовая информатизация служит удовлетворению этих интересов.

В соответствии с Указом Президента Российской Федерации от 28 июня 1993 № 966 «О Концепции правовой информатизации России» (Собрание актов Президента и Правительства РФ, 05.07.1993, № 27, ст. 2521) под правовой информатизацией понимается процесс создания оптимальных условий максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий.

Вопросы информатизации и систематизации сопутствуют всему процессу становления, развития и жизни права.

Вопрос о правовой информатизации в нашей стране был поставлен в 70-х годах в связи с развитием автоматизированных систем управления (АСУ) различных уровней.

Министерство юстиции СССР одно из первых применило новейшие технологии в области правового информирования.

В соответствии с постановлением ЦК КПСС и Совета Министров СССР от 25 июня 1975 г. N 558 «О мерах по дальнейшему совершенствованию хозяйственного законодательства» был образован Научный центр правовой информации (далее – НЦПИ, Центр) и введен государственный учет нормативных актов СССР и союзных республик.

В целях обеспечения государственных органов правовой информацией для дальнейшего совершенствования законодательства и ведомственных нормативных актов, а также практики их применения Минюстом СССР 18.03.1977 г. было утверждено Положение о государственном учете правовых актов СССР и союзных республик. Государственный учет нормативных актов СССР и союзных республик включал в себя централизованный сбор и регистрацию этих актов, создание и поддержание в контрольном состоянии их фондов и централизованную информацию о таких актах.

Наряду с государственным учетом нормативных актов министерства юстиции союзных республик также вели учет республикан-

ского законодательства и нормативных актов министерств и ведомств республик, обязательных для других министерств, ведомств, общественных организаций и граждан. Учет осуществлялся применительно к требованиям вышеуказанного Положения и с соблюдением указаний Министерства юстиции СССР.

В 1982 г. в НЦПИ была введена в действие автоматизированная информационно-поисковая система «АИПС-Законодательство». Работу АИПС сопровождал подготовленный в НЦПИ первый в стране информационно-правовой тезаурус.

Тогда же НЦПИ стал принимать в действующий фонд все без исключения правовые акты, принимаемые высшими органами власти и управления, нормативные акты министерств и ведомств [1].

В целях проведения государственной политики в области правовой информатизации в 90-х гг. была создана государственная система правовой информации «Законодательство» (ГСПИ), функционирование которой обеспечивает ФСО России.

Тексты федеральных конституционных законов, федеральных законов, правовых актов Президента и Правительства, а также тексты правовых актов органов государственной власти, опубликованные в Собрании законодательства РФ, Бюллетене нормативных актов федеральных органов исполнительной власти и распространяемые в электронном виде федеральным государственным унитарным предприятием Научно-технический центр правовой информации «Система» Федеральной службы охраны Российской Федерации, а также федеральными органами государственной охраны, являются официальными.

В соответствии с Положением о Федеральной службе охраны Российской Федерации, утвержденным Указом Президента РФ от 07.08.2004 № 1013 (Собрание законодательства РФ, 09.08.2004, № 32, ст. 3314), ФСО с 2011 года обеспечивает развитие Официального интернет-портала правовой информации (www.pravo.gov.ru), а также размещает (опубликовывает) в установленном порядке на Официальном интернет-портале правовой информации нормативные правовые акты Российской Федерации (далее – НПА) и иные акты, для которых в соответствии с законодательством Российской Федерации предусмотрен такой порядок размещения (опубликования).

В целях единообразного применения законодательства Российской Федерации и для обеспечения контроля за соответствием НПА субъектов РФ и муниципальных НПА законодательству Российской Федерации на Министерство юстиции Российской Федерации возложены задачи по ведению и методическому обеспечению федерального регистра НПА субъектов РФ и ведение федерального регистра муниципальных НПА (Указ Президента Российской Федерации от 10 августа 2000 г. № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» (Собрание законодательства РФ, 14.08.2000, № 33, ст. 3356), постановление Правительства Российской Федерации от 10 сентября 2008 г. № 657 «О ведении федерального регистра муниципальных нормативных правовых актов» (Собрание законодательства РФ, 22.09.2008, № 38, ст. 4301)).

Федеральный регистр НПА субъектов РФ ведется в электронном виде (на машиночитаемых носителях) и документальном виде (на бумажных носителях).

Федеральный регистр НПА субъектов РФ в электронном виде ведется с использованием подсистемы «Нормативные правовые акты Российской Федерации» Единой системы информационно-телекоммуникационного обеспечения Минюста России (далее – НПА ЕСИТО).

Федеральный регистр муниципальных НПА ведется в электронном виде с использованием автоматизированной информационной системы ведения федерального муниципального регистра.

Минюст России также осуществляет полномочия (с 15 мая 1992 г.):

- › по государственной регистрации нормативных правовых актов федеральных органов исполнительной власти, затрагивающих права, свободы и обязанности человека и гражданина, устанавливающих правовой статус организаций или имеющих межведомственный характер, а также актов иных органов в случаях, предусмотренных законодательством Российской Федерации;
- › по ведению государственного реестра нормативных правовых актов федеральных органов исполнительной власти и иных органов в случаях, предусмотренных законодательством Российской Федерации;
- › Минюст России ведет в установленном им порядке:

- › государственный реестр муниципальных образований Российской Федерации;
- › определяет порядок ведения государственного реестра уставов муниципальных образований Российской Федерации и обеспечивает доступность сведений, включенных в такой реестр;
- › участвует в работе по созданию и ведению специализированных баз данных правовой информации в соответствии с единой технической политикой в сфере правовой информатизации России.

Ведение федеральных регистров обеспечивает формирование единого информационного пространства нормативных правовых актов в Российской Федерации.

Информационное пространство ПС НПА ЕСИТО создается на основе интеграции информационных подпространств подсистемы федерального законодательства, федерального регистра НПА субъектов РФ, федерального регистра муниципальных НПА, реестра уставов муниципальных образований, реестра муниципальных образований, при этом взаимодействие процессов и пользователей осуществляется за счет использования общих информационных объектов, единой нормативно-справочной и нормативно-методической информации, системы классификаторов.

Единство принципов ведения федерального регистра определяется тем, что реестры и регистры представляют собой федеральный информационный ресурс [2].

Подсистема НПА ЕСИТО содержит более 4 000 000 нормативных правовых актов. По данным 2012–2013 гг. объем поступлений в регистры составляет 65–70 тысяч НПА в месяц [3].

Очевидно, объем современной правовой информации имеет тенденцию к неуклонному росту и постоянному изменению.

Государство всегда неизбежно сталкивалось с тем, что при определенных объемах правовой информации, помимо сохранения и распространения правовой информации, возникает вопрос упорядочения – т.е. систематизации правовых норм и правовых актов.

Систематизация (т. е. упорядочение) законодательства необходима для обеспечения доступности правовых актов, удобства пользования ими, устранения устаревших, неэффективных и коллизионных норм права, ликвидации пробелов.

Министерство юстиции Российской Федерации участвует в организации работы по

систематизации законодательства Российской Федерации и подготовке Свода законов Российской Федерации в целях совершенствования правовой системы Российской Федерации.

В соответствии с распоряжением Президента Российской Федерации от 18.03.2011 № 158-рп «Об организации работы по инкорпорации правовых актов СССР и РСФСР или их отдельных положений в законодательство Российской Федерации и (или) по признанию указанных актов недействующими на территории Российской Федерации» (Собрание законодательства РФ, 21.03.2011, № 12, ст. 1627) на Минюст России возложены следующие задачи:

- › осуществлять координацию деятельности федеральных органов исполнительной власти и органов государственной власти субъектов Российской Федерации по инкорпорации правовых актов СССР и РСФСР или их отдельных положений в законодательство Российской Федерации и (или) по признанию указанных актов недействующими на территории Российской Федерации;
- › утверждать ежегодно подготовленный на основе предложений федеральных органов исполнительной власти и органов государственной власти субъектов Российской Федерации план указанных мероприятий;
- › представлять ежегодно Президенту Российской Федерации доклад о результатах такой работы.

Соответственно федеральным органам исполнительной власти и органам государственной власти субъектов Российской Федерации предписано принимать в пределах своих полномочий соответствующие меры по инкорпорации правовых актов СССР и РСФСР.

Вопрос о необходимости создания Свода законов Российской Федерации обсуждается с середины 1990-х годов (Указ Президента Российской Федерации от 06.02.1995 № 94 «О подготовке к изданию Свода законов Российской Федерации», распоряжение Президента Российской Федерации от 25.12.1995 № 555-рп [О мерах по подготовке к изданию Свода законов Российской Федерации]).

Признавалось необходимым начать подготовку к составлению и изданию Свода законов Российской Федерации – официального систематизированного полного собрания действующих нормативных актов Российской Федерации. Утверждались Положение о Временной комиссии по подготовке к изданию Свода законов РФ и состав данной комиссии.

Отмечалось, что подготовка свода законов Российской Федерации является важнейшим направлением деятельности по совершенствованию российского законодательства.

В целях продолжения этой работы Минюсту России и Государственно-правовому управлению Президента Российской Федерации было поручено завершить в первом полугодии 1996 г. составление хронологического перечня на машиночитаемых носителях всех действующих, формально не отмененных федеральных законов, нормативных указов Президента Российской Федерации и постановлений Правительства Российской Федерации, иных нормативных правовых актов, а также нормативных актов Союза ССР, подлежащих рассмотрению для включения в Свод законов Российской Федерации.

На Институт государства и права Российской академии наук и Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации возлагались научное обеспечение подготовки и издания свода законов и создание групп специалистов для анализа актов законодательства, намечаемых к включению в Свод законов.

Данные положения правовых актов выполнены не были.

В соответствии с Указом Президента Российской Федерации от 14.02.1998 № 170 «О мерах по повышению эффективности работы, связанной с формированием свода законов Российской Федерации» (Собрание законодательства РФ, 16.02.1998, № 7, ст. 829) на Государственно-правовое управление Президента Российской Федерации с участием Министерства юстиции Российской Федерации и других заинтересованных федеральных органов исполнительной власти с 1 июля 1998 г. возложена обязанность приступить к работе по подготовке контрольных текстов нормативных актов, на машиночитаемых носителях и поддержанию их в контрольном состоянии.

В настоящее время работа по инкорпорации правовых актов продолжается. Минюстом России каждый год утверждается и реализуется план мероприятий по инкорпорации правовых актов СССР и РСФСР в законодательство Российской Федерации.

Необходимо отметить, что в ряде субъектов Российской Федерации уже приняты своды законов данных субъектов (например, в Республике Башкирия, Татарстан, Костромской области).

Свод законов Российской Федерации пока так и не принят.

Это актуализирует проблемы, связанные с совершенствованием процесса систематизации действующего в России законодательства.

Успех проведения систематизации законодательства во многом также зависит от создания научно обоснованной, логически завершенной системы классификации и эффективного ее использования.

При упорядочении законодательства объем массива правовых актов продолжает расти, и поэтому даже при объединении правовых актов в единую согласованную систему должен быть обеспечен оптимальный информационный поиск и ознакомление с необходимой правовой информацией.

Такую задачу должен выполнять классификатор правовых актов.

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 «О классификаторе правовых актов» (Собрание законодательства РФ, 20.03.2000, № 12, ст. 1260) взамен действующего был одобрен новый Классификатор правовых актов.

Решение о разработке данного классификатора принималось ввиду необходимости обеспечения согласованности, непротиворечивости издаваемых в стране правовых актов.

Классификация, отражающая массив правовых актов и организующая его в систему, является необходимым элементом формирования единого информационно-правового пространства.

Нормативные акты федерального уровня, акты субъектов Российской Федерации и нормативные акты органов местного самоуправления образуют единый правовой массив законодательства Российской Федерации.

Таким образом, при разработке общей, единой системы классификации следует стремиться к тому, чтобы она учитывала особенности регионального и местного правотворчества.

Важно совершенствовать юридическую технику, устранять имеющиеся противоречия и дублирования, в том числе за и счет инкорпорации советской нормативно-правовой базы.

На сегодняшний день требуются пересмотр и дополнения в действующую систему классификации правовых актов, а возможно и принятие нового Классификатора правовых актов с учетом развития и изменения законодательства, появления его принципиально новых институтов, а также федеративного устройства государства.

Необходимо также обеспечить полноту, достоверность, актуальность и доступность официальной правовой информации в электронном виде, в том числе за счет модернизации механизмов официального опубликования правовых актов, интеграции систем информационно-правового обеспечения органов государственной власти.

Важными также являются совершенствование порядка официального опубликования правовых актов, закрепление за текстами правовых актов в электронном виде статуса источника официального опубликования [4].

Систематизации действующего законодательства способствуют мероприятия, проводимые по официальному опубликованию правовых актов.

Официальный порядок опубликования правовых актов является завершающей стадией правотворческого процесса, с ним связано вступление в силу (действие) нормативных правовых актов. Официальное опубликование носит удостоверяющий характер.

Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения. Таким образом, законодательно закреплено право каждого на информацию, а на органы государственной власти и местного самоуправления возложена обязанность обеспечить это право [5].

Как может показаться, система официального опубликования правовых актов в Российской Федерации хорошо выстроена, но на практике она имеет ряд своих существенных недостатков и на сегодняшний день не позволяет осуществить быстрый поиск необходимой правовой информации.

Официальное опубликование на данный момент не дает возможности ознакомиться с актуальной редакцией нормативного правового акта, так как нет единого официального текста нормативного правового акта после внесения в базовый текст каких-либо изменений или дополнений. Измененный и дополненный правовой акт в актуальной редакции не публикуется,

информация об утрате силы или отмене правового акта в базовый текст также не вносится.

Пожалуй, единственным примером из всего массива законодательства, официально опубликованного властью нормативного правового акта в актуальной редакции, может служить только Конституция Российской Федерации. Данный нормативный акт был опубликован на официальном интернет-портале правовой информации www.pravo.gov.ru с официальным сообщением Президента Российской Федерации о выполненном им обязательстве [6].

Еще действуют правовые акты, принятые до установленного сейчас порядка официального опубликования нормативных правовых актов. Отдельные применяющиеся акты министерств и ведомств так и не были официально опубликованы. Многие правовые акты, принятые в советский период, продолжают действовать, но, даже если они и были официально опубликованы, найти источник данной публикации весьма затруднительно. Данные акты никогда не перепечатывались, и найти их текст иногда можно только в справочных правовых информационных системах, информация в которых не носит официального характера [7].

Вопрос о «переопубликовании» таких нормативных правовых актов не решен.

Проблема ограничения прав и свобод граждан путем присвоения нормативным правовым актам ограничительных грифов также остается актуальной.

Требуется четко регламентировать условия, при которых нормативный правовой акт не может быть опубликован.

В практике официального опубликования нормативных правовых актов часто встречаются случаи, когда публикуется только часть нормативного правового акта, а остальная его часть не публикуется, при этом часто и в электронном виде документ невозможно найти полностью [8].

Представляется, что в целях обеспечения единства правового пространства России целесообразно определить единый порядок электронного официального опубликования правовых актов Российской Федерации.

Судебная практика уже давно сталкивается с проблемами применения неопубликованных правовых актов, определением даты вступления в силу официально опубликованных правовых актов, определением нормативности, а также проблемами определения источника опубликования. Проблемы имеют многолетний

стаж, но тем не менее не решаются законодателем. Именно опубликование связывает гражданское общество и власть в системе взаимных прав и обязанностей [9].

Наиболее частыми вопросами, которые разрешал суд, были вопросы о том, что органы государственной власти принимают акты, которые фактически являются нормативными, но издают их в формах, которые не могут быть нормативными. Типичное злоупотребление такого рода – издание нормативного по содержанию текста акта в форме письма органом, который не наделен правотворческими функциями.

В результате судебная практика отказалась от абсолютизации опубликования как единственного способа признания акта действующим. Теперь абсолютизируется не внешнее оформление, а содержание (нормативность). Если документ обладает свойством нормативности, его можно оспаривать в суде, несмотря на то, что он не был официально опубликован [10].

В литературе указывается [11], что понятия «правовой акт» и «нормативный акт» подчас отождествляются. Это свидетельствует о необходимости более основательного исследования всего многообразия правовых актов.

В практике встречается большое количество смешанных актов, содержащих одновременно и нормативные, и ненормативные предписания. Такое положение, хоть и вызывает нарекания с точки зрения юридической техники, но составляет, тем не менее, существующую реальность.

Кроме этого, сейчас преобладают правовые акты, определить нормативный или ненормативный характер которых представляется затруднительным.

Бошно С. В. [9] справедливо отмечает, что «поощрять правотворческие органы, которые намеренно или случайно не разбираются в видах правовых актов, не различают акты нормативные и индивидуальные и, как следствие, не могут правильно решить вопрос о том, надо ли их публиковать, нет оснований. Надо защищать права граждан и других субъектов, которые страдают от указанного поведения органов государственной власти и местного самоуправления».

В указанной ситуации выстраивание единой системы правовых актов в рамках всего государства является одной из наиболее насущных проблем.

Отсутствие единых требований к нормативным правовым актам на федеральном уровне отрицательно сказывается и на качестве нормативных правовых актов субъектов РФ, местного

самоуправления, подрывает единообразие правовой системы России, способствует возникновению правовых коллизий.

На федеральном уровне необходимо принять Закон «О правовых актах в Российской Федерации», что позволило бы включить в предмет его регулирования и ненормативные правовые акты [12], а также Закон о системе правовых актов в целом [11].

Решение комплексной задачи обеспечения единства правового пространства Российской Федерации, конституционного права граждан на информацию, совершенствования законодательства, систематизации и кодификации информационного законодательства требует введения государственного учета всех нормативных правовых актов Российской Федерации – создания единого национального банка данных этих актов [13].

Необходимо помнить, что развитие правовой информатизации должно быть направлено на удовлетворение общегосударственных, а не местных интересов, правовая информатизация призвана служить всему обществу – как государственной власти, так и гражданам; управление процессами в этой области должно находиться в руках государства, которое обязано обеспечить права и свободы граждан путем контроля за достоверностью распространяемой правовой информации, ее своевременной актуализацией [14].

Исходя из вышеизложенного представляется целесообразным создать единый сводный портал правовой информации, на котором в электронном виде публиковались бы правовые акты федерального, регионального и муниципального уровня в полном объеме, за исключением актов ограниченного распространения.

В заключение хотелось бы еще раз обозначить имеющиеся проблемы в сфере правовой информатизации:

1. Проблема учета правовых актов. Нет законодательного закрепления, каким образом должны учитываться все правовые акты в Российской Федерации (федеральное, региональное, местное законодательство).
2. Проблема выстраивания единой системы правовых актов в рамках всего государства.
3. Проблема доступности актуального и актуализированного правового акта. Требуется создание актуализированного правового информационного ресурса Российской Федерации в целях обеспечения государственной политики по формированию единого информационно-правового пространства государства.
4. Проблема классификации для унифициро-

ванного ведения банка данных правовой информации. Используемый Классификатор правовых актов устарел. Требуется дополнение к нему или принятие нового. В случае принятия нового Классификатора возникает проблема «переклассификации» всего массива законодательства Российской Федерации без потери данных.

5. Проблема определения нормативности правовых актов. До сих пор не принят федеральный закон о правовых актах Российской Федерации, как нормативных, так и ненормативных, и системе правовых актов государства в целом.
6. Проблема официального опубликования правовых актов. Часто не представляется возможным найти источник опубликования правовых актов, принятых в начале 90-х годов и советского периода – в результате доступна только электронная версия правового акта или бумажный носитель, т.е. возникают вопросы «переопубликования» применяемых правовых актов).
7. Множественность источников опубликования, опубликование правового акта не полностью и как результат – проблема определения даты вступления в силу нормативных актов и начала регулирования соответствующих правоотношений.

Обозначенные проблемы требуют незамедлительного решения от законодателя на федеральном уровне с учетом обеспечения единства правового пространства государства.

Литература

1. Труды НЦПИ. Страницы истории Научного центра правовой информации. К 35-летию НЦПИ. Выпуск 6 / под ред. Н.С. Козленко. – М. : ФГУ НЦПИ при Минюсте России, 2010. – С. 4–6; Сергиенко Л.А. История формирования информационного права в СССР и Российской Федерации 1960–2000 гг. : монография. – М. : ЮРКОМПАНИ, 2013. – 272 с. – (Серия «Актуальные юридические исследования»).
2. Филатова Л.В. Вопросы систематизации законодательства в учетной деятельности органов государственной власти // Юридический мир. 2012. №2. – С. 33–36.
3. Благовещенский Н.Ю. Система ведения регистров как базовый информационный ресурс. Применение регистра для исполнения государственных функций // IV Всероссийская научно-практическая конференция «Ведение федеральных регистров и государственных реестров, их применение для исполнения государственных функций и обеспечения доступа к актуальной правовой информации» : материалы докладов. – М. : ФБУ НЦПИ при Минюсте России, 2013. – С. 13–18.
4. Распоряжение Правительства РФ от 20.10.2010 № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)» // СЗ РФ, 15.11.2010, № 46, ст. 6026.
5. Конституция Российской Федерации.
6. Сообщение Президента Российской Федерации «Об официальном опубликовании Конституции Российской Федерации» от 21.02.2014 № Пр-383. / [Электронный ресурс]. – Режим доступа: <http://pravo.gov.ru:8080/page.aspx?88942>, свободный (загрузка).
7. Червяковский А.В. Печатное и электронное официальное опубликование нормативных правовых актов // Современное право. 2011. № 3. – С. 8–11.
8. Червяковский А.В. Проблемы официального опубликования нормативных правовых актов // Государственная власть и местное самоуправление. 2012. № 12. – С. 17–20.
9. Бошно С.В. Судебная власть об опубликовании нормативных правовых актов в связи с оценкой их действия и применения // Ваш налоговый адвокат, 2009. № 2.
10. Бошно С.В. Нормативный правовой акт в условиях современной российской теории и практики // Ваш налоговый адвокат. 2008. № 11.
11. Гайворонская Я.В. Система правовых актов Российской Федерации // Lex russica. 2013. № 8. – С. 830–838.
12. О проекте Федерального закона «О нормативных правовых актах в Российской Федерации» // Журнал российского права. 2013. № 3. – С. 84–99; Рафалюк Е.Е. Концепция законопроекта «О нормативных правовых актах в Российской Федерации» // Журнал российского права. 2012. № 8. – С. 121–125.
13. Филатова Л.В. Развитие государственных электронных сервисов в области правовой информации // Российская юстиция. 2012. № 4. – С. 42–45.
14. Официальное электронное опубликование: история, подходы, перспективы / Под ред. проф. В.Б. Исакова. – М. : Формула права, 2012, стр. 154–167.



Магдилова

Лариса

Владимировна

кандидат экономических
наук, доцент

Особенности формирования информационно-правового пространства органов государственной власти в Республике Дагестан: правовой аспект

***Аннотация:** в статье уточнены понятие и признаки информационно-правового пространства субъекта России, проанализированы программные региональные положения его развития. Исследована готовность органов государственной власти к внедрению ИКТ, а также практика их функционирования. Выработаны некоторые направления развития информационно-правового пространства органов государственной власти Республики Дагестан.*

***Ключевые слова:** информационное пространство, информационное общество, информационное право, электронное правительство, Республика Дагестан, региональное информационное законодательство.*

Информационно-правовое пространство современного государства является основой для эффективного развития информационного общества. Учитывая территориальные особенности Российской Федерации, невысокую плотность населения в отдельных регионах, большие расстояния между населенными пунктами и неразвитость транспортной инфраструктуры, единое информационное пространство становится одной из главных составляющих равномерного развития регионов, наряду с единым правовым пространством России [1, с. 17]. Конституция Республики Дагестан, принятая в 2003 году, является правовой основой для формирования информационно-правового пространства данного субъекта Российской Федерации. В свою очередь, информационным механизмом или основой является подсистема «Федеральный регистр» Министерства Юстиции Республики Дагестан [2, с. 3], которая аккумулирует и систематизирует региональное законодательство, а также Государственная система правовой информации, в частности, Официальный интернет-портал правовой информации. При этом необходимо учитывать интеграцию информационно-правового пространства Дагестана в единое информационно-правовое пространство России и зарубежных стран. В этой связи, информационно-правовое пространство Дагестана можно определить как совокупность всех форм юридической деятельности, основан-

ной на действующем законодательстве, использующей информационно-правовые ресурсы, единые технологии и стандарты функционирования. Другими словами, информационно-правовое пространство субъекта РФ – это совокупность информационных технологий, информационных ресурсов, программно-технических и организационно-правовых средств, позволяющих осуществлять юридическую деятельность на основе федерального и регионального законодательства на базе современных информационно-телекоммуникационных средств связи.

Также необходимо отметить, что основными признаками информационно-правового пространства субъекта РФ являются:

- › действие единых информационно-правовых норм;
- › распространение суверенитета субъекта РФ в рамках всего информационно-правового пространства;
- › непрерывное функционирование на территории субъекта РФ;
- › наличие внутренней системы и структуры;
- › согласованность и непротиворечивость;
- › наличие взаимосвязи с информационно-правовыми нормами федерального и международного уровня;
- › ограниченность во времени;
- › базирование на деятельности участников информационно-правового взаимодействия.

Информационно-правовое пространство Дагестана, представляющее собой сложный механизм, позволяет осуществлять информационное взаимодействие государственных органов власти и местного самоуправления данного субъекта, физических и юридических лиц, реализовывать функции электронного правительства. Одной из основных проблем формирования и развития этого информационно-правового пространства является создание и использование информационно-правовых ресурсов, регламентирование информационных процессов, связанных с реализацией основных информационных прав и свобод, закрепленных в Конституции России и Дагестана, в органах государственной власти.

В Государственной программе Российской Федерации «Информационное общество (2011–2020 годы)» в целях развития единого информационно-правового пространства в органах государственной власти предусматривается:

- формирование единого пространства юридически значимого электронного взаимодействия;
- создание и развитие государственных межведомственных информационных систем, предназначенных для принятия решений в реальном времени;

➤ создание и развитие защищенного сегмента сети Интернет и системы межведомственного электронного документооборота.

Правовой основой для реализации обозначенных в программе целей и задач являются следующие федеральные законы: «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149; «О персональных данных» от 27 июля 2006 г. № 152; «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22 декабря 2008 г. № 262; «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8; «Об организации предоставления государственных и муниципальных услуг» от 27 июля 2010 г. № 210; «Об электронной подписи» от 6 апреля 2011 г. № 10; «О Государственной автоматизированной информационной системе «ЭРА-ГЛОНАСС» от 28 декабря 2013 г. № 395.

Необходимо отметить, что проведенное Институтом развития информационного общества исследование [3] показало, что существует разрыв между регионами в области использования информационно-коммуникационных технологий в деятельности органов государственной власти и местного самоуправления (рис. 1).

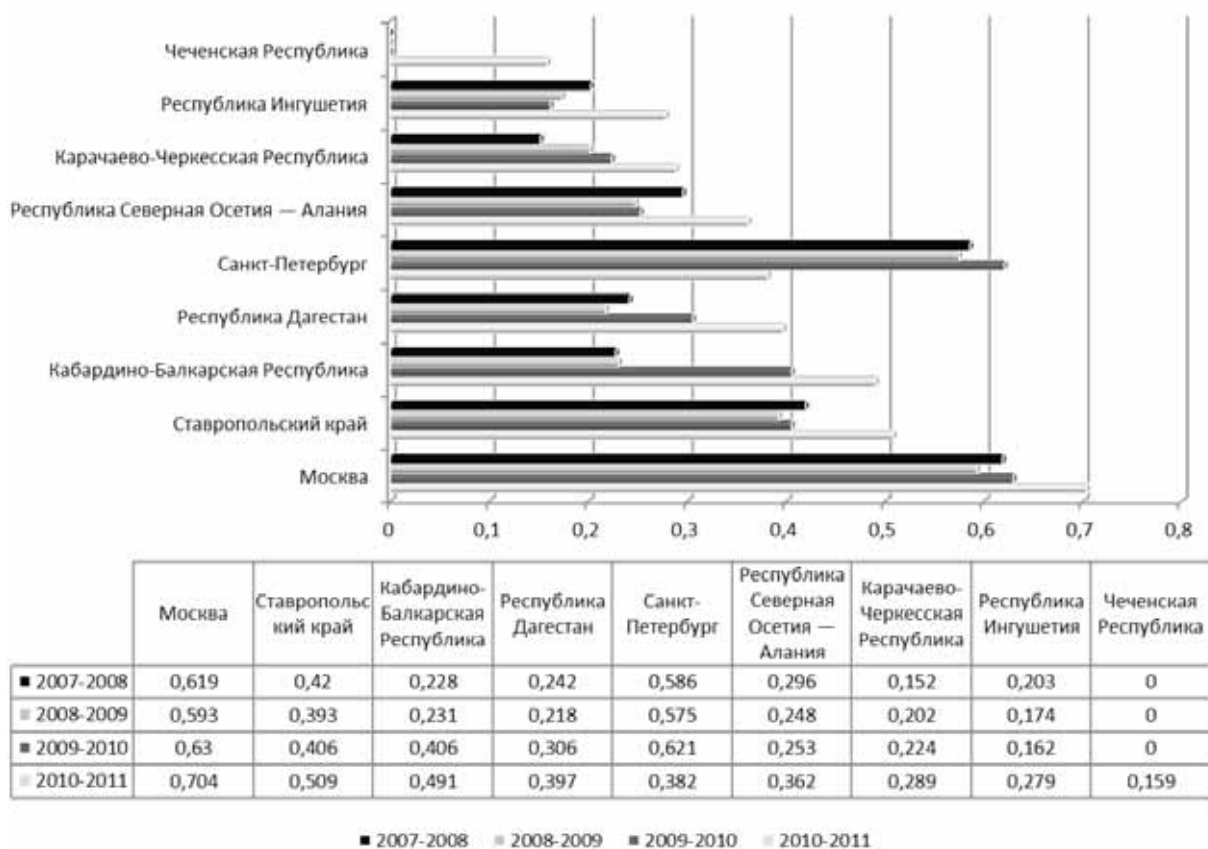


Рис. 1. Подындекс «ИКТ в органах государственной власти и местного самоуправления»

Подындекс «ИКТ в государственном и муниципальном управлении» строится на основе трех групп показателей:

- доступ органов местного самоуправления и государственной власти субъектов РФ к ИКТ;
- веб-присутствие органов государственной власти и местного самоуправления;
- использование технологий электронного правительства предприятиями региона.

Характерным является присутствие в аутсайдерах субъектов СКФО, а в лидерах Москвы, Санкт-Петербурга и ресурсообеспеченных регионов, например, Ханты-Мансийского округа «Югра».

В Государственной программе «Информационное общество (2011–2020 гг.)» определены особенности организации работ по проектам в интересах субъектов России, которые направлены на устранение цифрового неравенства между регионами на основе проведения трех видов мероприятий: пилотного, типового, инновационного.

В рамках типового мероприятия предусматривается разработка региональных программ информатизации, направленных на развитие информационно-правового пространства регионов, подготовленных в соответствии с распоряжением Правительства Российской Федерации от 3 июля 2007 г. № 871-р. Значимым результатом в этой области для Республики Дагестан является разработка и утверждение следующих региональных государственных программ: «Развитие электронного правительства Республики Дагестан до 2017 года»¹; «Комплексное внедрение и использование спутниковых навигационных технологий ГЛОНАСС в Республике Дагестан на 2012–2014 годы»²; «Снижение административных барьеров, оптимизация и повышение качества предоставления государственных и муниципальных услуг, в том числе на базе

многофункциональных центров предоставления государственных и муниципальных услуг в Республике Дагестан в 2011–2014 годах».

Республиканская целевая программа «Развитие электронного правительства Республики Дагестан до 2017 года» рассматривается как основной механизм координации и интеграции приоритетных проектов в сфере информатизации органов исполнительной власти и создания единого информационного пространства Республики Дагестан и призвана стать одним из главных инструментов реализации региональной политики в области формирования и развития электронного правительства Республики Дагестан, а также выполнять координирующие функции по реализации мероприятий в этом направлении.

В результате выполнения программы «Комплексное внедрение и использование спутниковых навигационных технологий ГЛОНАСС в Республике Дагестан на 2012–2014 годы» к настоящему времени создан региональный навигационно-информационный центр, навигационно-информационная система мониторинга транспорта для перевозки учащихся (107 единиц транспорта), пассажирских перевозок (2 единицы), транспортных средств скорой и неотложной медицинской помощи (355 единиц транспорта и 54 диспетчерских станции).

- В рамках реализации государственной программы «Снижение административных барьеров, оптимизация и повышение качества предоставления государственных и муниципальных услуг, в том числе на базе многофункциональных центров предоставления государственных и муниципальных услуг в Республике Дагестан в 2011–2014 годах» к настоящему времени создано 13 многофункциональных центров (МФЦ) в следующих муниципальных образованиях: городах Каспийске, Махачкале, Кизилюрте и Дагестанские Огни, в Гумбетовском, Догузпаринском, Кумторкалинском, Кулинском, Левашинском, Магарамкентском и Новолакском, Бабаюртовском и Карабудахкентском районах. В соответствии с расчетами, в Республике Дагестан к 2015 году количество МФЦ должно составить 54 и количество окон в них – 448.
- В Дагестане также созданы и функционируют информационные системы, являющиеся программно-технической основой формирования и развития информационно-правового пространства органов государственной власти. К ним относятся:

¹ О Концепции республиканской целевой программы «Комплексное внедрение и использование технологий ГЛОНАСС в Республике Дагестан на 2012–2014 годы»: Распоряжение Правительства РД от 07.07.2011 №153-р. // Собрание законодательства Республики Дагестан, 15.07.2011, №13, ст. 578.

² О государственной программе Республики Дагестан «Снижение административных барьеров, оптимизация и повышение качества предоставления государственных и муниципальных услуг, в том числе на базе многофункциональных центров предоставления государственных и муниципальных услуг в Республике Дагестан в 2011–2014 годах»: Постановление Правительства РД от 30.06.2011 г. № 212. // Собрание законодательства Республики Дагестан, 30.06.2011, №12, ст. 485.

- › Реестр государственных и муниципальных услуг (функций), внедренный в 2011 году, в котором содержится и актуализируется информация обо всех органах исполнительной власти и органах местного самоуправления Республики Дагестан, всех подведомственных организациях и их услугах. Сотрудниками Министерства связи и телекоммуникаций и Министерства юстиции Республики Дагестан проверяется правильность заполнения обязательных полей в системе, занесение новых пользователей в систему и редактирование органов власти и их услуг, нормативных документов, административных регламентов, а также производится публикация информации в системе. После прохождения всех проверок, информация публикуется на Едином портале государственных и муниципальных услуг;
- › Информационно-учетная процессная подсистема, внедренная в 2012 году, организующая межведомственное электронное взаимодействие в органах исполнительной власти, не имеющих ведомственных информационных систем, использующаяся для работы с заявлениями, полученными в электронной форме с Единого портала государственных и муниципальных услуг, а также получения необходимой информации и документов по оказанию услуги;
- › Портал государственных и муниципальных услуг Республики Дагестан, позволяющий получить информацию и обратиться за услугой в электронном виде;
- › Система электронного документооборота в органах государственной власти Республики Дагестан, основанная на системе «Дело», успешно используемая в качестве единой СЭД в 28 регионах РФ;
- › Система «Электронный паспорт муниципальных районов и городских округов Республики Дагестан».

Для повышения эффективности взаимодействия между органами государственной власти в оказании государственных и муниципальных услуг, осуществления межведомственного документооборота, развития квалификационных компетенций кадров в области информационных технологий реализуется приоритетный проект Президента РД «Эффективное государственное управление», среди направлений которого в данном исследовании интерес представляют:

- › Интранет-портал (Intranet/«внутренней сети»), объединяющий органы государствен-

ной власти РД (Администрацию Президента и Правительства РД, Народное Собрание РД, органы исполнительной власти РД, органы местного самоуправления), разработчиком которого стало ОАО НПО «Бизнес Автоматика», г. Москва;

- › Единое «Web-решение», предусматривающее создание единого информационного пространства для органов государственной власти Республики Дагестан на базе структурированного Интернет-портала;
- › «Система электронных паспортов компетенций государственных служащих» и формирование соответствующей правовой базы;
- › Республиканский центр обработки данных, на ресурсах которого уже запущены в работу сайт Президента Республики Дагестан, система электронного документооборота, единый портал органов государственной власти, сайт «Общественный надзор» и др.

В направлении совершенствования правовых основ развития информационного общества, в частности, информационно-правового пространства органов государственной власти, в Дагестане в результате совместной работы Министерства связи и телекоммуникаций, Министерства юстиции и Министерства торговли и инвестиций Республики Дагестан разработан «Стандарт открытости органов исполнительной власти Республики Дагестан», а также внесен проект постановления по формированию Правительственной комиссии по защите информации Республики Дагестан.

Таким образом, проведенное исследование показало, что субъекты России различаются по уровню развития информационно-правового пространства органов государственной власти, в том числе Республика Дагестан, которая отстает от центральных и ресурсобеспеченных регионов. Однако в Дагестане проводится определенная работа по преодолению цифрового неравенства, формированию нормативной базы развития информационного общества, практической реализации программных положений.

В Республике Дагестан формируется региональная правовая база, регулирующая практические вопросы формирования и реализации информационной политики субъекта, предусматривающей развитие информационного пространства как основы построения информационного общества, принимаются нормативно-правовые акты, регламентирующие порядок создания информационных ресурсов и информационной инфраструктуры, перехода органов государствен-

ной власти на электронный документооборот, осуществление функций управления в электронном режиме («электронного правительства»).

В связи с этим актуальными для совершенствования и развития информационно-правового пространства органов государственной власти в Республике Дагестан представляются следующие направления:

- регистрация органов государственной власти Республики Дагестан на официальном интернет-портале правовой информации Государственной системы правовой информации, в том числе организация публичных центров правовой информации в сети библиотек и системе «Почта России»;
- совершенствование системы оценки и развития кадрового потенциала, обеспечивающего создание и сопровождение современных информационно-коммуникационных технологий в органах государственной власти, в том числе сотрудничество с ведущими вузами республики, осуществляющими подготовку специалистов в области прикладной информатики по различным профилям (экономика, государственное и муниципальное управление, менеджмент, юриспруденция) на основе заключения договоров о прохождении практики и стажировки;

- мониторинг конкурсов проектов на субсидирование из федерального бюджета развития информационного общества и подача заявок для участия республики в них, со своевременным соблюдением всех необходимых условий;
- разработка и принятие региональной целевой программы по информатизации муниципальных образований на основе «облачных технологий».

Литература

1. Азизова В. Т. Роль обеспечения единства правового пространства Российской Федерации как фактор укрепления ее национальной безопасности. // Вестник ДГУ. 2013. №2.
2. Морозов А. В., Полякова Т. А., Филатова Л. В. Этапы и проблемы формирования единого информационно-правового пространства России. // Информационное право. 2012. №1.
3. Индекс готовности регионов России к информационному обществу 2010–2011. Анализ информационного неравенства субъектов Российской Федерации / Под ред. Т.В. Ершовой, Ю.Е. Хохлова, С.Б. Шапошника. М.: 2012.





**Танимов
Олег Владимирович**
кандидат юридических
наук, доцент

Обеспечение информационной безопасности при управлении крупными городами

***Аннотация:** в статье проводится исследование проблем обеспечения информационной безопасности при управлении крупными городами с правовой и практической точек зрения. Отмечается роль информационной безопасности в процессе управления и ее влияние. Подчеркивается необходимость совершенствования механизма правового регулирования в ходе решения данных проблем, с учетом специфики крупного города. Предлагаются новые шаги в решении рассматриваемых проблем.*

***Ключевые слова:** информация, информационная безопасность, крупные города, информационные отношения, управление, проблемы.*



**Богатова
Марина
Константиновна**

Современный мир – это мир информационных технологий. Научно-техническая революция, начавшаяся еще в XX веке, в корне изменила всю нашу жизнь. За довольно небольшой срок, особенно если его рассматривать в масштабах всей истории, произошли, несомненно, грандиозные изменения. Человечество шагнуло в новую эпоху – эпоху постиндустриального общества. Его также называют информационным, и на это название стоит обратить внимание. Оно не случайно. Практически все новые гаджеты и другие технологии – это носители информации. Они служат нам для создания, хранения и передачи информации, которая с каждым днем представляет собой все большую ценность. Они создаются и совершенствуются именно с целью ее наиболее комфортной обработки.

Для более четкого понимания проблемы необходимо кратко охарактеризовать такие понятия, как: «информация», «информационная безопасность», «крупный город».

Так что такое информация и почему она так важна в современном обществе? Давайте рассмотрим несколько подходов к ее определению. Начнем с того, что термин «информация» имеет латинские корни. Его уже употребляли такие древние мыслители, как Цицерон и Августин, в частности, можно его найти в контексте теории идей Платона. С помощью слова «informare» Цицерон разъяснял эпикурейское понятие «prolepsis», переводящееся как «представление, внедренное в ум».

Во Франции же слово «информация» появляется в XV веке, причем на разговорном языке оно получило несколько значений, такие как: «исследование», «образование», «акт информирования или сообщения знания» и «разведки» [1, с. 4].

Поговорим и о других подходах к определению «информация». Например, один из них дает такое определение: «все, что может быть переведено в цифровую форму, как закодированный поток в битах, является информацией». Некоторые другие подходы имеют деловую ценность или, например, предназначены для развлечения [2, с. 20.]

Переходя к современным определениям этого слова, обратимся сначала к зарубежным изданиям. Там тоже отсутствует единство

в определении данного термина. Информация представляется и как «знания, полученные посредством обучения, опыта или инструкции, также сбор фактов или данных» [3], и как «то, что известно; совокупность восприятия, открытия или выводов» [4], а также «информация определяется как осведомленность, которая может обмениваться и выражаться» [5].

Что касается определений этого термина в российском законодательстве, то здесь их тоже немало. Но из всех них основным и для российского законодательства, и для рассмотрения «информации» с юридической точки зрения является определение, данное в ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» [6]. Трактовку мы можем увидеть в ч. 1 ст. 2: информация – это сведения (сообщения, данные) независимо от формы представления.

Переходя к исследованию термина «информационная безопасность», возможно «утонуть» в различных проблемах как теоретического, так и практического характера. Сегодня мы не можем говорить о разработанной системе обеспечения информационной безопасности, учитывая один лишь факт отсутствия легального определения «информационная безопасность». В ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» оно отсутствует, а иного, специализированного нормативного правового акта на этот счет пока не создано. Это отсутствие можно рассматривать как некоторый пробел в праве, который следует заполнить в ближайшее время, ибо проблема информационной безопасности, в связи с ростом количества информации, становится все актуальнее, а пробел все зримее.

Тем не менее, в ряде документов содержится дефиниция рассматриваемого понятия. В Доктрине информационной безопасности России под **информационной безопасностью** Российской Федерации понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [7].

В Решении Совета глав государств СНГ (принято в г. Бишкеке 10.10.2008) **информационная безопасность** трактуется как «состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства» [8].

Однако стоит отметить очень интересный факт: несмотря на отсутствие упомянутого определения, в нашем законодательстве существует такое понятие, как «информационная безопасность детей».

Его трактовка дается в ст. 2 ФЗ от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [9]: это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Это понятие можно рассматривать как более узкое по отношению к понятию «информационная безопасность», так как последнее должно касаться всех групп граждан, а не только определенной категории (в данном случае детей). И неправильно, что узкое (видовое) понятие, которое должно входить в более широкое, существует, а общее (родовое) – нет. В этом можно увидеть отсутствие должного внимания законодателя к данной проблеме.

Кроме того, существует проблема отождествления понятий «информационная безопасность» и «кибербезопасность» [10].

Но не будем углубляться в семантические проблемы, а перейдем к термину «крупный город». К сожалению, в российском законодательстве не содержится понятий «город», «крупный город», «управление городом» и пр. Можно найти лишь понятие «городское поселение» – город или поселок, в котором местное самоуправление осуществляется населением непосредственно и (или) через выборные и иные органы местного самоуправления. Как видим, данное понятие определяется через термин «город», который, в свою очередь, не определен легально.

В литературе выделяются особенности крупнейшего города, который отличается [11]:

- › многомиллионным населением;
- › высоким уровнем ежедневной внутригородской и пригородной миграции;
- › средоточием общефедеральных государственных, общественных и политических структур;
- › наличием крупнейших систем жизнеобеспечения федерального значения (железнодорожные, автомобильные и авиационные узлы, центры управления энергетическими системами и др.);
- › наличием большого количества иностранных посольств и представительств.

К таким городам относятся Москва и Санкт-Петербург – крупнейшие научные и культурные центры страны.

Естественно, что и управление такими городами обладает рядом особенностей. Специфика заключается в том, что:

1. В городах федерального значения установление и изменение границ внутригородских муниципальных образований, а также их преобразование осуществляются законами городов федерального значения, с учетом мнения населения соответствующих внутригородских территорий.
2. Перечень вопросов местного значения, источники доходов местных бюджетов внутригородских муниципальных образований городов федерального значения определяются законами этих городов, исходя из необходимости сохранения единства городского хозяйства.
3. Установленные федеральными законами источники доходов местных бюджетов, не отнесенные законами городов федерального значения к источникам доходов бюджетов внутригородских муниципальных образований, зачисляются в бюджеты городов.
4. Состав муниципального имущества внутригородских муниципальных образований городов федерального значения определяется законами этих городов в соответствии с перечнем вопросов местного значения, установленным для муниципальных образований законами этих городов.

В век развития электронных технологий невозможно осуществлять управление крупным городом (далее – город) без цифровых телекоммуникационных средств передачи информации. Вполне естественно возникает проблема защиты информации и обеспечения информационной безопасности в ходе управленческих процессов.

Учитывая национальный и зарубежный опыт [12], можно утверждать, что обеспечение информационной безопасности должно осуществляться как внутри города, так и вне его. Защита изнутри и извне – это два слагаемых информационной безопасности, два ее элемента, без которых город, как корабль с пробойной, неустойчив и может утонуть при первой же серьезной волне.

Сегодня уже не вызывает удивление спектр электронных услуг, существующих в сфере управления. Здесь в *процессе обеспечения информационной безопасности* возникает серьезная проблема – **защита персональных**

данных, вызывающая беспокойство как представителей аппарата управления городом, так и его жителей. Данная проблема появляется в ходе обработки персональных данных.

Основные принципы обработки персональных данных граждан закреплены в ст. 23 и 24 Конституции РФ – каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются [13]. Вопросы обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных нашли детальное регулирование в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [6] (далее – Закон).

Однако, по мнению В. И. Торговченкова, анализ результатов практической реализации основополагающих положений и начал в области персональных данных вызывает необходимость корректировки как деятельности органов и организаций всех форм собственности, так и самого законодательства [14].

Проведенные органами прокуратуры Тамбовской области проверки показали, что на территории области субъекты персональных данных, осуществляющие их обработку, допускают многочисленные нарушения в этой сфере правоотношений.

В нарушение ст. 22.1 Закона не назначены лица, ответственные за организацию обработки персональных данных: в ООО «Дмитриевская управляющая компания» Никифоровского района, МБОУ ДОД «Школа искусств» Гавриловского района, ОАО «Мордовагрохимия», ТОГБУЗ «Мордовская ЦРБ», ОАО «Маслосырзавод «Новопокровский» Мордовского района, ООО «ЖКХ», ООО «Солидарность» Рассказовского района, администрациях сельсоветов Уваровского района.

Операторами персональных данных игнорируется предусмотренная ч. 2 ст. 18.1 Закона обязанность по обеспечению неограниченного доступа к документу, определяющему политику оператора в отношении персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Так, ТОГБУЗ «Городская больница г. Котовска» не обеспечило гражданам неограниченный доступ к указанным документам – локальные акты не опубликованы и не размещены ни на официальном сайте, ни на информационных стендах учреждения [14, с.4].

Кроме того, административные органы, различные службы и иные вовлеченные в этот процесс управления структуры, к сожалению, практически неизбежно в той или иной степени будут сталкиваться с проблемами утечки информации как исходя из множественности субъектов, которые будут обладать доступом к данной информации в силу своих служебных обязанностей, так и вследствие недобросовестности отдельных государственных служащих, вызванной в том числе и невысоким уровнем их доходов.

Как отмечает Правительство Москвы, «остаются актуальными вопросы обеспечения информационной безопасности и защиты персональных данных в органах исполнительной власти города Москвы».

Проблемы, препятствующие росту эффективности использования информационных технологий для повышения качества жизни, развития экономической, социальной, культурной и духовной сфер жизни города Москвы, совершенствования системы государственного управления, носят комплексный межведомственный характер и не могут быть решены на уровне отдельных органов государственной власти города Москвы. Их устранение требует скоординированного проведения организационных изменений и обеспечения согласованности действий всех органов государственной власти города Москвы» [15].

За последние годы в России, как и во всем мире, усилилась угроза терроризма, что потребовало принятия соответствующих дополнительных мер безопасности со стороны государства и общества. Под терроризмом понимается насилие или угроза его применения в отношении физических лиц, уничтожение (повреждение) или угроза уничтожения (повреждения) имущества либо других материальных объектов, незаконное вмешательство или угроза незаконного вмешательства в *информационные ресурсы и системы*, а также иные действия, создающие угрозу гибели людей, причинения значительного материального ущерба либо наступления иных общественно опасных последствий. Террористические акты совершаются в целях устрашения населения или оказания воздействия на принятие должностными лицами, органами государственной власти и местного самоуправления или международными организациями решений, обеспечивающих удовлетворение социально-политических и имущественных требований и интересов террористов.

В этой ситуации особую актуальность вызывает **защита самих информационных систем и находящейся в них информации**, что является еще одной проблемой обеспечения информационной безопасности в процессе управления крупным городом.

В информационной системе подлежат реализации следующие меры защиты информации [16]:

- › идентификация и аутентификация субъектов доступа и объектов доступа;
- › управление доступом субъектов доступа к объектам доступа;
- › ограничение программной среды;
- › защита машинных носителей информации;
- › регистрация событий безопасности;
- › антивирусная защита;
- › обнаружение (предотвращение) вторжений;
- › контроль (анализ) защищенности информации;
- › обеспечение целостности информационной системы и информации;
- › обеспечение доступности информации;
- › защита среды виртуализации;
- › защита технических средств;
- › защита информационной системы, ее средств и систем связи и передачи данных.

Указанные меры защиты, в условиях бурного роста количества хакеров и различного вида вирусов, не всегда являются эффективными. В связи с этим в полном объеме не будут обеспечены: идентификация и аутентификация субъектов доступа, управление доступом субъектов к объектам доступа, защита машинных носителей информации, антивирусная защита, своевременное обнаружение и предотвращение вторжений, контроль защищенности информации.

Кроме того, усиление технических мер обеспечения целостности информационной системы и информации (защита среды виртуализации, защита технических средств, защита информационной системы, ее средств и систем связи и передачи данных) ограничит доступ к информации.

Рассмотренные нами проблемы обеспечения информационной безопасности при управлении крупными городами составляют лишь часть общих проблем в данной сфере.

Для их решения необходимо:

- › формирование оптимизированной системы законодательства в сфере информационной безопасности и создания на ее основе комплексной системы регулирования процессов управления городом (регионом);

- › обеспечение высокой оперативности и максимальной достоверности информации;
- › создание системы эффективной и сбалансированной защиты информационно-статистических ресурсов на современном программно-технологическом и техническом уровне;
- › максимальное соблюдение требований по обеспечению информационной безопасности в сфере управления, включая защиту от несанкционированного доступа, при сборе, обработке, накоплении, предоставлении информации.

Таким образом, решение указанных проблем обеспечения информационной безопасности при управлении крупными городами возможно путем синтеза оптимизации законодательства и совершенствования технических мер защиты информации и информационных систем.

Нельзя упускать из виду, что эффективному процессу обеспечения информационной безопасности при управлении городом (регионом) должно сопутствовать повышение качества жизни населения крупного города. Это возможно осуществить за счет широкомасштабного использования информационно-коммуникационных технологий в социальной сфере, в сфере обеспечения комплексной безопасности города, во всех сферах управления городским хозяйством, а также в повседневной жизни. Немаловажную роль при этом будет играть повышение эффективности и прозрачности государственного управления в городе (регионе).

Город, как и государство, управляет или, лучше сказать, направляет общество в правильное русло, – во всяком случае, должен это делать. Пока в нашей стране ни юридически, ни фактически не налажено регулирование информационных отношений: еще много пробелов в праве, еще не все реализуется на практике. Поэтому об эффективности в обеспечении информационной безопасности при управлении крупными городами судить рано. Надо тщательнее работать в этой сфере, уделять ей больше внимания, потому что с каждым годом информация все больше наполняет мир, и упущения в этой сфере может привести к упадку в другой сфере и вообще всей страны в целом. Кроме того, информационная безопасность все чаще стала приобретать международные масштабы, поэтому для процветания государства надо иметь мощную правовую базу, которая сможет не только разрешить внутригосударственные конфликты в сфере информационных правоотношений в городе (регионе), но и

обеспечить защиту всего государства в нужный момент.

Литература

1. Handbook of Philosophy of Information. by Dov M. Gabbay, John Wood, Paul Thagard. UK. Oxford. 2008 Elsevier B.V.
2. Carl Shapiro, Hal R. Varian. Information Rules: A Strategic Guide to the Network Economy. Harvard Business Press; 1st edition. 1998. P. 20.
3. The American Heritage Dictionary of the English Language, Fourth Edition Copyright 2007, 2000 by Houghton Mifflin Company. Updated in 2007. Published by Houghton Mifflin Company.
4. Roget's II: The New Thesaurus, Third Edition; by the Editors of the American Heritage Dictionary. Copyright 1995 by Houghton Mifflin Company. Published by Houghton Mifflin Company.
5. OASIS Information definition. / [Электронный ресурс]. – Режим доступа: http://nost.gsfc.nasa.gov/isoas/presentations/USDA_19990219/sld013.htm , свободный (загрузка).
6. «Российская газета», 2006, № 165.
7. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // «Российская газета», 2000, № 187.
8. Решение Совета глав государств СНГ «О Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год» // Документ опубликован не был.
9. «Российская газета», 2010, № 297.
10. Танимов О. В. Законодательное регулирование кибербезопасности. Доклад на заседании НТС ФБУ НЦПИ при Минюсте России 25 марта 2014 г. / Доклад опубликован не был.
11. Система муниципального управления: Учебник для вузов / Р. В. Бабун, В. Б. Зотов, А. Н. Кириллова и др.; под ред. В. Б. Зотова. 3-е изд., перераб. и доп. Спб. : Питер-Пресс, 2007. – 560 с.
12. Право цифровой администрации в России и во Франции. Сборник научных материалов

- Российско-французской международной конференции, 27–28 февраля, 2013 г. – М.: ИГП РАН – Изд-во «Канон+» РООИ «Реабилитация», 2014. – 178 с.
13. Собрание законодательства РФ. 2014, № 9, ст. 851.
 14. Торговченков В. И. Нормативно-правовое регулирование в сфере оборота персональных данных // Законность. 2013. № 4. С. 3.
 15. Постановление Правительства Москвы от 22.02.2012 № 64-ПП (ред. от 10.07.2013) «О внесении изменений в государственные программы города Москвы и об утверждении государственной программы «Открытое Правительство» на 2012–2016 гг.» (вместе с «Государственной программой города Москвы «Информационный город (2012–2016 годы)», «Государственной программой города Москвы «Развитие транспортной системы на 2012–2016 гг.», «Государственной программой «Социальная поддержка жителей города Москвы на 2012–2016 годы», «Государственной программой города Москвы «Энергосбережение в городе Москве» на 2011, 2012–2016 гг. и на перспективу до 2020 года», «Государственной программой города Москвы «Имущественно-земельная политика города Москвы на 2012–2016 гг.», «Государственной программой «Спорт Москвы» на 2012–2016...». // Вестник Мэра и Правительства Москвы. 2012. № 40. Том 1.
 16. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014) // Документ опубликован не был.





**Фадеева
Наталья
Анатольевна**

Повышение квалификации специалистов по ведению регистров нормативных правовых актов в ФБУ НЦПИ при Минюсте России

Аннотация: В статье рассматривается образовательная деятельность по повышению квалификации государственных гражданских служащих, государственных гражданских служащих субъектов Российской Федерации, муниципальных служащих, обучение специалистов по ведению регистров.

Ключевые слова: образовательная деятельность, учебный процесс, нормативные правовые акты, регистр, реестр, информационное общество, Концепция, автоматизированные информационные системы.

Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти.

Основой овладения разнообразными информационными технологиями и эффективным их использованием является образование.

Фундамент новой модели образования, заложенный еще в 2007 году соответствующими изменениями в законодательстве об образовании, в настоящее время закреплён в Федеральном законе от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

В Российской Федерации по уровням общего и профессионального образования, по профессиональному обучению реализуются основные образовательные программы, по дополнительному образованию – дополнительные образовательные программы.

Необразованный человек не в состоянии понять научно-технические и культурные достижения, общественно-политические процессы. Специальная профессиональная подготовка позволяет человеку утвердиться как личности, участвовать в приумножении культурных ценностей, повысить свое благосостояние.

Адаптация человека к условиям информационного общества возможна только в том случае, если общество обеспечит доступность образования и обучения в течение всей жизни.

Недопустима финансовая недоступность информации для людей. Поэтому важна организация свободного доступа к информаци-

онным массивам через образовательные учреждения и электронные библиотеки.

Достойная реализация права на образование во многом определяет уровень развития государства как особой формы организации общества и самостоятельной единицы на мировой арене. Именно необходимостью улучшения качества образовательных услуг обусловлен весь комплекс осуществляемых в настоящий момент в Российской Федерации мероприятий. Качество образовательных услуг и уровень развития всего современного общества – самостоятельные, но тесно связанные показатели эволюции любого государства. Причем ни один из них не может развиваться обособленно [1].

Информационно-правовой массив охватывает практически все сферы человеческой деятельности [2].

В настоящее время информационно-правовая деятельность как вид деятельности юристов и государственных служащих других профессий с непосредственным применением компьютерных систем требует знаний о закономерностях, принципах и тенденциях построения автоматизированных информационных систем, создания государственных информационных ресурсов в целях информационного обеспечения интересов граждан, общества, государства. Развитие системы правовой информатизации Министерства юстиции Российской Федерации имеет общие цели для законотворческих, правоохранительных и правоприменительных органов. Это обеспечение доступа к информации о деятельности государственных органов и

должностных лиц, повышения уровня правовой информированности общества путем всестороннего обеспечения государственных органов, должностных лиц и граждан полной и достоверной информацией о действующих в России законодательных и иных правовых актах, в том числе муниципальных, в условиях автоматизации информационных процессов.

Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации» (далее – НЦПИ) – одно из учреждений, которое стояло у истоков информатизации. НЦПИ имеет наибольший опыт в России по автоматизированной обработке правовой информации. Он был создан почти 40 лет назад и является создателем первой в стране автоматизированной системы правовой информации «АИПС-Законодательство»; это первая удачная попытка систематизации большого правового массива. НЦПИ оказывает информационную поддержку деятельности Минюста России и является оператором Единой системы информационно-телекоммуникационного обеспечения (далее – ЕСИТО). В соответствии с приказом Минюста России от 14.04.2009 № 109 «О вводе в постоянную эксплуатацию подсистемы «Нормативные правовые акты Российской Федерации» [3] ЕСИТО Минюста России» (далее – Подсистема НПА ЕСИТО) НЦПИ обеспечивает выполнение функций оператора этой подсистемы и осуществляет ее информационно-технологическое сопровождение. Отсюда вытекают задачи НЦПИ по кадрам: для надлежащего функционирования всей системы необходимо квалифицированное выполнение работ на всех этапах.

Эффективность работы любой организации во многом зависит от профессионального уровня персонала.

Целью повышения квалификации является обновление теоретических и практических знаний специалистов в связи с повышением требований к уровню квалификации и необходимостью освоения современных методов решения профессиональных задач (п. 7 Типового положения об образовательном учреждении дополнительного профессионального образования (повышения квалификации) специалистов, утвержденное постановлением Правительства РФ от 26.06.1995 № 610 [4]).

Система государственной службы Российской Федерации находится в процессе постоянного совершенствования и развития. Одним из основополагающих документов, опреде-

ляющих направление этого развития, является Федеральная программа «Реформирование и развитие системы государственной службы Российской Федерации (2009–2013 годы)», утвержденная Указом Президента Российской Федерации от 10 марта 2009 года № 261. Отдельные задачи, поставленные в этой программе, имеют непосредственное отношение к теме дистанционного обучения, а именно:

- › актуализация содержания программ подготовки и дополнительного профессионального образования государственных служащих;
- › внедрение современных образовательных технологий в процессе обучения.

К тому же процесс развития образовательной сферы не может не опираться на достижения других сфер в целях реализации и учета всесторонних потребностей общества. Так, развитие компьютерных технологий стимулирует все большее использование их в различных областях. Именно поэтому образовательный процесс модернизируется посредством внедрения в него качественно новых элементов. И одним из таких элементов, несомненно, является интернетизация образования, использование компьютерной техники, электронных образовательных ресурсов в процессе обучения. В связи с этим в последнее время в научном и практическом употреблении прочно утвердились такие категории, как «дистанционные образовательные технологии» и «дистанционное образование».

Так, Федеральным законом от 10 января 2003 года № 11-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации «Об образовании» и Федеральный закон «О высшем и послевузовском профессиональном образовании» закреплено следующее определение: «дистанционные образовательные технологии – это образовательные технологии, реализуемые в основном с применением средств информатизации и телекоммуникации при опосредованном или не полностью опосредованном взаимодействии обучающегося и педагогического работника». Способы организации обучения посредством дистанционных образовательных технологий были зафиксированы в Приказе Министерства образования России от 18 декабря 2002 года № 4452 «Об утверждении Методики применения дистанционных образовательных технологий в образовательных учреждениях высшего, среднего и дополнительного профессионального образования Российской Федерации» [1].

Таким образом, на государственном уровне получила закрепление объективная по-

требность в повышении квалификации юристов, приобретении ими навыков и специальных знаний, позволяющих работать с современными техническими средствами ведения различных учетных систем Минюста России, в частности, федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации.

С учетом постоянного совершенствования программного обеспечения, используемого для ведения этих регистров, становится актуальной задача соответствующего обучения специалистов, которое должно проводиться на постоянной или регулярной основе и с использованием современных образовательных технологий. Для решения этой задачи в НЦПИ было организовано обучение специалистов по ведению регистров с использованием очно-дистанционной формы учебного процесса. Программа обучения включает две составляющих:

- › заочное (дистанционное) обучение с использованием системы дистанционного обучения, разработка которой ведется в настоящее время в НЦПИ;
- › очное обучение на практических семинарах.

Кроме того, созданы и проводятся выездные обучающие семинары по теме «Организация и ведение регистра муниципальных нормативных правовых актов субъектов Российской Федерации. Совершенствование нормотворческой деятельности органов местного самоуправления» для специалистов муниципальных образований.

По поручению Минюста России обеспечено:

- › проведение обучения федеральных государственных гражданских служащих Минюста России,
- › работа с системой электронного документооборота «Дело» на учебных площадях НЦПИ.

Для ведения регистров с применением единых правил – правовых, технологических, технических форматов – необходим мониторинг не только муниципальных правовых актов, но и актов субъектов Российской Федерации, поэтому был разработан учебно-методический комплекс [9].

Этот курс подготовлен для служащих, исполняющих функции по формированию и ведению федерального регистра муниципальных нормативных правовых актов. Комплекс содержит целевую установку, организационно-методические указания, программу курса и практических занятий. Эта учебная дисциплина принципиально новая, логически взаимосвязанная,

она представляет собой авторскую разработку, предметное содержание которой обусловлено главным образом требованиями федеральных государственных образовательных стандартов.

В этой учебной дисциплине представлены общие вопросы организации и содержания работы по ведению федерального регистра и реестров (сбор и ввод информации в регистр; хранение информации в регистре; ведение классификаторов, доступ к информации, информационная безопасность, а также проведение юридической экспертизы муниципальных актов, поддержание их текстов в актуальном состоянии и проведению мониторинга правовой системы муниципальных образований по вопросам ведения соответствующих регистров).

В связи с тем, что федеральный регистр имеет информационное и технологическое сопряжение с федеральным регистром нормативных правовых актов субъектов Российской Федерации, реестром уставов муниципальных образований и реестром муниципальных образований, частью этого курса является ознакомление слушателей с правовым обеспечением и методикой ведения указанных реестров.

Уровень информационно-правовой подготовки слушателей (государственных и муниципальных служащих) в условиях наступающего информационного общества определяется не только глубиной и качеством самой информационной подготовки обучения, но и ее непрерывностью, которую необходимо обеспечивать при повышении квалификации: конференции, дистанционное образование и т. д.

В учебном процессе (любом, не только организованном дистанционно) можно выделить несколько задач, которые решаются в ходе обучения:

- › передача обучающемуся определенного объема знаний;
- › первичный контроль;
- › окончательный контроль усвоения знаний курса.

Если первые две задачи могут быть решены и вполне успешно решаются при использовании заочной формы обучения, то для решения третьей задачи необходим контакт с преподавателем – аудио, аудио-визуальный или непосредственный.

Предполагается, что разрабатываемая в НЦПИ система дистанционного обучения будет решать все эти задачи. Для этого создается интерактивный сайт, на котором размещаются следующие учебно-методические материалы,

разработанные при непосредственном участии специалистов-профессионалов по ведению регистров:

- › учебные материалы текстово-графического характера (для удобства пользования, возможно, в различных форматах) – тексты лекций, таблицы, схемы и т.д.;
- › аудио/видео лекции преподавателей, известных практических специалистов;
- › интерактивные формы [5].

Программа обучения включает заочное (дистанционное) обучение с использованием системы дистанционного обучения, разработка которой ведется в настоящее время в НЦПИ, очное обучение на практических семинарах.

Для специалистов в программе обучения рассматриваются наиболее значимые темы и вопросы, знание которых позволит эффективно осуществлять свои служебные полномочия в правоприменительной, правотворческой, образовательной деятельности.

В учебной дисциплине логически последовательно рассматриваются основные вопросы:

- › правовое обеспечение ведения федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации (регистров);
- › цели и принципы ведения регистров муниципальных нормативных правовых актов;
- › система муниципальных нормативных правовых актов;
- › организация доступа к информационным ресурсам регистров муниципальных нормативных правовых актов;
- › структура автоматизированной информационной системы ведения федерального регистра муниципальных нормативных правовых актов.

Одна из актуальных тем при изучении курса – мониторинг правовой системы муниципального образования ведения регистров муниципальных нормативных правовых актов.

Кафедра информационного права в Российской правовой академии Минюста России (РПА) сотрудничает с НЦПИ при Минюсте России. По линии деятельности кафедры создана лаборатория мониторинга правовой информации, которая является структурным подразделением Научно-исследовательского института РПА. Результатом совместной деятельности является научно-образовательный портал «Юстиция».

Основываясь на результатах исследований, в рамках курса осваивается методика ве-

дения регистров муниципальных нормативных правовых актов, виды обеспечения ведения регистров муниципальных нормативных правовых актов.

Особое внимание уделяется вопросам обеспечения информационной безопасности системы ведения регистров муниципальных нормативных правовых актов.

В результате изучения курса «Ведение федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации» слушатели должны знать:

- › нормативные правовые акты в области информации, информатизации и защиты информации, регулирующие отношения по созданию и ведению федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации;
- › состояние правового регулирования ведения федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации, государственного реестра уставов муниципальных образований и реестра муниципальных образований;
- › структуру информационной системы всех регистров нормативных правовых актов и реестров;
- › основные критерии и принципы функционирования системы Минюста России;
- › основы построения и организации функционирования информационных систем в правовой сфере;
- › методику проведения юридической экспертизы муниципальных правовых актов и ведения регистров указанных актов;
- › порядок принятия и вступления в силу муниципальных правовых актов, их особенности, определяемые уставами муниципальных образований;
- › правовые, организационные, технологические, технические вопросы обеспечения информационной безопасности.

После изучения курса слушатели должны уметь:

- › использовать автоматизированные информационные технологии, автоматизированные рабочие места (АРМ) в целях проведения мониторинга муниципальных правовых актов и

принятия решений по вопросам их совершенствования;

- › применять технологию ведения федерального регистра муниципальных нормативных правовых актов и документооборота;
- › В процессе изучения необходимо иметь представление о:
- › требованиях к программному, техническому обеспечению, осуществляющему обработку, хранение, передачу и предоставление информации;
- › функциональных возможностях программного обеспечения автоматизированного делопроизводства;
- › организационном и инженерно-техническом обеспечении безопасности и автоматизированных информационных систем.

Дисциплина изучается на лекциях, групповых и семинарских занятиях, проводимых в традиционных и нетрадиционных (активной и интерактивной) форме, а также в процессе самостоятельной работы.

Необходимо отметить, что 16 августа 2013 года в целях обеспечения осуществления государственных функций по оказанию правовой поддержки государственным органам и гражданам распоряжением Правительства Российской Федерации № 1453-р утвержден план реализации [6] Государственной программы Российской Федерации «Юстиция» [7], предусматривающий создание федеральной информационной системы нормативных правовых актов как информационно-технологической основы Единого регистра, что приводит к необходимости проведения научных исследований данного направления государственной деятельности.

Согласно этой программе, в ФБУ НЦПИ при Министерстве юстиции РФ была разработана Концепция развития подсистемы «Нормативные правовые акты Российской Федерации» Единой системы информационно-телекоммуникационного обеспечения Минюста России до 2020 года. Она была разработана во исполнение п. 5.1 плана реализации Государственной программы Российской Федерации «Юстиция» на 2013 год и на плановый период 2014 и 2015 годов.

Подсистема «Нормативные правовые акты Российской Федерации» Единой системы информационно-телекоммуникационного обеспечения Минюста России (далее – подсистема НПА) является государственной информационной системой, обеспечивающей выполнение задач по ведению федеральных регистров и государственных реестров Министерства юстиции

Российской Федерации и их применение для исполнения государственных функций и обеспечения доступа к актуальной правовой информации.

Одной из задач подпрограммы «Обеспечение защиты публичных интересов, реализации прав граждан и организаций» государственной программы Российской Федерации «Юстиция», утвержденной распоряжением Правительства РФ от 04.04.2013 № 517-р [7] является создание механизма регулярного профессионального совершенствования и подтверждения квалификации.

Таким образом, несмотря на многолетнюю историю, на сегодняшний момент процесс создания нормативной правовой базы электронного образования государственных и муниципальных служащих не завершен. Предстоит длительная и напряженная работа по официальному признанию нормотворческими органами того, что уже вошло в мировую и российскую образовательную практику в качестве неотъемлемой части [8].

К сожалению, следует отметить, что наряду с преимуществами электронного обучения существует и ряд проблем. Характер этих проблем связан отнюдь не с противоречивостью правовых норм, а скорее с их недостаточностью, слабым развитием нормативной правовой базы электронного обучения (регламентация требований к специальным учебно-методическим материалам, подготовке преподавателей-консультантов, системам и процессу администрирования дистанционного процесса, информационной поддержки процесса и электронным библиотекам, образовательных технологий и т. д.)

На сегодняшний день требуется создание соответствующей образовательной среды, научно-методическое обеспечение новых технологий обучения, преподавания и оценки полученных знаний государственными и муниципальными служащими.

Сегодня продолжается дальнейшее развитие информационного обмена в области правовой информации со странами Содружества Независимых Государств и Евразийского Экономического Сообщества. НЦПИ регулярно принимает участие в российских и международных научно-технических программах, конференциях, совещаниях, форумах, конгрессах по вопросам информатики, лингвистики, права. Конференции призваны внести весомый вклад в насыщение конкретными делами и новыми идеями деятельности в области совершенствования федеральных регистров и государственных реестров.

Проводятся работы по созданию ведомственного удостоверяющего центра Минюста России.

Создан аттестационный центр Минюста России на базе НЦПИ и осуществляется аттестация объектов информатизации системы Минюста России. Проводятся работы по созданию комплексной системы безопасности Минюста России.

Учитывая изложенное, необходимо обратить внимание на проблемы, возникающие при ведении регистров. Переход на ведение федерального регистра только в электронном виде является перспективным и необходимым. Вместе с тем следует обратить внимание, что такой переход требует всесторонней подготовки как на правовом, так и на технологическом уровне, который должен сопровождаться внесением изменений в нормативные правовые акты, определяющие ведение регистров. Сегодня это является необходимым условием для перехода к информационному обществу, развитию системы единства правового пространства и повышения эффективности законодательства на территории Российской Федерации.

Из всего вышесказанного можно сделать вывод, что для достижения поставленных задач необходим комплексный подход к разработке и развитию дистанционных образовательных технологий по ведению федеральных регистров и государственных реестров – это имеет важное значение для эффективного функционирования государственных правовых механизмов, обеспечения конституционного права граждан на получение достоверной информации, повышения качества подготовки нормативных правовых актов. От того, на каком уровне будет осуществляться эта работа, во многом зависит развитие всей юридической сферы в обозримой перспективе [10].

Литература

1. Гинзбург И. В., Трошкина Т. Н. Дистанционное образование в Российской Федерации: Понятие и вопросы правового регулирования. // Реформы и право. 2013, № 2.
2. Кузнецов П. У. Информационные ресурсы развития Российской Федерации: Правовые проблемы / Институт государства и права. М.: Наука, 2003.
3. Приказ Минюста России от 14.04.2009 № 109 «О вводе в постоянную эксплуатацию подсистемы «Нормативные правовые акты Российской Федерации» ЕСИТО Минюста России».
4. Колинко А. «Повышаем квалификацию персонала». // «ЭЖ-Юрист», 2013, № 2.
5. Галатов Т. В., Сергин М. Ю., Система дистанционного обучения по ведению регистров муниципальных нормативных правовых актов субъектов Российской Федерации: вопросы разработки и общее описание / IV Всероссийская научно-практическая конференция «Ведение федеральных регистров и государственных реестров, их применение для исполнения государственных функций и обеспечения доступа к актуальной правовой информации». Материалы докладов под общей редакцией к. т. н. доцента А. В. Федичева. – М., 2013. С. 24–26.
6. Федеральный закон от 02.12.2013 № 349-ФЗ (ред. от 02.04.2014) «О федеральном бюджете на 2014 год и на плановый период 2015 и 2016 годов». // Собрание законодательства Российской Федерации, 2013 г., № 49, ст. 6350.
7. Распоряжение Правительства Российской Федерации от 16.08.2013 № 1453-р «Об утверждении плана реализации государственной программы Российской Федерации «Юстиция», утв. распоряжением Правительства Российской Федерации от 04.04.2013 № 517-р // Собрание законодательства Российской Федерации, 2013, № 34, ст. 4479.
8. Сухотин С. О., Белявский А. А. «Организационно-правовое обеспечение электронного обучения с использованием дистанционных образовательных технологий» // Информационное право. 2013. № 3. С. 29–30.
9. Морозов А. В., Филатова Л. В., Благовещенский Н. Ю. Ведение Федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации: Учебно-методический комплекс учебной дисциплины. М.: Москва, 2010. С. 5.
10. Приветствие Министра юстиции Российской Федерации А. В. Коновалова участникам и гостям 4-й Всероссийской научно-практической конференции «Ведение федеральных регистров и государственных реестров, их применение для исполнения государственных функций и обеспечения доступа к актуальной правовой информации». / [Электронный ресурс]. – Режим доступа: <http://www.scli.ru/upload/Приветствие%20Министра%204Конференции.pdf>, свободный (загрузка).

Сведения об авторах

АТАГИМОВА Эльмира Исамудиновна – кандидат юридических наук, начальник научно-исследовательской лаборатории мониторинга правоприменения и развития информационных ресурсов ФБУ НЦПИ при Минюсте России, г. Москва.

E-mail: atagimova75@mail.ru

БОГАТОВА Марина Константиновна – студентка института Прокуратуры Московской государственной юридической академии имени О. Е. Кутафина, г. Москва.

E-mail: marinabogatova2012@mail.ru

МАГДИЛОВА Лариса Владимировна – кандидат юридических наук, доцент кафедры информационного права и информатики ФГБОУ ВПО «ДГУ», г. Махачкала.

E-mail: maglar@mail.ru

МАКАРЕНКО Татьяна Николаевна – начальник отдела анализа и обработки правовой информации ФБУ НЦПИ при Минюсте России, г. Москва.

E-mail: makarenko_tn@scli.ru

РАЙКОВА Наталья Олеговна – специалист ЗАО НПО «Эшелон», г. Москва.

E-mail: partners@npo-echelon.ru

САРАПКИНА Елена Николаевна – заместитель начальника отдела анализа и обработки правовой информации ФБУ НЦПИ при Минюсте России, г. Москва.

E-mail: esarapkina@scli.ru

ТАНИМОВ Олег Владимирович – кандидат юридических наук, доцент, старший научный сотрудник научно-исследовательской лаборатории ФБУ НЦПИ при Минюсте России, г. Москва.

E-mail: tanimov@mail.ru

ЦИРЛОВ Валентин Леонидович – кандидат технических наук, исполнительный директор, CISSP, AMBCI ЗАО НПО «Эшелон», г. Москва.

E-mail: partners@npo-echelon.ru

ШАХАЛОВ Игорь Юрьевич – заместитель генерального директора ЗАО НПО «Эшелон», г. Москва.

E-mail: i.shahalov@npo-echelon.ru

ШИХНАБИЕВА Тамара Шихгасановна – доктор педагогических наук, профессор, действительный член Академии информатизации образования, заведующий лабораторией Института информатизации образования Российской академии образования, г. Москва.

E-mail: shetoma@mail.ru

Abstract and keywords

L. V. Chkhutiashvili

Banking information technology under market economic conditions

Abstract: *this paper is devoted to banking technologies in modern market economic conditions. Banks may develop and introduce new kinds of services based on information technologies, using the latest data encoding methods, “smart” networks and other means of security. The introduction of such services will require creating partner relationships between banks that provide the services, telecommunication organisations and entrepreneurs themselves.*

Keywords: *information society, banking system, technology, business, commercial banks, bank transfers.*

V. L. Tsirlov

Legal issues of cyberspace security in the system of domestic normative documents

Abstract: *the paper is dedicated to legal-normative aspects of cyberspace security. An overview of the new international standard, ISO/IEC 27032, is given. Cyberspace security guiding principles and mechanisms are considered in detail. Possibilities for using the standard in the information security industry are analysed.*

Keywords: *security, cyberspace, guiding principles, standards, normative document.*

E.I. Atagimova, I.M. Ramazanova

Some aspects of the legislative level of ensuring information security in the Russian Federation

Abstract: *some aspects of legislative regulation in the sphere of information security in Russia are considered in the paper. The most significant normative legal acts in the field under consideration are treated.*

Keywords: *legislation, law, information, security, informatisation, personal data, Internet, protection, technology.*

I. Yu. Shakhalov, N. O. Raikova

On the issue of integration of quality and information security management systems

Abstract: *the ISO 27001 and ISO 9001 international standards are considered. An analysis of similarities and differences between quality and information security management systems is made. The possibility to integrate a quality management system and an information security management system is shown. The main stages of building and introducing an integrated information security management system are presented. The advantages of the integrated approach are shown.*

Keywords: *information security management system, integrated management system, ISMS, QMS, ISO 27001.*

T.Sh. Shikhnabieva

On some approaches to modernisation of educational systems using intellectual methods and models

Abstract: *for an efficient functioning of information systems used in education it is necessary to solve a number of problems related to presentation, processing, and use of knowledge. For accessing and efficiently using knowledge, it should be classified and structured. Some approaches to the improvement and development of learning systems based on the achievements of today’s system analysis, cybernetics, and synergetics are proposed in the paper.*

Keywords: *education technologies, distance education, semantic net, adaptive semantic model, automated learning system.*

T.N. Makarenko, E.N. Sarapkina

Topical issues of systematisation of legal acts

Abstract: *the paper considers issues of preservation, dissemination of, and search for legal information. Problems of systematisation, classification, and official publishing of legal acts are touched upon.*

Keywords: *legislation systematisation, automated information search systems, classification of legal acts, electronic publishing, official electronic publishing sources.*

L.V. Magdilova

Specific features of forming the legal information space of public authorities in the Republic of Dagestan: the legal aspect

Abstract: *in this paper, the notion and characteristics of legal information space of the subject of the Russian Federation are defined more exactly and major regional provisions of its development are analysed. The readiness of public authorities for the introduction of ICT as well as the practice of their operation is examined. Some lines of development of the legal information space of public authorities of the Republic of Dagestan are worked out.*

Keywords: *information space, information society, information law, electronic government, the Republic of Dagestan, regional information legislation.*

O.V. Tanimov, M.K. Bogatova

Ensuring information security in management of large cities

Abstract: *a study of problems of ensuring information security in management of large cities from the theoretical and practical viewpoint is conducted in the paper. The role of information security in the management process is noted. The need to improve the mechanism of legal regulation in the process of solving these problems with due regard for the specific features of large cities is emphasised. New steps in solving the problems under consideration are proposed.*

Keywords: *information, information security, large cities, information relationships, management, problems.*

N.A. Fadeeva

Advanced training of specialists in maintenance of normative legal acts registers at the Scientific Centre of Legal Information under the Ministry of Justice of the Russian Federation

Abstract: *the paper considers educational activities directed at advanced training of federal public officers, public officers of the subjects of the Russian Federation, municipal public officers, and training of register maintenance specialists.*

Keywords: *educational activities, educational process, normative legal acts, register, information society, Concept, automated information systems.*



В редакционный Совет нашего журнала вошел в качестве члена Совета Абдусаламов Руслан Абдусаламович – заведующий кафедрой информационного права и информатики юридического факультета ФГБОУ ВПО «Дагестанского государственного университета», кандидат юридических наук, доцент.

Руслан Абдусаламович родился в 1978 году в с. Сулевкент Хасавюртовского района Республики Дагестан. В 1995 году с отличием закончил Сулевкентскую среднюю школу и поступил на первый курс физического факультета Дагестанского государственного университета по специальности «Физика».

В 2000 году закончил Дагестанский государственный университет с присвоением квалификации «Физик. Преподаватель физики и информатики» по специальности «Физика». В 2009 году после обучения по сокращенной программе в Российской правовой академии получил второе высшее образование с присвоением квалификации «Юрист» по специальности «Юриспруденция».

В 2006 году защитил кандидатскую диссертацию по специальности 13.00.08 - Теория и методика профессионального образования на заседании Диссертационного совета Д 212.051.04 по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук при ФГБОУ ВПО «Дагестанский государственный педагогический университет».

В период с 2000 по 2008 гг. работал в Северо-Кавказском филиале Российской правовой академии Минюста России в должностях старшего преподавателя, заместителя декана юридического факультета. С 2008 года работает в ФГБОУ ВПО «Дагестанский государственный университет» в должностях начальника информационно-аналитического отдела учебно-методического управления, доцента кафедры информационного права и информатики юридического факультета. С 2013 года по настоящее время является заведующим кафедрой информационного права и информатики юридического факультета ДГУ.

Сфера научных интересов:

- информационная культура студентов-юристов;
- правовые основы внедрения информационных технологий в юридическую деятельность;
- информационное право и правовая информатика.

Автор более 30 опубликованных научных и научно-методических публикаций.

Откликаясь на наше предложение войти в состав редакционного Совета журнала «Правовая информатика», доцент Р.А. Абдусаламов выразил уверенность в необходимости актуализации освещения научных тем, связанных с правовыми информационными системами.

Редакция надеется, что энергия и опыт Руслана Абдусаламовича будут способствовать широкому освещению на страницах нашего журнала новых идей и решений в области информационного права и информационной безопасности.

К 50-ЛЕТИЮ

ОЛЕГА ВЛАДИМИРОВИЧА ТАНИМОВА



В 2014 году член редакционной коллегии научного журнала «Правовая информатика» и научного журнала «Мониторинг правоприменения» Олег Владимирович Танимов отметил свой юбилей.

Олег Владимирович ТАНИМОВ – старший научный сотрудник Научного центра правовой информации Министерства юстиции Российской Федерации (НЦПИ при Минюсте России), кандидат юридических наук, доцент, третейский судья при Торгово-промыш-

ленной палате Республики Мордовия, член Методического совета Мордовской лаборатории судебной экспертизы Минюста России в РМ, действительный член международной организации бухгалтеров и аудиторов, член Ассоциации выпускников МГИМО; родился 20 апреля 1964 года. Место рождения с-з «Красная Пресня» Ковылкинского р-на МАССР. По образованию – юрист (юриспруденция), психолог (практическая психология), военный (командная тактическая), инженер (электрооборудование летательных аппаратов).

О.В. Танимов – учёный в области теории права, информационного права с приложениями в сфере информационной безопасности, юридической техники. Автор более 100 научных и учебно-методических работ, в том числе шести монографий¹, двух словарей², шести учебных пособий³, статей в научных журналах российских и зарубежных изданий (30), а также интернет-обзоров, интернет-интервью и др. Завершает работу над диссертационным исследованием на соискание ученой степени доктора юридических наук (докторантура МГЮА им. О.Е. Кутафина). Организовал межвузовское виртуальное студенческое научное общество, в котором участвуют более 70 человек из 12 вузов России.

Разработал, в том числе в соавторстве, ряд руководящих концепций развития деятельности структурных элементов органов государственной власти.

Основные труды: «Правовое регулирование деятельности бюджетных учреждений в Российской Федерации» (2006), «Деятельность бюджетных учреждений в Российской Федерации» (2006), «Информационное право» (2009), «Историческая мозаика: социальная, юридическая, экономическая и культурная повседневность мордовского края» (2011), «Юридические фикции: история, предпосылки возникновения и развития» (2011), «Фикция как категория юридической науки» (2012), «Этапы становления и развития юридических фикций» (2014 – в печати), а также в соавторстве: «Из истории мордовского края: право, экономика, демография, статистика» (2007), «Выявление и раскрытие изготовления или сбыта поддельных кредитных либо расчетных карт» (2007), «Учебные программы и методические материалы кафедры теории и истории государства и права» (2009), «Словарь основных понятий и категорий международного права» (2010),

Увлечения: спорт (киокушин-каратэ – I дан), музыка (гитара).

Женат, имеет троих детей.

Ведёт общественно-научную работу. Член редколлегии журналов: «Информационное право» (ответственный секретарь), «Мониторинг правоприменения» (ответственный редактор), «Правовая информатика» (член редакционной коллегии).

¹ См., например: Танимов О.В. Юридические фикции: история, предпосылки возникновения и развития. Монография. Москва : ФГБОУ ВПО «РЭУ им. Г.В. Плеханова», 2012. – 8,5 п.л.; Фикция как категория юридической науки. Монография. Саарбрюккен (Германия): LAP LAMBERT Academic Publishing. – 2012. – 15,25 п.л. и др.

² Танимов О.В., Баршова О.А., Гарькина Т.А., Цыганова Е.В. Словарь основных понятий и категорий международного права. Справочное издание. Саранск: Издательство ООО «Вектор-принт», 2010. (112/50 с.)

³ См., например: Танимов О.В. Правовое регулирование деятельности бюджетных учреждений в Российской Федерации : учеб. пособие - Саранск, 2006. – 14 п.л.; Выявление и раскрытие изготовления или сбыта поддельных кредитных либо расчетных карт. Учебное пособие. – Саранск: Тип. «Рузаевский печатник», 2007. (126/42) (в соавторстве с В.П. Кувалдиным и И.Н. Волосевич). – 4,7 п.л. и др.

Разработал и поставил впервые в Мордовском государственном университете им. Н.П. Огарева учебные дисциплины «Проблемы ответственности в международном праве» и «Правовые фикции», а также разработал 3 новых учебных плана. Подготовил 45 дипломированных специалистов в области теории государства и права, информационного права, международного права.

О.В. Танимов проявил себя как высококвалифицированный учёный и преподаватель, отличается большой творческой инициативой и ответственностью в работе. За заслуги перед Отечеством награжден тремя медалями Минобороны (1988, 1991, 1996); за достижения в научно-педагогической деятельности и подготовке высококвалифицированных кадров получил Благодарность Министра юстиции Российской Федерации (2010); за вклад в правовое просвещение граждан удостоен Благодарности Общественной палаты Российской Федерации (2014).

Коллеги, ученики, редакция журнала «Правовая информатика» от всего сердца поздравляют Олега Владимировича Танимова с юбилеем, желают ему крепкого здоровья, семейного благополучия и творческих успехов!

Над номером работали:

Главный редактор	М.Ю. Сергин
Ответственный секретарь	Э.И. Атагимова
Ответственный редактор	Ю.В. Матвиенко
Литературный редактор	Е.В. Горбачева, Т.В. Галатонов
Научный редактор	Г.И. Макаренко
Выпускающий редактор	И.Г. Колмыкова
Компьютерная верстка	А.С. Михеева
Тиражирование (печать)	Н.Г. Шабанова

Требования, предъявляемые к рукописям, направляемым в редакцию

1. В структуру статьи должны входить: название статьи, полностью Ф.И.О. автора, его ученая степень и ученое звание, e-mail автора, аннотация статьи, ключевые слова. Все эти данные следуют сначала на русском, затем на английском языках, далее текст собственно статьи на русском языке.
2. Автору статьи рекомендуется придерживаться следующей последовательности изложения материала: введение (краткое), цель исследования, материалы и методы исследования, результаты исследования и их обсуждение, выводы или заключение, список литературы. Статья должна содержать результаты самостоятельных исследований автора и обладать научной новизной.
3. К рукописи прикладываются отдельным файлом сведения об авторе на русском языке: Фамилия, Имя, Отчество, год рождения, место работы (без сокращений) или учебы, ученая степень и ученое звание, e-mail и телефон для связи. К публикации принимаются научные статьи объемом не менее 4 страниц и не более 16 страниц (страница – 2500 знаков, включая пробелы).
4. Статья оформляется в любом текстовом редакторе. Рисунки, использованные в статье, прилагаются в виде отдельных файлов в формате *.jpg или *.tif с разрешением не менее 300 dpi для оригинального размера в печатном издании. Цвет приветствуется. Имена файлов рисунков должны быть такими, какое они имеют в тексте. Математические выражения, имеющиеся в статье, представляются в формате редактора формул.
5. Допускаются сокращения и условные обозначения, принятые в Международной системе единиц (сокращения мер, физических, химических и математических величин и терминов). Сокращение типа «т.к.», вместо «так как» и тому подобные, не допускаются.
6. Цитируемая литература и источники приводятся в конце статьи по порядку упоминания в тексте (ГОСТ Р 7.0.5–2008). В списке литературы приводят следующие данные: а) фамилию и инициалы автора (авторов), б) название журнала (книги, диссертации), год, том, номер, первую страницу (для книг сообщают место издания, издательство и количество страниц, для диссертации институт, в котором выполнена работа). Подстрочные ссылки не допускаются, так как журнал верстается в профессиональных издательских программах и геометрические параметры статьи не будут соответствовать виду в текстовом редакторе. Ссылки даются в тексте строго в квадратных скобках: [16, с.5], [7, 25, 105].
7. Стиль статьи должен быть научным, ясным и лаконичным.
8. Аннотация объемом 200–400 печатных знаков должна содержать характеристику основной темы исследования. Аннотация должна быть на русском и английском языках. После аннотации следуют ключевые слова (5–10 слов) также на двух языках.
9. Рукописи, направленные в редакцию без выполнения настоящих требований, не рассматриваются. Редакция оставляет за собой право отбора статей. Рукопись может быть отправлена автору на доработку или отклонена как по формальным, так и по научным признакам. Критериями отбора являются соответствие профилю журнала, новизна, актуальность и обоснованность результатов. Присланные рукописи обратно не возвращаются. Не допускается направление в редакцию работ, которые опубликованы и/или приняты к печати в других изданиях.
10. Предоставление своего фото автором статьи – обязательное условие для принятия решения к рассмотрению для публикации.

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВЕДЕНИЯ ФЕДЕРАЛЬНЫХ РЕГИСТРОВ И ГОСУДАРСТВЕННЫХ РЕЕСТРОВ

ФБУ НЦПИ при Минюсте России проводит обучение специалистов по программам повышения квалификации в области информационных технологий, ведения федеральных регистров, государственных реестров и их применения для исполнения государственных функций и обеспечения доступа к актуальной правовой информации. Продолжительность курсов — 72 часа. По окончании обучения выдается удостоверение о краткосрочном повышении квалификации установленного образца.



Методы и формы обучения:

- **Автоматизированное тестирование** — используется перед началом обучения, когда каждый слушатель проходит процедуру проверки текущего уровня знаний, и в конце обучения с целью проведения оценки полученных знаний.
- **Индивидуальное обучение** — это гибкая адаптация базовой учебной программы под вопросы конкретного слушателя, что позволяет слушателям изучать именно тот материал, который им нужен для выполнения своих профессиональных задач.
- **Применение перспективных форм предоставления учебного материала** — лекционные занятия построены в форме дискуссии, в которой преподаватель, раскрывая материал, ведет диалог со слушателями, в то время, как сама лекция построена в виде презентации и отображается через мультимедийный проектор.
- **Обучающий компьютерный класс** — позволяют слушателям совершенствовать навыки практической работы при выполнении своих профессиональных задач.

КОНТАКТЫ

Федеральное бюджетное учреждение
«НАУЧНЫЙ ЦЕНТР ПРАВОВОЙ ИНФОРМАЦИИ
ПРИ МИНИСТЕРСТВЕ ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ»

125438, г. Москва,
ул. Михалковская, д. 65, корп. 1
Тел.: (495) 539-23-90
e-mail: helix@yandex.ru
www.scli.ru

Лицензия Федеральной службы по надзору в сфере образования и науки
от 05.04.2012 Серия ААА №002952