МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НЦПИ

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

ПРАВОВАЯ ИНФОРМАТИКА

Периодический научный журнал

Выпуск № 3 – 2013

Москва, 2013

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

Правовая информатика. Выпуск 3–2013. — М. : ФБУ НЦПИ при Минюсте России, 2013. — 76 с.
ISSN 1994-1404

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)539-23-17, E-mail: pravo360@gmail.com
www.pravo360.ru

ISSN 1994-1404

СОДЕРЖАНИЕ

Шахалов Игорь Юрьевич
доцент
Дорофеев Александр Владимирович

Основы управления информационной безопасностью современной организации

Аннотация: *рассматриваются основы внедрения и управления систем информационной безопасности. Дается краткий исторический экскурс, определяются цели, показатели, методики для создания эффективной системы управления информационной безопасности. В Приложении дается перечень международных стандартов ISO 27000 и их российских аналогов в рассматриваемой области.*

Ключевые слова: *информационная безопасность, защита данных, управление безопасностью, планирование, мониторинг, стандарты, цикл Деминга-Шухарта.*

Современный стиль ведения бизнеса стимулирует компании активно развиваться и максимально использовать информационные технологии. Быстрое развитие, в свою очередь ,неизбежно ведет к хаосу в бизнес-процессах и появлению новых рисков, среди которых не последнее место занимают риски информационной безопасности (ИБ). Сегодня, к примеру, утечка персональных данных клиентов легко может привести не только к удару по имиджу компании и финансовым потерям, но и проблемам с регулирующими органами.

Многие зарубежные национальные институты стандартов и организации, специализирующиеся в решении комплексных проблем информационной безопасности, предложили концепции проведения аудита и управления информационными рисками, которые нашли отражение в соответствующих международных и национальных стандартах оценки информационной безопасности и управления ею — ISO 15408, ISO 270xx, COBIT, SAC, COSO, SAS 55/78 и другие.

В соответствии с этими стандартам организация режима ИБ в любой компании предполагает следующее [1, 2]:

- определение целей обеспечения информационной безопасности компании;
- создание эффективной системы менеджмента информационной безопасности;
- расчет показателей для оценки соответствия информационной безопасности и оценки ее текущего состояния;
- использование методик анализа рисков и управления ими, позволяющих объективно оценить текущее состояние дел.

На сегодняшний момент как на российском, так и на международном рынке ИБ накоплен значительный опыт построения эффективных систем менеджмента информационной безопасности (СМИБ), который нашел отражение в целой серии международных стандартов серии ISO 27000.

1. Из истории вопроса

В первой половине 90-х годов прошлого века Британским институтом стандартов (British Standards Institution, BSI) при участии ряда крупных коммерческих организаций

(Shell UK, National Westminster Group, Unilever, British Telecommunications, British Computer Society, Association of British Insurers, Marks & Spencer, Logica и др.) был разработан стандарт **BS 7799**, который в 1995 году в качестве свода установленных норм и правил по отношению к обеспечению ИБ получил в Великобритании статус государственного.

Первая часть стандарта **BS 7799** «Практические правила управления информационной безопасностью» была разработана в 1995 г. по заказу правительства Великобритании.

Как следует из названия, первая часть стандарта является практическим руководством по управлению информационной безопасностью в организации. Она описывает 10 областей и 127 механизмов контроля, необходимых для построения СМИБ, определенных на основе лучших примеров из мировой практики.

В 1998 году появилась вторая часть этого стандарта **BS 7799** «Системы менеджмента информационной безопасности. Спецификация и руководство по применению», определившая общую модель построения СМИБ и набор обязательных требований, на соответствие которым должна производиться сертификация. С появлением второй части BS 7799, определившей, что должна представлять из себя СМИБ, началось активное развитие систем сертификации в области менеджмента безопасности.

В начале 2006 г. был принят новый британский национальный стандарт в области управления рисками информационной безопасности **BS 7799-3** «Системы менеджмента информационной безопасности — Часть 3: Руководство по управлению рисками информационной безопасности», который получил индекс 27005. Также в настоящий момент действуют международные стандарты по внедрению и измерению эффективности СМИБ, которые получили индексы 27003 и 27004 соответственно.

В 1999 году обе части BS 7799 были пересмотрены и гармонизированы с международными стандартами систем менеджмента ISO 9001 и ISO 14001, а год спустя технический комитет ISO без изменений принял BS 7799-1 в качестве международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).

Вторая часть BS 7799 пересматривалась в 2002 г., а в конце 2005 г. была принята ИСО в качестве международного стандарта **ISO/IEC 27001:2005** «Информационные технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности— Требования». В это же время была обновлена и первая часть стандарта. Последней версией данного стандарта, принятой в 2005 году, является ISO/IEC 17799:2005. В настоящий момент ISO/IEC 17799:2005 переименован в ISO/IEC 27002.

С выходом ISO 27001 спецификации СМИБ приобрели международный статус, и значительно повысили роль и престижность СМИБ, сертифицированных по стандарту ISO 27001.

Семейство стандартов ISO 27000 продолжает активно развиваться. В соответствии с планами ISO оно будет включать стандарты, определяющие требования к СМИБ, систему управления рисками, метрики и измерения эффективности механизмов контроля, а также руководство по внедрению. Для этого семейства стандартов будет использоваться последовательная схема нумерации, начиная с 27000 и далее. Обзор стандартов серии 27000 приведен в Приложении.

2. Основные положения стандарта

Международный стандарт ISO/IEC 27001:2005 «Информационные технологии — Методы и средства обеспечения безопасности — Системы менеджмента информационной безопасности — Требования» имеет российский аналог — ГОСТ Р ИСО/МЭК 27001-2006.

Стандарт определяет информационную безопасность как «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность».

Конфиденциальность — обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);

Целостность — обеспечение точности и полноты информации, а также методов ее обработки;

Доступность — обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Стандарт является рабочим инструментом для внедрения СМИБ в организации, а также по проведению аудита по подтверждению того, что средства управления безопасности существуют и функционируют в соответствии с требованиями стандарта. Стандарт описывает СМИБ как всеохватывающую систему менеджмента, построенную на принципах бизнес-рисков, для вне-

дрения, эксплуатации, мониторинга и поддержки системы менеджмента безопасности.

В основу модели организации процессов СМИБ стандарта ISO/IEC27001:2005 заложен классический замкнутый цикл менеджмента Plan-Do-Check-Act (PDCA, «планирование — осуществление — проверка — действие»), который известен как «цикл Деминга» или «цикл Деминга-Шухарта» [3].

Рисунок 1 отражает модель PDCA (Plan-Do-Check-Act), используемую для внедрения СМИБ (цикл СМИБ).

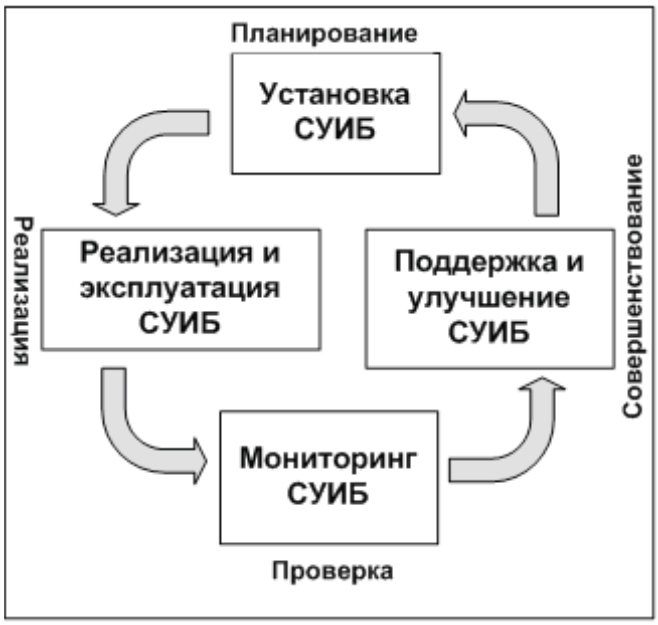

Рисунок 1.Цикл СМИБ

Выполнение требований ISO/IEC 27001:2005 позволяет организациям формализовать и структурировать процессы управления информационной безопасностью по следующим направлениям:

- разработка политики безопасности;
- организация информационной безопасности;
- организация управления внутренними активами и ресурсами, составляющими основу ключевых бизнес-процессов;
- защита персонала и снижение внутренних угроз;
- физическая безопасность и безопасность окружающей среды;
- управление средствами связи и эксплуатацией оборудования;
- управление и контроль доступа;
- разработка и обслуживание аппаратно-программных систем;
- управление непрерывностью бизнес-процессов;
- соответствие требованиям стандарта и соблюдение правовых норм по безопасности.

Цели и механизмы контроля стандарта ISO/IEC 27001:2005 по каждому из направлений работ заимствованы из стандарта ISO/IEC 17799:2005 (разделы 5-15) и перечислены в его Приложении А — Control objectives and controls [4].

3. Основные этапы работ по созданию СМИБ

Построение корпоративной СМИБ — это сложный, многоэтапный, циклический организационно-технологический процесс. Внедрение данного стандарта целесообразно осуществлять в несколько последовательных этапов (Рисунок 2).

Началом разработки СМИБ является **аудит организации** на соответствие положениям ISO/IEC 27001:2005.

Изначально в организациях, как правило, существуют разного рода положения, инструкции и иные организационно-распорядительные документы, которые регламентируют работу структурных подразделений. Аудит позволяет выявить и систематизировать такие документы в соответствии с требованиями ISO/IEC 27001:2005. После этого можно определить направления работ по созданию системы менеджмента информационной безопасности организации. Основная цель аудита — объективно оценить состояние существующей системы

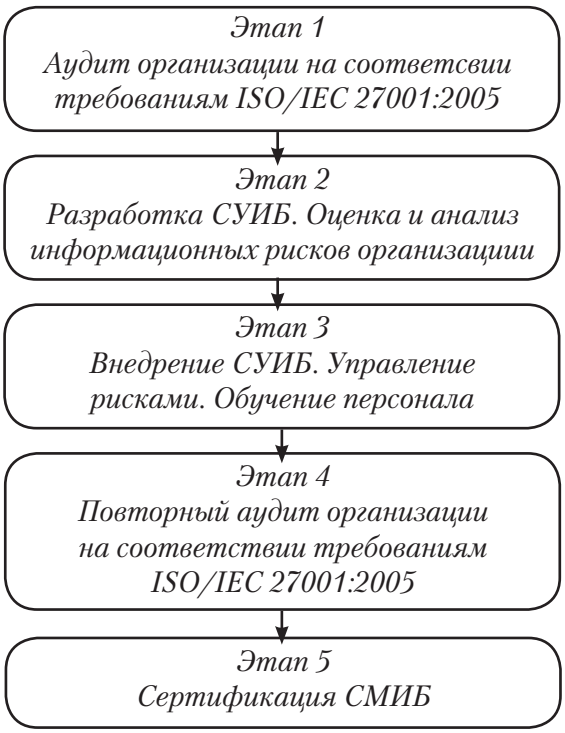

Рисунок 2.Этапы построения СМИБ

менеджмента информационной безопасности и ее адекватность целям и задачам бизнеса, после чего разработать рекомендации по совершенствованию имеющейся СМИБ, либо по построению и внедрению новой.

Во время выполнения аудиторских работ решаются следующие основные задачи:

- анализ структуры организации;
- анализ защищаемой области деятельности и организационно-распорядительных документов;
- анализ структуры и функциональных особенностей, используемых информационных технологий автоматизированной системы сбора, обработки, передачи и хранения информации;
- проверка выполнения требований ISO/IEC 27001:2005 к СМИБ;
- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, техническому и аппаратно-программному обеспечению для создания, построения или совершенствования СМИБ.

В большинстве случаев решение данных задач выполняется в четыре основных этапа (Рисунок 3) [2]:

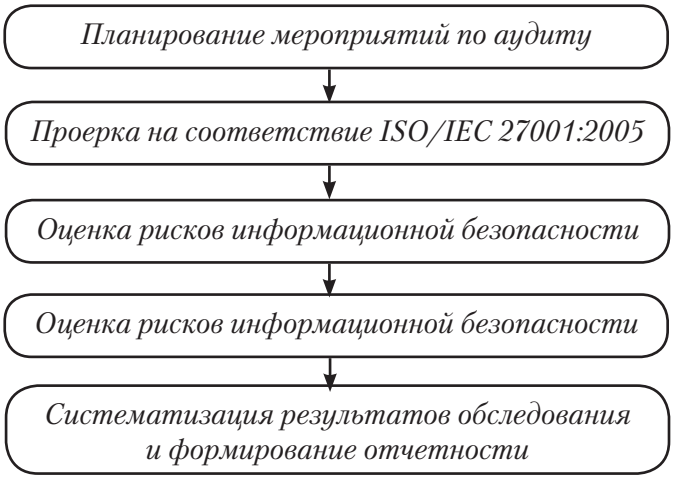

Рисунок 3. Этапы аудита СМИБ

Планирование мероприятий по аудиту. На данном этапе осуществляется сбор организационно-распорядительных документов, отраслевых стандартов, недокументированных проектных решений и других рабочих материалов, касающихся вопросов создания системы менеджмента информационной безопасности и информационных систем организации, способствующих использованию механизмов и средств обеспечения информационной безопасности, проводится разработка, согласование и утверждение планов мероприятий по аудиту.

Проверка на соответствие ISO/IEC 27001:2005. Этот этап включает: определение области деятельности и ключевые бизнес-процессы организации, которые необходимо защитить в первую очередь; проведение анкетирования и интервьюирования сотрудников организации, анализ организационно-распорядительных и нормативных документов и анализ информационной безопасности на соответствие ISO/IEC 27001:2005.

Оценка рисков информационной безопасности. Аналитический и инструментальный анализ АС и информационных ресурсов организации. Проведение консультаций со специалистами, оценка соответствия фактического уровня безопасности информации и анализ рисков [5].

Систематизация результатов обследования и формирование отчетности. Предоставление итогового отчета руководству организации.

После выполнения аудиторских работ организация приступает к **разработке, внедрению или совершенствованию** системы менеджмента информационной безопасности.

При этом предполагается решение следующих основных задач:

- анализ структуры организации, функциональных особенностей построения бизнес-процессов и используемых в них информационных технологий. Определение защищаемой области деятельности организации;
- идентификация, систематизация и определение ценности активов организации;
- анализ рисков ИБ, определение возможных путей их реализации (несанкционированных воздействий на подсистемы и бизнес-процессы организации), категорирование рисков по степени критичности. Оценка возможного ущерба от реализации угроз. Расчет эффективности внедрения комплексных мероприятий по снижению рисков;
- разработка Политики информационной безопасности организации;
- разработка Процедуры по снижению рисков;
- разработка Положения о применимости контролей — комплексов мероприятий информационной безопасности в соответствии с Приложением А стандарта ISO/IEC 27001:2005;
- разработка и внедрение СМИБ;
- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, техническому и аппаратно-программному обеспечению режима информационной безопасности организации;
- анализ и оценка результатов внедрения СМИБ.

Рассмотрим основные этапы работ (Рисунок 4) по построению и внедрению СМИБ организации.

В зависимости от специфики работы, защищаемой области деятельности компании и числа сотрудников, количество этапов и их детализация могут изменяться. Рассмотрим все этапы работы детально.

Планирование и подготовка планов мероприятий. На данном этапе осуществляется сбор организационно-распорядительных документов и других рабочих материалов, касающихся вопросов построения и функционирования информационных систем организации, планируемых к использованию механизмов и средств обеспечения информационной безопасности, а также осуществляется разработка, согласование и утверждение планов мероприятий по этапам работ и утверждение их у руководства организации.

Проверка на соответствие ISO/IEC 27001:2005. Проведение интервьюирования и анкетирования менеджеров и сотрудников различных подразделений организации. Анализ СМИБ организации на соответствие требованиям стандарта ISO/IEC 27001:2005.

Анализ нормативных и организационно-распорядительных документов. Анализ ОРД осуществляется исходя из организационной структуры. После этого уточняется или выполняется определение защищаемой области деятельности и разрабатывается эскиз политики информационной безопасности организации.

Анализ и оценка рисков ИБ. Разработка методики по анализу и управлению рисками организации. Аналитический и инструментальный анализ локальной вычислительной сети и информационных ресурсов организации, с целью выявления угроз и уязвимостей защищаемых активов ОД. Инвентаризация активов. Проведение консультаций со специалистами организа-

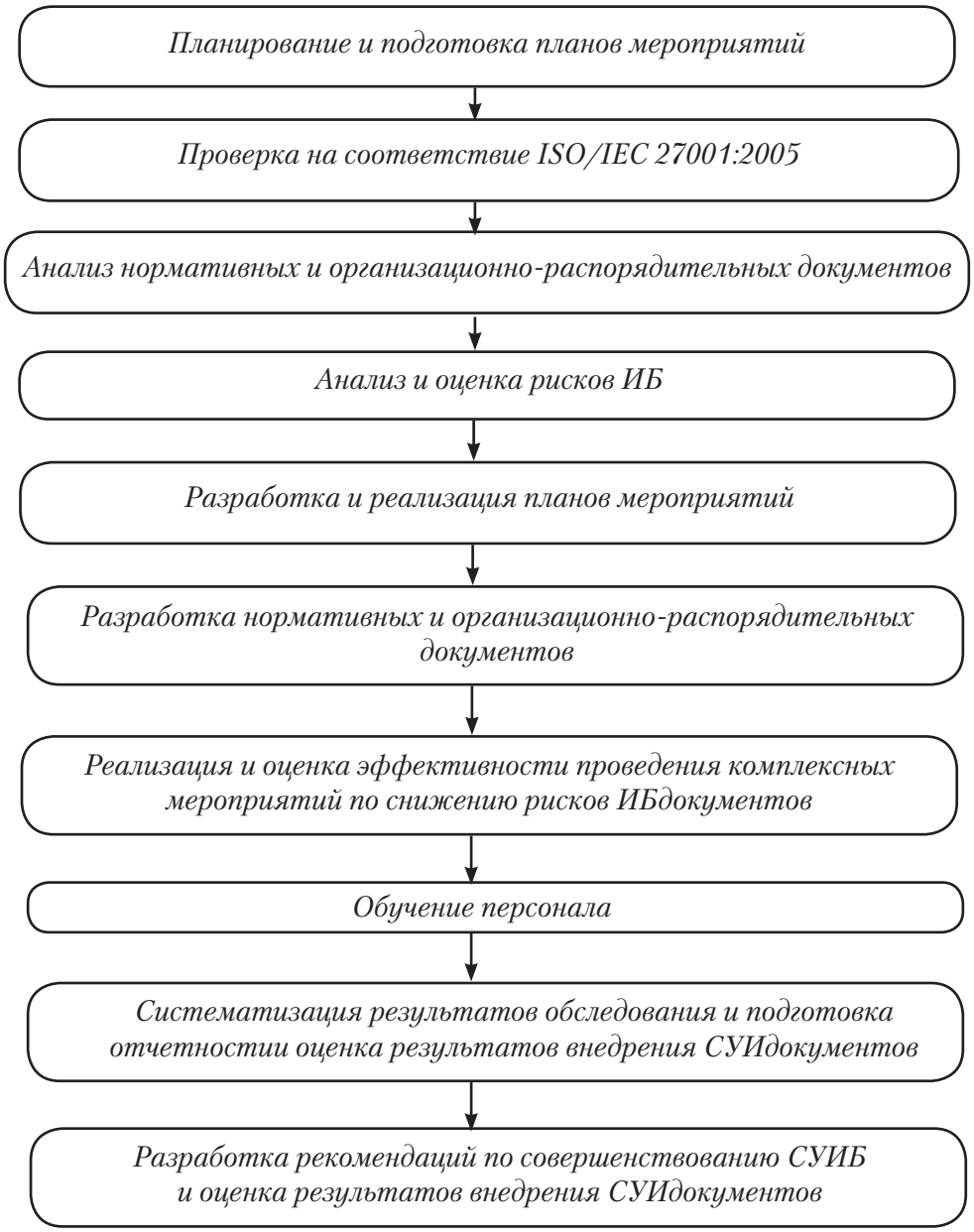

Рисунок 4. Этапы работ по построению и внедрению СМИБ организации

ции и оценка соответствия фактического уровня безопасности. Расчет рисков, определение текущего и допустимого уровня риска для каждого конкретного актива. Ранжирование рисков, выбор механизмов контроля по их снижению и расчет теоретической эффективности внедрения.

Разработка и реализация планов мероприятий. Разработка Положения о применимости механизмов контроля в соответствии с ISO/IEC 27001:2005. Разработка Плана обработки и устранения рисков. Подготовка отчетов для руководителя организации.

Разработка нормативных и организационно-распорядительных документов. Разработка и утверждение окончательной Политики информационной безопасности и соответствующих ей положений. Разработка стандартов, процедур и инструкций, обеспечивающих нормальное и стабильное функционирование и эксплуатацию СМИБ.

Реализация и оценка эффективности применения механизмов контроля по снижению рисков ИБ, в соответствии с утвержденным руководителем Планом обработки и устранения рисков.

Обучение персонала. Разработка планов мероприятий и внедрение программ по обучению и повышению компетенции сотрудников организации с целью эффективного донесения принципов информационной безопасности для

всех руководителей и сотрудников, и в первую очередь для тех из них, структурные подразделения которых участвуют в обеспечении ключевых бизнес-процессов.

Систематизация результатов обследования и подготовка отчетности. Представление результатов работ для руководителей организации. Подготовка документов на сертификацию на соответствие ISO/IEC 27001:2005 и передача их в сертифицирующую организацию.

Анализ и оценка результатов внедрения СМИБ (осуществляется на основании методики оценки надежности функционирования СМИБ). Разработка рекомендаций по совершенствованию СМИБ.

Стоит подчеркнуть, что **этап повторного аудита** после создания корпоративной СМИБ не является обязательным (хотя он в модели Шухарта и присутствует), но вполне целесообразным перед сертификацией с целью уточнения выполнения требований стандарта и рекомендаций консалтинговой компании.

Последний этап формирования СМИБ — **сертификация** на соответствие требованиям международного стандарта ISO/IEC 27001:2005.

Процедура сертификации по ISO/IEC 27001:2005 достаточно проста [6].

После трех-шести месяцев эксплуатации СМИБ организация-заказчик подает заявку на сертификацию в одну из уполномоченных организаций, которые имеют право выдачи сертификатов соответствия.

После утверждения заявки уполномоченная организация присылает аудиторов для изучения документации с целью выявления слабых мест в СМИБ, и если таковых не обнаружено, проводит сертификационный аудит в организации, представляя график проведения аудита и сметы.

При успешном завершении аудита выдается сертификат соответствия.

Выводы

Таким образом, продуманная внутренняя система документов по информационной безопасности, качественное обучение специалистов и беспристрастный контроль в виде регулярного аудита серьезно продвинут компанию к построению эффективной системы менеджмента информационной безопасности.

В случае если компания при построении СМИБ полностью выполнит требования стандарта ISO/IEC 27001:2005, она сможет пройти сертификацию в аккредитованной организации и повысить доверие к себе со стороны клиентов и партнеров, для которых важно обеспечение безопасности информации.

Очень важно понимать, что привлечение компании-интегратора для построения СМИБ на условиях аутсорсинга не является достаточным для того, чтобы система заработала [7]. Система менеджмента информационной безопасности требует ответственного отношения от всех сотрудников компании и серьезной поддержки руководства, но когда она реально становится частью системы управления бизнесом, компания позиционируется как надежный и безопасный партнер.

Литература

1. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов; под ред. А.С.Маркова. – М.: Радио и связь, 2012. 192 с.
2. Основы информационной безопасности: краткий курс / В.Л.Цирлов — Ростов н/Д: Феникс, 2008. — 253с.
3. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011г. / Матвеев В.А., Медведев Н.В., Троицкий И.И., Цирлов В.Л. // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. – 2011. – Спец. вып. Технические средства. – С. 3-6.
4. О внедрении ГОСТ ИСО/МЭК 17799 и 27001 / А.С.Марков, С.А.Леденко и др. // Information Security – 2006 – №3/4.
5. Управление рисками — нормативный вакуум информационной безопасности / А.С.Марков и В.Л.Цирлов // Открытые системы. СУБД. 2007. №8. С. 63-67.
6. Лицензирование в области защиты информации: Новые требования. / И.Ю.Шахалов — Сочи: ИнфоБерег-2012 (11-16 сентября 2012 г.).
7. Возможности применения аутсорсинга в сфере обеспечения информационной безопасности: Критерии эффективности. / И.Ю.Шахалов — Инфофорум-2010 (28-29 января 2010 г.).

Приложение

Международные стандарты серии 27000 (опубликованные)*

Серия ИСО 27000 (ISO/IEC 27000 ISMS) Системы менеджмента информационной безопасности			
Обозначение	**На английском**	**На русском**	**ГОСТ**
ISO / IEC 27000:2012	Information technology – Security techniques -Information security management systems – Overview and vocabulary	Информационные технологии. Методы обеспечения защиты. Системы менеджмента защиты информации. Обзор и словарь	ГОСТ Р ИСО / МЭК 27000 (проект 1-я редакция)
ISO / IEC 27001:2005	Information technology – Security techniques – Information security management systems – Requirements	Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	ГОСТ Р ИСО / МЭК 27001-2006
ISO / IEC 27002:2005	Information technology – Security techniques – Code of practice for information security management	Информационные технологии. Свод правил по управлению защитой информации	ГОСТ Р ИСО / МЭК 17799-2005
ISO / IEC 27003:2010	Information technology – Information security management system implementation guidance	Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности	ГОСТ Р ИСО /МЭК 27003 (проект 1-я редакция)
ISO / IEC 27004:2009	Information technology – Security techniques – Security techniques -Information security management measurements	Информационнаятехнология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения	ГОСТ Р ИСО / МЭК 27004-2011
ISO / IEC 27005:2011	Information technology – Security techniques – Information security risk management	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности	ГОСТ Р ИСО / МЭК 27005-2010

Серия ИСО 27000 (ISO/IEC 27000 ISMS) Системы менеджмента информационной безопасности			
Обозначение	**На английском**	**На русском**	**ГОСТ**
ISO / IEC 27006:2011	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	Информационные технологии. Методы и средства обеспечения безопасности. Требования для органов, осуществляющих аудит и сертификацию систем менеджмента информационной безопасности	ГОСТ Р ИСО/ МЭК 27006-2008
ISO / IEC 27007:2011	Information technology – Security techniques – Guidelines for information security management systems auditing	Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по аудиту систем менеджмента систем информационной безопасности	
ISO / IEC TR 27008:2011	Information technology — Security techniques — Guidelines for auditors on information security management systems controls	Информационные технологии. Методы обеспечения защиты. Руководящие указания для аудиторов по оценке органов управления	
ISO / IEC 27010:2012	Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications	Информационные технологии. Методы обеспечения защиты. Менеджмент обеспечения защиты информации между секторами и организациями	
ISO / IEC 27011:2008	Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Информационные технологии. Методы защиты. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002	
ISO / IEC 27013:2012	Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Информационные технологии. Методы обеспечения безопасности. Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1	

Серия ИСО 27000 (ISO/IEC 27000 ISMS) Системы менеджмента информационной безопасности			
Обозначение	**На английском**	**На русском**	**ГОСТ**
ISO / IEC 27014:2013	Information technology — Security techniques — Governance of information security	Информационные технологии. Техника безопасности. Руководство по информационной безопасности	
ISO / IEC TR 27015:2012	Information technology — Security techniques — Information security management guidelines for financial services	Информационная технология. Техника обеспечения защиты. Структура обеспечения защиты. Руководящие указания по менеджменту защиты информации для финансовых операций	
ISO / IEC TR 27019:2013	Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	Информационные технологии. Методы обеспечения безопасности. Руководящие указания, касающиеся менеджмента информационной безопасности, на основе ISO/IEC 27002 для систем управления процессами, характерными для энергетики	
ISO / IEC 27031:2011	Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity	Информационные технологии. Методы обеспечения защиты. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса	
ISO / IEC 27032:2012	Information technology — Security techniques — Guidelines for cybersecurity	Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности	
ISO / IEC 27033-1:2009	Information technology — Security techniques — Network security — Part 1: Overview and concepts	Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции	
ISO / IEC 27033-2:2012	Information technology — Security techniques — Network security — Part 2:Guidelines for the design and implementation of network security	Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети	

Серия ИСО 27000 (ISO/IEC 27000 ISMS) Системы менеджмента информационной безопасности			
Обозначение	**На английском**	**На русском**	**ГОСТ**
ISO / IEC 27033-3:2010	Information technology — Security techniques — Network security — Part 3:Reference networking scenarios — threats, design techniques and control issues	Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления	
ISO / IEC 27033-5:2013	Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	Информационные технологии. Методы обеспечения безопасности. Безопасность сети. Часть 5. Обеспечение безопасности связи в сетях с использованием виртуальных частных сетей (VPN)	
ISO / IEC 27034-1:2011	Information technology — Security techniques — Application security —Part 1:Overview and concepts	Информационные технологии. Методы обеспечения безопасности. Безопасность применения. Часть 1. Обзор и понятия	
ISO / IEC 27035:2011	Information technology — Security techniques — Information security incident management	Информационные технологии. Методы обеспечения безопасности. Управление случайностями в системе информационной безопасности	
ISO / IEC 27037:2012	Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence	Информационные технологии. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, приобретению и сохранению цифровых данных	

* – в соответствии с каталогом стандартов, опубликованном на официальном сайте Международной организации по стандартизации (ИСО):
http://www.iso.org/iso/ru/home/store/catalogue_ics.htm

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

Лазарев
Виктор Михайлович
доктор технических наук, профессор

Любимов
Алексей Евгеньевич
кандидат технических наук

Международный опыт правового регулирования информационной безопасности и возможности по его комплексному использованию в Российской Федерации

Аннотация: *в статье представлено обобщенное описание международного опыта правового регулирования информационной безопасности и возможности его применения в Российской Федерации. Представлены результаты систематизации международно-правовых норм в сфере информационной безопасности и их соотнесения с международными стандартами информационной безопасности, данные по международному опыту правоприменительной практики в сфере информационной безопасности на основе применения международных стандартов информационной безопасности. Кроме того, в обобщенной форме дано описание информационных отношений в сети Интернет, как инфраструктуры глобального информационного и ноосферных обществ, перспективных международных отношений, а также особенности сетевых информационных угроз. Показана важность использования этого опыта применения современных информационно-аналитических систем для практической реализации процессов информационного обеспечения.*

Ключевые слова: *международный опыт, правовое регулирование информационной безопасности, моделирование процессов информационной безопасности, аналитические системы анализа правового регулирования информационной безопасности, информационные отношения в глобальной сети Интернет.*

По мере развития человечества, при переходе от одного типа общества к другому: *индустриальное — постиндустриальное — информационное — ноосферное* (рис.1) информация и знания становятся ключевым фактором обеспечения конкурентоспособности страны.

Нынешний этап развития информационных технологий характеризуется возможностью массированного информационного воздействия на индивидуальное и общественное сознание вплоть до проведения крупномасштабных информационных войн, в результате чего неизбеж-

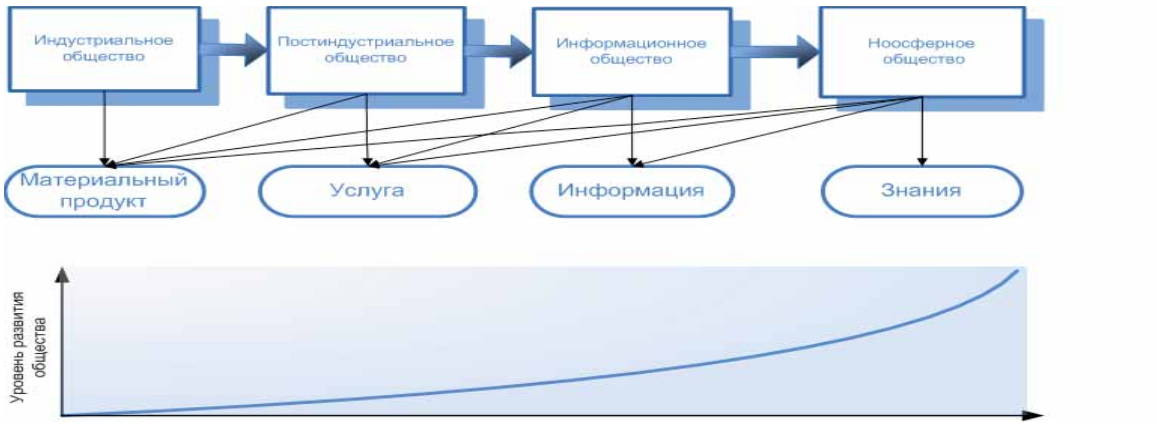

Рис.1. Развитие общества и производственных возможностей человека

ным противовесом принципу свободы информации становится принцип информационной безопасности (ИБ).

Этот принцип обусловлен глобальной информационной революцией, стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникации. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует планетарное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

Вместе с тем становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере с целями, несовместимыми с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. Опасным источником угроз является растущая отечественная и международная компьютерная преступность [1-7].

Системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности, и вместе с тем максимально учитывались бы национальные интересы.

Международную правовую основу регулирования общественных отношений в сфере информационной безопасности составляет достаточно большое количество директив, конвенций, деклараций, хартий, резолюций, рекомендаций и иных международных актов. Среди них необходимо выделить такие, как Резолюция 54/49 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», принятая 1 декабря 1999 года на 54-й сессии Генеральной Ассамблеи ООН; Конвенция Совета Европы о киберпреступности от 23.11.2001 г.; Конвенция ООН об использовании электронных сообщений в международных договорах 2005 г.; Декларация «О европейской политике в области новых информационных технологий» 1999 г.; Декларация принципов построения информационного общества, принятая на Всемирной встрече на высшем уровне в Женеве в декабре 2003 г.; Рамочное решение Европейского Союза об атаках на информационные системы от 24.02.2005 г.; Рекомендация Совета Европы по защите неприкосновенности частной жизни в Интернете от 23.02.1999 г.; Рекомендация Совета Европы № Rec (2001) 3 по предоставлению судебных и других правовых услуг гражданам с помощью новых технологий от 28.02.2001 г.; Рекомендация Совета Европы № 1706 «Средства массовой информации и терроризм» 2005 г.; Тунисское обязательство, принятое на Всемирной встрече на высшем уровне по вопросам информационного общества в 2005 г. и др.

Среди методов обеспечения информационной безопасности системообразующими являются методы нормативного правового регулирования общественных отношений в информационной сфере. При этом в силу глобализации информационного общества весьма существенным является международно-правовой режим информационной безопасности. Такой режим создается нормами международного права, в том числе нормами *международного гуманитарного*

права, которое устанавливает правила ведения военных конфликтов, включая нормы регулирования отношений *в информационной сфере*. Эти нормы в равной степени должны распространяться и на *информационные войны* (операции). Концепция международного гуманитарного права основана на триаде *«гуманность — боевая необходимость — соразмерность»*. Важнейшими международными актами новейшей истории являются Окинавская хартия глобального информационного общества, Декларация о европейской политике в области новых информационных технологий, Декларация Комитета Министров Совета Европы о правах человека и верховенстве права в информационном обществе и др. Каждый из таких актов предусматривает меры по обеспечению информационной безопасности. Рекомендуется поощрять установление международных *стандартов* и гарантий, необходимых для обеспечения подлинности передаваемых электронными средствами документов и сообщений, имеющих обязательную юридическую силу. Наряду с этим принят также ряд нормативных актов в области *стандартизации*. К их числу можно отнести такие, как Устав международного союза электросвязи от 22.12.1999 г.; Рекомендации Европейской экономической комиссии ООН относительно политики в области стандартизации (1996); Рекомендация № 25 Европейской экономической комиссии ООН «Использование стандарта Организации Объединенных Наций для электронного обмена данными в управлении, торговле и на транспорте» от 09.1996 г.; Рекомендация № 26 Европейской экономической комиссии ООН «Коммерческое использование соглашений об обмене для электронного обмена данными» от 03.1995 г.; Директива Совета Европейского Сообщества № 89/336 «О согласовании законодательных актов государств-участников Сообщества, касающихся электромагнитной совместимости» от 03.05.1989 г.; Рекомендация № R (2003) 15 Комитета министров Совета Европы «Об архивации электронных документов в правовой сфере» от 09.09.2003 г. и др.

Среди нормативных правовых актов государств-участников СНГ необходимо отметить Решение Совета глав правительств СНГ «О концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере» от 04.06.1999 г.; Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств-участников Содружества Независимых Государств в сфере информатизации от 24.12.1999 г.; Соглашение об основах гармонизации технических регламентов государств-членов Евразийского экономического сообщества от 24.03.2005 г. и др.

На международном уровне первая попытка комплексного рассмотрения проблем компьютерной безопасности в уголовном праве была предпринята Организацией экономического сотрудничества и развития (ОЭСР) в 1986 году, затем аналогичные попытки предпринимались в 1989 г. Комитетом Министров стран-членов Совета Европы, в 1996 г. был принят Модельный уголовный кодекс для стран-участниц СНГ, а 23.11.2001 г. была принята Конвенция Совета Европы о киберпреступности, которая упорядочила составы компьютерных преступлений. Однако трансграничный характер таких преступлений, трудности их локализации и доказывания в судах стимулировали развитие практики комплексного обеспечения информационной безопасности на основе ведомственных, отраслевых, национальных и международных стандартов, которые стали динамично разрабатываться и повсеместно использоваться. Это привело к созданию Международной Электротехнической Комиссии (МЭК), а затем и Международной Организации по Стандартизации (ИСО) (см.: http://www.isaudit.ru/itvalue.html). Стандарты часто еще называют лучшими практиками. Их количество увеличивается в связи с растущим многообразием обстоятельств, в которых они применяются как стандарты de facto. Стандарты образуют иерархическую систему. По состоянию на апрель 2007 г. такая система насчитывает несколько десятков стандартов, применение которых комплексно обеспечивает безопасность и качество функционирования человеко-машинных систем на всех этапах их жизненного цикла. Высокоуровневые стандарты часто называют процессными, процедурными или тактическими, так как они описывают процессы, процедуры. К их числу относятся такие, как:

- Управление информационными системами — COBIT, BS 15000, Microsoft Operations Framework и ITIL;
- Управление проектами — PRINCE2 и PMBOK;
- Управление безопасностью — ИСО 13335, ИСО 13569 (банковские и финансовые услуги), ИСО 17799/BS 7799-2 (оба локализованы для многих стран), IT Baseline Protection Manual (Германия), ACSI-33 (Австралия), множество стандартов Национального инсти-

тута стандартов и технологий США (НИСТ/NIST) — *NIST Handbook* (SP800-12, USA), CobiT® *Security Baseline*™, ENV12924 (Медицинская информатика) и Information Security Forum *Standard of Good Practice*[1];

- Управление качеством — ИСО 9001, EFQM и Baldrige National Q-Plan;
- Программирование — TickIT, Capability Maturity Model Integration (Институт технологий разработки программного обеспечения, SEI);
- IT Governance — COBIT, *IT Governance Implementation Guide*, COSO *Internal Control — Integrated Framework* и COSO *Enterprise Risk Management — Integrated Framework*, а также недавно разработанный Австралийский стандарт AS 8015-2005 (корпоративное управление информационными и коммуникационными технологиями);
- Управление рисками — Австралийский стандарт AS/NZS 4360[2];
- BCP (планирование непрерывности бизнеса) — PAS-56 Британского института стандартов и Австралийский стандарт HB 221-2004;
- Аудит ИС — COBIT и ИСО 19011;
- Наибольшее и универсальное распространение из процессных стандартов получили стандарты ИСО 17799, COBIT, ИСО 9001, BS 7799-2 и их сочетания.

Кроме большого числа процессных стандартов, имеется еще большее число эксплуатационных, технических стандартов. Международная организация по стандартизации (ИСО), Европейский институт по стандартизации в области телекоммуникаций и Национальный институт стандартов и технологий США (НИСТ/NIST) издали стандарты по таким вопросам, как шифрование (FIPS 197), критерии (технические) оценки безопасности ИТ (ИСО 15408), планирование непрерывности бизнеса (FIPS 87), использование паролей (FIPS 112) и др. Стандарты информационной безопасности, качества и управления в обязательном порядке учитываются при проведении сертификации и аудита. Использование стандартов увеличивает ценность продуктов, создаваемых информационными технологиями, но нет таких стандартов, которые охватывали бы все аспекты управления информационной безопасностью. Состояние вопроса в этой области аналогично состоянию вопроса в системном анализе, ибо последний вырабатывает плохие решения по сложным проблемам, по которым другими методами вырабатываются еще худшие решения.

Начало нынешнего века на уровне Международной организации по стандартизации (ИСО) ознаменовалось тем, что подкомитет «Программная инженерия» был преобразован в подкомитет «Системная и программная инженерия» (SC7 JTC1), что отражает стремление к целостному решению проблем стандартизации информационных технологий в направлении всеобъемлющего качества именно используемых систем в их жизненном цикле (а не составных компонентов или процессов).

Сложившаяся на начало 21-го века структурная организация разработки международных стандартов в области системной и программной инженерии и участие в ней России отражены на рис 2.

Национальные органы по стандартизации платят ежегодные членские взносы, из которых финансируется деятельность международных секретариатов до уровня подкомитетов включительно. По заявкам национальных органов подкомитеты разрабатывают согласованные планы выпуска стандартов.

Каждый международный стандарт разрабатывается в среднем 3-5 лет. Проекты разрабатываются и обсуждаются коллегиально в рабочих группах (при этом учитываются тысячи замечаний), после чего рассылаются на согласование в национальные органы. Деятельность участников рабочих групп ведется на английском языке без перевода и финансируется, как правило, национальными промышленными компаниями, заинтересованными в создании соответствующих стандартов. Стандарт считается принятым, если за него положительно проголосовали более 75% членов Международной организации по стандартизации (ИСО).

Центральное место в ИСО и Международной электротехнической комиссии (МЭК) занимает 7-й подкомитет объединенного технического комитета «Информационные технологии» (SC7 JTC1 ИСО/МЭК). Секретариат располагается в Канаде. Область деятельности подкомитета охватывает стандартизацию процессов, обеспечивающих средств и технологий для проектирования программных продуктов и систем, созданных человеком. Стандарты увязывают различные дисци-

---

[1] Совет Европы и Россия. Сборник документов / Отв. ред. Ю.Ю. Берестнев. — М.: Юрид. лит., 2004. — 928 с. — С. 860.

[2] Australian Communications-Electronic Security Instruction 33, www.dsd.gov.au/infosec/publications/acsi33.html.

Рис. 2 Структурная схема организации разработки международных стандартов в области системной и программной инженерии

плины, такие, как промышленная инженерия, менеджмент качества, безопасность, надежность, информационные технологии, управление проектами.

Подкомитет SC7 «Системная и программная инженерия» включает в свой состав системные рабочие группы SWG1 («Группа планирования») и SWG5 («Группа управления архитектурой») и рабочие группы по направлениям: WG2 «Документация», WG4 «Средства и среда», WG6 «Измерение и оценка программного продукта», WG7 «Управление жизненным циклом», WG9 «Системные гарантии», WG10 «Оценка процесса», WG12 «Измерение функционального размера», WG19 «Языки моделирования», WG20 «Орган знаний в программной инженерии», WG21 «Управление активами», WG22 «Терминология».

Стратегическими направлениями подкомитета до 2008 г. выбраны:

- системная интеграция с ориентацией на разработку общесистемных стандартов во взаимодействии с техническими комитетами по качеству (ТС176), надежности (ТС56), функциональной безопасности (SC65A), информационной безопасности (SC27) и др.;
- ключевое партнерство с международными организациями в области стандартизации — Институтом инженеров по электронике и электротехнике, отделением компьютерных наук (IEEE-CS), Международным Советом по системной инженерии (INCOSE) и др.;
- активная связь с рынком и расширение на рынке ниши системной инженерии.

К апрелю 2004 г. всего за время существования SC7 с 1997 г. было создано 79 стандартов. Основными достижениями являются стандарты ИСО/МЭК 15288-2002 «Системная инженерия — Процессы жизненного цикла систем», ИСО/МЭК 12207-95 «Программная инженерия — Процессы жизненного цикла программных средств», ИСО/МЭК 9126-2000 «Информационная технология — Качество программного продукта», ИСО/МЭК 14598 «Информационная технология — Оценка программных продуктов», ИСО/МЭК 15504 «Информационная технология. Оценка процессов, осуществляемых с программными средствами». В 2003-2004 гг. подкомитетом «Системная и программная инженерия» были опубликованы стандарты и технические отчеты (ТО):

- ИСО/МЭК ТО 9126-2: «Программная инженерия — Качество программного продукта — Часть 2: Внутренние показатели»;
- ИСО/МЭК ТО 9126-3: «Программная инженерия — Качество программного продукта — Часть 3: Внешние показатели»;
- ИСО/МЭК ТО 14143-3:2003 «Информационная технология — Измерение программных средств — Измерение функционального размера — Часть 3: Верификация методов измерения функционального размера»;
- ИСО/МЭК ТО 19500-2:2003 «Информационная технология — Открытая распределенная обработка — Часть 2: Общий ORB-протокол взаимодействия (GIOP)/ Интернет ORB-протокол взаимодействия (IIOP)»;
- ИСО/МЭК ТО 19760 «Системная инженерия — Руководство для ИСО/МЭК 15288 (Процессы жизненного цикла системы)»;
- ИСО/МЭК ТО 19761 «Программная инженерия — COSMIC-FFP — Метод измерения функционального размера»;
- ИСО/МЭК ТО 20926 «Программная инженерия — IFPUG 4.1 Опытный метод измерения функционального размера — Практическое руководство для расчетов»;
- ИСО/МЭК ТО 9126-4 «Программная инженерия — Качество программного продукта — Часть 4: Показатели потребительского качества (при использовании)»;
- ИСО/МЭК ТО 14143-5 «Информационная технология — Измерение программных средств — Определение измерения функционального размера — Часть 5: Определение функциональной области для использования функционального размера»;
- ИСО 90003 «Руководство для применения ИСО 9001:2000 для программных средств»;
- ИСО/МЭК 15504-3 «Программная инженерия — Оценка процесса — Часть 3: Выполнение оценки»;
- ИСО/МЭК 18019 «Системная и программная инженерия — Руководство для проектирования и подготовки пользовательской документации для применения программных средств».
- Проекты, находящиеся по состоянию на 2004 г. в разработке и ожидании окончательного решения:
- FDIS 15476 «Программная инженерия — CDIF Семантическая метамодель — части 3, 4, 5»;
- FDIS 15909 «Программная инженерия — Сети Петри высокого уровня — Часть 1: Концепции, Определения и графические обозначения»;
- DIS 19501-1 «Унифицированный язык моделирования UML PAS»;
- DTR 19759 «Руководство для органов знаний в области программной инженерии» (SWEBOK);
- DIS 24570 «Программная инженерия — Руководства по определениям и расчетам для применения анализа функционального смысла»;
- ИСО/МЭК FCD 9127 «Программная инженерия — Пользовательская документация и информация для пакетов программ потребителя»;
- ИСО/МЭК DTR 9249 «Информационная технология — Руководство для управления программной документацией»;
- ИСО/МЭК FDIS 15504-4 «Программная инженерия — Оценка процесса — Часть 4: Руководство по использованию процесса усовершенствования и процесса определения возможности»;
- ИСО/МЭК FCD 15940: «Информационная технология — Программная инженерия — Сервисы среды»;
- «Системная и программная инженерия» — Словарь;
- проект по гармонизации ИСО/МЭК 15288 и 12207;
- ТО 14143-6 «Информационная технология — Измерение программных средств — Определение измерения функционального размера — Часть 6: Руководство для использования серии стандартов ИСО/МЭК 14143 и связанных с ними международных стандартов»;
- ИСО/МЭК 16085 «Программная инженерия — Процессы жизненного цикла программных средств — Управление рисками»;
- ревизия стандартов серии «Программная инженерия — Процессы жизненного цикла программных средств — Сопровождение ИСО/МЭК 14764»;
- ревизия ТО 14471-99: «Программная инженерия — Руководство для усвоения CASE-средств»;
- ревизия стандарта IS 14102-95 «Информационная технология — Руководство для оценки и выбора CASE-средств».

Новыми рассматриваемыми проектами, планируемыми подкомитетом «Системная и программная инженерия» на ближайшую перспективу, являются:

- перенос стандарта МЭК/ТС 56 (проект 61720): «Руководство по методикам и средствам для достижения доверия к программному обеспечению»;

- ревизия и отслеживание стандарта IEEE 1220 «Стандарт IEEE по применению и управлению процессом в программной инженерии»;
- ревизия и отслеживание стандарта EIA 632 «Стандарт Альянса отраслей электронной промышленности США — Процессы для проектирования систем»;
- ревизия стандарта ИСО/МЭК 14102 «Информационная технология — Руководство для оценки и выбора CASE-средств»;
- ревизия стандарта ИСО/МЭК ТО 14143-1:1998;
- сопровождение проекта по использованию ITU-T Rec/X/901-3 ИСО/МЭК 10746 Части 1-3 «Эталонная модель для открытой распределенной обработки»;
- отслеживание стандарта IEEE 2001 «Рекомендованная IEEE практика для Интернета — Инженерия, управление и жизненный цикл сайтов»;
- отслеживание стандарта ANSI NCITS 354-2001 «Американский национальный стандарт для информационных технологий — Общий промышленный формат для отчетов по испытаниям применимости».

Наибольший интерес представляет международная практика регулирования информационных отношений и угроз, связанных с использованием глобальной сети Интернет. К основным элементам информационного правоотношения относятся: субъекты, вступающие в правоотношения при осуществлении информационных процессов; объекты, в связи с которыми субъекты вступают в информационные правоотношения, содержание прав и обязанностей субъектов по осуществлению действий над объектами информационного правоотношения, ответственность субъектов при нарушении прав или невыполнении обязанностей по отношению к другим субъектам правоотношения. Субъектами информационных правоотношений являются оператор Интернет-связи, его абонент, другие пользователи Интернет, правоохранительные органы. Содержание прав и обязанностей перечисленных субъектов взаимосвязано с их возможностями совершать определенные действия с объектами информационных правоотношений, в том числе и причиняющие вред. Объектами в информационных отношениях абонента и оператора Интернет-связи являются информация, информационные продукты и услуги, состояние защищенности личности, защищенность информации. Действия субъектов таких отношений, способных повлиять на информационную безопасность личности, являются основанием их ответственности. К возможным действиям абонента относятся: просмотр веб-страниц, получение и отправка электронных сообщений, хостинг. К возможным действиям оператора Интернет-связи относятся сбор сведений об информационном обмене абонента, воздействие на информационный обмен абонента путем изменения скорости обмена, фильтрации содержимого передаваемой информации, воздействия на информацию, опубликованную пользователем на веб-странице, размещенной на сервере оператора, сбор персональных данных о пользователе. Возможные действия правоохранительных органов заключаются в истребовании от оператора Интернет-связи или его абонента необходимой им информации об информационном обмене абонента. К действиям других пользователей Интернета, имеющих значение для информационной безопасности абонента, можно отнести только намеренные действия по получению несанкционированного доступа к его информации на веб-странице, в компьютере, в электронном письме. Просмотр веб-страниц несет в себе две угрозы. Это вредная информация, размещенная непосредственно на странице (фото, видео, аудио, текстовые данные), и вредоносные программные коды, запускаемые с различными приложениями, которые обеспечивают правильное отображение просматриваемой страницы, способные изменить состояние информации в компьютере пользователя. Вредная информация способна оказывать воздействие на пользователя при посещении веб-страниц, на которых она расположена. Попадание вредной информации на экран монитора пользователя зависит, в основном, от действий самого пользователя, так как он сам осуществляет передвижение по сети Интернет, и решает, какая информация подлежит его вниманию. Ограничение на доступ к вредной информации может быть установлено самим оператором Интернет-связи. Это возможно за счет применения им специальных программных фильтров, позволяющих перекрывать доступ к информации определенного содержания, в том числе и не относящейся к вредной. Большинство операторов Интернет-связи имеют программные фильтры и могут применять их по договоренности с абонентом. Другим видом действий абонента является получение электронных сообщений. В этом случае существуют угрозы воздействия вредной информации, размещенной в электронном сообщении, получение и заражение компьютерными вирусами, получение не за-

прашиваемой информации (*спам*). В действиях пользователя по отправке электронных писем существуют такие угрозы, как недоставка отправленного письма адресату и нарушение конфиденциальности информации, содержащейся в письме. Данные угрозы могут быть реализованы как в результате действий самого пользователя, так и в результате действий или бездействия оператора Интернет-связи. Так, при отсутствии соединения или при некачественном соединении с сетью Интернет абонент не сможет отправить электронную корреспонденцию. Кроме того, угроза недоставки электронного письма или нарушения его конфиденциальности может быть реализована в результате неправильной работы почтовых серверов оператора Интернет-связи, в результате использования фильтров на исходящую от абонента информацию или в силу форс-мажорных обстоятельств. Нарушение конфиденциальности электронной переписки абонента может произойти в результате несанкционированного доступа третьих лиц к его компьютеру или электронному почтовому ящику. При опубликовании своей веб-страницы в сети Интернет для информационной безопасности пользователя существуют такие угрозы, как несанкционированный доступ к опубликованной информации и, следовательно, нарушение данных аутентификации абонента, изменение или удаление веб-страницы пользователя и ее блокировка как результат несанкционированного доступа. Источником таких угроз может быть как оператор Интернет-связи, так и другие пользователи Интернет. В первом случае возможность несанкционированного доступа возможна в силу того, что оператор Интернет-связи является хранителем данных аутентификации (пароля и логина) пользователя при доступе к редактированию своей страницы. Во втором случае доступ к странице абонента может быть осуществлен в силу получения другими пользователями Интернет данных аутентификации, необходимыми для управления страницей. Данная информация может быть получена в результате ее хищения путем несанкционированного доступа к файлам (взлома) оператора Интернет-связи или любым другим способом. Еще существуют угрозы, возникновение которых не зависит от деятельности абонента в глобальной сети. К ним относятся диффамация, нарушение авторских прав, распространение персональных данных.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос аудита «как оценить уровень безопасности корпоративной информационной системы» обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Государственной комиссии по техническому и экспортному контролю (ранее Гостехкомиссии, далее по тексту Гостехкомиссии по тем подзаконным актам, которые были выпущены ею до Административной реформы) России приходится адаптировать к нашим условиям и применять методики международных стандартов (ИСО 17799, 9001, 15408, стандартов Британского института стандартов и пр.), а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиты информации. В зарубежных нормативных документах установлен набор требований для различных типов средств и систем информационных технологий, в зависимости от различных условий их применения. Особенности развития отечественной нормативной базы в данной области заключаются в том, что отсутствует комплексный подход к проблеме защиты информации (рассматриваются в основном вопросы несанкционированного доступа к информации и вопросы обеспечения защиты от побочных электромагнитных излучений и наводок) и, кроме того, разработанные национальные стандарты и руководящие документы Гостехкомиссии России 1992-1996 не принимали во внимание международные стандарты ИСО/МЭК. На сегодняшний день эти недостатки начали устраняться. В целях совершенствования отечественной нормативной базы с 2001 года Гостехкомиссия и Госстандарт России совместно с другими заинтересованными министерствами и ведомствами реализуют новые инициативы в этом направлении. В частности, утверждены три стандарта, определяющие критерии оценки безопасности информационных технологий. Они устанавливают требования к формированию заданий по оценке безопасности в соответствии с положениями международных стандартов. По линии Гостехкомиссии созданы несколько руководящих документов, в том числе «Руководство по разработке профилей защиты», «Руководство по регистрации профилей

защиты», «Методология оценки безопасности информационных технологий» и «Автоматизированный комплекс разработки профилей защиты». Перечисленные документы, по сути, представляют собой прямую трансляцию положений международных стандартов ИСО на российскую нормативно-техническую базу. В дополнение к ним создаются еще шесть спецификаций на защитные профили для операционных систем, межсетевых экранов, систем управления базами данных, автоматизированных систем учета и контроля ядерных материалов и др. Утвержден государственный стандарт РФ, определяющий процессы формирования средств проверки электронной цифровой подписи, идет работа по переводу данного стандарта в категорию межгосударственного. В 2000-2001 гг. была создана «Программа комплексной стандартизации в области защиты информации на 2001-2010 годы» (ПКС), в которой применен комплексный метод стандартизации. ПКС предусматривает появление примерно 40 ГОСТов. Кроме того, ВНИИ «Стандарт» разрабатывает проект «Программы комплексной стандартизации в области защиты информации, составляющей государственную тайну». В ее рамках планируется принятие 42 национальных стандартов и других нормативных документов. В свою очередь, Госстандарт разработал и представил на утверждение в Правительство РФ проект «Программы по разработке технических регламентов на 2003-2010 годы». В ходе ее выполнения создаются следующие документы: «Общий технический регламент безопасности информационных технологий», «Общий технический регламент требований к системам безопасности информационных технологий», «Общий технический регламент требований по защите информации, обрабатываемой на объектах информатизации» и «Специальный технический регламент требований по защите информации в оборонной промышленности». В 2003 году Госстандарт разработал проект классификатора техники и средств защиты информации, требований к контролю над эффективностью средств защиты информации и соответствующих систем управления. Создан проект государственного стандарта, включающего в себя общие положения по формированию системы управления качеством при разработке, изготовлении, внедрении и эксплуатации техники защиты информации. Внедрение этих нормативных документов обеспечит единую классификацию механизмов и техники защиты информации, позволит определить основные характеристики систем качества техники защиты информации. Благодаря этому уменьшится разобщенность разработчиков и изготовителей, повысится уровень координации производителей специальной аппаратуры. Из анализа действующих нормативных документов по стандартизации в данной области следует, что по охвату регулирования аспектов безопасности ИТ, по детализации рассматриваемых в них проблем российские национальные стандарты все еще уступают международным. Вопросы стандартизации в сфере безопасности ИТ решаются на международном уровне — совместным техническим комитетом СТК1 ИСО/МЭК «Информационные технологии», на региональном — европейскими организациями CEN, ECMA и др., на национальном уровне — ANSI, NIST (США), DIN (Германия) и др.

При использовании международного правового регулирования информационной безопасности можно сформулировать следующие проблемы, связанные с его использованием:

- необходимость работать с информацией разного типа (структурированная и неструктурированная);
- разнородность источников и форматов данных (телевидение, радио, печатные издания, Интернет, базы данных и пр.);
- большие объемы данных;
- необходимость гибко и оперативно настраивать систему на различные задачи в соответствии с меняющейся обстановкой;
- необходимость синхронизации мощностей системы с нарастающими потоками данных («масштабируемости»);
- необходимость эффективно анализировать данные в распределенной среде;
- необходимость прогнозирования развития ситуаций, например, по модели «что, если...»;
- необходимость мониторинга открытого информационного пространства (Интернет/СМИ);
- необходимость применять максимально стандартизованные решения.

Решение перечисленных проблем требует применения современных аналитических систем для качественного обеспечения использования международного опыта правового регулирования информационной безопасности [8]. На этой основе представляется возможным создание и использование единого международного правового пространства, которое, по нашему мнению, сделает возможным эффективное использование международного опыта нормативно-правового регулирования процессов обеспе-

чения информационной безопасности в Российской Федерации.

Основные процессы сегодняшнего этапа государственного строительства России в области информационной безопасности требуют от структур, обеспечивающих принятие органами государственной власти обоснованных решений, постоянного совершенствования эффективности работы на следующих направлениях деятельности:

- непрерывный мониторинг и взвешенная аналитическая оценка глобальных направлений укрепления безопасности России;
- формализация этих направлений в виде частных проблем и формулировка их путей их решения;
- интегрированное ситуационное моделирование этих проблем;
- выработка ранжированных вариантов (способов и средств) решения сформулированных частных проблем.

Перечисленные направления деятельности характеризуются:

- коллективностью — участием в процессе большого количества взаимодействующих физических и юридических лиц;
- интеллектуальностью — вследствие объективно нечеткой постановки и слабой формализованности проблемы доля интеллектуальных действий остается значительной;
- интерактивностью — частой чередуемостью действий, выполняемых человеком и программно-техническими средствами;
- уникальностью — отсутствием типовых полномасштабных технологий реализации обсуждаемых проблем;
- важностью визуальной и аудиоинформации, доля которой в общем объеме значительна.

Функционально указанные выше направления деятельности реализуются формированием высококвалифицированных групп экспертов (по перечню проблем) и оснащением их технологиями извлечения и анализа информации, содержащейся в источниках различной природы, а также эффективного контроля состояния защищенности и обеспечения безопасности, в том числе от несанкционированного доступа, добытой и используемой в работе информации.

В настоящее время эффективным инструментом решения проблемы информационного обеспечения групп экспертов являются программно-аппаратные комплексы (ПАК) автоматизированного поиска и обработки информации, а также контроля защищенности собственных информационных ресурсов, разрабатываемые рядом российских компаний, специализирующихся в области создания автоматизированных систем и информационных технологий в интересах противодействия криминальным структурам и терроризму.

Основными задачами, решаемыми программно-аппаратными комплексами, являются:

- обеспечение лиц, принимающих решения, актуальной, достоверной и полной информацией, в том числе поиск во внешних и внутрикорпоративных сетях структурированных и неструктурированных данных, получение, подготовка и хранение информации, обеспечивающей принятие оптимальных решений;
- упреждающее выявление угроз финансово-экономического, социально-психологического и иного характера как внутри организаций, так и в сфере их интересов;
- обнаружение среди анализируемых лиц и организаций субъектов, имеющих признаки связи с вероятными источниками угроз (криминальными и террористическими организациями, лицами, а также структурами, аффилированными с ними, конкурентами, мошенниками, фирмами-банкротами, предъявителями фальшивых документов и др.);
- информационная поддержка расследования случаев нанесения ущерба организации, систематизация результатов расследований для последующего использования;
- оценка кандидатов при приеме на работу (места прежней работы, репутация кандидата и фирм, где он работал; возможные связи с лицами и организациями, конкурентами, партнерами по рынку, криминальными и мошенническими структурами; причастность к чрезвычайным происшествиям, характер и объекты собственных коммерческих интересов и т. п.);
- контроль и анализ состояния защищенности информационных ресурсов, конфиденциальных сведений организаций, а также внутренних и внешних коммуникационных сетей организации (Интранет и Интернет), в том числе:
  - комплексный анализ трафика глобальных и локальных сетей передачи данных, включающий прием и декодирование протоколов, выделение из трафика данных (сообщений) и регистрация их, контент-анализ в реальном масштабе времени или в отложенном режиме;

- возможность как анализа сетевого трафика, так и реконструкции сессий, выделения сообщений и проведения анализа контента (содержимого), передаваемого в локальных сетях;
- широкий спектр поддерживаемых протоколов для всех семи уровней модели OSI и обеспечение одновременной работы по нескольким каналам.

В последнее время бурно развиваются информационные технологии, что сопровождается стремительным увеличением объемов передаваемой информации; это значительно усложняет ее непосредственную обработку. Меняются характер и формы представления информации. Большая часть информации является неструктурированной и содержится в динамических потоках и файлах разнообразных форматов: текстовых, мультимедийных и пр. Значительная часть информации является паразитной (реклама, спам), дублируется полностью или частично.

Необходимость охвата и обобщения огромных динамических разнородных информационных потоков, а также непредсказуемость характера представляющих интерес данных приводит к постепенному отказу от использования в качестве единственного критерия отбора наличия в них определенных слов и развитию новых подходов к их обработке. Все большее применение получают интеллектуальные технологии работы с информацией. Основанные на таких технологиях новые методы обработки данных направлены на более эффективное выявление необходимой информации из огромных объемов, с одной стороны, и ее комплексный анализ для извлечения скрытых, ранее неизвестных знаний — с другой. В результате внедрения таких технологий значительно повышается эффективность и оперативность обработки информации, снижаются объемы ресурсов и влияние человеческого фактора.

Информационно-аналитическая система (ИАС) предназначена для отбора информации из разнородных источников, ее автоматической аналитической обработки, извлечения знаний с целью раннего выявления угроз безопасности и поиска путей их нейтрализации, оповещения о появлении искомой информации в режиме, близком к режиму реального времени, углубленного анализа, составления и представления аналитических отчетов и прогнозов развития ситуации. Другими словами, ИАС позволяет осуществлять круглосуточный мониторинг информационного пространства.

Принципиальной особенностью, отличающей ИАС от существующих на рынке систем, является, во-первых, способность системы обрабатывать как текстовую, так и мультимедийную информацию (аудио- и видеопотоки и записи) и, во-вторых, поддержка полного цикла обработки данных, то есть преобразование данных в информацию, извлечение знаний из информации путем фактографического и контент-анализа, концептуальное моделирование.

В качестве источников данных для ИАС могут выступать любые известные источники информации (интернет, файловые системы, базы данных, аудио- и видеоканалы). ИАС способна работать как с потоком, так и с файлами практически всех известных форматов. Обобщенная схема функционирования ИАС приведена на рис. 3.

- Основу ИАС составляют следующие модули (инструменты):
- Модуль анализа и визуализации результатов;
- Модуль моделирования ситуаций и прогнозирования;
- Модуль поиска и анализа информации;
- Модуль обработки структурированных данных;
- Хранилище данных.

Взаимодействие модулей показано на рис.4.

Модуль поиска и анализа информации предназначен для решения задач сбора данных из различных источников (Интернет, СМИ, телевидение, радио, базы данных); создания единого индекса по всем источникам; извлечения информационных объектов и связей для автоматизации процессов анализа; классификации, категоризации и кластеризации; обеспечения различных видов поиска, поддержки справочной информации по объектам.

Модуль обработки структурированных данных реализует набор методик и математических алгоритмов, позволяющих рассчитывать комплексные и интегрированные показатели на основе структурированной части результатов социологических опросов населения, показателей социально-политической ситуации и социально-экономического развития регионов.

Модуль анализа и визуализации результатов поддерживает виды анализа, позволяющие полноценно оценивать ситуации: многомерный, выборочный, непоследовательный, анализ временных рядов и анализ рынков. Ключевыми функциями модуля являются организация единой аналитической среды для поль-

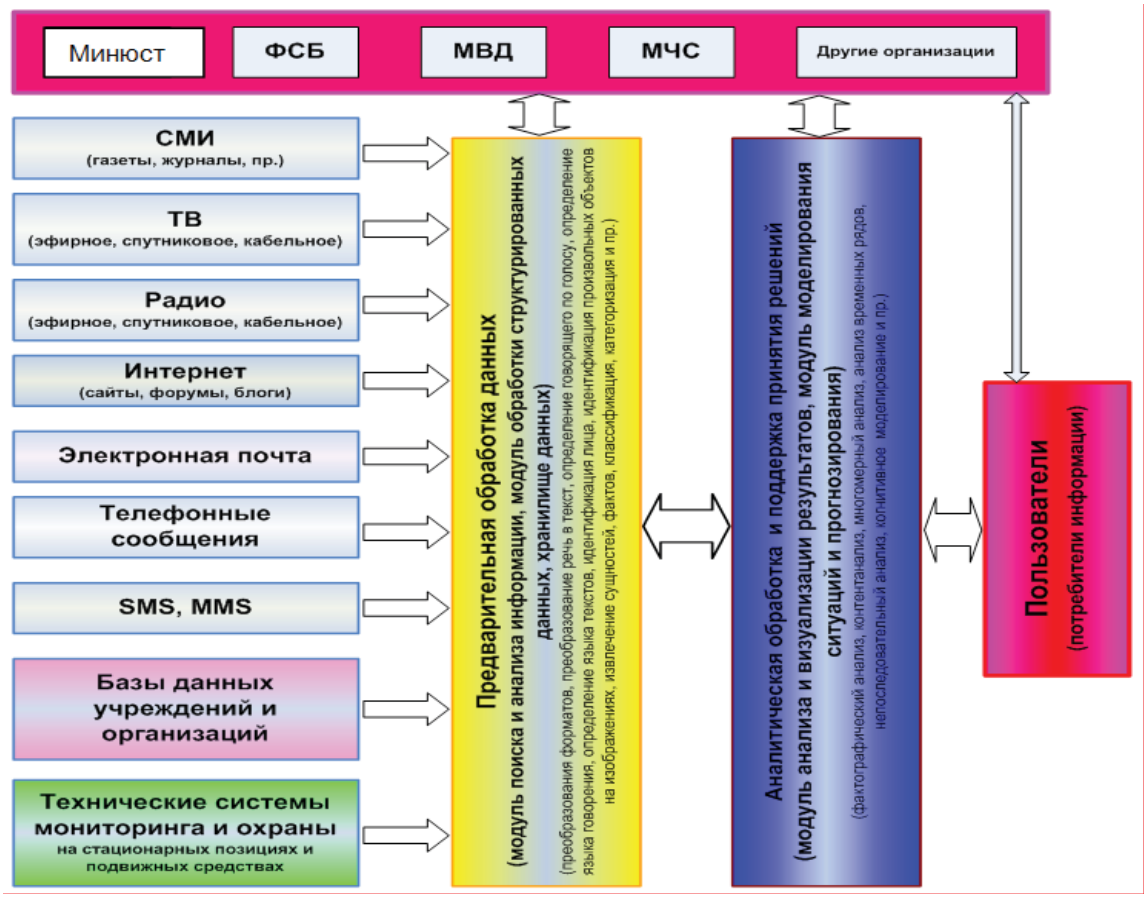

Рис.3. Схема функционирования ИАС

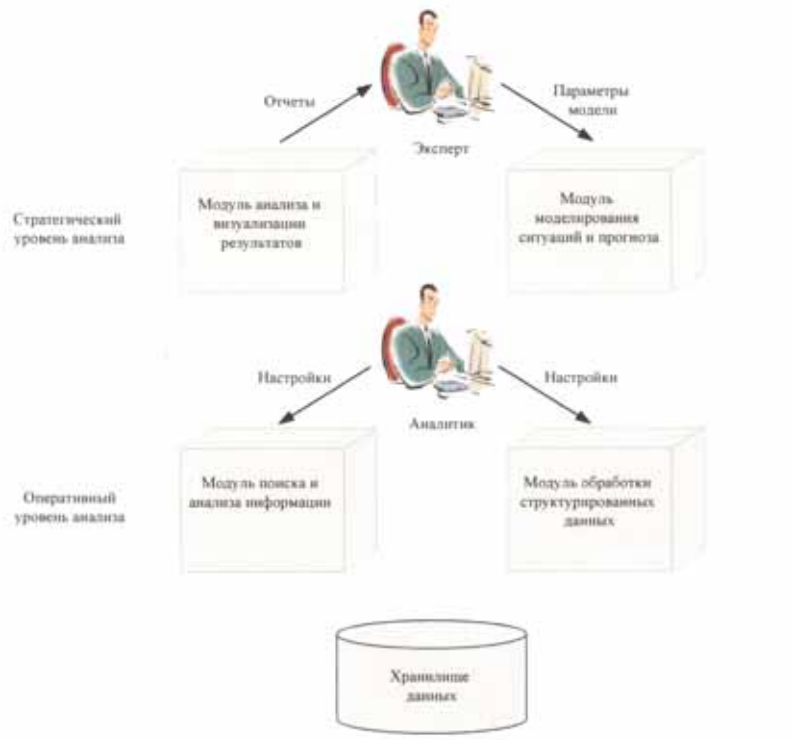

Рис. 4 Взаимодействие аналитиков и специалистов с модулями системы

зователей; реализация аналитической функциональности и визуализация; интеграция в единой системе отчетности данных из различных источников; создание аналитической платформы для стратегического развития путем формирования фундаментальной информационной модели.

Основными функциями **модуля моделирования ситуаций и прогнозирования** являются организация аналитической среды, сценарное моделирование развития ситуаций и поддержка принятия решений о выборе эффективных способов достижения целей развития ситуации.

Хранилище данных предназначено для создания единого информационного пространства, позволяющего сформировать масштабируемую платформу для анализа информации в гетерогенной среде. Оно позволяет интегрировать различные функциональные модули системы, объединяя их через базу данных. Сбор данных из существующих источников осуществляется модулем поиска и анализа информации.

Информационно-аналитическая система построена по **модульному принципу**, т. е. возможен выбор любой комбинации модулей и языков для решения конкретных задач. ИАС построена по технологии «тонкого клиента», т. е. как сама система, так и ее пользователи могут быть пространственно разнесены. При этом от пользователей системы не требуется установки какого-либо специального программного обеспечения.

ИАС в своем функционировании реализует следующие технологии:

- интеллектуальный поиск, индексация, классификация и категоризация;
- фонемный поиск;
- идентификация говорящего по голосу;
- распознавание образов;
- идентификация лиц;
- распознавание текста и бегущей строки;
- преобразование речи в текст;
- анализ и визуализация результатов;
- концептуальное моделирование.

Каждый входящий файл (сообщение, документ) подвергается предварительной обработке. **Документы** (файлы форматов doc, pdf, html и др.) анализируются на предмет содержания в них графических объектов. В случае наличия таких объектов они выделяются в отдельные файлы. **Речь**, содержащаяся в аудиофайлах и звуковых дорожках видеофайлов, преобразовывается в текст, и определяется принадлежность голоса говорящего (диктора). **Видеофайлы** анализируются на предмет наличия в них бегущей строки. Если бегущая строка найдена, она преобразуется в текст. **В графических файлах**, извлеченных из текста, а также кадрах видеофайлов производится поиск и распознавание печатного текста и образов (логотипов, силуэтов и т. п.) и идентификация лиц. Такая информация, содержащаяся в файлах в неявном виде (метаинформация), так же как и текстовое содержание документов, индексируется и становится доступной для поиска и мониторинга.

Основные методы, используемые в работе программно-аппаратного комплекса:

- динамическая категоризация и классификация, аннотирование и аналитическая обработка текстовой и другой неструктурированной информации.
- регистрация, ввод, отбор, хранение и обработка аналогового и цифрового видео, текстов субтитров, временных кодов и метаданных;
- текстовый и визуальный поиск, поиск и распознавание лиц и иных биометрических данных, автоматическая категоризация и классификация текстовой, графической и другой неструктурированной информации, а также распознавание речи;
- фонетический поиск и профилирование аудио- и видеофайлов на основе звуковых образов в человеческой речи;
- многоканальный режим работы; семиуровневое декодирование;
- поддержка более 600 протоколов; экспертная система и автоматическое распознавание протоколов;
- анализ, декодирование и обработка сетевых потоков в реальном масштабе времени;
- анализ взаимодействия сетевых объектов и анализ инкапсулированных протоколов;
- выделение сообщений с формированием файлов из каналов передачи данных с возможностью записи их на диск и последующий контент-анализ их; сбор статистики в режиме онлайн, с записью результатов на диск для последующего анализа;
- LAN интерфейсы: Ethernet 10/100/1000 Мбит/с; WAN интерфейсы: G.703;
- портативность;
- мощный встроенный макроязык, позволяющий писать сценарии работы анализатора в зависимости от изменяющихся характеристик трафика; комплект средств разработки (SDK) для создания собственных декодеров протоколов;

Основными преимуществами ПАК, предложенного в статье [7], являются:

- расширенные поисковые возможности (логический, нечеткий и смысловой поиск), в том числе с использованием естественного языка запросов;
- масштабируемость ПАК по объему архивов;
- гибкость ПАК, в том числе относительно аппаратно-программной платформы;

- эффективная реализация механизма «горячего развертывания» — доступность архивов во время обновления информации;
- поддержка большого, по сравнению с другими ПАК, количества форматов данных — около 250, а также реализованная возможность подключения к системе собственных конверторов данных;
- поддержка широкого круга источников информации (файловые системы, сайты Интернета, базы данных, почтовые системы, специализированные системы управления документами и т. п.);
- реализованная многоуровневая защита информации;
- обеспечение контроля доступа на уровне отдельных документов, возможность передачи данных в зашифрованном виде, что обеспечивает гибкое управление правами пользователя;
- универсальное решение для анализа LAN, WAN сетей; отдельные и комбинированные конфигурации;
- применение гибкой системы фильтров для разнообразных применений;
- возможность модернизации программного и аппаратного обеспечения; функциональная гибкость; модульная структура программного и аппаратного обеспечения;
- оптимальное соотношение: «цена/функциональность».

Представленная в статье информация свидетельствует об актуальности использования международного опыта правового регулирования информационной безопасности для Российской Федерации. Эффективное его использование требует реального создания единого международного нормативно-правового пространства. Создание такого пространства невозможно без использования мощных информационно-аналитических платформ. Таким образом, предлагаемые компанией программно-аппаратные комплексы автоматизированного поиска и обработки информации, а также контроля защищенности собственных информационных ресурсов являются эффективными инструментами информационно-аналитической поддержки государственных структур, обеспечивающих информационную безопасность России.

Литература

1. Крылов Г.О. Международные проблемы информационного права: учеб. пособие, М.: РПА Минюста России, 2013. — 122 с. — ISBN 978-5-89172-465-5/.
2. Полякова Т.А. Информационная безопасность в условиях построения информационного общества. М.: РПА Минюста России, 2007.
3. Андреев О.О. и др. Под редакцией Васенина В. А. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. М:. МЦМНО, 2008.
4. Андреев О.О. и др. Под редакцией Васенина В. А. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. М:. МЦМНО, 2008.
5. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М., изд. «Вооружение, политика, конверсия», 2004, 395 с. — www.mathmodels.net
6. Костогрызов А. И., Лазарев В.М., Нистратов Г.А. Математические модели для эффективного контроля и управления качеством компьютеризированных систем в контексте требований системообразующих стандартов. Сборник СФ ФС РФ «Научные основы национальной безопасности», 2005 г.
7. Лазарев В.М., Любимов А.Е. Предложения по использованию информационно-аналитических систем в информационно-правовом обеспечении органов законодательной и исполнительной власти федерального, регионального и местного уровней, статья в сборнике НЦПИ «Правовая информатика», вып. № 1, 2013.
8. Стрельцов А.А. Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации. // Сборник и методологические проблемы информационной безопасности под редакцией В.П. Шерстюка. — МГУ, 2004.

Ермоленко Александр Владимирович

Практика применения электронной цифровой подписи в деятельности организаций: реальность и перспективы

Аннотация: *В статье анализируется практика применения электронной цифровой подписи коммерческими структурами. Приводится информация о сферах деятельности хозяйствующих субъектов, где электронная цифровая подпись нашла широкое применение. Исследуются экономические предпосылки и юридические основания для внедрения ЭЦП в бизнес-процессы. Кроме того, в рамках указанной статьи затрагиваются вопросы направлений развития законодательства для повышения заинтересованности бизнеса в применении электронной подписи.*

Ключевые слова: *электронная цифровая подпись, электронный документ, электронный документооборот, электронная подпись, юридическая значимость, применение электронной подписи.*

В последние годы растет степень внедрения бизнесом информационных технологий в производственную деятельность, а значительное число организаций строят свой бизнес на выполнении работ и оказании услуг исключительно в рамках информационного пространства сети Интернет.

Любое взаимодействие организации должно находить свое отражение в различных документах, составленных по форме, предписанной законодательными и иными нормативно-правовыми актами.

В соответствии со ст. 161 Гражданского кодекса РФ [1] всякие сделки, заключаемые юридическими лицами между собой и с гражданами, должны совершаться в простой письменной форме. Статья 23 Гражданского кодекса РФ [1] устанавливает, что к предпринимательской деятельности граждан, осуществляемой без образования юридического лица, соответственно применяются правила, которые регулируют деятельность юридических лиц, являющихся коммерческими организациями, если иное не вытекает из закона, иных правовых актов или существа правоотношения.

Взаимодействие юридических лиц между собой осуществляется в рамках договоров, заключаемых для достижения цели организации в соответствии с действующим законодательством и обычаями делового оборота.

Возможность заключения договора в письменной форме путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору, закреплена в ст. 434 Гражданского кодекса РФ [1]. Пунктом 2 ст. 160 Гражданского кодекса РФ [1] устанавливается возможность при письменной форме использовать электронную подпись в качестве средства, позволяющего достоверно определить сторону по договору. Возможность использования документов, полученных по электронной связи, и применение электронно-цифровой подписи (ЭЦП) была закреплена уже в первой редакции Гражданского кодекса РФ, введенного в 1994 году [2].

Приведенные нормы, закрепленные в основном законодательном акте отрасли гражданского права, значительное время не находили широкого применения на практике. С бурным развитием и массовым внедрением информационных технологий в конце 90-х — начале 2000

годов потребовалось принятие специальных норм, регулирующих порядок применения электронных документов и электронной цифровой подписи. Первым этапом принятия этих специальных норм явился Федеральный закон «Об электронной цифровой подписи» № 1-ФЗ, принятый 10.01.2002 г. [3].

Работа над проектом указанного закона в России началась еще в 1997 г. [4, 80 с.] Законопроект разрабатывался по поручению Правительства РФ Министерством связи России совместно с ФАПСИ, Гостехкомиссией России, Минюстом России, ФКЦБ РФ, Госстандартом РФ с участием Банка России [5, 6 с.].

Наибольшую заинтересованность в принятии закона высказывали финансовые структуры и, в частности, коммерческие банки, давно использующие в своей деятельности аналоги собственноручной подписи [7].

Еще до разработки и вступления в силу Закона «Об электронной цифровой подписи» в силу специфики банковской сферы и на основании мировой практики был разработан ряд положений, регламентирующих применение аналогов собственноручной подписи в платежных документах и платежных системах. 10 февраля 1998 г. ЦБ РФ принял временное положение № 17-П «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями» [6]. Другими основополагающими документами, регламентирующими отношения по использованию ЭЦП в банковской сфере, являются:

1. Положение ЦБ РФ от 12 марта 1998 г. № 20-П «О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России»;
2. Положение ЦБ РФ № 36-П от 23 июня 1998 г. «О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России».

Центральным Банком России выпущено достаточно большое количество нормативных актов, регламентирующих отношения по использованию ЭЦП или позволяющих использование ЭЦП в банковско-правовых отношениях.

На данный момент основной объем используемых ЭЦП приходится именно на сферу финансовой деятельности организаций. Подавляющее большинство организаций применяют в своей деятельности информационные системы «клиент-банк» для осуществления операций со своими счетами, открытыми в кредитно-финансовых организациях.

Другим субъектом правоотношений, стремившимся к внедрению электронного документооборота с применением средств, позволяющих идентифицировать отправителя и проверить подлинность документа, является государство в лице различных контролирующих органов. С целью внедрения информационных технологий в деятельность налоговых органов проводилось поэтапное изменение Налогового кодекса.

В первой редакции ст. 80 Налогового кодекса РФ [7] закреплялась возможность подачи налоговой декларации на дискете или ином носителе, допускающем компьютерную обработку. В следующей редакции указанной статьи Налогового кодекса РФ [8] введена возможность подачи налоговой декларации по телекоммуникационным каналам связи в соответствии с действующим законодательством Российской Федерации, а также закреплена обязанность налогового органа передать налогоплательщику квитанцию о приемке в электронном виде.

С целью реализации положений, закрепленных в Налоговом кодексе, разработаны подзаконные акты, регулирующие порядок и форму взаимодействия при передаче деклараций по каналам связи. Это приказ МНС РФ от 02.04.2002 № БГ-3-32/169 «Об утверждении Порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи» [9] и приказ МНС РФ от 10.12.2002 № БГ-3-32/705@ «Об организации и функционировании системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи» [10], которые содержат требования о подписании сведений, передаваемых в электронной форме, посредством применения ЭЦП.

На текущей момент в Налоговом кодексе РФ [11] в п. 3 ст. 80 закреплена императивная норма о предоставлении налоговых деклараций в электронной форме в случае превышения среднесписочной численности работников в 100 человек за предшествующий календарный год.

В практику деятельности подавляющего числа организаций вошли электронные системы документооборота с государственными органами, реализующие требования указанных нормативно-правовых актов и требования Федераль-

ного закона «Об электронной цифровой подписи» № 1-ФЗ, принятого 10.01.2002 г. [3].

Следующим этапом, а, вернее, стимулом к развитию законодательства, регламентирующего применение электронного документооборота и ЭЦП, послужило принятие законов, направленных на противодействие коррупции.

После вступления в силу Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» [12] у каждого субъекта, подпадающего под действие закона, появилась необходимость использования ЭЦП. В соответствии с п. 4.2 ст. 10 заказчик обязан проводить размещение заказов на поставку товаров, выполнение работ, оказание услуг путем проведения открытого аукциона в электронной форме.

В рамках мероприятий, направленных на реализацию Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» [12], в соответствии со ст. 65 Правительством РФ разработан ряд нормативно правовых актов:

- постановление Правительства РФ от 10.03.2007 № 147 «Об утверждении Положения о пользовании официальными сайтами в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами» [13],
- постановление Правительства РФ от 29.12.2010 № 1191 «Об утверждении Положения о ведении реестра государственных и муниципальных контрактов, а также гражданско-правовых договоров бюджетных учреждений на поставки товаров, выполнение работ, оказание услуг и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования официальным сайтом в сети Интернет, на котором размещается указанный реестр» [14]

и другие.

В указанных подзаконных актах устанавливаются требования о применении ЭЦП при размещении информации на сайте www.zakupki.gov.ru , определенном ст. 16 Федерального закона от 21.07.2005 № 94-ФЗ [15].

Принятый в 2011 году Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» [16] расширил перечень субъектов, которые обязаны размещать информацию о проводимых закупках на официальном сайте. Также, п. 4 ст. 3 указанного закона императивно устанавливается норма о проведении закупочных процедур в электронной форме в случае закупки товаров, работ, услуг, попавших в перечень, утвержденный постановлением Правительства РФ № 616 от 21.06.2012 [17].

Автор солидарен с мнением Белова В.Е., который отмечает, что данное требование вводится государством императивно. Субъекты, которым предписано проводить электронные закупки, рассматривают процедуру организации и проведения государственных закупок как дополнительное обременение, выполнение несвойственных им функций, влекущее возникновение дополнительных проблем [18, 110 с.]. Также, как указывает Белов В.Е., участие в процедурах закупки в электронной форме различных категорий поставщиков, например, субъектов малого предпринимательства, должно стимулироваться государством дополнительно [18, 122 с.].

Организация деятельности хозяйствующих субъектов в рамках двух приведенных законов, регламентирующих проведение закупок, требует внедрения электронной подписи (ЭП), однако в данном случае применение ЭП — не реализация диспозитивных установок гражданского законодательства, которые требуются для оптимизации бизнес-процессов и внедрения новых технологий, а, скорее, регулирующее воздействие государства.

Анализ извещений о проведении закупок, размещенных на сайте www.zakupki.gov. ru , показывает, что зачастую заказчик, помимо требования о предоставлении документации в электронной форме, подписанной ЭП, требует направления бумажных копий документов. Данная практика скорее свидетельствует о наличии суррогатной надстройки в виде дополнительного предоставления электронной документации, чем об оптимизации деятельности организации с помощью применения информационных технологий.

В связи со стремлением бизнеса к снижению затрат на выполнение работ и услуг, не требующих фактического присутствия в месте исполнения, и появлением с развитием информационных технологий новых видов подобных услуг существует потребность в дальнейшем совершенствовании законодательства, регламен-

тирующего порядок применения ЭП. Подобная необходимость обусловлена также потребностью в интенсификации ведения юридически значимого делового документооборота.

В последние годы законодателем был проведен ряд изменений нормативно-правовых актов, способствующих более широкому применению ЭП.

В 2010 г. в ст. 169 Налогового кодекса РФ внесены положения о возможности применения в хозяйственной деятельности и представления для налогового вычета по НДС счетов-фактур, составленных в электронном виде, в соответствии с установленными форматами и порядком [19]. Фактическое применение данной статьи стало возможным после разработки и введения в действие в 2011 г. «Порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи» [20].

В соответствии с п. 1 ст. 9 Федерального закона от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» [21] каждый факт хозяйственной жизни организации, ведущей бухгалтерский учет, подлежит оформлению первичным учетным документом. Пунктом 5 указанной статьи устанавливается форма первичного учетного документа, который может быть представлен на бумажном носителе и (или) в виде электронного документа, подписанного электронной подписью. Данный закон вступил в силу с 01.01.2013 г., однако о фактической возможности применения приведенной нормы говорить еще не приходится ввиду отсутствия разъяснительных документов, изданных Министерством финансов РФ. Автор согласен с мнением Головы И. о преждевременности применения электронных первичных документов, разработанных непосредственно организацией, в связи с наличием перспектив разработки и утверждения единых форм указанных документов [22].

Приведенные выше нормы направлены именно на реализацию потребностей бизнеса по организации юридически значимого документооборота в электронной форме при межкорпоративном взаимодействии.

Основным шагом законодателей, направленным на более широкое внедрение электронного документооборота в отношения между хозяйствующими субъектами, можно считать принятие в 2011 г. Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» [23], который вступил в силу со дня его опубликования, а должен был отменить действие Федерального закона от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» [6] только с 1 июля 2013 г.

К действовавшему с 2002 г. Федеральному закону «Об электронной цифровой подписи» [6] имелись значительные замечания, как на этапе прохождения им законотворческой процедуры [24, 25, 26], так и на этапе использования его в правоприменительной практике.

Исследование законодательного регулирования общественных отношений по использованию ЭЦП, проведенные Хадыковым Р.О., свидетельствуют о необходимости проведения значительной корректировки нормативно-правовых актов для реализации потребностей в применении электронного документооборота [27].

В пояснительной записке к проекту Федерального закона «Об электронной подписи» [28] приведены следующие причины, обуславливающие необходимость принятия нового законодательного акта взамен Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» [3]:

- наличие в изменяемом законодательном акте концептуальных и юридико-технических недостатков, которые не позволили обеспечить правовые условия, необходимые для широкого применения электронной цифровой подписи в Российской Федерации;
- вопреки сложившейся мировой практике Федеральный закон «Об электронной цифровой подписи» допускает использование единственной технологии электронной цифровой подписи (основанной на так называемой технологии асимметричных ключей подписи), делает необходимой единую иерархическую систему удостоверяющих центров, обязывает применять сертифицированные средства электронной цифровой подписи;
- положения отменяемого закона не соответствуют основным принципам, реализуемым в иностранном законодательстве и международном праве при осуществлении правового регулирования электронных подписей, таким как «технологическая нейтральность» законодательства, правовое признание различных видов электронной подписи, свободное использование средств электронной подписи, аккредитация удостоверяющих центров;
- недостаточна сфера регулирования закона, из нее исключены как отношения по использованию иных видов электронной подписи, так и отношения, не являющиеся гражданско-правовыми сделками;

- в преобразуемом законе не допускается электронная цифровая подпись юридических лиц;
- Федеральный закон «Об электронной цифровой подписи» не согласован с иными законодательными актами Российской Федерации, в том числе о лицензировании отдельных видов деятельности и о техническом регулировании.

По мнению многих авторов, в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» нашли свою реализацию концепции, за отсутствие которых критиковался Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» [29, 30].

Законотворческая практика практически не знает случаев подготовки и принятия законов, в которых устранялись бы все коллизии действующего законодательства, и полностью отвечающим требованиям субъектов регулируемых правоотношений.

В принятом Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» есть внутреннее противоречие, касающееся сертификатов ЭЦП, которые были выданы еще в соответствии с законом № 1-ФЗ «Об электронной цифровой подписи». В ст. 19 указанного закона установлено, что сертификаты действуют до конца срока, на который были выданы. Но вторая часть этой же статьи говорит, что электронный документ, подписанный ЭЦП с таким сертификатом, действует только до 1 июля 2013 г.

Однако данные противоречия были устранены и «срок жизни» старых сертификатов продлен до 31.12.2013 г. [31].

Также, в связи со вступлением в силу Закона был выпущен противоречивый подзаконный акт – приказ ФНС России от 08.04.2013 № ММВ-7-4/142@ «Об утверждении порядка применения квалифицированных сертификатов ключей проверки электронной подписи в информационных системах ФНС России» [32], устанавливающий с 1 июля 2013 г. запрет в органах ФНС на применение сертификатов, выпущенных по Федеральному закону «Об электронной цифровой подписи». На данный момент указанный приказ неприменим в связи с выходом Федерального закона от 02.07.2013 № 171-ФЗ и отказом в регистрации указанного акта Минюстом.

Какие еще проблемы ожидают бизнес при применении Федерального закона № 63-ФЗ «Об электронной подписи», покажет практика.

Литература

1. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 № 51-ФЗ (ред. от 02.07.2013). Официальный интернет-портал правовой информации http://www.pravo.gov.ru .
2. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 № 51-ФЗ. «Российская газета», № 238-239, 08.12.1994.
3. Федеральный закон от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007) «Об электронной цифровой подписи». «Российская газета», № 6, 12.01.2002.
4. Ильиных Е.В., Козлова М.Н. Комментарий к Федеральному закону от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (постатейный). М.: Юстицинформ, 2005.
5. Леонтьев К.Б. Комментарий к Федеральному закону «Об электронной цифровой подписи» (постатейный). М.: ООО «ТК Велби», 2003.
6. Временное положение № 17-П «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями». Вестник Банка России, 18 февраля 1998 г., № 10.
7. «Налоговый кодекс Российской Федерации» от 31.07.1998 № 146-ФЗ. «Российская газета», № 148-149, 06.08.1998.
8. Федеральный закон от 28.12.2001 № 180-ФЗ «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации». «Российская газета», № 255, 30.12.2001.
9. Приказ МНС РФ от 02.04.2002 № БГ-3-32/169 «Об утверждении Порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи». «Российская газета», № 89, 22.05.2002.
10. Приказ МНС РФ от 10.12.2002 № БГ-3-32/705@ «Об организации и функционировании системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи». Опубликован не был.
11. «Налоговый кодекс Российской Федерации» от 31.07.1998 № 146-ФЗ (ред. от 28.06.2013). Официальный интернет-портал правовой информации http://www.pravo.gov.ru .
12. Федеральный закон от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». «Российская газета», № 163, 28.07.2005.
13. Постановление Правительства РФ от 10.03.2007 № 147 «Об утверждении Положения о пользовании официальными сайтами в

сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами». «Российская газета», № 54, 16.03.2007.
14. Постановление Правительства РФ от 29.12.2010 № 1191 «Об утверждении Положения о ведении реестра государственных и муниципальных контрактов, а также гражданско-правовых договоров бюджетных учреждений на поставки товаров, выполнение работ, оказание услуг и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования официальным сайтом в сети Интернет, на котором размещается указанный реестр». «Собрание законодательства РФ», 24.01.2011, № 4, ст. 604.
15. Федеральный закон от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». «Российская газета», № 163, 28.07.2005.
16. Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц». «Российская газета», № 159, 22.07.2011.
17. Постановление Правительства РФ от 21.06.2012 № 616 «Об утверждении перечня товаров, работ и услуг, закупка которых осуществляется в электронной форме». «Собрание законодательства РФ», 25.06.2012, № 26, ст. 3533.
18. Белов В.Е. Поставка товаров, выполнение работ, оказание услуг для государственных нужд: правовое регулирование. М.: Норма, Инфра-М, 2011.
19. Федеральный закон от 27.07.2010 № 229-ФЗ «О внесении изменений в часть первую и часть вторую Налогового кодекса Российской Федерации и некоторые другие законодательные акты Российской Федерации, а также о признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации в связи с урегулированием задолженности по уплате налогов, сборов, пеней и штрафов и некоторых иных вопросов налогового администрирования». «Собрание законодательства РФ», 02.08.2010, № 31, ст. 4198.
20. Приказ Минфина РФ от 25.04.2011 № 50н «Об утверждении Порядка выставления и получения счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной цифровой подписи» (зарегистрирован в Минюсте РФ 25.05.2011, № 20860). «Российская газета», № 119, 03.06.2011.
21. Федеральный закон от 06.12.2011 № 402-ФЗ (ред. от 28.06.2013) «О бухгалтерском учете». Официальный интернет-портал правовой информации http://www.pravo.gov.ru .
22. Голова И. Электронная первичка // Расчет. 2012. № 3. С. 72-73.
23. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». «Российская газета», № 75, 08.04.2011.
24. Заключение Комитета Государственной Думы по безопасности по проекту федерального закона «Об электронной цифровой подписи», внесенному Правительством РФ. http://asozd2.duma.gov.ru .
25. Заключение Комитета Государственной Думы по информационной политике по проектам федерального закона «Об электронной цифровой подписи» и постановления Государственной Думы о нем (I чтение) от 17.05.2001. http://asozd2.duma.gov.ru .
26. Заключение Комитета Государственной Думы по информационной политике по проекту федерального закона № 78684-3 «Об электронной цифровой подписи» и проекту постановления Государственной Думы о принятии его во втором чтении (повторно ко второму чтению) от 08.11.2001. http://asozd2.duma.gov.ru .
27. Хадыков Р.О. Диссертация на соискание ученой степени кандидата юридических наук на тему «Правовой режим электронного документооборота: вопросы использования электронной цифровой подписи». Казань, 2006 г.
28. Пояснительная записка к проекту федерального закона «Об электронной подписи». http://asozd2.duma.gov.ru/ .
29. «Комментарий к Федеральному закону от 06.04.2011 № 63-ФЗ «Об электронной подписи» (постатейный). Амелин Р.В., Бевзюк Е.А., Волков Ю.В., Марченко Ю.А., Холодная Е.В. Подготовлен для системы КонсультантПлюс, 2012.
30. Кирилловых А.А. «Комментарий к Федеральному закону «Об электронной подписи» (постатейный). Юстицинформ, 2011 г.
31. Федеральный закон от 02.07.2013 № 171-ФЗ «О внесении изменений в Федеральный за-

кон «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» и отдельные законодательные акты Российской Федерации». Официальный интернет-портал правовой информации http://www.pravo.gov.ru , 03.07.2013.

32. Приказ ФНС России от 08.04.2013 № ММВ-7-4/142 «Об утверждении Порядка применения квалифицированных сертификатов ключей проверки электронной подписи в информационных системах ФНС России». Опубликован не был.

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

Солдатова Нина Викторовна
Леонтьев Борис Борисович
доктор экономических наук, профессор

Государственная стратегия интеллектуальной собственности: опыт Японии

Аннотация: *сегодня во всем мире интеллектуальная собственность является одним из основных источников создания новых рабочих мест, новых товаров и услуг. В качестве национальной идеи Правительство Японии в 2000 году определило превращение нации в информационное общество, основанное на интеллектуальной собственности. Государственная политика, осуществляемая органами власти, первостепенное внимание уделяет изобретениям, творчеству и производству инновационных товаров и услуг. Использование интеллектуальной собственности в качестве главного ресурса в экономике – единственный путь для поддержания лидирующего положения в мировой экономике для страны, испытывающей недостаток в природных ресурсах.*

Ключевые слова: *государство, законодательство, интеллектуальная собственность, инновации, инструменты, модель, стратегия, управление, экономика.*

Начало нового тысячелетия ознаменовано всплеском интеллектуализации во всем мире. Это явление проявляется, прежде всего, через процессы системного усиления всестороннего влияния интеллектуальной собственности на экономику наиболее развитых стран. Институт интеллектуальной собственности ежегодно вовлекает в мировую экономику высоких технологий, масс-медиа, высокой моды, информационных и интеллектуальных услуг не менее пятидесяти миллионов человек во всем мире, то есть, новый миллиард за двадцать лет. Интеллектуальная собственность становится основным источником создания новых рабочих мест и новых товаров и услуг во всем мире.

Медленные, но устойчивые мировые процессы и тенденции, наблюдаемые в обществе, подсказывают нам, что человечество из состояния преимущественно биологической природы постепенно переходит в свое новое качество – в преимущественно интеллектуальную природу, где есть свои, более сложные, законы и закономерности, не противоречащие биологической природе. Понимание и использование данных законов и закономерностей дает нарастающий мультипликативный и синергетический эффекты. Интеллектуализация законодательства и нормотворчества, судебной системы, наблюдаемая нами во всех мировых общественных процессах, наиболее интенсивно проявляются там, где интеллектуальная элита данные тенденции видит, понимает и поддерживает. К таким странам, в первую очередь, относятся США, Германия, Сингапур и Япония, где уровень жизни наиболее высокий и привлекательность интеллектуального труда наивысшая.

В качестве национальной идеи Правительство Японии еще в 2000 году определило «превращение нации в информационное общество, основанное на интеллектуальной собственности». Принимается государственная политика, осуществляемая органами власти, где перво-

степенное внимание уделяется изобретениям, творчеству и производству инновационных товаров и услуг.

Использование интеллектуальной собственности в качестве главного ресурса в экономике – единственный путь для поддержания лидирующего положения в мировой экономике для страны, испытывающей недостаток в природных ресурсах. Согласно результатам анализа, сообщенным руководителем Патентного ведомства Японии в 1996 году, национальная система управления интеллектуальной собственностью (НСИС) японскими экспертами была охарактеризована как негибкая и устаревшая, а законодательство и государственная политика в этой сфере нуждались в пересмотре в связи с обновлением роли интеллектуальной собственности в инновационной политике Японии.

План реализации стратегических направлений политики в сфере интеллектуальной собственности Японии [1] указывает на необходимость повышения валового внутреннего продукта и экспорта товаров и услуг путем увеличения доходов компаний за счет: экспорта продукции, основанной на интеллектуальной собственности; обеспечения соблюдения прав интеллектуальной собственности в соответствии с международными обязательствами; расширения региональных и международных возможностей ТВ в сфере торговли путем гармонизации законов в целях снижения препятствий в торговле; стимулирования развития человеческого капитала и его применения в ключевых отраслях промышленности; превращение знаний в важный источник национального богатства.

При разработке НСИС акцент был сделан на системные изменения по следующим направлениям:

Во-первых, национальная патентная система должна была стать более удобной, особенно для исследователей и руководителей малых и средних предприятий. Главным приоритетом стало ускорение процедуры экспертизы патентных заявок для удовлетворения потребностей пользователей. В этих целях было принято решение о привлечении на определенный срок порядка 500 специалистов для проведения патентной экспертизы, а предшествующий ей патентный поиск производился на основе аутсорсинга. Указанные меры были нацелены на сокращение сроков патентной экспертизы с 26 до 11 месяцев к 2013 году.

Во-вторых, крайне важным в развитии Японии стал вопрос урегулирования отношений исследователей и работодателей – распределение прав на изобретения, оформление патентов и выплата компенсаций и создания взаимовыгодной системы отношений в целях повышения инновационной активности и стимулирования японской и мировой экономики.

В-третьих, в целях поддержания инновационного цикла была пересмотрена роль университетов и исследовательских институтов, которым было предоставлено право участвовать в коммерциализации результатов исследований, особенно финансируемых государством.

Дополнительной была поставлена задача добиться увеличения размера возмещения убытков, присуждаемых патентообладателям в случаях нарушения их прав. Если Япония должна была стать государством, в основе развития экономики которого лежит интеллектуальная собственность, то на лиц, умышленно нарушающих права интеллектуальной собственности, должно налагаться более суровое наказание. В этих целях были предложены существенные поправки в патентное законодательство, которые включали, в том числе, изменение критериев оценки ущерба за нарушения прав интеллектуальной собственности.

По мнению Правительства Японии, именно такая система интеллектуальной собственности должна побуждать к созданию новых технологий, а не к неправомерному использованию существующих объектов интеллектуальной собственности.

История создания НСИС

В 2001 году была сформирована небольшая специализированная группа, которая провела Национальный форум по стратегии в области интеллектуальной собственности.

Под девизом «Интеллектуальная собственность: основная сила обеспечения лидерства Японии к 2010 году» (Intellectual property: powering Japan to the top by 2010) в январе 2002 года был опубликован список из 100 предложений Форума, а также десятилетний план действий.

Предложения охватывали семь основных сфер – исследования, образование, частные предприятия, правительственные органы, дипломатическую сферу (внешние сношения), законодательство и судебную систему – и были направлены на коренной пересмотр политики на основе комплексного подхода.

Поворотным моментом для Японии по переходу к национальной стратегии в сфере интеллектуальной собственности считается 2002 год. В ежегодном обращении к Парламенту премьер-министр страны отметил, что одной из национальных целей является повышение международной конкурентоспособности японских отраслей промышленности путем надлежащего оформления и использования прав на результаты интеллектуальной деятельности в научных исследованиях. Под председательством премьер-министра был создан Совет по стратегии интеллектуальной собственности. Проект документа был подготовлен в ноябре 2002 года. В том же году был принят Основной закон по интеллектуальной собственности [2]. Одним из главных нововведений закона можно считать создание Штаб-квартиры по интеллектуальной собственности в рамках Кабинета министров Японии (далее – Штаб-квартира).

Штаб-квартира является постоянно действующим органом, деятельность которого основана на работе Совета по стратегии Интеллектуальной собственности. Возглавляет Штаб-квартиру Генеральный директор, которым по должности является премьер-министр Японии. В состав Штаб-квартиры согласно статье 30 Основного закона назначаются следующие лица:

- все государственные министры
- эксперты, обладающие выдающимися знаниями в вопросах создания, охраны и использования объектов интеллектуальной собственности, в т.ч. руководители ведущих национальных компаний.

Основной задачей Штаб-квартиры является разработка Программы интеллектуальной собственности Японии и мер по содействию ее реализации.

Поскольку руководство Японии приняло решение о стратегическом развитии экономики на основе активного использования интеллектуальной собственности, Основной закон (глава третья) в целях организации системы планирования вводит обязательную разработку и утверждение Программы интеллектуальной собственности Японии и определяет требования к порядку ее подготовки, реализации и мониторинга применения.

В рамках Программы интеллектуальной собственности должны быть решены следующие основные вопросы:

1. Основные направления политики в данной сфере;
2. Конкретные меры, которые правительство должно целенаправленно и планомерно реализовать для создания, охраны и использования объектов интеллектуальной собственности;
3. Конкретные меры, которые правительство должно реализовать в целях содействия образованию и обучению в области интеллектуальной собственности.

В Программе должны также устанавливаться конкретные цели и сроки реализации. Согласно Основному закону обязательной является публикация проекта программы в сети Интернет. Штаб-квартира должна обеспечить мониторинг реализации Программы и оценивать достижение поставленных целей и соблюдение сроков. Предусмотрена обязательная публикация результатов в сети Интернет. По итогам анализа эффективности реализации мер и оценки влияния происходящих экономических и иных изменений, Штаб-квартира должна по меньшей мере ежегодно актуализировать Программу и вносить соответствующие изменения. Таким образом, с 2003 года Япония ежегодно утверждает Национальную программу в области интеллектуальной собственности.

О национальных программах

Первая Стратегическая программа для создания, охраны и использования объектов интеллектуальной собственности [3] была утверждена правительством Японии в июле 2003 (далее – Стратегия).

Во введении к Стратегии говорится, что интеллектуальный творческий цикл состоит из трех стадий – создание результата творческой деятельности, его правовая охрана и последующее использование. При этом все три стадии составляют единый процесс, и меры по стимулированию каждой стадии должны разрабатываться и рассматриваться в совокупности.

При этом поставленная государством цель по превращению японцев в «нацию, развивающуюся на основе интеллектуальной собственности», не может быть достигнута без внедрения механизма, соединяющего процесс создания новых результатов творческой деятельности с исследованиями и их использованием для получения максимальной общественной пользы. Важнейшую роль в этом процессе играют университеты и исследовательские институты, в которых сосредоточено большинство творческих ресурсов Японии.

Именно поставленная цель – необходимость внедрения указанного выше механизма – определила структуру Стратегии-2003, которая состоит из соответствующих глав – создание объектов интеллектуальной собственности, охрана и защита объектов интеллектуальной собственности, использование объектов интеллектуальной собственности. Последние две главы направлены на развитие бизнеса в творческих отраслях, развитие человеческих ресурсов и повышение общественного внимания к интеллектуальной собственности.

Глава 1 Стратегии«Создание объектов интеллектуальной собственности» содержит перечень правительственных мер, направленных на увеличение финансирования процесса создания объектов интеллектуальной собственности.

Значительная часть предложенных мер относится к научной и исследовательской сферам. Соответствующие расходы предусматриваются в ежегодном бюджете страны (в Стратегии все финансовые обязательства правительства Японии указаны на 2003 фискальный год, который не совпадает с календарным и длится с 1 апреля по 31 марта).

В Стратегии отмечается, что выделение государственной поддержки на рядовые исследования не приведет к резкому росту экономического потенциала на основе инноваций. Поэтому Стратегия предусматривает создание системы оценки результатов деятельности университетов и научно-исследовательских организаций, использующих интеллектуальную собственность.

Для этого Стратегия предусматривает разработку «комплексных показателей оценки», касающихся интеллектуальной собственности. Он включает как количественные показатели (например, количество полученных патентов или поданных патентных заявок, так и качественные аспекты, такие как количество лицензионных договоров, сумма дохода от таких контрактов, частота цитирования в научных статьях, создание штаб-квартиры интеллектуальной собственности в университете и прочие). Данные критерии оценки должны быть использованы в оценке научно-исследовательской деятельности организаций и при распределении бюджетных средств для соответствующих фондов и других ресурсов на ее поддержку.

Стратегия также предусматривает проведение независимой национальной оценки деятельности университетов и научно-исследовательских организаций, связанной с созданием, защитой и использованием интеллектуальной собственности. Кроме того, предусмотрена разработка правил сотрудничества между промышленностью, академическими кругами и правительством с целью обеспечения большей гибкости при заключении контрактов.

Стратегия предусматривает, начиная с 2004 года, меры по укреплению японской системы лицензирования технологий путем предоставления соответствующей государственной поддержки, особенно для организаций по лицензированию технологий. Отдельный блок вопросов посвящен мерам содействия созданию новых предприятий в рамках университетов. Речь идет преимущественно о старт-апах как продуктов бизнес-инкубаторов.

Глава 2 Стратегии определяет направления развития системы охраны объектов интеллектуальной собственности.

Усилия государства в этой сфере распределены по ряду конкретных направлений.

Первым из них является совершенствование системы правовой охраны интеллектуальной собственности. По данному вопросу в Стратегии констатируется, что компаниям необходимо быстро принимать деловые решения в условиях интенсивной международной конкуренции и проводить более ускоренную патентную экспертизу. Такое ускорение является обязательным условием коммерциализации качественных изобретений и оживления экономики. В целях ускоренного рассмотрения патентных заявок, важно снизить число заявок, ожидающих своего рассмотрения (то есть, портфель нерассмотренных заявок), составляющее 500 000, и заняться ожидаемым быстрым дополнительным ростом количества ходатайств о проведении экспертизы, которое, как ожидается, составит около 300 000.

Конкретными мерами являются обеспечение патентного ведомства необходимым количеством экспертов, использование опытных ассистентов, проведение структурной реформы процедуры предоставления заявителями ходатайств о подаче патентной заявки, расширение и совершенствование функций частных организаций по проведению патентного поиска, усиление роли патентных поверенных. В качестве временной меры по сокращению портфеля нерассмотренных заявок стало привлечение внешних экспертов на определенный срок работы. Первоначально процедура ускоренной экспертизы должна применяться к заявкам, подаваемым университетами и малым

бизнесом, иностранным заявкам и заявкам на изобретения, ожидающим скорой коммерциализации или нуждающимся в неотложном патентовании.

Вторым важнейшим направлением является система защиты прав. Активное использование результатов интеллектуальной деятельности в экономике должно сопровождаться не только развитием мер поддержки и системы правовой охраны прав на них, но и совершенствованием системы их защиты. Здесь выделяются три аспекта.

Во-первых, необходимо совершенствование системы возмещения убытков в отношении интеллектуальной собственности и предоставление правообладателям надлежащих средств судебной защиты.

Во-вторых, с целью совершенствования сдерживающих эффектов против нарушений прав интеллектуальной собственности необходимо усиление уголовной ответственности.

В-третьих, необходимо совершенствовать систему урегулирования самих споров. Было принято решение о создании специализированного судебного органа – Высшего суда по интеллектуальной собственности.

Одновременно в Стратегии была поставлена задача совершенствования знаний экспертов, задействованных в системе судебных споров по интеллектуальной собственности.

Третьим является международный аспект. Поскольку развитие национальной системы правовой охраны и защиты интеллектуальной собственности невозможно без участия в совершенствовании международной охраны интеллектуальной собственности, в Стратегии предусмотрены следующие направления:

1. Содействие усилиям по созданию глобальной патентной системы, в т.ч. содействие сотрудничеству в области патентной экспертизы:

› сотрудничество в области патентной экспертизы с национальными патентными ведомствами других стран в направлении уменьшения процессуального бремени на заявителей, подающих патентные заявки во многих странах, снижения рабочей нагрузки на национальные патентные ведомства и достижения взаимного признания патентных законов и руководств по патентной экспертизе путем международной гармонизации.

› Содействие реформе Договора о патентной кооперации (PCT) в целях создания системы, которая облегчит приобретение прав на международном уровне.

› Содействие приобретению прав в развивающихся странах.

› Содействие международной гармонизации патентных систем.

› Создание международных сетей для обмена информацией по вопросам патентной экспертизы.

2. Содействие международной гармонизации систем авторского права.

3. Содействие разработке международных правил по урегулированию споров.

В качестве четвертого направления определен аспект контрафакции. В главе 2 Стратегии выделены система мер борьбы с контрафакцией и изготовлением пиратских копий. Для защиты интересов японского народа и компаний, а также для предоставления стимула к созданию новых объектов интеллектуальной собственности в Стратегии предусмотрено три блока необходимых государственных мер.

1. Ужесточение мер на зарубежных рынках:

› помощь в приобретении и защите прав японскими компаниями в других странах;

› создание информационных сетей, содержащих сведения о контрафактной и пиратской продукции;

› принятие мер против изготовления подделок и пиратских копий в сотрудничестве с государственным и частным секторами;

› активизация действий правительства в отношении стран, в которых выявлены случаи нарушения прав.

2. Ужесточение пограничных и внутренних правил:

› разработка национальных законов, ограничивающих частный ввоз товаров, выпущенных в нарушение прав интеллектуальной собственности;

› ужесточение мер по соблюдению пограничных и внутренних правил

› поправки в таможенное законодательство;

› совершенствование уголовного законодательства в части, касающейся таких преступлений, как продажа подделок и пиратских копий на улицах;

› ужесточение правил, касающихся нарушения прав в сети Internet;

› активизация деятельности по повышению информированности общественности.

3. Укрепление структур по борьбе с подделками и пиратскими копиями в государственном и частном секторах. Здесь предлагается ряд специальных мер.

Глава 3 Стратегии посвящена использованию объектов интеллектуальной собственности в экономике.

В Стратегии справедливо указывается, что, несмотря на выдающиеся результаты по созданию новых объектов интеллектуальной собственности и их надлежащую охрану, неэффективное использование этих результатов следует расценивать как «растрату казны», что явно не приведет к оживлению экономики. Именно для решения проблемы, когда значительное количество патентов не находит промышленного применения, и инвестиции в НИОКР не всегда способствуют экономическому развитию. В Стратегии был разработан ряд мер, стимулирующих компании использовать такие активы в их хозяйственной деятельности.

Основной задачей Правительства в этой сфере является поддержка стратегического использования интеллектуальной собственности частным бизнесом. Компаниям необходимо рассматривать интеллектуальную собственность как «источник» конкурентоспособности, которая в будущем принесет экономические выгоды и станет стержнем их управленческой стратегии. Правительство Японии должно поддерживать усилия компаний по разработке управленческой политики в рамках «Руководства по приобретению и административному управлению правами интеллектуальной собственности», «Руководства по административному управлению коммерческой тайной» и «Руководства по предотвращению утечки технологий». Типовые документы опубликованы Министерством экономики, торговли и промышленности в январе-марте 2003 г.) [4].

В целях создания благоприятной среды для использования интеллектуальной собственности в Стратегии предусмотрен блок следующих мер:

1. Укрепление стабильности лицензионных договоров в области охраны интеллектуальной собственности. Здесь рассматриваются аспекты охраны лицензий в случае банкротства лицензиара, повышения правовой стабильности лицензий на открытые программные средства и другие.
2. Улучшение доступа к информации об интеллектуальной собственности. Здесь предусматриваются новые издания и сайты.
3. Содействие предприятиям, использующим интеллектуальную собственность (в части проведения патентно-лицензионного поиска, оценки интеллектуальной собственности, отчетности в области охраны интеллектуальной собственности, планирования стратегии в области охраны интеллектуальной собственности, переговорных процессов по вопросам лицензирования и т.д.).
4. Содействие МСП и венчурным компаниям в более эффективном использовании интеллектуальной собственности.

Глава 4 Стратегии содержит необходимый комплекс мер по защите авторских и смежных прав.

Здесь предусмотрены меры по совершенствованию договорных обязательств и судебной практики.

Заключительная пятая глава Стратегии посвящена вопросам развития человеческих ресурсов и повышения уровня информированности общественности.

Ввиду того, что именно люди содействуют должному функционированию всех форм той или иной системы, то достижение национальной цели по превращению Японии в «нацию, основанную на интеллектуальной собственности», возможно только при наличии высококвалифицированных специалистов, способных создавать новые объекты интеллектуальной собственности, а также предоставлять прогрессивные специализированные услуги, такие как приобретение прав на созданные объекты интеллектуальной собственности, урегулирование споров и заключение лицензионных соглашений.

В соответствии с этим правительство Японии включило в Стратегию меры по увеличению числа адвокатов, патентных поверенных и других экспертов, обладающих солидным запасом знаний в вопросах интеллектуальной собственности и являющихся конкурентоспособными на международном уровне.

Кроме того, с целью подготовки компетентных специалистов в области охраны интеллектуальной собственности правительство Японии намерено оказать содействие обучению в области охраны интеллектуальной собственности, отвечающему самым высоким стандартам качества и количества, и совершенствованию знаний широкого круга специалистов в различных отраслях экономики и областях знаний, таких как право, технологии и управление коммерческими предприятиями (менеджмент).

Помимо этого правительство Японии направит усилия на подготовку большого числа учащихся и исследователей, сведущих в вопросах интеллектуальной собственности, в целях

содействия образованию в области охраны интеллектуальной собственности.

В дополнение к этому правительство Японии предложило обстоятельное обучение вопросам интеллектуальной собственности исследователям, учащимся начальной, средней и высшей школ, студентам университетов и взрослому населению, с целью улучшения информированности общественности в вопросах, относящихся к интеллектуальной собственности.

Стратегическая программа в сфере интеллектуальной собственности 2006 года (далее – Стратегия 2006) является весьма объемным документом, ориентированным на национальную цель, поставленную правительством Японии – перевод результатов научных исследований и творческой деятельности в охраняемые объекты интеллектуальной собственности, и использования в целях повышения международной конкурентоспособности японской промышленности. Стратегия 2006 также главной целью имеет соединение процесса создания новых результатов творческой деятельности и исследований и их использования в промышленности. Поэтому структура Стратегии повторяет структуру Стратегии 2003 года и состоит из 5 разделов: создание объектов интеллектуальной собственности, охрана объектов интеллектуальной собственности, использование объектов интеллектуальной собственности, развитие бизнеса с использованием цифрового контента, развитие человеческих ресурсов.

Отдельно в Стратегии 2006 выделен раздел, в котором приводятся основные достижения в политике в сфере интеллектуальной собственности (в соответствии со сложившейся структурой стратегии) и основные законодательные изменения (2003 – 2006 годы), а также краткая информация о проведенных мероприятиях по имплементации Стратегии (заседания Штаб-квартиры интеллектуальной собственности, встречи экспертов и рабочих групп, проведенные общественные обсуждения по отдельным положениям проекта стратегии).

В качестве основных достижений в сфере создания объектов интеллектуальной собственности отмечается, что:

- создано 43 штаб-квартиры интеллектуальной собственности в университетах, более 40 организаций по лицензированию технологий в университетах и научно-исследовательских организациях (по состоянию на март 2005 года);
- принципы передачи прав на изобретения, ранее созданные преподавателями университетов, были приняты 87 из 94 национальных университетов (93%) и в 145 из 578 государственных и частных университетов, что составляет 25% (по состоянию на март 2005 года);
- количество национальных патентов, полученных университетами и государственными научно-исследовательскими организациями, выросло в 2,5 раза в период с 2002 по 2005 год, количество лицензионных договоров и сумма выплат по ним увеличились в 2,1 раза и 5 раз соответственно с 2002 по 2004 фискальный год.
- по состоянию на конец 2005 финансового года, общее число университетских стартапов достигло 1503.
- были изменены положения Патентного закона, касающиеся прав сотрудников на изобретения (статья 35), которые вступили в силу в апреле 2005 года

В сфере совершенствования правовой охраны объектов интеллектуальной собственности за трехлетний период в Стратегии отмечены следующие достигнутые результаты по поставленным целям:

- произведено укрепление функций по урегулированию споров. В частности, с апреля 2005 года действует Высший суд по вопросам интеллектуальной собственности, а также были внесены изменения в законодательство, касающиеся расширения функций сотрудников судов, обладающих специальными знаниями для рассмотрения споров, связанных с интеллектуальной собственностью;
- обеспечено ускорение экспертизы патентных заявок. В частности, были внесены изменения в патентное законодательства, в т.ч. содержащие меры дерегулирования, был создан Совет по внедрению быстрой и эффективной патентной экспертизы, возглавляемый министром экономики, торговли и промышленности, были назначены по 98 новых срочных экспертов в 2004, 2005 и 2006 финансовых годах;
- было принято более 30 изменений в действующие законодательные акты по интеллектуальной собственности, в том числе:
- произведено усиление системы интеллектуальной собственности. Уголовное наказание за нарушение авторских прав было ужесточено путем внесения поправок в Закон об авторском праве и Закон о недопущении недобросовестной конкуренции;
- актуализированы нормы права в отношении уголовного наказания, налагаемого за нарушение патентных прав, прав на дизайн и

прав на товарные знаки, а также при нарушении коммерческой тайны. Верхний предел для срока лишения свободы и сумма штрафа были увеличены, соответственно, до 10 лет и до 10 миллионов йен;

- была введена в эксплуатацию система доступа к информации трех патентных ведомств Японии, США и Европейского патентного ведомства;
- принятие системных мер по проблеме контрафакции.

3. Усиление мер по борьбе с контрафактной и пиратской продукцией произошло за счет организации Штаб-квартиры интеллектуальной собственности, где был принят пакет мер по усилению мер по борьбе с контрафактом и пиратством. В сентябре 2004 года Ассоциацией по распространению контента за рубежом (The Content Overseas Distribution Associate (CODA)) был учрежден специальный знак – Content Japan (CJ) для размещения на товарах, произведенных в Японии [5]. С этой целью были внесены изменения в таможенное законодательство. Дополнительно была введена система уведомления правообладателей об экспортерах и импортерах продукции, нарушения патентных и иных интеллектуальных прав было включено в качестве основания для приостановления экспорта продукции. В структуре министерства экономики, торговли и промышленности создано в августе 2004 года агентство по нарушениям прав интеллектуальной собственности.

Значительная часть стратегии посвящена проблемам экономики. В целях повышения активности использования объектов интеллектуальной собственности в экономике для малых и средних предприятий, а также венчурных компаний были предусмотрены специальные меры. В частности, намечалось обеспечение бесплатного доступа к базам патентной информации для использования ее при подготовке патентных заявок. Намечено снижение пошлин за рассмотрение патентных заявок и выдачу патентов.

В целях стимулирования органов местной власти было предложено стратегии разрабатывать и применять на нижнем территориальном уровне. В результате органы власти 22 префектур по состоянию на апрель 2006 года полностью закончили подготовку своих локальных стратегий в сфере интеллектуальной собственности, а 15 готовили соответствующие проекты. В 9 регионах при Региональных бюро экономики, торговли и промышленности были учреждены штаб-квартиры интеллектуальной собственности в форме государственно-частных организаций

В Стратегии 2006 года в качестве главной краткосрочной цели – на 2006-2008 финансовые годы указывалось, что поскольку 21 век является эрой мегаконкуренции в сфере знаний, то в развитие проведенных в 2003-2006 годах законодательных изменений, должны быть проведены реформы, которые обеспечат Японии лидирующие мировые позиции в сфере создания, охраны и использования интеллектуальной собственности. Правительство Японии предполагало, что будет создана наиболее передовая, прогрессивная система интеллектуальной собственности.

Исходя из главной цели, Стратегия была направлена на решение семи основных задач:

1. Осуществление политики в области интеллектуальной собственности в глобальных масштабах.
2. Расширение политики в области интеллектуальной собственности на региональном уровне и поддержки МСП и венчурных компаний.
3. Поощрение создание интеллектуальной собственности в университетах и государственных научно-исследовательских институтах и обеспечение содействия сотрудничеству между наукой и промышленностью.
4. Реформирование структуры системы подачи и рассмотрения патентных заявок и обеспечение оперативности патентной экспертизы.
5. Развитие сферы авторского права и смежных прав.
6. Продвижение бренда Японии.
7. Развитие человеческих ресурсов, касающихся интеллектуальной собственности.

Исходя из указанных семи задач, в Стратегии 2006 содержится перечень приоритетных мер по каждому направлению.

Стратегическая программа в сфере интеллектуальной собственности (далее – Стратегия 2007). Структура Стратегии повторяет структуру предшествующего документа 2006 года и состоит из вводной части, перечня основных мер по ключевым направлениям, и основных положений, раскрывающих более подробно необходимые меры с указанием конкретных ответственных государственных органов.

Особенностью развития Стратегии как документа является то, что ежегодно значительно возрастает внимание к проблеме развития отрасли авторского права и смежных прав, защита прав авторов в цифровой среде. Отдельным направлением является развитие бренда Японии,

в рамках которого предусматриваются меры по популяризации национальной культуры питания, создание привлекательных брендов регионов страны, создание в качестве мирового бренда для национальной модной индустрии, стимулирование творческой деятельности в стране, поддержка участия в зарубежных выставках, повышение привлекательности для иностранных туристов и средств массовой информации. Основным источником информации для бизнеса было активное использование международного вещания и многих других источников, но не интеллектуальная собственность.

В мае 2012 года премьер-министр Японии заявил, что именно эта сфера является «скрытым сокровищем Японии», которая может оживить экономику страны [6].

Основная концепция Стратегии 2007 года была основана преимущественно на двух документах, принятых Правительством Японии в мае 2007 года – «Инновации 25» и Стратегия культурной/творческой индустрии Японии. В эпоху глобальной конкуренции эти два документа созданы для содействия росту Японии и распространения уникальных особенностей не только в технологической, но и в культурной сфере бизнеса, выходящего за рубеж.

Поэтому при подготовке Стратегии 2007 особое внимание уделялось реализации Стратегии в глобальном масштабе.

Комментарий к стратегической программе в сфере интеллектуальной собственности 2010 года

В предисловии к Программе [7] дается краткое описание мировой ситуации и положение Японии. В частности, отмечается, что, несмотря на предпринятые усилия в условиях экономической глобализации и усиления международной конкуренции европейские страны в качестве мирового лидера вновь опередили Японию. Однако Япония обладает таким интеллектуальным потенциалом как система общенационального высшего образования, научные и технические достижения во многих областях, национальный цифровой контент. При правильном и полном использовании указанных сильных сторон, возможно будет добиться не только лидирующей роли в конкуренции на зарубежных рынках, но и активизировать внутренние рынки и достичь устойчивого экономического роста. Для того чтобы в полной мере использовать такие объекты интеллектуальной собственности как наилучшие технологии и контент, должна быть создана и реализована стратегия развития человеческих ресурсов, стратегия создания инноваций, стратегия создания международных стандартов и стратегия развития глобального бизнеса.

Отраслевые стратегии играют исключительную роль для развития отраслевых технологий и техники.

Именно совместно с реализацией отраслевых стратегий (в сфере промышленной политики, политики в сфере науки и технологий, политики в сфере информационных и компьютерных технологий и т.д.) возможно достичь цели роста в каждой из областей.

Исходя их поставленных целей, Программа 2010 разделена на три стратегии и содержит приоритетные меры к каждой из них. При этом указаны целевые количественные показатели реализации всех мер, ориентированных на 2020 год.

Первая подстратегия направлена на повышение конкурентоспособности путем создания международных стандартов в конкретных стратегических областях для международной стандартизации.

Для обеспечения будущего роста Япония выбрала и сконцентрировала усилия на развивающихся отраслях промышленности, включенных в перечень стратегических отраслей для международной стандартизации, в которых Япония имеет технологические преимущества. В качестве первого шага основное внимание было сосредоточено на семи стратегических отраслях Японии для международной стандартизации (передовые медицинские технологии, вода, транспортные средства следующего поколения, железные дороги, энергетический менеджмент, цифровой контент, роботы и робототехника), в которых должно быть оказано содействие управлению интеллектуальной собственностью для использования объектов интеллектуальной собственности и установления международных стандартов, что приведет к повышению конкурентоспособности на мировом рынке.

Именно в указанных стратегических областях ставится задача по повышению уровня знаний в сфере интеллектуальной собственности руководителей организаций, имеющих высокую международную конкурентоспособность. Это следует делать в целях изменения понимания и подходов к управлению интеллектуальной собственностью, в том числе международной стратегии стандартизации.

В качестве ожидаемых результатов от реализации первой подстратегии к 2020 году указывается увеличение доли японских товаров на мировом рынке в определенных стратегических областях путем развития международной стандартизации в сочетании с научными исследованиями, за счет реализации стратегии коммерциализации, а также за счет приобретения и использования прав интеллектуальной собственности у мировых лидеров НИОКР.

Вторая подстратегия посвящена содействию стратегии роста на основе развития цифрового контента.

В целях содействия расширению использования контента за рубежом, приобретения зарубежных каналов распределения и передачи информации за границу, необходимо срочно сформировать государственно-частный инвестиционный фонд и принять меры по оказанию поддержки, а также рассмотреть, как оказать помощь в плане формирования эффективной налоговой системы. Следует внимательно изучить законодательства ведущих стран и призвать правительства этих стран к изъятию из их национального законодательного регулирования положения, которые препятствуют распространению японского контента.

Следует активно формировать инфраструктуру развития человеческих ресурсов и технологии накопления человеческих ресурсов даже из-за рубежа через содействие формированию контента, использование информационно-коммуникационных технологий, включая цифровые учебники для образования, содействие увеличению творческой активности в образовательной среде.

В целях активизации разработки и предоставления цифрового контента и услуг, следует оперативно организовать комплексную правовую систему в отношении коммуникационных технологий, связи и вещания, и необходимо срочно разработать меры для эффективного использования радиоволн, в том числе для использования *белого* пространства в 2010 финансовом году.

В качестве мер, применяемых к нарушителям авторских и смежных прав в сети Интернет, было намечено ввести механизм отслеживания контрмер, принимаемых со стороны провайдеров интернет-услуг, к разработке плана реформ по усилению ограничений и контролю доступа. Этот механизм предполагалось реализовать в течение 2010 финансового года.

Прогноз ожидаемых результатов (по состоянию на 2020)

1. Доходы от авторского контента, ожидаемые из-за рубежа:

Предполагается, что рост составит от ~ 1,2 триллиона иен (2009) до ~ 2,6 трлн. иен.

2. Количество иностранных студентов, связанных с национальным контентом, будет равно 10 000.
3. Масштабы рынка цифрового/Интернет контента:

рост составит от ~ 1,4 триллиона иен (2008) до ~ 7 трлн. иен в 2020 году.

Третья подстратегия направлена на усиление мер, связанных с интеллектуальной собственностью, межотраслевого промышленного характера.

Предусматривалось расширить систему освобождения от уплаты патентных сборов для венчурных компаний и МСП (малых и средних предприятий). Кроме того, в качестве мер по оказанию помощи компаниям, не имеющим опыта в патентных заявках, рассмотреть необходимые меры, включая такие из них как снижение уровня сборов, взимаемых патентными поверенными и т. д.

С 2010 года предполагалось создать единые консультационные пункты («одного окна») по всей стране, чтобы коллективно получать различные консультации в отношении управления интеллектуальной собственностью, способствующих развитию бизнеса.

В связи с формированием основы для инноваций было намечено пересмотреть некоторые положения патентной системы в целях поощрения вклада, вносимого в повышение использования патентов, в расширение круга пользователей, включая университеты. В частности, предусматривалось укрепление системы лицензирования на основе применения упрощенных процедур для университетов и исследователей.

Совершенствование патентной системы намечалось также с целью интеграции и упрощения процедуры подачи заявок, а также принятие мер для достижения более быстрого и глубокого взаимного признания результатов патентной экспертизы в каждой стране между Японией, США, Европой, Кореей и Китаем. Кроме того, намечалось завершить переговоры по международному договору по борьбе с пиратством (АСТА), чтобы уменьшить ущерб, причиненный контрафактной и пиратской продукцией.

Прогноз ожидаемых результатов (по состоянию на 2020 год)

1. Содействие использованию интеллектуальной собственности, и создание новых видов бизнеса и направлений.

* Синий светодиод (годовые продажи в среднем: 0,400 млрд йен) является примером использования технологии, разработанной в университете и получившей распространение по всему миру .

2. Объем экспорта технологий возрастет от 2 трлн до ~ 3 трлн иен.
3. Создание большого количества конкретных направлений бизнеса, играющего активную роль во всем мире.
4. Сумма экспорта малых и средних предприятий возрастет от ~ 10 трлн. до ~ 14 трлн. иен.

Второй раздел Стратегии 2010 представляет собой таблица мер по ее реализации. Она представляет собой перечень конкретных мероприятий, предусмотренных в других разделах Стратегии, их описание, перечень ответственных за реализацию в органах государственной власти и сроки. При этом меры четко разделены по срокам реализации на краткосрочные (2010-2011 финансовый год), среднесрочные (2012-2013 финансовый год) и долгосрочные (2014-2019 финансовые годы).

Комментарий к последней программной стратегии, принятой в начале финансового года – 29 мая 2012 года

Современный мир сегодня находится в стадии постоянной динамичной трансформации. Информация, денежные средства, продукция, технологии и люди свободно и быстро перемещаются через границы в так называемом «мире без границ». Высокоскоростной Интернет соединяет мир в «Глобальную сетевую эпоху» (“Globally Networked Age”).

В Стратегии отмечаются новые вызовы, на которые необходимо ответить, чтобы выжить в новую эпоху.

Во-первых, международный патентный ландшафт изменяется в свете укрепления системы интеллектуальной собственности. Поскольку увеличивается число патентных заявок и объем патентной документации, составленных не на английском, а на китайском и корейском языках, осторожные патентные стратегии для конкуренции на мировом рынке имеют ключевое значение для компаний, развивающих свой бизнес в глобальном масштабе. Кроме того, соответствующие стратегии интеллектуальной собственности незаменимы для средних и малых предприятий и таких отраслей, как железные дороги, водное хозяйство, фармакология, предприятия которых в последние годы быстро расширили свой бизнес за рубежом. И как видно на проекте корейского центра интеллектуальной собственности (Korean IP hub project), патентная система также подвержена конкуренции в сфере международных услуг. В случае, если правоприменительная практика и судебная система не будут соответствовать международному уровню, ведущие мировые компании могут отказаться от японской патентной системы.

Изменения касаются международных стандартов, «нормотворчества», которые являются ключом к международной конкуренции. До сих пор, стратегическая важность международного стандарта не была должным образом признана руководителями компаний, представителями науки и государственных организаций, несмотря на усилия, предпринимаемые некоторыми экспертами.

Помимо отдельных институциональных проблем, комплексное управление интеллектуальной собственностью стала еще более важным. В прошлом японские компании рассматривали объекты интеллектуальной собственности в качестве вторичных активов. А процедуры, направленные на приобретение этих прав были реализованы в подчинении к стратегии бизнес-управления и развития научных исследований и разработки (R & D). Однако, для того, чтобы выжить в условиях жесткой международной конкуренции сегодня, необходимо объединение всех трех элементов в корпоративной стратегии: интеллектуальной собственности, управления бизнесом и стратегии НИОКР.

Во-вторых, использование возможностей программного обеспечения в цифровую эпоху и активным развитием свободных отношений на мировом рынке, система авторского права, созданная для защиты авторских произведений, сейчас сталкивается со многими трудностями.

Технологические инновации снизили стоимость тиражирования и передачи информации практически до нуля. В среде, где скопированная информация легко передается в глобальные сети, требуются новые идеи и разработки для обмена знаниями и должной защиты автор-

ских прав, чтобы не снижать темпы создания произведений.

Программа-2012 в Японии будет мощно стимулировать комплексную стратегию развития разнообразных авторских произведений. Рассматривая глобальные изменения, вызванные цифровой эпохой как новые большие возможности, правительством Японии планируется ускорить процессы совершенствования инновационной среды, направленные на создание новых предприятий и новых рынков, и тем самым повысить динамизм развития Японской экономики.

Учитывая вышеобозначенные причины и прогноз на десятилетнюю перспективу, разработана комплексная стратегия интеллектуальной собственности, имеющая разносторонний, всеобъемлющей и междисциплинарный характер. Поэтому в Программу 2012 включены две всеобъемлющие дополнительные стратегии, направленные на укрепление конкурентоспособности Японии на мировом рынке:

1.Комплексная стратегия инноваций в интеллектуальной собственности
2. Комплексная стратегия по наращиванию цифрового контента.

Выводы

Исследование специфики японской экономики, их достижений и проблем, которые формулируются, обсуждаются и системно разрешаются, позволяет отметить ряд важных факторов успеха:

- правительство Японии весьма чутко реагирует на запросы бизнеса и ведущих специалистов, работающих в сфере высоких технологий и интеллектуального консалтинга. Отсюда возникают возможности выявления и привлечения лучших японских специалистов для разработки и систематического совершенствования государственных стратегий. Наиболее компетентные специалисты по ИС в Японии определяются по публикациям, выступлениям на конференциях, по созданным системам в этой сфере, опубликованным учебникам, учебным пособиям и количеству ссылок на этих специалистов. Практически все эти критерии, к сожалению, в России не работают. Поэтому аналогичные проблемы в России не решаются, власть хронически запаздывает всюду, где требуется развитие, и особенно там, где накапливаются интеллектуальные проблемы и должны формироваться и распространяться интеллектуальные системы и технологии для процветания нации и перспектив молодых людей.

В японской экономике во власти сложилась критическая масса весьма дальновидных руководителей и умных специалистов, которые методично разрабатывают и практически развивают те направления, где требуются интеллектуальная изощренность и знания в этой отрасли. В то же время, ведущие японские специалисты и руководители, формирующие и развивающие данную Стратегию, не демонстрируют никаких открытий или восхитительных изобретений в этой области. В России все, о чем написано в японской Стратегии, давно уже складывается и развивается на уровне существенно более низком, чем правительственный или парламентский. Эти технологии создаются в российском консалтинге на уровне отдельных предприятий, организаций, малых предприятий. Правительство РФ не видит этих инициатив, не поддерживает их, что ведет к застою в этой сфере.

Отношение власти и общества в Японии к интеллектуальной собственности может быть примером для всех современных стран, пытающихся использовать интеллект в качестве основного ресурса нации, что достойно всяческого уважения и восхищения умной властью, создающей умную экономику. Все это на системной основе формирует умную нацию, способную стойко переживать любые трагедии и делать из своих неудач правильные выводы. Способность нации понимать проблемы, стоящие перед ней, и системно их разрешать, не подражая никому, говорит о том, что в Японии интеллектуальное начало последние полвека является доминирующим и, пожалуй, лидирующим в мире в рамках Восточного полушария. Асимметрия «США – Япония» – это ось интеллектуального вызова цивилизации, где России еще предстоит найти свое место и сказать свое веское слово. Для этого у нас есть все основания.

Литература

1. IP Strategic Policy Outline. Утвержден Стратегическим советом по интеллектуальной собственности 3 июля 2002 года. http://www.kantei.go.jp/foreign/policy/titeki/kettei/020703taikou_e.html
2. Basic Law on Intellectual Property No.122 of 2002, Japan.
3. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan010247.pdf

4. Strategic Program for the Creation, Protection and Exploitation of Intellectual Property. http://www.kantei.go.jp/foreign/policy/titeki/kettei/030708f_e.html.
5. Стратегии интеллектуальной собственности компании HITACHI (IP STRATEGY of HITACHI). Министерство экономики, торговли и промышленности. 2003 г.
6. The Content Overseas Distribution Association (CODA). http://www.coda-cj.jp/en.html
7. Intellectual Property Strategy Headquarters (news). May, 2012.
8. http://www.kantei.go.jp/foreign/noda/actions/201205/29chiteki_e.html
9. Intellectual Property Strategic Program – 2010. May, 2010.

Фадеева Наталья Анатольевна

Актуальные вопросы систематизации законодательства Российской Федерации

Аннотация: *в настоящей статье рассматриваются формы систематизации законодательства и перевод в электронный вид государственной учетной деятельности. Статья содержит обзор и аналитический перечень правовых актов в данном направлении.*

Ключевые слова: *систематизация, инкорпорация, консолидация, подсистема, информационные ресурсы, архивы, информационные системы.*

Второе десятилетие XXI века ознаменовалось для Российской Федерации принятием очередной государственной программы «Информационное общество» (2011-2020 годы)» [1], утвержденной распоряжением Правительства Российской Федерации от 20.10.2010 г. № 1815-р., которая позиционируется как принципиально новый подход к информации общества с учетом задач по модернизации экономики. Целью программы определено получение гражданами и организациями преимуществ от применения информационных и телекоммуникационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий, радикального повышения эффективности государственного управления.

Использование существующих технологий и возможностей автоматизации деятельности государственных органов и учреждений, налаживание системы межведомственного взаимодействия, электронного документооборота являются неотъемлемыми условиями повышения качества жизни граждан, реализации их конституционных прав, обеспечения эффективности и прозрачности государственного аппарата, устойчивости и конкурентоспособности экономики, интеграции Российской Федерации в глобальное информационное общество. И, как следствие, находясь на этапе своего становления, информационное законодательство нуждается в серьезной методологической «подпитке», разработке основ теории информационного права. На сегодняшний день действующие нормативные акты не представляют собой ту систему информационного законодательства, которая в полной мере обеспечивает регулирование складывающихся правоотношений в информационной среде.

Система действующих нормативных актов в современном цивилизованном государстве является весьма сложной вследствие как значительного числа органов, принимающих такие акты, так и множественности актов, издающихся правотворческими органами. Кроме того, система нормативных актов подвержена быстрым изменениям. Вновь принятые законы, акты Президента и иные источники права нередко вносят коррективы в действующие акты. Одни из них дополняются новыми предписаниями, другие изменяются, а третьи признаются утратившими силу полностью или частично [2].

Чтобы в массе действующих и изменяющихся источников российского права оперативно находить нужные нормы, государственные органы, предприятия, да и работники, имеющие дело с нормативными актами, вынуждены постоянно заниматься работой по приведению их в упорядоченную совокупность, систему. Подобного рода деятельность охватывается понятием систематизации нормативных актов.

Правотворчество не может остановиться на определенном этапе, а все время находится в

движении, развитии в силу динамизма социальных связей, возникновения новых потребностей общественной жизни, требующих правового регулирования. Постоянно меняющаяся правовая система, ее развитие и совершенствование, принятие новых нормативных актов, внесение в них изменений, отмена устаревших нормативных решений объективно обуславливают упорядочение всего комплекса действующих нормативных актов, их укрупнение, приведение в определенную научно обоснованную систему, издание разного рода сборников и собраний законодательства. Такая деятельность по приведению нормативных актов в единую, упорядоченную систему обычно называется систематизацией законодательства [3].

Систематизация используется прежде всего в качестве эффективного способа обеспечения права необходимой нормативной правовой информацией. Достаточно широко систематизация применяется в процессе правотворческой деятельности.

Целями систематизации законодательства в информационной сфере являются: создание стройной системы нормативных правовых актов, обладающей качествами полноты, доступности и удобства пользования нормативными правовыми актами, устранение устаревших и неэффективных норм права, разрешение юридических коллизий, ликвидация пробелов и обновление законодательства.

Сегодня есть полярные точки зрения относительно возможности кодификации информационного законодательства; в частности, утверждается, что кодификация как форма его систематизации несвоевременна или неактуальна, но именно в информационной сфере с учетом ее многоаспектности, глобальности имеются основания рассматривать этот вопрос, основываясь на анализе информационного законодательства. Это необходимо, так как ни консолидированный акт, ни инкорпорация не решат проблему систематизации законодательства в информационной сфере.

Тот факт, что информационное законодательство продолжает развиваться, не исключает возможности его кодификации. В настоящее время нельзя назвать ни одну отрасль права, которая бы не развивалась и не претерпевала изменений. И если несколько лет назад разработка Информационного кодекса была невозможна в силу неразработанности основных принципиальных положений, отсутствия как теоретической, так и нормативной базы, то сейчас положение изменилось. Мы имеем обширную правовую базу, содержащую как законодательные акты, так и подзаконные акты федерального уровня и уровня субъектов Российской Федерации, большой объем теоретических разработок. Систематизация законодательства необходима, во-первых, для дальнейшего развития законодательства. Анализ и обработка действующих нормативных актов, группировка правовых предписаний по определенной схеме, создание внутренне единой системы актов являются необходимыми условиями эффективности правотворческой деятельности, способствуют ликвидации пробелов, устарелостей и противоречий в действующем законодательстве. Во-вторых, систематизация законодательства нужна как эффективное средство расчистки накопившихся массивов нормативных актов, ревизии действующей правовой системы. В-третьих, она обеспечивает возможность хорошо ориентироваться в законодательстве, оперативно находить и правильно толковать все нужные нормы. Наконец, в-четвертых, систематизация является необходимой предпосылкой целенаправленного и эффективного правового просвещения и воспитания, научных исследований, обучения студентов. Государственный учет и систематизация законодательства, иначе говоря, необходимы для создания систем «навигации» на основе мониторинга нормативных правовых актов, а также обеспечения решения задач по предоставлению государственных информационных услуг и по организации межведомственного взаимодействия органов государственной власти и создания единого федерального регистра [4].

В юридической науке и практике принято выделять такие виды систематизации законодательства, как учет нормативных правовых актов, инкорпорация, консолидация и кодификация.

Учет осуществляется практически всеми государственными органами и юридическими лицами для удовлетворения собственных потребностей в правовой информации либо в коммерческих целях, для обеспечения правовой информацией иных субъектов. Данным видом деятельности систематизации нормативных актов занимается ФБУ НЦПИ при Министерстве юстиции. На сегодняшний день нашим учреждением ведется учет Федерального законодательства Российской Федерации. Основной задачей учета является сбор, хранение и поддержание в контрольном состоянии правовых актов, а также создание поисковой системы, обеспечивающей нахождение необходимой правовой информации в массиве актов, взятых на учет. Ведется

автоматизированный учет законодательства на базе применения современной компьютерной техники и новейших достижений информатики.

Сбор подлежащих учету актов осуществляется различными способами. Значительную часть можно получить из официально публикуемых сборников нормативных актов. Совокупность нормативных актов, взятых на учет, составляет информационный фонд, в котором нормативные акты хранятся в определенном порядке. В фонде, состоящем из нескольких сотен или тысяч актов, выделяются разделы. Внутри разделов акты размещаются в хронологическом порядке. Чтобы знать, какие нормативные акты действуют, какие в них внесены изменения и дополнения, в тексты актов, взятых на учет, заносятся сведения обо всех изменениях и дополнениях, иначе говоря, они поддерживаются в контрольном состоянии. Это необходимо для удобства пользования ими.

В прошлом столетии учет вели в соответствии с Приказом Министерства юстиции СССР «Положение о государственном учете нормативных актов СССР и Союзных республик». В настоящее время документ признан не действующим в соответствии с Приказом Министерства юстиции РФ от 19 февраля 2002 г. № 52.

На научный центр правовой информации ВНИИ советского законодательства возлагалась функция — оказание министерствам и ведомствам СССР методической помощи по вопросам государственного учета нормативных актов, учет нормативных актов СССР и союзных республик.

Необходимо отметить, что Министром юстиции СССР В.И. Теребиловым был подписан Приказ от 18.03.1977 г. № 3 «Об утверждении Положения о государственном учете нормативных актов СССР и союзных республик», который обязал Министерства юстиции союзных республик обеспечить своевременное, по мере выхода в свет, направление в Научный центр правовой информации при ВНИИ советского законодательства издаваемых томов собраний действующего законодательства союзных республик в двух экземплярах.

В тот период очень много работы проводилось на бумажных носителях, в том числе и в нашем научном центре.

Тогда же ввели и формы регистрационной карты, они были тоже на бумажных носителях. В дальнейшем эти карты были переведены в электронную форму для ведения базы данных с использованием новой автоматизированной программы.

Конечно, на сегодняшний день данная программа еще требует существенных доработок, но путем проб и ошибок мы осваиваем эту инновационную разработку.

В настоящее время, когда в сфере управления все шире применяется современная техника, в том числе и высокопроизводительные компьютеры, открываются большие возможности для создания автоматизированных информационно-поисковых систем. В отличие от систем с ручным поиском, автоматизированные поисковые системы позволяют значительно усовершенствовать поиск правовой информации и обеспечить наиболее полное удовлетворение потребности в ней государственных органов и юридических лиц.

В настоящее время в Государственно-правовом управлении Президента Российской Федерации создается единый эталонный банк данных правовой информации, включающий в себя, наряду с актами федеральных органов законодательной и исполнительной ветвей власти, нормативные акты всех субъектов Федерации.

Систематизация нормативных правовых актов в форме консолидации — это такой прием, когда множественность нормативных актов преодолевается путем их сведения в один укрупненный акт.

Еще несколько лет назад представлялось, что консолидация нормативных правовых актов позволит решить задачу систематизации законодательства. Новый укрупненный акт полностью заменяет вошедшие в него нормативные акты, поскольку заново принимается компетентным правотворческим органом и имеет собственные официальные реквизиты. Однако недостаток консолидации в том, что содержание правового регулирования общественных отношений не меняется, все нормативные установления ранее принятых актов объединяются в новом акте без изменений. Это представляется неприемлемым для информационно-телекоммуникационной сферы, в которой динамика правоотношений, нуждающихся в правовом регулировании, несравнима ни с какой другой. В связи с этим требования сегодняшнего дня при построении информационного общества и активное нормотворчество позволяют назвать в качестве наиболее эффективной формы систематизации законодательства кодификацию, направленную на систематизацию и коренную переработку действующего законодательства.

Следующая форма систематизации — это инкорпорация. Систематизация нормативных

правовых актов в форме инкорпорации выражается в подготовке и издании разного рода сборников (собраний) таких актов. Инкорпорация нормативных правовых актов связана с их учетом, поскольку базируется на определенном, максимально полном фонде соответствующих актов и поисковой системе, способной обеспечить нахождение всех необходимых актов, ибо первой задачей инкорпорации является подготовка перечня актов, из которых должен состоять подготавливаемый сборник.

Инкорпорация позволит исключить случаи дублирования регламентации одного и того же вопроса несколькими актами. Работа была бы проделана эффективней и оперативней, если бы «старые» акты были оцифрованы.

С каждым годом наблюдается активизация законотворческого процесса. Создаются сотни и тысячи новых нормативных актов, существенно меняющих характер и основные принципы правового регулирования. Поэтому если сейчас не заниматься упорядочением действующей нормативной базы, которая увеличивается весьма быстрыми темпами, в будущем возникнут большие трудности в нахождении и использовании действующих норм права, хаос и неразбериха в российском нормативном хозяйстве. Дело осложняется еще и тем, что сейчас, когда создается практически новая правовая система в Российской Федерации, нужно также срочно решить судьбу формально действующих нормативных актов России и их частей, которые полностью либо частично противоречат новым нормативным решениям или попросту безнадежно устарели. В связи с этим проводятся революционные преобразования правовой системы, отменяются целые нормативные блоки, регулирующие отживающие, подлежащие существенному реформированию отношения, когда по сути дела создается качественно новая общественно-экономическая система, объективно требующая обновленных законов. Так, в соответствии с распоряжением Президента Российской Федерации от 18 марта 2011 г. № 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» [5] был проведен ряд масштабных работ. В целях совершенствования правовой системы Российской Федерации необходимо координировать деятельность федеральных органов исполнительной власти и органов государственной власти субъектов Российской Федерации.

К сожалению, придется признать, что имеется большое число формально действующих, но фактически утративших силу нормативных правовых актов, многие предписания не приведены в соответствие с Конституцией Российской Федерации. Все это создает опасность правовой инфляции в стране и способствует правовому нигилизму в обществе. Возникла необходимость активно совершенствовать юридическую технику, устранять имеющиеся противоречия и дублирования, в том числе, за счет инкорпорации советской нормативно-правовой базы. Все это обеспечит в дальнейшем стабильность и системность российского права, в результате чего законодательство, несмотря на свое многообразие, станет более доступным для граждан.

В рамках инкорпорации рассматриваются только правовые акты, принятые в период с 1917 года по декабрь 1991 года. Министерство юстиции одновременно с работой над правовыми актами СССР и РСФСР, затрагивающими сферу деятельности юстиции, координирует деятельность по инкорпорации актов иных федеральных органов исполнительной власти. Россия получила «в наследство» от Советского Союза советскую правовую систему.

В качестве примеров приведу первые декреты советской власти (из фондов нормативных правовых актов): «О редактировании и печатании законодательных и правительственных актов», «Об обязанности газет печатать декреты и распоряжения органов Советской власти», от 14 сентября 1918 года «О введении Международной Метрической системы мер и весов». В некоторых частях эти документы устарели, но применяются в той части, которая не противоречит современному законодательству. Главное — проверить, возможно ли применение правового акта советской эпохи в современных условиях, не противоречит ли он Конституции Российской Федерации и действующему законодательству.

В качестве примера назову еще ряд интересных актов: от 23 декабря 1917 года «Изменения правописания и новые правила» газеты Временного Рабочего и Крестьянского Правительства, подписан Народным Комиссаром по просвещению А.В. Луначарским, от 17 октября 1918 года «О введении новой орфографии». На сегодняшний день есть акты, которые действуют: Декрет Всероссийского Центрального Исполнительного Комитета ст. 702 от 29 августа 1922 года «О печатании постановлений и рас-

поряжений местной власти в органах периодической печати», подписан Председателем Всероссийского Центрального Исполнительного Комитета М. Калининым. Также интересный документ: Постановление Центрального Исполнительного Комитета и Совета Народных Комисаров от 7 августа 1937 года № 104/1341 «О введении в действие Положения о переводном и простом векселе». Оно до сих пор является действующим: «В соответствии с международными обязательствами Российской Федерации, вытекающими из ее участия в Конвенции от 7 июня 1930 года, устанавливающей Единообразный закон о переводном и простом векселях, установить, что на территории Российской Федерации применяется Постановление Центрального Исполнительного Комитета и Совета Народных Комиссаров СССР» (11 марта 1997 года № 48-Федеральный Закон).

Последние годы характеризуются широким внедрением информационных технологий в сферу работы государственного аппарата и предоставления государственных услуг в электронном виде. Согласно Федеральному закону от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [6], «обязанность государства перед гражданами — предоставление государственных и муниципальных услуг в электронной форме».

Последние решения Правительства РФ и Совета при Президенте РФ по развитию информационного общества в Российской Федерации направлены на внедрение электронного документооборота во всех федеральных органах. В связи с этим перед архивистами также встают глобальные задачи. Началась большая работа по оцифровке материалов, что приведет к сокращению доли бумажных документов и повышению удобства их использования. Эта работа предусмотрена Стратегией развития информационного общества. Колоссальный объем архивной информации предопределил создание Национального электронного архива законодательства России. Создание этого электронного архива — задача огромного культурного, научного и практического значения. Она имеет целью предоставить неограниченному кругу пользователей (политикам, ученым, государственным служащим, аспирантам, студентам) весь массив законодательства России, от первых кодексов до актов действующего законодательства, принятых в последние годы. Национальный архив может быть использован для изучения истории правового регулирования, сравнительных правовых исследований, кодификации законодательства и проработки различных версий правовой реформы. Имеющиеся в нашей стране правовые базы данных содержат не более 20% необходимой информации о правовых актах. Большое значение для научных исследований имеет и фонд правовых актов, признанных утратившими силу. Актуальным является вопрос кодификации и систематизации законодательства, подготовки свода законов. Эту работу всегда осуществляло Министерство юстиции с участием научных учреждений.

Одним из примеров было обращение Минкультуры с просьбой представить перечень утративших силу правовых актов в сфере культуры за период с 1917 по 1927 г.

В соответствии с запросом Минкультуры России НЦПИ при Минюсте России в адрес Департамента законопроектной деятельности и мониторинга правоприменения была направлена информация о действии нормативных правовых актов в сфере культуры за период 1917-1922 гг.

На основании сведений, представленных НЦПИ при Минюсте России, Минкультуры России был подготовлен и внесен в Правительство Российской Федерации проект постановления Правительства «О признании недействующими на территории Российской Федерации некоторых нормативных правовых актов Российской Советской Федеративной Социалистической Республики».

В настоящее время прослеживается следующая проблематика: систематизированный фонд правовых актов РСФСР, СССР и Российской Федерации с 1917 г., а также источников опубликования, поддерживаемых в актуальном состоянии более 80 лет, представляющий собой уникальный массив государственных информационных ресурсов, не велся уже много лет. Вопрос о доступной форме правовых актов также приобретает особую актуальность в связи с ориентацией на предоставление информации посредством применения информационных систем общего пользования и сети Интернет, поскольку далеко не все граждане имеют возможность реализовать свое право на доступ к информации другим способом.

Федеральным законом «Об информации, информационных технологиях и о защите информации» установлено, что запрещено относить к информации с ограниченным доступом документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объ-

единений, организаций, которые представляют общественный интерес или необходимы для реализации прав, свобод и обязанностей граждан.

Как было сказано ранее, для научных исследований, подготовки предложений о совершенствовании законодательства и повышения эффективности его применения, необходим анализ всех действующих, официально не отмененных нормативных актов (федеральных законов, нормативных указов Президента Российской Федерации, постановлений Правительства Российской Федерации, иных нормативных актов, а также актов Союза ССР, продолжающих действовать на территории Российской Федерации). В соответствии с Программой совместных мероприятий по реализации Соглашения между Российской правовой академией (РПА) и Научным центром правовой информации, лабораторией мониторинга правовой информации НИИ РПА в настоящее время проводится правовой анализ архивного фонда правовых актов Минюста России, находящихся в НЦПИ, и силами студентов Академии осуществляется методологическая обработка архива и ввод правовых актов в базу данных через выделенный НЦПИ компьютер. Перевод текстов нормативных правовых актов фондов Министерства юстиции СССР и Министерства юстиции РСФСР в электронно-цифровую форму обеспечит доступность этой уникальной правовой информации, в том числе и через Интернет. Устранение проблемных вопросов требует значительных ресурсов, скоординированного проведения организационных мероприятий Минюста России и НЦПИ, а также РПА. В связи с этим Российской правовой академией совместно с Научным центром правовой информации разработан учебно-методический комплекс по программе повышения квалификации специалистов территориальных органов Минюста России и служащих муниципальных образований.

Следует отметить актуальность вопросов, затронутых в Постановлении Правительства «Мониторинг правоприменения». Это дает возможность оценить положения действующего законодательства в актуальном состоянии, ознакомиться с официальными и неофициальными толкованиями права, быть в курсе законопроектной деятельности государственных органов и общественного обсуждения проектов нормативных правовых актов, а также выявить пробелы отечественного законодательства и сформулировать предложения по его совершенствованию.

Задачей правового мониторинга является реализация одного из приоритетных направлений государственной политики — повышения качества и эффективности законодательства как важного фактора развития государства.

Целями организации системы правового мониторинга являются:

- систематическое получение информации о состоянии действующего законодательства и его систематизация; упрядочение законотворческой деятельности;
- определение эффективности правового регулирования, причин и пробелов в правоприменительной практике на основе изучения правоприменительной практики;
- выявление соответствия законодательства планируемому результату правового регулирования и выработке мер по его совершенствованию.

Принимая во внимание актуальность поставленных задач, необходимо продолжить поиск путей решения, уделяя внимание вопросам перехода к электронному документообороту в органах государственной власти. Внедрение электронного документооборота и архива, в том числе, позволит осуществить:

- перевод в цифровой формат материалов, хранящихся в архивах Российской Федерации,
- создание порталов государственных услуг,
- создание и поддержание Интернет-порталов на базе архивных материалов Гостелерадиофонда,
- создание и развитие единого российского Интернет-портала, содержащего исчерпывающую информацию о российских библиотеках, архивах и музеях, благодаря которому облегчается доступ Интернет-пользователей к информации в сфере культуры России,

а также

- создание общероссийской архивно-информационной системы
- сделает возможным перехода к единому информационному пространству.

Россия до сих пор не имеет единого национального архива законодательства. Сведения о принятых и действующих нормативных правовых актах распылены по 14 федеральным архивам, десяткам тысяч опубликованных и неопубликованных источников. Создание Национального архива станет важным стимулом и даст толчок развитию аналогичных работ на региональном уровне (архивы регионального законодательства).

24 апреля 2013 года в РИА Новости прошла пресс-конференция, посвященная оцифровке документов одного из фондов Российского

государственного архива древних актов (РГАДА). Как сообщил журналистам заместитель руководителя Росархива О.В. Наумов, конкурс на проведение этих работ выиграла корпорация ЭЛАР. За два года предстоит оцифровать свыше 5 млн. листов, создать электронную опись фонда. Директор РГАДА М.Р. Рыженков рассказал об истории документов фонда, являющегося по сути фискальным памятником. По своему содержанию это добротный источник для изучения различных аспектов социальной истории, а также генеалогии. В последние десятилетия из-за всплеска интереса населения к своим корням документы этого фонда крайне востребованы, что стало угрожать их физической сохранности [7].

Необходима тщательная проработка всех вопросов и в самые сжатые сроки. В противном случае мы рискуем утерять целые пласты документов и отечественная история начала XXI в. останется белым пятном для последующих поколений.

Литература

1. Распоряжение Правительства Российской Федерации от 20.10. 2010 № 1815-р. «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)» // СЗ РФ. — 2010. — № 46. — Ст. 6026.
2. Сырых В.М. Теория государства и права. Юридический Дом «Юстицинформ». Москва — 2001.
3. Сырых В.М. Теория государства и права. Юридический Дом «Юстицинформ». Москва — 2001.
4. Пиголкин А.С. Систематизация законодательства в Российской Федерации. Издательство Юридический центр Пресс Санкт — Петербург. — 2003.
5. Распоряжение Президента Российской Федерации от 18 марта 2011г. № 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» // СЗ РФ. —2011.— № 12. — Ст. 1627.
6. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ.— 2010.— № 31.— Ст. 4179.
7. Богомолова Н.Г. Информация и хроника. «В РГАДА создается цифровой банк генеалогических документов» // Научно-практический журнал «Отечественные архивы» 2013. № 3 С. 133.

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

Сухотин Сергей Олегович

Повышение квалификации специалистов территориальных органов юстиции с использованием инструментов электронного обучения

Аннотация: *Статья содержит описание создания специализированных курсов электронного обучения для повышения квалификации специалистов территориальных органов юстиции и муниципальных образований.*

Ключевые слова: *рекомендации, совершенствование, электронное обучение, обучение, повышение квалификации, образовательные, технологии, нормы, развитие, образование, наука, дистанционные образовательные технологии, государственная служба, муниципальная служба.*

В формирующемся едином образовательном пространстве наблюдается возрастание спроса на подготовку специалистов, владеющих вопросами юриспруденции в сочетании с компьютерными технологиями, изменение взгляда на содержание и способы преподавания. Это привело к появлению новых программ подготовки с использованием инновационных форм образования, к числу которых, безусловно, относится дистанционное обучение (ДО).

При непосредственном участии автора создан портал дистанционного обучения муниципальных служащих «Ведение Федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации», который доступен в сети Интернет по адресу: http://elearning.scli.ru/ .

Программа курса посвящена изучению основ современных информационных технологий и методов ведения Федерального регистра муниципальных нормативных правовых актов.

В учебном курсе представлены общие вопросы организации и содержания работы по ведению Федерального регистра и регистров (сбор и ввод информации в регистр; хранение информации в регистре; ведение классификаторов, словарей и справочников регистра; доступ к информации, информационная безопасность), а также проведения правовой экспертизы муниципальных актов, поддержания их текстов в актуальном состоянии и проведения мониторинга правовой системы муниципальных образований по вопросам ведения соответствующих регистров.

Дистанционный образовательный курс предполагает выполнение слушателями практических заданий по работе в информационно-телекоммуникационной сети. Помимо этого, слушатели получают навыки оптимизированного поиска правовой информации с помощью электронной справочной правовой системы «Эталон». Слушатели осуществляют поиск актуальной правовой информации в федеральном регистре нормативных правовых актов Российской Федерации, представленном в Интернете по адресу http://zakon.scli.ru . Дополнительно в курсе представлены коммуникативные опции: переписка-чат по электронной почте; дискуссионные телемосты и Интернет-конференции; оптимизированный поиск коллег в корпоративной сети; выработка навыков этичного поведения в сети Интернет при переписке и коммуникации.

В данном курсе дистанционного обучения применяются следующие инновационные технологии:

- Работа с гипертекстом. Обучающемуся предстоит изучить текстовый материал по курсу, выполненный в виде гипертекстовых WWW-страничек. Напомним, что гипертекст – это текст со вставленными в него словами (командами) разметки, ссылающимися на другие ме-

ста этого текста, другие документы, изображения и т.д. Если во время чтения такого текста обучающийся увидит выделенное слово, то, наведя на него курсор, надо нажать клавишу мыши. На экране появится текст (другой кусок данного текста или вообще другой документ), на который ссылалось это слово.

- Дискуссии в сети. При выполнении заданий обучающемуся может быть предложено обсудить тот или иной вопрос с участниками данного курса дистанционного обучения. Модератором (т.е. ведущим) дискуссий в сети будет ваш координатор (НЦПИ), в дальнейшем эту роль сможет сыграть каждый из вас.
- Работа в электронной библиотеке. Для того чтобы обучающийся досконально разобрался с новыми информационными технологиями, авторы данного курса советуют обратиться к дополнительным материалам, представленным в «Библиотеке». Предполагается, что, изучив список материалов в «Библиотеке», обучающийся найдет нужную информацию.

Особенность дистанционных курсов заключается в трансграничной передаче информации между регионами России. Преподаватель из Москвы может, не выходя из кабинета, прочесть лекцию для слушателей из Калининграда. Для входа следует запустить браузер и в адресной строке ввести: http://elearning.scli.ru/ (учебный сервер). После этого загрузится главная страница системы.

Для дальнейшей работы с системой необходимо пройти авторизацию. Чтобы войти в систему (авторизоваться), требуется ввести Ваши персональные данные на главной странице системы в левой части экрана. После успешной авторизации происходит переход к персональной главной странице ДО. Открывается окно, где в центре экрана станет доступным список курсов, на которые зачислен обучающийся.

Темы, доступные в курсе, открываются путем однократного нажатия на активную ссылку. Например, Вы выбрали тему: «Руководство пользователя АРМ «Муниципал»; нажав на название этой темы, Вы будете перемещены на страницу, где изложен материал обучения. В системе дистанционного обучения предусмотрен отдельный модуль для общения с преподавателем дистанционных курсов, для этого Вам потребуется перейти по ссылке http://elearning.scli.ru:5080/openmeetings/. Вы попадете на страницу с формой входа в модуль для проведения онлайн-лекций.

После выбора комнаты обучающемуся предложат провести тест на проверку оборудования. Тест поможет понять, подходит ли выбранное оборудование для онлайн-конференции.

После проверки оборудования обучающийся попадает на страницу конференции. Здесь будет предложено выбрать оборудование для использования во время онлайн-конференции.

На странице конференции доступны следующие возможности:

- В левой части экрана можно увидеть список участников;
- В нижней части находится чат для общения между участниками;
- В верхней части находится панель инструментов для работы с доской;
- Доступны окна для наблюдения за другими участниками.

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

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

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

Маркин Михаил Николаевич

Проблемы ограничения распространения информации в сети Интернет

Аннотация: *Предлагается отмена судебного запрета на распространение информации в сети Интернет в силу фактической неисполнимости такого запрета. Исследуется зарубежный опыт ограничения распространения информации в сети Интернет.*

Ключевые слова: *интернет-цензура, распространение информации, проект «Золотой Щит».*

В последнее время все больше правоведов озабочены появлением и развитием в России так называемой «интернет-цензуры», то есть внедрением комплекса технических средств и мер, направленных на ограничение доступа пользователей российского сегмента сети Интернет к информации.

Так, еще в 2007 году Федеральным законом «О противодействии экстремистской деятельности» № 114-ФЗ от 25 июля 2002 года на Федеральную регистрационную службу (ныне — на Министерство юстиции РФ) была возложена обязанность ведения списка экстремистских материалов, доступ к которым запрещен на всей территории Российской Федерации. Признание материалов (то есть любых сведений, вне зависимости от способа их представления) экстремистскими осуществляется судом. Запрет на распространение подобных сведений устанавливается в ст. 13 Федерального закона «О противодействии экстремистской деятельности». При этом Кодексом об административных правонарушениях предусмотрена ответственность за массовое распространение экстремистских материалов, внесенных в вышеуказанный список (ст. 20.29 КоАП РФ).

В настоящее время список пополняется и на момент написания этой статьи (7 ноября 2012 года) содержит 1480 записей [1]. Список содержит указание на материалы, как размещенные в сети Интернет, так и на материальных (в том числе бумажных) носителях. Надо сказать, что список сам по себе выполняет не только функцию изобличения уже созданных (и распространенных) материалов, но выступает также и критерием «законности» вновь создаваемых информационных материалов.

То есть, механическое копирование текста документа, признанного экстремистским материалом и внесенного в список, будет образовывать (с точки зрения прокурора как лица, уполномоченного возбуждать дела об административных правонарушениях по ст. 20.29 КоАП РФ) объективную сторону административного правонарушения. При этом в списке, как правило, указывается название конкретного документа (или литературного, музыкального произведения) и автор этого документа. Однако в списке можно встретить и пункты довольно неопределенного содержания, например, пункт № 600.

В пункте под номером 600 экстремистским материалом признан CD-диск бело-желтого цвета с названием «РОНС Русский общенациональный союз» и с надписью «информационный медиа-журнал, выпуск № 2» (решение Ленинского районного суда г. Владимира от 15.03.2010).

Синтаксическая конструкция этого пункта позволяет определить каждый CD-диск бело-желтого цвета, существующий в мире, как

экстремистский материал, если на этот диск нанесена надпись «информационный медиа-журнал, выпуск № 2» и название «РОНС Русский общенациональный союз». При этом на самом диске может не быть никакой информации вообще. В таком случае, что же является собственно экстремистским материалом — оптический диск определенного цвета, надпись на диске или все-таки информация, содержащаяся на нем и считываемая с этого диска приводом компьютера? О содержимом этого диска в пункте № 600 не сказано ни слова. Чтобы узнать содержимое диска, придется отправляться в архив Ленинского районного суда города Владимира и знакомится с материалами дела, по которому вынесено такое решение.

Таким образом, пункт № 600 списка не несет сам по себе ни смысловой, ни юридической нагрузки. В то же время, если взглянуть на диспозицию статьи 20.29 КоАП РФ, мы можем предположить, что возбуждение дела об административном правонарушении происходит по формальным основаниям (внешним признакам правонарушения), а именно, сам факт массового распространения экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, уже является поводом к возбуждению дела.

Пункт № 600 и сотни подобных ему пунктов в Списке создают неопределенность повода для возбуждения дела об административном правонарушении, а в некоторых случаях и уголовного дела по статье 282 УК РФ.

Кроме того, изучение Списка позволяет сделать вывод о том, что решение суда о признании материала экстремистским и о запрете доступа к такому материалу необязательно для исполнения сотрудниками органов исполнительной власти.

Так, например, в пункте № 985 Списка утверждается, что Сайт «Кавказ-Центр» (www.kavkazcenter.com), его зеркала: kavkaz.tv, kavkaznews.com, kavkaz.org.uk, kavkazcenter.com, kavkazcenter.net, kavkazcenter.info, признаны решением Никулинского районного суда г. Москвы от 12.09.2011 экстремистским материалом. При этом предполагается, что доступ к указанному сайту должен быть запрещен на всей территории Российской Федерации. То есть ни один человек, использующий доступ в Интернет в России, не должен попадать на этот сайт.

Из решения Никулинского районного суда г. Москвы от 12.09.2011 можно сделать вывод о том, что весь Сайт «Кавказ-Центр», все существующие на нем материалы и все вновь появляющиеся являются экстремистскими.

Однако под номером 1063 в списке указывается статья «Идель-Урал. Воззвание к мусульманам Идель-Урала», расположенная по электронному адресу информационно-телекоммуникационной сети Интернет http://kavkazcenter.com/russ/content/2011/01/09/78000.shtml и включенная в список по решению Кировского районного суда г. Уфы от 17.11.2011.

Мы видим, что как минимум с момента вынесения решения Никулинского районного суда г. Москвы от 12.09.2011 года до момента вынесения решения Кировского районного суда г. Уфы от 17.11.2011 доступ к сайту «Кавказ-Центр» не был полностью закрыт на всей территории Российской Федерации для всех людей, находящихся на этой территории. В противном случае, суд не смог бы узнать о наличии на указанном сайте статьи «Идель-Урал. Воззвание к мусульманам Идель-Урала». Кроме того, остался невыясненным мотив, по которому Кировский районный суд г. Уфы решил особо выделить одну статью на уже признанном экстремистским сайте.

Бесполезность, если не бессмысленность ведения списка экстремистских материалов в том формате, в котором он ведется, обнаруживается в пункте № 1254.

Ниже приведем его полностью (орфография и пунктуация сохранена).

«1254. Видеоролик «Русский очнись! Против тебя идет война», размещенный 26.02.2010 г. Евглевским А.С. на интернет-сайте социальной сети «Вконтакте», имеющий электронный адрес http://vkontakte.ru (решение Промышленного районного суда города Курска от 22.03.2012)».

Как видно из этого пункта Списка, весь сайт «Вконтакте», расположенный по адресу http://vkontakte.ru должен быть признан экстремистским материалом, так как адрес конкретного видеоролика на сайте социальной сети имеет вид: «http://vkontakte.tu/video_ext.php <...> =1».

В данном же пункте указан лишь общий адрес сайта, что говорит о невозможности идентифицировать конкретный видеоролик и конкретного автора этого ролика.

С 1 ноября 2012 года введен в эксплуатацию «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети „Интернет“ и сетевых адресов, позволяющих идентифицировать сай-

ты в информационно-телекоммуникационной сети „Интернет“, содержащие информацию, распространение которой в Российской Федерации запрещено», в соответствии с требованиями ст. 151 Федерального закона «Об информации, информационных технологиях и о защите информации».

В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети Интернет, содержащих информацию, распространение которой в Российской Федерации запрещено;
2) сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

Создание и ведение реестра осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в соответствии с Постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101.

Основаниями для включения в реестр сведений об информации, распространение которой в Российской Федерации запрещено, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет»:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призыва к совершению самоубийства;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

Следует отметить, что все вышеуказанные ограничения, установленные Федеральным законом об информации, и комплекс технических мер, предпринятых органами государственной власти с целью ограничения доступа к информации, распространение которой запрещено, вызвали довольно бурную реакцию общественности. Федеральный закон № 139-ФЗ от 28 июля 2012 года (в прошлом Законопроект № 89417-6) — Федеральный закон Российской Федерации «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет», внесший изменения в том числе и в Федеральный закон «Об информации, информационных технологиях и о защите информации» (статья 151), породил волну протеста русскоязычных пользователей Всемирной сети.

10 июля 2012 года на одни сутки была прекращена работа русскоязычного раздела сайта «Википедия», по решению, принятому на голосовании большинством ее сообщества, путем сокрытия содержимого всех страниц, а также размещение на главной странице проекта информационного баннера в течение следующего дня (11 июля), в знак протеста против рассматривавшихся в Государственной думе России поправок к закону «О защите детей от информации, причиняющей вред их здоровью и развитию», а также для привлечения внимания к законопроекту № 89417-6.

Стоит ли говорить о мгновенно появившихся бесчисленных публикациях о введении «цензуры» в сети Интернет?

Вместе с тем, когда все изменения, касающиеся так называемой «цензуры» вступили в силу, пришло время понять — действительно ли ограничивают предпринятые государством меры доступ к «запрещенной информации»?

Ответ один — фактически никаких (!) ограничений на распространение какой бы то ни было информации в сети Интернет до сих пор нет, и никаким законом эти ограничения реально не введены. То есть все принятые в 2002-2012 годах законы в области ограничения доступа к информации, размещенной во Всемирной сети, никак отношения между распространителями и пользователями информации не изменили. Это тезис.

Поскольку каждый тезис должен быть доказан, то докажем и последний.

Коль скоро государство в законах провозглашает запрет на распространение той или иной информации, оно должно этот запрет обеспечить. И обеспечить не только карательными мерами (мерами административной и уголовной ответственности), но и мерами превентивными.

Одной из главных превентивных мер является ведение списков запрещенных к распространению в сети Интернет материалов и предписание организациям, предоставляющим доступ в Интернет, блокировать доступ пользователей к «запрещенной» информации. При этом блокируется доступ со всех IP-адресов [2] пользователей к конкретным сайтам, указанным в Федеральном списке экстремистских материалов и Едином реестре доменных имен и сайтов с информацией, распространение которой в Российской Федерации запрещено. Однако сама информация или сайт, доступ к которому ограничен, не блокируется и не удаляется.

В сети Интернет существуют так называемые «сайты-анонимайзеры» (www.anonymouse.org и др.); с их помощью сам пользователь сети Интернет может изменить свой IP-адрес случайным образом. Используя измененный IP-адрес, пользователь перестает быть связанным какимлибо ограничениями своего провайдера (то есть организации, предоставившей ему доступ в Интернет). Следовательно, пользователь с таким измененным адресом может получить доступ к любой информации на любом находящемся в сети Интернет сайте.

Таким образом, любой пользователь с помощью «сайта-анонимайзера» может преодолеть защитные или запретительные меры, предпринимаемые всевозможными органами государственной власти и организациями. Простейшая для пользователя методика преодоления разного рода запретов и «цензуры» демонстрирует бессмысленность и неэффективность предпринимаемых мер. Кроме того, ни один закон не ограничивает и не запрещает пользователю получать доступ к сайтам с «запрещенной» информацией. Тезис, обозначенный выше, доказан — реально доступ к информации ничем не ограничен. Законы в области ограничения доступа к информации, размещенной в сети Интернет, лежат вне права, так как реально не влияют и не могут повлиять на взаимоотношения между распространителем информации и конечным ее потребителем, разве что немного усложняют доступ к некоторой информации, так как приходится изыскивать новые способы доступа к ней. Кроме того, информация на многих сайтах, особенно в социальных сетях (Facebook, «Вконтакте» и т.п.) не проходит предварительного контроля при размещении — «премодерации», а значит, может быть удалена администраторами таких сайтов только в порядке реагирования на запросы органов государственной власти, при этом сам факт размещения и нахождения такой информации в открытом доступе хотя бы несколько часов уже предполагает, что некоторые пользователи получили доступ к этой информации, сохранили ее на своих материальных носителях и могут впоследствии распространить эту информацию любым другим способом.

Из всего вышесказанного можно сделать следующий вывод: на сегодняшний день в России нет сколько-нибудь эффективной «цензуры» в сети Интернет.

В заключении встает вопрос — а нужен ли вообще контроль способов распространения информации, и если нужен, как он должен осуществляться?

Опыт зарубежных стран показывает, что самая эффективная система контроля способов распространения информации в сети Интернет создана в Китайской Народной Республике.

Проект «Золотой щит» в Китае — это обширная сеть цензуры в национальном масштабе. Она блокирует вход информации в Китай и выход информации за пределы Китая, а также контролирует движение информации внутри страны.

В 1998 году министерство общественной безопасности Китая начало проект под названием “Golden Shield Project”. В средствах всенародного оповещения он больше известен как “The Great Firewall of China” (игра слов, в значении как «сетевой фильтр», так и древняя «Великая Китайская стена»). Его основной целью является цензура и контроль всей активности пользователей сети Интернет в Китае.

Основным шагом стало создание Национального криминалистического информационного центра (1994), который позже стал частью проекта «Золотой щит». В 1998 году правительство заявило, что для получения доступа к Интернету всей нации должны быть установлены определенные правила. Позже, в том же году, министр общественной безопасности КНР представил документ, в котором говорилось о том, что Коммунистическая Партия Китая должна иметь возможность контролировать информацию, которую получает население. После глубоких исследований и проведения ряда встреч с органами общественной безопасности мини-

стром общественной безопасности было принято решение об осуществлении проекта, направленного на обеспечение общественной безопасности информационных технологий. Проекту дали название "Golden Shield Project" («Проект «Золотой щит»).

После долгой разработки соответствующих технологий, в сентябре 2003 года проект начал свою работу.

Согласно нормам китайского законодательства, сайты, размещенные на вычислительных мощностях, находящихся на территории Китая, не могут публиковать новости, взятые с зарубежных новостных сайтов, без специального одобрения. Существует список новостных сайтов, которые имеют разрешение публиковать новости в Интернете. Все другие сайты могут предоставлять только ту информацию, которая уже обнародована уполномоченным средством всенародного оповещения. Они также должны получить одобрение со стороны информационного агентства Государственного Совета и несут ответственность за законность распространения информации. Каждая организация, предоставляющая доступ в сеть Интернет, «должна сохранять копии записей в течение 60 дней» и быть готовой предоставить эту информацию для органов государственной власти по первому требованию. Организации, предоставляющие доступ в Интернет, также обязаны ограничивать информацию, которую они публикуют. Несоблюдение любого из вышеупомянутых требований приводит к блокированию доступа к сайту.

Итак, столь эффективная система ограничения доступа к сети Интернет не может быть внедрена и использована российскими органами власти, поскольку статья 29 Конституции Российской Федерации запрещает цензуру и гарантирует свободу средств массовой информации. Проект «Золотой щит» представляет собой не что иное, как цензуру китайского сегмента всемирной сети.

В то же время органы государственной власти стран Европейского союза и США не видят необходимости в законодательном ограничении способов распространения информации в сети Интернет, так как сами провайдеры и организации, предоставляющие хостинг [3], осуществляют контроль распространяемой информации. На государственном уровне принимается лишь ряд законов, ограничивающих распространение той или иной информации или предписывающих вообще не распространять ее. Органы государственной власти этих стран не занимаются исследованием разных видов средств всенародного оповещения с целью выявить вредную информацию или ограничить к ней доступ. Ограничение распространения отдельных видов информации в зарубежных странах установлено по ее содержанию (порнография, сведения, разжигающие межнациональную рознь и т.д.).

Из настоящего исследования автор делает вывод, что Федеральный закон № 139-ФЗ от 28 июля 2012 года [4] и нормы статьи 13 Федерального закона № 114-ФЗ от 25 июля 2002 года [5] избыточны. Ряд давно существующих законов ограничивает распространение информации по ее содержанию, а способ распространения не заслуживает особого внимания, так как все способы распространения информации перечислить невозможно, да и вряд ли нужно.

Литература

1. Сайт Министерства юстиции Российской Федерации. Федеральный список экстремистских материалов // эл. адрес: http://minjust.ru/ru/extremist-materials.
2. IP-адрес — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP. Травин А. Толковый словарь интернет-терминов / М.: 2010.
3. От англ. hosting — услуга по предоставлению вычислительных мощностей для физического размещения информации на сервере, постоянно находящемся в сети. Мюллер В. К. Англо-русский словарь / изд-во: Оникс, 2007г.
4. Федеральный закон «О противодействии экстремистской деятельности» № 114-ФЗ от 25 июля 2002 года // «Российская газета», N 138-139, 30.07.2002;
5. Федеральный закон № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет» // «Российская газета — Федеральный выпуск» № 5845 от 30 июля 2012 года.

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

Крутикова Дарья Ильинична

Сравнительно-правовой анализ понятий «банковская тайна» и «персональные данные» в рамках вопроса охраны информации о клиентах банка

Аннотация: *рассмотрены определения понятия банковской тайны, а также персональных данных клиента, оказывающих важнейшее влияние на то, каким будет режим конфиденциальности информации о клиенте, получаемой банками в процессе осуществления их деятельности, и предоставлении этой информации третьим лицам.*

Ключевые слова: *банковская тайна, персональные данные, банковская деятельность, охрана информации, клиент банка*

В нашем исследовании важное место занимает понятие «тайна». Начнем с того, что постараемся дать толкование этому понятию. В общем виде «тайна» — это особый правовой режим информации, предполагающий ограниченный доступ к ней.

Существует множество видов тайн, упомянутых в различных законодательных актах. Упомянем лишь основные их виды: государственная, коммерческая (производственная, научно-техническая, финансово-экономическая, технологическая), профессиональная, служебная, банковская, следствия и судопроизводства, связи, персональные данные, врачебная, нотариальная, адвокатская, аудиторская, страховая, налоговая, частной жизни, переписки и др. Какие-то из них имеют более широкое толкование, другие имеют подвиды, третьи частично пересекаются друг с другом и т.д.

Предметом нашего исследования в первую очередь является банковская тайна, а также тесно связанные с нею персональные данные. Вопрос правового регулирования института банковской тайны всегда занимал одно из значительных мест в юридической литературе.

Понимание того, что включается в понятие банковской тайны, а также персональных данных клиента, является принципиально важным моментом, оказывающим влияние на то, каким образом будет применяться режим конфиденциальности информации о клиенте, получаемой банками в процессе осуществления их деятельности. В зависимости от того, к чему относятся те или иные сведения о клиенте, устанавливается определенный режим конфиденциальности данной информации.

На данный момент существует несколько точек зрения по рассматриваемым проблемам, которые будут представлены ниже.

Нет единства мнений относительно принадлежности банковской тайны к какому-либо виду конфиденциальной информации. Банковская тайна зачастую рассматривается и как разновидность служебной тайны, и как подвид коммерческой тайны, связанной с профессиональной деятельностью банка.

Законодательное понятие банковской тайны отсутствует, но оно может быть выведено из ст. 857 ГК РФ [1] и ст. 26 Закона РФ «О банках и банковской деятельности» (далее — Закон о банках) [2].

При этом необходимо отметить, что по сравнению с ГК РФ ст. 26 Закона о банках предполагает более широкое понимание банковской тайны с точки зрения перечня сведений, ее составляющих, и субъектов, обязанных ее охранять. Некоторое противоречие норм указанных

статей должно разрешаться в пользу Закона о банках как специального нормативного акта, регулирующего банковскую деятельность.

Исходя из этого, можно полагать, что информацией, составляющей банковскую тайну, являются сведения об операциях, счетах и вкладах клиентов и корреспондентов, а также иные сведения о клиентах и корреспондентах, установленные кредитной организацией в процессе осуществления ее деятельности [3].

Интерес к банковской тайне в последнее десятилетие не случаен. С одной стороны, банковская тайна — это принцип деятельности любого банка. С другой стороны, доступ к информации, составляющей банковскую тайну, позволяет государству решать многие публичные задачи, одной из основных среди них является контроль за своими гражданами.

По общему правилу клиенты банков, будь то юридические лица или граждане, не хотят, чтобы кто-либо знал об их капиталах, а также о движении денежных средств по их счету. Однако как государство, так и международные контрольные органы стремятся получить такую информацию. Банковская тайна служит тем инструментом, который призван найти компромисс между названными интересами. Для достижения такого компромисса законодатель должен, во-первых, четко определить, что представляет собой банковская тайна, во-вторых, регламентировать порядок и случаи ее предоставления, а также указать органы, которые вправе получать такую информацию. Однако сегодня ни в науке, ни в законодательстве нет единообразного понимания банковской тайны. Причин тому несколько. Прежде всего это серьезные противоречия в законодательстве, которые позволяют достаточно вольно трактовать банковскую тайну. Во-вторых, неоднозначное соотношение банковской тайны с другими видами тайны, в том числе с коммерческой тайной. В-третьих, изменение подходов к банковской тайне и ее защите в последние десятилетия.

Таким образом, исходя из анализа действующего законодательства, можно предложить и такое определение банковской тайны.

Банковская тайна — это защищаемые банками и иными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить их право на неприкосновенность частной жизни.

Основными объектами банковской тайны выступают: а) тайна банковского счета; б) тайна операций по банковскому счету; в) тайна банковского вклада; г) тайна частной жизни клиента или корреспондента.

Нарушение банковской тайны состоит в раскрытии соответствующей информации (части информации) без согласия управомоченного лица (клиента, корреспондента) или в использовании ее банковским служащим в своих интересах, если такие действия могут причинить моральный или материальный вред.

Сегодня нет единообразия в понимании банковской тайны и на уровне разных государств. Отличия в подходах зависят прежде всего от того, допускается ли и при каких условиях раскрытие информации, составляющей банковскую тайну, третьим лицам.

Международное законодательство стремится к унификации законодательных норм о раскрытии банковской тайны.

Россия, исходя из принятого и действующего законодательства, ориентируется на самую либеральную по отношению к банковской тайне страну — Соединенные Штаты Америки. В США законодательство обязывает банки предоставлять любую информацию о вкладчиках, которыми заинтересовались правоохранительные органы, при наличии официального запроса властей.

Сегодня принято выделять три основные, официальные причины отмирания банковской тайны. Во-первых, борьба с теневыми деньгами, во-вторых, финансирование терроризма, в-третьих, налоговые преступления. В действительности имеется и еще одна, скрытая, причина. Речь идет о стремлении государства контролировать доходы своих граждан и юридических лиц, а также любое движение денежных средств.

Подавляющее большинство экспертов считают, что банковская тайна переродится в ближайшее время в защиту банковской информации от несанкционированного доступа. При этом любые государственные органы в конечном итоге получат право доступа к банковским счетам юридических и физических лиц во всем мире [4].

При этом актуальным можно считать то, чтобы полученная соответствующими фискальными, контролирующими и иными уполномоченными органами информация не получила распространения среди третьих лиц, которым такая информация необходима для целей, не совпадающих с законными.

Экономический кризис обозначил новый виток нарушений основных принципов частной жизни, связанных с неприкосновенностью личной жизни физического лица. При этом данные нарушения прав человека проявились в различных сферах деятельности. В таких областях, как банковская деятельность, нарушения принципов частной жизни не только являются угрозой для каждого отдельного клиента банка, но и подвергают опасности устойчивость всей банковской системы, зависящей во многом от доверия клиентов к кредитным организациям.

Таким образом, для кредитной организации правовой режим банковской тайны дополняется правовым режимом персональных данных на основании ст. 26 Закона о банках. В данной статье предусмотрено, что справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, органам принудительного исполнения судебных актов, актов других органов и должностных лиц, организации, осуществляющей функции по обязательному страхованию вкладов, при наступлении страховых случаев, органам предварительного следствия. Кроме того, ст. 857 ГК РФ устанавливает, что сведения, составляющие банковскую тайну, предоставляются самим клиентам, их представителям, в бюро кредитных историй, государственным органам и их должностным лицам.

Совершенно ясно, что правовой режим банковской тайны тесно взаимосвязан с правовым режимом персональных данных. При этом следует учесть, что императивное дозволение законодателя на предоставление сведений, составляющих банковскую тайну вышеперечисленным органам, в определенной степени ограничивает правовой режим конфиденциальности персональных данных. В данном случае следует учитывать, что согласно п. 4 ч. 2 ст. 1 Закона о персональных данных [5] сведения, относящиеся к государственной тайне, действием Закона не охватываются. В Перечне сведений, относящихся к государственной тайне, Банк России отнесен к организациям, наделенным полномочиями по распоряжению сведениями, относящимися к государственной тайне (п.п. 79-82). Вполне возможно, что ограничение правового режима конфиденциальности персональных данных основывается на особом субъектном составе банковской системы, в которой имеются два уровня: Банк России и кредитные организации (а также филиалы и представительства иностранных банков) (ч. 1 ст. 2 Закона о банках). Перечень субъектов банковской системы в указанной выше статье не является исчерпывающим. Сюда же можно отнести также союзы и ассоциации, банковские группы и банковские холдинги (ст. 3, 4 Закона о банках). К деятельности указанных субъектов относится использование правового режима банковской тайны. При этом персональные данные субъектов при их предоставлении в кредитные организации переходят под правовой режим банковской тайны и становятся одной из составляющих банковской тайны, как для субъекта банковской системы, так и для обладателя персональных данных. Наличие правового режима банковской тайны и правового режима персональных данных в банковской системе РФ предопределяет необходимость изучения перечисленных субъектов банковской системы и иных участников инфраструктуры, которые взаимодействуют с субъектами, непосредственно осуществляющими банковскую деятельность.

Некоторые участники банковской деятельности не являются частью ее инфраструктуры: это физические и юридические лица, компетентные органы, обеспечивающие и создающие условия для нормального функционирования банковской деятельности. К компетентным органам можно отнести Агентство по страхованию вкладов, Финансовую службу по финансовым рынкам, кредитные бюро и иные субъекты инфраструктуры банковской системы, которые могут обращаться с запросами в кредитные организации. Например, в Гражданском кодексе РФ прямо установлено, что сведения, составляющие банковскую тайну, могут быть предоставлены в бюро кредитных историй (ч. 2 ст. 857 ГК РФ). То есть становится совершенно ясно, что правовой режим персональных данных является самостоятельным режимом конфиденциальной информации и пересекается с иными правовыми режимами информации с ограниченным доступом [6].

Согласно ст. 9 Закона о персональных данных, сведения о субъекте персональных данных предоставляются оператору с письменного согласия обладателя, а их распространение возможно только с согласия субъекта персональных данных. Под конфиденциальностью персональных данных понимается обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

В Законе о персональных данных предусмотрены меры по сохранению персональных

данных и защите их конфиденциальности, заключающиеся в возложении на оператора персональных данных обязанностей применения шифровальных (криптографических) средств для недопущения неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий (ст. 19 Закона о персональных данных).

Следует заметить, что в последнее время получило распространение такое явление, как включение в типовые договоры физических лиц с различными организациями пункта о персональных данных. Причем хотелось бы обратить внимание, что в ряде случаев там прописаны такие действия, как изменение, и, более того, уничтожение персональных данных подписавшего договор физического лица. И если следовать формальному согласию физического лица на изменение и уничтожение его персональных данных, то последствия могут быть самыми драматическими.

По нашему мнению, правовой режим банковской тайны дополняется правовым режимом персональных данных. Сведения, составляющие банковскую тайну, включают в себя ряд сведений, составляющих персональные данные. Вследствие этого представляется логичным расширительное толкование института банковской тайны и понятия банковской информации. Ведь, с одной стороны, персональные данные физического лица являются отражением частной жизни индивида, неприкосновенность которого охраняется законом. С другой стороны, персональные данные представляют собой своеобразную визитную карточку индивида в обществе и являются юридической основой для реализации его праводееспособности [7]. Не подлежит сомнению, что для кредитной организации персональные данные представляют собой коммерческую ценность, а обеспечение конфиденциальности сведений, составляющих коммерческую тайну, является одним из способов достижения поставленной цели — получения прибыли.

Литература

1. Гражданский кодекс Российской Федерации (ГК РФ). http://www.zakonrf.info/gk/ .
2. Федеральный закон Российской Федерации от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (в редакции от 14.03.2013 г. со всеми изменениями и дополнениями). http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=148341 .
3. Ершова И.В., Отнюкова Г.Д. (отв. ред.). Российское предпринимательское право. Учебник. – Москва: Проспект, 2011. 1072 с.
4. Самсонова А.Е. К вопросу о современном состоянии банковской тайны. «Юрист», 2011, № 3, с. 23-29.
5. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных». http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html .
6. Палехова Е.А. Конфиденциальная информация и институт персональных данных в банковской деятельности. http://www.juristlib.ru/book_7226.html .
7. Петрыкина Н.И. К вопросу о конфиденциальности персональных данных. «Законы России: опыт, анализ, практика», 2007, № 5; СПС «КонсультантПлюс».

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

Морозов Антон Андреевич

Единый государственный регистр нормативных правовых актов как базовый государственный информационный ресурс и его правовой режим в контексте информационной безопасности

Аннотация: *в статье дается характеристика единого государственного регистра нормативных правовых актов, рассматриваются его особенности и возможность придания ему режима базового государственного информационного ресурса.*

Ключевые слова: *право, информация, информационное право, базовый государственный информационный ресурс.*

Основополагающие документы в сфере информационной безопасности, такие как Доктрина информационной безопасности, Стратегия национальной безопасности и Стратегия развития информационного общества, указывают, что большая часть современных угроз исходит в направлении информационных ресурсов страны. Опыт развитых стран свидетельствует, что защита своих информационных ресурсов требует не только решений в сфере компьютерных и информационно-телекоммуникационных технологий, но и организационно-правовых.

14 сентября 2012 г. было принято постановление Правительства Российской Федерации № 928 «О базовых государственных информационных ресурсах», которое позволило автору провести диссертационное исследование и по-новому оценить статус и состояние информационной безопасности исследуемых в работе информационных ресурсов.

Распоряжением Правительства РФ от 25 апреля 2006 г. № 584-р утвержден прилагаемый перечень регистров, реестров, классификаторов и номенклатур, отнесенных к учетным системам федеральных органов государственной власти.

В числе этих документов — Единый регистр нормативных правовых актов (НПА) Российской Федерации. Этот регистр состоит из:

- Государственного реестра нормативных правовых актов федеральных органов исполнительной власти, который ведется в соответствии с постановлением Правительства Российской Федерации от 13 августа 1997 года № 1009 «Об утверждении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации»;
- Федерального регистра нормативных правовых актов субъектов Российской Федерации, который ведется в соответствии с Указом Президента Российской Федерации от 10.08.2000 № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» и постановлением Правительства Российской Федерации от 29.11.2000 г. № 904 «Об утверждении Положения о порядке ведения федерального регистра нормативных правовых актов субъектов Российской Федерации»;
- Федерального регистра муниципальных нормативных правовых актов, который ведется в соответствии с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления» и постановлением Правительства Российской Федерации от 10.09.2008 № 657 «О ведении федерального регистра муниципальных нормативных правовых актов».

К тому же, с учетом уникальных архивов, Министерство юстиции обладает фондом НПА с

1917 года, которые, в соответствии с распоряжением Президента РФ от 18 марта 2011 г. № 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», должны быть подвергнуты анализу и инкорпорации в действующее законодательство. Таким образом, Минюст имеет в распоряжении четвертый уникальный ресурс, подобный по важности трем предыдущим.

Во исполнение Указа Президента Российской Федерации от 10.08.2000 № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» в системе Минюста был разработан Единый регистр государственных нормативных правовых актов.

Система ведения Федерального регистра основана на использовании распределенной базы данных Регистра, представляющей собой совокупность региональных баз данных отдельных структурных единиц, связанных между собой в иерархическую систему.

Федеральные регистры ведутся в целях обеспечения верховенства Конституции Российской Федерации и федеральных законов; учета и систематизации нормативных правовых актов; реализации конституционного права граждан на получение достоверной информации о правовых актах; создания условий для получения правовой информации органами государственной власти, органами местного самоуправления, должностными лицами и организациями.

С учетом актуальных редакций нормативных правовых актов, заключений антикоррупционной и правовой экспертизы, актов органов прокуратуры и судебных органов в системе содержится более 5 млн полнотекстовых документов.

Ежемесячный рост базы данных составляет в среднем свыше 60 тыс. актов, при этом основную часть составляют нормативные правовые акты регионального и муниципального уровня.

С начала 90-х годов подобными задачами занимаются и коммерческие структуры, такие как «Консультант», «Гарант», «Кодекс», достигшие больших успехов в этой области. Подавляющее большинство юристов пользуются данными правовыми системами и мало знают о существовании такого уникального информационного ресурса, как Единый регистр. В условиях глобальных кризисных явлений базы данных коммерческих структур гораздо более подвержены угрозам ликвидации как по экономическим соображениям, так и по требованиям информационной безопасности. В то же время Единый регистр отличается от них наличием гораздо большего объема уникальных правовых актов (муниципальные акты, действующие акты первых лет советской власти, действующие акты СССР). И, безусловно, информационные ресурсы Единого государственного регистра, сосредоточенные в НЦПИ Минюста России, защищаются на уровне требований информационной безопасности, предъявляемым государственным структурам.

Представляется, что за основу концепции эталонного ресурса нормативных правовых актов на базе системы ведения федеральных регистров и государственных реестров Минюста России можно принять систему требований, предъявляемых к базовым информационным ресурсам.

Согласно постановлению Правительства Российской Федерации № 928 от 14 сентября 2012 г. базовые государственные информационные ресурсы формируются путем размещения в созданных или создаваемых государственных информационных ресурсах уникальных сведений об объекте либо о субъекте (физическом или юридическом лице), которые предназначены для использования при осуществлении межведомственного информационного взаимодействия в целях предоставления государственных и муниципальных услуг и на создание которых указанные органы уполномочены в соответствии с федеральными законами. Эталонные сведения могут создаваться уполномоченным органом с использованием эталонных сведений, созданных другим уполномоченным органом.

Развитие информатизации в России неизбежно должно привести к тому, что информационные системы станут неотъемлемой частью жизни, причем основным этапом лет через 5-7 будет взаимопроникновение систем. Целью такой информатизации является эффективное государство, в котором процессы отличаются прозрачностью, а также актуальностью, доступностью, достоверностью и ссылочной целостностью общественно и юридически значимой информации. Необходимо отметить, что прозрачность процессов формирования правовой информации в государстве может быть одним из условий и эффективного противодействия коррупции.

Тот факт, что в Едином регистре содержатся нормативные правовые акты всех уровней — от федерального до муниципального, а также то, что в Едином регистре однозначно опреде-

лены источники поступления информации для каждого нормативного правового акта, являются объективными предпосылками развития Регистра как официального государственного банка данных нормативных правовых актов, интегрированного с другими информационными ресурсами и используемого для решения широкого круга общественных и государственных задач.

Таким образом, Единый регистр нормативных правовых актов Российской Федерации представляет высокую ценность для государства в связи с наличием у него всех признаков базового государственного информационного ресурса.

Первое. Проведенный анализ критериев и требований, предъявляемых к базовому государственному информационному ресурсу, позволил сформулировать его авторское определение: базовый государственный информационный ресурс — это формируемый для предоставления государственных услуг банк данных, содержащий эталонные сведения, поддерживаемые уполномоченным органом власти в состоянии полноты, достоверности и актуальности, к которому с соблюдением требований информационной безопасности обеспечивается круглосуточный непрерывный автоматизированный доступ в электронном виде.

Второе. Единый регистр нормативных правовых актов, созданный на базе автоматизированной информационно-поисковой системы федеральных регистров и государственных реестров, должен иметь открытый доступ к сведениям, которые он содержит, для того, чтобы обеспечить как можно большее количество граждан, организаций и органов власти правовой поддержкой для принятия обоснованных решений.

Третье. Можно сделать вывод о том, что Единый регистр нормативных правовых актов Российской Федерации имеет в себе все признаки базового государственного информационного ресурса и его ведение должно осуществляться в соответствии с законом.

Четвертое. Можно сделать вывод о том, что Единый регистр нормативных правовых актов Российской Федерации как базовый государственный информационный ресурс имеет существенное значение для обеспечения информационной безопасности страны, поскольку его утрата влечет потерю актуальной, достоверной, полной информации о состоянии нормативных правовых актов, необходимой для принятия важнейших государственных решений.

Пятое. Предлагается внести в проект закона «О нормативных правовых актах» норму о придании Единому регистру нормативных правовых актов Российской Федерации статуса базового государственного информационного ресурса и использования его актуализированного вида как основу для ведения Свода законов Российской Федерации в электронной форме.

Шестое. Проведенное автором исследование уникальных архивов Министерства юстиции с 1917 года позволяет утверждать, что Министерство юстиции располагает подобным по значимости трем составляющим Единого регистра нормативных правовых актов Российской Федерации четвертым уникальным ресурсом, который в соответствии с распоряжением Президента Российской Федерации от 18 марта 2011 г. № 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», является источником эталонных сведений о нормативных правовых актах, подлежащих инкорпорации в действующее законодательство Российской Федерации.

Седьмое. Можно сделать вывод о необходимости построения государственной системы правовой информации на базе Единого регистра нормативных правовых актов Российской Федерации, состоящего из эталонных сведений, поддерживаемых уполномоченным органом власти (Минюстом России) в состоянии полноты, достоверности и актуальности как базового государственного информационного ресурса, к которому с соблюдением требований информационной безопасности обеспечивается круглосуточный непрерывный автоматизированный доступ в электронном виде.

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

Севостьянов Валерий Леонидович
кандидат технических наук

Общественное обсуждение концепции регулирования правоотношений в сети интернет

Аннотация: *рассматриваются итоги общественных слушаний по проблемам правового регулирования обмена информацией в сети Интернет, особое внимание уделяется вопросам защиты интеллектуальной собственности.*

Ключевые слова: *информационно-коммуникационные технологии, общественная экспертиза, авторские права, объекты интеллектуальной собственности.*

В Комитете Государственной Думы по информационной политике, информационным технологиям и связи группой депутатов под руководством Р. А. Шлегеля во взаимодействии с парламентским экспертным сообществом разработана «Концепция правоотношений, возникающих при использовании сети Интернет». Проблемы этих правоотношений вызывают большой общественный интерес, поэтому депутаты представили Концепцию для обсуждения в Общественную палату Российской Федерации. 12 июля 2013 г. Общественная палата провела слушания. На рассмотрение общественности были вынесены текст Концепции и подготовленный «Российской ассоциацией электронных коммуникаций» комментирующий документ с анализом нерешенных проблем законодательного регулирования оборота информации в Интернете. Модератором общественных слушаний был председатель Комиссии Общественной палаты по поддержке средств массовой информации, обеспечению свободы слова и доступа к информации, генеральный директор Издательского дома «Московский комсомолец» П. Н. Гусев. В мероприятии участвовали члены Общественной палаты, Совета при Президенте РФ по развитию гражданского общества и правам человека, представители ассоциированных структур Интернет-сообщества.

Приведем основные положения рассматриваемой Концепции. Довольно краткий документ состоит из 5 разделов. Первый раздел называется «Общая характеристика и предпосылки создания правовой платформы взаимоотношений субъектов сети Интернет». В нем отмечается, что число российских пользователей сети достигает 50 млн. человек, а общий объем российской Интернет-экономики составляет 4,6% ВВП страны. При этом годовой ущерб от правонарушений превышает 60 млрд руб. Указывается, что отечественное законодательство недостаточно регулирует права и обязанности субъектов, действующих в Сети, и недостаточно гармонизировано с международным правом. Второй раздел посвящен анализу проблем взаимоотношений, возникающих при использовании сети Интернет. Среди них названы недоработанность понятийного аппарата и его несоответствие современному технологическому уровню (в частности, неопределенность правового статуса облачных вычислений), несогласованность российского и международного законодательства (включая неразвитость механизмов управления и охраны интеллектуальной собственности), недостаток правовых норм использования сети Интернет для развития институтов гражданского общества. Третий раздел Концепции посвящен целям и задачам правового регулирования сети Интернет в Российской Федерации. В качестве основных целей правового регулирования названы защита конституционных прав

граждан и интересов общества, а также развитие Интернет-экономики. Ставятся задачи обеспечения прав и свобод граждан в Сети, повышения доли Интернет-экономики в ВВП страны, снижения доли правонарушений, совершаемых с использованием информационно-коммуникационных технологий (ИКТ), повышения качества услуг в Сети. Четвертый раздел целиком посвящен предложениям по нормативному регулированию. Детально рассматриваются необходимые новации в описании прав и обязанностей субъектов правоотношений (например, ставится вопрос об уточнении обязанностей операторов связи и провайдеров хостинга по хранению и предоставлению органам государственной власти, осуществляющим оперативно-розыскную деятельность, соответствующей информации о пользователях — этот вопрос в последнее время оказался в центре внимания мировой общественности в связи с известными международными скандалами, вызванными деятельностью спецслужб США). Указывается на необходимость определения границ юрисдикции Российской Федерации, а также определения правовых условий обработки персональных данных в соответствии с Конвенцией «О защите физических лиц при автоматизированной обработке персональных данных». Даны предложения в сфере развития электронной коммерции и определения особенностей деятельности электронных СМИ. Отдельный параграф называется «Защита авторских, интеллектуальных и смежных прав». В нем говорится о приравнивании электронных способов принятия лицензионного договора к письменной форме, введении института «открытых лицензий» и уточнении способов передачи произведений в общественное достояние. Ставятся вопросы определения степени и условий привлечения к ответственности информационных посредников и пользователей за контент, нарушающий законодательство об авторском праве, а также определения порядка информационного взаимодействия всех заинтересованных субъектов при выявлении фактов нарушения авторских прав. Говорится также о расширении сферы свободного использования произведений и культурных ценностей в информационных, научных, учебных или культурных целях. Важное общественно-политическое значение имеет параграф «Использование сети Интернет для реализации прямой демократии». В нем указывается на необходимость создания правовой основы для участия граждан в государственном управлении и местном самоуправлении, а также в принятии общественно значимых решений с использованием Сети. В заключительном, пятом разделе документа, озаглавленном «Выводы», указано на общественную пользу, которую принесет регулирование правоотношений в сети Интернет.

После краткого представления рассматриваемого документа модератор предоставил слово председателю Совета при Президенте РФ по развитию гражданского общества и правам человека М. А. Федотову. По мнению выступающего, все существующие попытки регулирования правоотношений в Интернете напоминают попытку построить здание без фундамента — ведь на сегодня юридически не «закреплена» даже используемая в отношении Интернета терминология. Роль фундамента, как он считает, должен сыграть базовый федеральный закон «Об Интернете». Кроме того, следует учитывать, что с появлением Интернета коренным образом изменилась ситуация с числом нарушителей авторских и смежных прав — «во времена Гутенберга пираты были, но их было чрезвычайно мало по отношению к населению, а теперь многие миллионы людей скачивают нелегальный контент». (Следует отметить, что при недавнем процессе комплектования нового состава Совета при Президенте РФ по развитию гражданского общества и правам человека в круг планируемых направлений его деятельности не вошла защита авторских и смежных прав — не было и соответствующей номинации специалистов для выдвижения кандидатур в состав Совета, что безусловно свидетельствует о недостаточном внимании к указанным проблемам).

В отсутствие депутатов-инициаторов разработки Концепции и в силу профессионального состава большинства аудитории дальнейшая дискуссия сосредоточилась в основном на условиях работы СМИ. Член Общественной палаты, главный редактор «Комсомольской правды» В. Н. Сунгоркин рассказал, что в одном из районных судов Ульяновской области было принято решение, обязывавшее региональный филиал ОАО «Ростелеком» блокировать доступ к сайту «Комсомольской правды» после публикации в газете материалов о взяточничестве чиновников. По оценке выступающего, только низкая компетентность представителей исполнительной и судебной власти на местах в вопросах специфики работы электронных средств массой коммуникации могла вызвать появление такого решения — закрыть доступ к информации федеральной печати в одном отдельно взятом регионе и только у одного из провайдеров. В целом же

это свидетельствует о настоятельной необходимости регулирования правоотношений при использовании Интернета на уровне федерального законодательства.

По мнению президента «Ассоциации Интернет-издателей» И.И. Засурского, попытки защитить авторские и смежные права российских авторов от несанкционированного доступа в Интернете приведут не к росту доходов правообладателей, а лишь к отлучению российских пользователей от произведений отечественного искусства и литературы, Так, по искам американских кинопродюсеров (а именно их продукция практически монополизировала российский кинорынок) могут быть закрыты возможности бесплатного доступа ко всем фильмам, а это означает, что в Интернете прервется ознакомление российских зрителей в том числе и с классикой отечественного кино — для массового отечественного сознания неприемлемо платить за просмотр «своего родного». Поэтому единственным выходом в интересах государства может быть передача всех таких отечественных фильмов в открытый бесплатный доступ.

Позиция наиболее либерально настроенной части российского общества нашла отражение в выступлении члена Общественной палаты телепублициста Н. К. Сванидзе. Он считает, что всякое стремление к правовому регулированию Интернета обусловлено боязнью со стороны государственных властей политических «неприятностей»; всякие попытки в этой сфере означают «наступление на свободу слова» и должны «получать отпор».

В то же время в дискуссии звучали и мнения в пользу конструктивного сотрудничества органов государственной власти, структур бизнеса и широкой общественности в создании правовой базы регулирования Интернета. Так, руководитель агентства «Румянцев и партнеры» О. Г. Румянцев (один из разработчиков ныне действующей Конституции РФ) отметил, что мы уже значительно отстаем в этом отношении от развитых зарубежных стран и целесообразно использовать их опыт. Так, в Германии ответственность возлагается в большинстве случаев не на провайдеров, а на пользователей Интернета, что воспитывает ответственного потребителя информационных услуг. Он отметил позитивное значение создания суда по интеллектуальной собственности и его сотрудничества с Роскомнадзором. Нужно также развивать практику досудебного взаимодействия сторон для устранения возникающих конфликтов (во многих случаях это позволит ограничиться оперативным изъятием нелегального контента из общественного доступа).

Директор «Российской ассоциации электронных коммуникаций» (РАЭК) С. А. Плуготаренко познакомил собравшихся с основными результатами проведенного Ассоциацией анализа проблем регулирования правоотношений в Интернете, не решенных действующим в нашей стране законодательством. В розданном участникам общественных слушаний материале были в табличном виде представлены возникающие вопросы, указаны регулирующие их нормативно-правовые акты и даны конкретные предложения по необходимым мерам по развитию законодательной базы для устранения тех или иных правовых коллизий. Выступающий отметил, что многие недостатки в сфере использования сети Интернет вызваны не столько недостаточностью действующего законодательства, сколько негативной правоприменительной практикой, во многом обусловленной низкой квалификацией персонала. В заключение он сказал, что РАЭК готова объединить усилия лучших профессионалов отрасли и видных юристов с тем, чтобы обеспечить качественное решение возникающих правовых проблем.

Эту позицию поддержал участвовавший в Общественных слушаниях заместитель министра связи и массовых коммуникаций Д. Л. Свердлов. Он отметил готовность своего ведомства сотрудничать с общественными экспертами в формировании правовой базы дальнейшего развития электронных коммуникаций.

Завершая дискуссию, ее модератор П. Н. Гусев проинформировал собравшихся о принятом решении продолжить обсуждение рассматриваемых проблем осенью текущего года на площадке Совета при Президенте РФ по развитию гражданского общества и правам человека.

Состоявшееся мероприятие свидетельствует о реально сложившейся в обществе «разноголосице мнений» по вопросам правового регулирования Интернета. По мнению многих представителей парламентского экспертного сообщества, необходимо активизировать роль Федерального Собрания в решении существующих проблем. Возможно, целесообразно более широко поставить вопрос об обороте информации с использованием современных электронных средств массовой телекоммуникации и приступить к разработке «Информационного кодекса Российской Федерации». Парламентское экспертное сообщество готово участвовать в этой работе.

Сведения об авторах

ДОРОФЕЕВ Александр Владимирович – директор по развитию ЗАО «НПО «Эшелон», CISA, CISSP, г. Москва.
E-mail: ad@cnpo.ru

ЕРМОЛЕНКО Александр Владимирович – главный специалист службы безопасности ОАО «Рязаньтранснефтепродукт», г. Рязань
E-mail: ave-1984@yandex.ru

КРУТИКОВА Дарья Ильинична – аспирант кафедры информационного права, информатики и математики Российской правовой академии Минюста России, г. Москва
E-mail: dkrutikova@gmail.com

КРЫЛОВ Григорий Олегович – доктор физико-математических наук, кандидат юридических наук, профессор кафедры информационного права, информатики и математики Российской правовой академии Минюста России, г. Москва.
E-mail: nik122@yandex.ru, op50@mail.ru

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

ЛЕОНТЬЕВ Борис Борисович – доктор экономических наук, профессор, генеральный директор ЗАО «Федеральный институт сертификации и оценки интеллектуальной собственности и бизнеса» (ЗАО «СОИС»).
E-mail: info@sois.ru

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

МАРКИН Михаил Николаевич – аспирант кафедры информационного права, информатики и математики Российской правовой академии Минюста России, г. Москва
E-mail: markin@russian-lawyers.ru

МОРОЗОВ Антон Андреевич – аспирант Национального исследовательского ядерного университета «МИФИ».
E-mail: backintothetop@gmail.com

СЕВОСТЬЯНОВ Валерий Леонидович – кандидат технических наук, ученый секретарь Парламентского Центра «Наукоемкие технологии, интеллектуальная собственность».
E-mail: valery.sewostyanov@yandex.ru

СОЛДАТОВА Нина Викторовна – главный эксперт департамента по развитию предпринимательства Торгово-промышленной палаты Российской Федерации.
E-mail: soldatovanina@rambler.ru

СУХОТИН Сергей Олегович – аспирант кафедры информационного права, информатики и математики Российской правовой академии Министерства юстиции Российской Федерации.
E-mail: sukhotin@inbox.ru

ФАДЕЕВА Наталья Анатольевна – старший научный сотрудник ФБУ НЦПИ при Минюсте России, г. Москва.
E-mail: n-fadeeva@yandex.ru

ШАХАЛОВ Игорь Юрьевич – заместитель генерального директора ЗАО «НПО «Эшелон», доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва.
E-mail: i.shahalov@npo-echelon.ru

Abstract and keywords

I. Yu. Shakhalov, A. V. Dorofeev
The basics of information security management in a modern organisation

Abstract: *The basics of introduction and management of information security systems are considered in the paper. A concise insight into history is given, objectives, indicators, and methods for creating an efficient information security management system are determined. A full list of international and Russian standards in the field of research is provided in the Appendix.*

Keywords: *information security, data protection, security management, planning, monitoring, standards, Deming/ Shewhart cycle (PDCA).*

G.O. Krylov, V.M. Lazarev, A.E. Lyubimov
The international experience of legal regulation of information security and the possibilities for its versatile application in the Russian Federation

Abstract: *A generalised description of the international experience of legal regulation of information security and the possibilities of its application in the Russian Federation are presented in the paper. The results of systematisation of international legal norms in the field of information security and their relationship to the international information security standards as well as data on the international experience of law enforcement practice in the field of information security based on the application of international information security standards are given. The paper also contains a description, in generalised form, of the information relationships in the Internet as the infrastructure of global information and noosphere societies, prospective international relations, as well as the specific features of web information threats. The importance of using this experience of applying modern information and analytical systems for practical implementation of information support processes is shown.*

Keywords: *international experience, legal regulation of information security, information security processes modelling, analytical systems for the analysis of legal regulation of information security, information relationships in the Internet.*

A.V. Ermolenko
Practical application of the digital signature in the activities of organisations: reality and prospects

Abstract: *Practical application of the digital signature by commercial entities is analysed in the paper. Information on the fields of activities of economic agents where the digital signature is widely applied, is provided. Economic prerequisites and legal grounds for implementing the digital signature in business processes are examined. Additionally, issues concerning the lines for developing legislation with a view to increase the motivation of businesses to use the digital signature are touched upon in the paper.*

Keywords: *digital signature, electronic document, electronic document flow, electronic signature, legal value, use of the digital signature.*

N.V. Soldatova, B.B. Leontyev
State strategy of intellectual property: experience of Japan

Abstract: *At present the intellectual property is one of the principal global sources of new jobs, new products and services. In 2000 the Government of Japan has identified the national idea - transformation of nation into the IP-based state. The Government of Japan has adopted the public policy with primary importance to inventions, creativity, innovative products and services. Widespread use of intellectual property as principal economic resource is the only way for maintaining the leading state's position in global economy for the country lacking in natural resources.*

Keywords: *state, legal system, intellectual property, innovation, strategy, tools, model, management, economy.*

N.A. Fadeeva
Topical issues of systematisation of the legislation of the Russian Federation

Abstract: *Forms of systematisation of legislation and converting of state registration documents into electronic form are considered in the paper. The paper also contains an overview and analytical list of appropriate legal acts.*

Keywords: *systematisation, incorporation, consolidation, subsystem, information resources, archives, information systems.*

S.O. Sukhotin
Advanced training of specialists of territorial bodies of justice making use of e-learning tools

Abstract: *The paper contains a description of how specialised e-learning courses for advanced training of specialists of territorial bodies of justice and municipalities are created.*

Keywords: *recommendations, improvement, e-learning, training, advanced training, educational, technologies, standards, development, education, science, distance education technologies, public service, municipal service.*

M.N. Markin
Problems of restricting the dissemination of information over the Internet

Abstract: *It is proposed to cancel the judicial prohibition for restricting the dissemination of information over the Internet due to practical unenforceability of such a prohibition. The experience of foreign countries in restricting the dissemination of information over the Internet is examined.*

Keywords: *Internet censorship, information dissemination, the Golden Shield Project.*

D.I. Krutikova
Comparative legal analysis of the concepts of "bank secrecy" and "personal data" within the framework of protection of information on bank customers

Abstract: *Definitions of the concepts of bank secrecy and personal data of the customer which have a crucial effect on the treatment of confidential information on the customer obtained by banks in the course of their operations as well as on the provision of this information to third parties, are considered.*

Keywords: *bank secrecy, personal data, banking, data protection, bank customer.*

A.A. Morozov
The General Register of Normative Legal Acts as the basic public information resource and its legal regime in the context of information security

Abstract: *A description of the General Public Register of Normative Legal Acts is given in the paper, its specific features and the possibility of granting it the status of the basic public information resource are considered.*

Keywords: *law, information, information technology law (IT law), basic public information resource.*

V.L. Sevostyanov
A public hearing on the Concept of regulating legal relations on the Internet

Abstract: *The results of a public hearing on problems of legal regulation of information exchange on the Internet are considered, special attention being given to issues of intellectual property protection.*

Keywords: *information and communications technology, public evaluation, copyright, intellectual property objects.*

В редакционный Совет нашего журнала вошел в качестве члена Совета Марков Алексей Сергеевич – генеральный директор НПО «Эшелон», кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Алексей Сергеевич родился 14 декабря 1963 года, окончил Военный Краснознаменный институт им. Д.Ф. Можайского по специальности «Программное обеспечение функционирования автоматизированных систем управления» в 1986 году.

В 1992 году закончил адъюнктуру при Военно-космической академии им. Д.Ф. Можайского и защитил кандидатскую диссертацию по специальности 20.02.12 на тему «Разработка методики оценки и обеспечения надежности функционирования специального программного обеспечения автоматизированной системы специального назначения». В 1995 году ему присвоено ученое звание старшего научного сотрудника по специальности «Военная информатика, кибернетика».

А.С. Марковым опубликовано 4 монографии и свыше 120 научных публикаций по вопросам контроля и повышения качества, надежности и безопасности автоматизированных систем. В последние годы сфера научных интересов Алексея Сергеевича сосредоточена в области дефектоскопии программного обеспечения – нового научного направления, в становление и развитие которого А.С. Марковым внесен заметный вклад.

Алексей Сергеевич является руководителем аттестационного центра Минобороны России, внештатных испытательных лабораторий Минобороны России, ФСТЭК России и ФСБ России. Имеет международный сертификат специалиста в области безопасности и непрерывности бизнеса (CISSP, SBCI). Входит в состав Технического комитета по стандартизации Российской Федерации (ТК-362).

Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 3.09.2009 № 113л/с генеральный директор ЗАО НПО «Эшелон» Марков Алексей Сергеевич награжден медалью ФСТЭК России «За укрепление государственной системы защиты информации» I степени.

Редакция надеется, что энергия и опыт А.С. Маркова будут способствовать широкому освещению на страницах нашего журнала новых идей и решений в области безопасности информационных систем.

Публикацию подготовил член редакционного Совета

Макаренко Григорий Иванович

Над номером работали:

Главный редактор	М.Ю. Сергин
Ответственный секретарь	О.В. Челнокова
Начальник РИО	Ю.В. Матвиенко
Литературный редактор	Е.В. Горбачева
Научный редактор	Г.И. Макаренко
Выпускающий редактор	И.Г. Колмыкова
Компьютерная верстка	А.С. Михеева
Тиражирование (печать)	Н.Г. Шабанова