

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ



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

ПРАВОВАЯ ИНФОРМАТИКА

Периодический научный журнал

№ 3 – 2014

Москва, 2014

Редакционный совет

Леонтьев Борис Борисович	Председатель редакционного Совета, доктор экономических наук, профессор, академик РАЕН, г. Москва
Атагимова Эльмира Исамудиновна	кандидат юридических наук, ответственный секретарь, г. Москва
Бусов Владимир Иванович	доктор экономических наук, профессор, зав.кафедрой Государственного университета управления, г. Москва
Винслав Юрий Болеславович	доктор экономических наук, профессор, главный редактор журнала «Менеджмент бизнес-администрирование», г.Москва
Горбещкий Иван Иванович	заместитель директора департамента Министерства юстиции Российской Федерации, г. Москва
Костогрызов Андрей Иванович	Заслуженный деятель науки РФ, доктор технических наук, профессор, член-корреспондент Российской академии ракетных и артиллерийских наук и Российской академии естественных наук, действительный член Академии информатизации образования, г. Москва
Курбанов Габил Сурхай оглы	доктор юридических наук, профессор, иностранный член редакционного Совета, г. Баку, Азербайджан
Макаренко Григорий Иванович	ответственный редактор — заместитель Главного редактора, г. Москва
Мамаджанов Хамид Абиджанович	доктор технических наук, профессор, г. Москва
Сергин Михаил Юрьевич	доктор технических наук, профессор, г. Москва
Стародубцев Юрий Иванович	доктор военных наук, профессор, г. С-Петербург
Степанов Владимир Иванович	доктор экономических наук, профессор, научный редактор научно-практического журнала «ЛОГИСТИКА», г. Москва
Федичев Андрей Валерьевич	кандидат технических наук, доцент, действительный государственный советник Российской Федерации 3 класса, главный редактор, г. Москва
Шаршун Виктор Александрович	кандидат юридических наук, иностранный член редакционного Совета, Минск, Белоруссия

Редакционная коллегия

Федичев Андрей Валерьевич	Главный редактор, кандидат технических наук, доцент, действительный государственный советник Российской Федерации 3 класса, г. Москва
Абдусаламов Руслан Абдусаламович	кандидат юридических наук, доцент, г. Махачкала
Атагимова Эльмира Исамудиновна	кандидат юридических наук, ответственный секретарь, г. Москва
Ветров Александр Григорьевич	кандидат физико-математических наук, начальник отдела аппарата Совета Федерации Федерального собрания Российской Федерации, г. Москва
Гречишников Евгений Владимирович	доктор технических наук, доцент, г.Орел
Гулка Зинаида Николаевна	доктор философии в технике, профессор, иностранный член, г. Кишинев, Молдова
Костогрызов Андрей Иванович	Заслуженный деятель науки РФ, доктор технических наук, профессор, член-корреспондент Российской академии ракетных и артиллерийских наук и Российской академии естественных наук, действительный член Академии информатизации образования, г. Москва
Лазарев Виктор Михайлович	доктор технических наук, профессор, г. Москва
Леонтьев Борис Борисович	доктор экономических наук, профессор, академик РАЕН, г. Москва
Макаренко Григорий Иванович	ответственный редактор — заместитель Главного редактора, г. Москва
Марков Алексей Сергеевич	кандидат технических наук, доцент, генеральный директор НПО Эшелон, г. Москва
Миндрова Екатерина Анатольевна	кандидат юридических наук, г. Чебоксары
Стародубцев Юрий Иванович	доктор военных наук, профессор, г. С-Петербург
Танимов Олег Владимирович	кандидат юридических наук, доцент, г. Москва
Шихнабиева Тамара Шихгасановна	доктор педагогических наук, академик Академии информатизации образования, профессор, г. Москва

Журнал «Правовая информатика» является периодическим рецензируемым изданием, выходит 4 раза в год. Подписка на журнал производится по объединенному каталогу «Пресса России» или письмом в редакцию.

Индекс подписки: 44723

Адрес редакции: 125437, Москва, Михалковская ул, 65, стр.1

Телефон: +7(495)539-23-63, E-mail: pravo360@gmail.com

www.pravo360.ru

СОДЕРЖАНИЕ

<i>Тонконогов Александр Викторович</i> Обеспечение кибернетической безопасности России в современных геополитических условиях	4
<i>Али Гейдар оглы Рзаев</i> Содержание и сущность государственного управления	6
<i>Цирлов Валентин Леонидович, Никулин Михаил Юрьевич</i> Правовые основы сертификации средств защиты информации	14
<i>Чхутиашвили Лела Васильевна</i> Электронные денежные переводы в современном банковском законодательстве	18
<i>Ерохина Юлия Владимировна</i> Проблемы информационного обеспечения противодействия коррупции	21
<i>Добрякова Галина Эдуардовна</i> Проблемы идентификации в информационных системах	28
<i>Леонтьева Валерия Борисовна</i> Технико-правовые основы стоимостнообразования	33
<i>Савичев Алексей Аркадьевич</i> Сравнительный анализ обеспечения доступа к информации в системе городского самоуправления: история и современность	41
<i>Горбачева Елена Викторовна</i> Информатика как теория, определяющая оптимальную организацию информационной работы	45
<i>Барабанов Александр Владимирович</i> Нормативные вопросы безопасного производства программ	49
<i>Цирлов Валентин Леонидович</i> Правовые основы кибербезопасности Российской Федерации	54
<i>Родина Валерия Владимировна</i> Особенности формирования законодательной базы промышленной политики на примере России и Германии	57
<i>Кубанков Александр Николаевич, Половникова Людмила Сергеевна</i> Уточнение содержания учебной дисциплины «Правовые вопросы доступа к информации»	64
Сведения об авторах	66
Abstract and keywords	68



**Тонконогов
Александр
Викторович**
доктор философских наук

Обеспечение кибернетической безопасности России в современных геополитических условиях

Аннотация: статья посвящена проблемам обеспечения кибернетической безопасности современной России, даны авторские определения понятиям «кибернетическая безопасность», «кибернетическая война», «кибернетическая революция», предложены правовые и организационные меры противодействия угрозам в сфере кибернетической безопасности.

Ключевые слова: кибернетическая безопасность, обеспечение национальной безопасности, кибернетическая война, кибернетическая революция, современная Россия, геополитическое соперничество.

Современное геополитическое соперничество характеризуется тенденцией к эскалации противостояния государств и наций не только в исторически сложившемся геостратегическом пространстве (общедоступной реальности), но во многом и усилением противоборства в искусственно создаваемой моделируемой виртуальной реальности (кибернетическом пространстве электронных средств массовой коммуникации стремительно глобализирующегося мирового социума). Таким образом, возрастает необходимость в организации эффективного обеспечения кибернетической безопасности государств.

Кибернетическая безопасность – это один из видов национальной безопасности, являющаяся частью информационно-психологической (духовной) безопасности, представляющая собой состояние защищенности от внутренних и внешних угроз виртуальной реальности в кибернетическом пространстве социума, средств массовой коммуникации военного, общегосударственного и гражданского назначения, а также общественного сознания как одного из основных национальных информационных ресурсов. Угрозы кибернетической безопасности государства соизмеримы по своей деструкции угрозам военного характера. Поэтому киберпространство объявлено обычной средой деятельности Вооруженных сил США как суша, море и воздушное пространство.

Обеспечение кибернетической безопасности – одно из важнейших направлений обеспечения национальной безопасности любой страны в целом. Именно поэтому в США существуют «Национальный центр кибербезопасности и интеграции коммуникаций», координирующий деятельность военных, правоохранительных и гражданских структур в сфере обеспечения кибербезопасности (пресечения киберпреступлений, кибератак на государственные и частные электронные средства массовой коммуникации), «Кибернетическое командование Вооруженных сил США», а в качестве законодательной базы принимаются к реализации различные правовые акты. В частности таким документом является «Стратегия Министерства обороны по операциям в киберпространстве» [1]. В Китае, который является ближайшим к России геополитическим конкурентом, наращивают потенциалы национальной армии в сфере подготовки к ведению кибернетической войны.

Кибернетическая война представляет собой особый вид войны нового типа, осуществляемой в целях дезорганизации всех уровней управления силами и средствами противника, выраженной в прове-

дении специальных технологических операций, направленных на психологическое подавление и разрушение или использование в своих целях информационно-технических ресурсов социумов и армий противника посредством создания и контроля через кибернетические (электронные) коммуникационные сети (главным образом, интернет) виртуальной реальности, моделирующей жизнь личности, социальных групп и в целом общества отдельных государств.

К сожалению, в России до сих пор не уделяется должного внимания данной области обеспечения национальной безопасности. Идея некоторых руководителей Генерального штаба Министерства обороны Российской Федерации о создании информационных войск (кибервойск) только начала воплощаться в жизнь. Вместе с тем в условиях развития у нас в стране информационного общества, реализации программы электронного правительства опасность для отечественных вооруженных сил, правоохранительных, специальных и иных государственных служб и ведомств, общества в целом подвергнуться кибернетическим ударам извне вполне реальна. Кибератакам подвергаются даже США, которые оставляют за собой право считать их прямой угрозой национальной безопасности, требующей ответных мер, не исключая военные операции. При этом следует отметить, что феномен «бархатных революций» – это феномен войн нового типа, направленных на передел сфер влияния в существующих геополитически условиях. Можно говорить о таких явлениях, как Интернет и SMS-революции (кибернетические революции).

Кибернетическая революция – это геополитическая операция, направленная на изменение социальных, в том числе духовных основ жизни общества и государства, осуществляемая без явного вмешательства внешних военно-политических сил в целях воздействия на сознание обществ геополитических конкурентов или предполагаемых геополитических объектов влияния через электронные средства массовой коммуникации, посредством использования потенциалов пассивной протестно настроенной части общества государства-объекта геополитического интереса в целях манипуляции. Локальные кибернетические революции, по мнению автора, являются частью глобальных кибернетических войн.

Эскалацию Интернет и СМС-революций провоцируют в Северной Африке и всем постсоветском пространстве третьи страны, стремясь лишить Россию реальных геополитических со-

юзников. При этом и сама Россия, видимо, является одной из ближайших потенциальных геополитических целей. Это подтверждается тем, что З. Бжезинский, обосновавший разрушение СССР, высказал идею (и ее наверняка пытаются реализовать политики развитых стран) о необходимости создания на территории современной России центральной, уральской и дальневосточной самостоятельных республик [2, с.85], то есть превращения ее в конфедерацию.

В связи с этим представляется вполне очевидным и необходимым в кратчайшие сроки осуществить ряд мер под координирующим руководством соответствующей комиссии Совета Безопасности Российской Федерации:

1. Организовать всестороннее научное изучение проблем обеспечения кибернетической безопасности Российской Федерации.
2. Разработать и принять к реализации Стратегию кибернетической безопасности Российской Федерации с условием ее ежегодной комплексной и системной корректировки.
3. Создать Информационные (кибернетические) войска в структуре Вооруженных Сил Российской Федерации.
4. Обеспечить подготовку специалистов в области обеспечения кибернетической безопасности для Минобороны России, правоохранительных органов, специальных служб и ведомств.

Реализация предлагаемых автором правовых и организационных мер позволит субъектам обеспечения национальной безопасности эффективно противостоять вызовам и угрозам в кибернетической сфере современной России [3,4].

Литература

1. Иванов В. Кибервойна – неизбежна: Пентагон объявляет виртуальное пространство полем боя // Независимое военное обозрение. 2010. № 37. – С. 12.
2. Бжезинский З. Великая шахматная доска. – М. : Международные отношения, 1999. – 256 с.
3. Обеспечение кибернетической безопасности Российской Федерации (основы общей киберологии) : монография / Стельмах А.П., Тонконогов А.В. – М. : Изд-во РГАУ-МСХА им. К.А. Тимирязева, 2012. – 102 с.
4. Тонконогов А.В. Кибернетическая безопасность: понятие и сущность феномена // Право и кибербезопасность. 2013. № 2. – С. 36–43.

Содержание и сущность государственного управления

Аннотация: в статье анализируется значение и понятие государственного управления, исследуются его системность, такие составные части системы управления, как субъект, объект, прямая и обратная связь, информация. Также рассматриваются взаимосвязь управления и регулирования, система управления в живом организме как классическая кибернетическая система.

Ключевые слова: государственное управление, субъект и объект управления, прямая и обратная связь, системный анализ, кибернетика, информация, регулирование, живой организм, гомеостазис.

Как известно, государственный аппарат функционирует в трех направлениях, принятых в международной системе:

- а) сфера управления;
- б) охрана правопорядка;
- в) внутренняя и внешняя безопасность.

Среди этих функций главнейшую роль играет управление, так как остальные две функции осуществляются при его помощи. Естественно, без управления невозможно поддержать порядок и организованность людей и безопасность государства. Человечество вступило в третье тысячелетие. В это время никакую проблему невозможно решить без управления. Без управления немислимо и распределение материальных и духовных благ и потребления. «Всякий непосредственный общественный и совместный труд, – писал К. Маркс, – нуждается в большей и меньшей степени в управлении, которое направляет согласованную работу... Отдельный скрипач сам управляет собой, оркестр нуждается в дирижере» [1, с. 342].

Роль и место государственного управления в жизни общества, государства и человека не случайны, оно позволяет осуществлять единообразное, властное регулирование соответствующих общественных отношений на всей территории государства.

После распада СССР в бывших союзных республиках, в том числе в Азербайджане, в принятых новых конституциях с закреплением принципа разделения властей органы государственного управления, являющиеся ведущей частью государственного аппарата, были заменены субъектами исполнительной власти, разделение труда – разделением властей. Проблемы управления вызвали неоднозначную реакцию научной общественности на «внезапное исчезновение» государственного управления из текста Конституции. По этому поводу позиции ученых разошлись по трем направлениям. Первые отстаивают прежнее понимание данного феномена; вторые авторы заменяют термин «государственное управление» на просто «управление»; третье направление – авторы радикально меняют содержание понятия государственного управления либо вовсе отказываются от его использования [2, с. 77–78].

Несмотря на замену выражений органов управления и органов исполнительной власти, функция управления государства, государственного аппарата остается без изменения и данное понятие существует.

Без государственного воздействия на ответствующие общественные отношения исчезнет само государство, превратившись в разрезанные, плохо управляемые составные части, постоянно стремящиеся доказать свое право на существование. От государственного управления не отказалась еще ни одна страна, и вряд ли для этого имеются какие-либо основания. Должное место государственному управлению и его постоянному совершенствованию уделяется в США, Японии, Великобритании, Германии, Франции (которая считается родоначальником административного права и термина «государственное управление»), Швеции, Китае, Индии, Италии и других государствах. В них управление выступает ведущим источником качественных преобразований и средством мобилизации всех общественных явлений для решения возникающих проблем. Они направили свои усилия на развитие теории и практики управления, постарались перевести управление на научный уровень.

По мнению блестящего представителя теории государственного управления профессора Г.В. Атаманчука, «Если мы действительно ... хотим жить в условиях благополучия, упорядоченности и безопасности, в стране суверенной, свободной, при реальном соблюдении наших конституционных прав и свобод, то просто обязаны осознать управление в качестве важнейшей социально-философской категории, определяющей как судьбы отдельных людей, так и любых их объединений» [3, с. 38].

Следует отметить, что до появления кибернетики управление рассматривалось как внутренняя простая система. После второй мировой войны с возникновением кибернетики понятие «управление» вошло в число важнейших общенаучных понятий. Понятия «кибернетика», «информация», «система», «обратная связь» и т. д. субординированы или же координированы с понятием «управление». Исследование любого из этих понятий в отрыве от понятия «управление» невозможно. Предметом кибернетики являются законы управления, организации и связи как законы общие для динамики машин, живого организма, общества и других объектов, представляющих собой системы, которым свойственны информация, организация и управление.

Управление – многоаспектное, многогранное, многокачественное явление. Все виды управления, независимо от степени их общности, различаются не только по характеру своих объектов, но и по присущим им целям, методам, принципам, органам и т. д. Управление как со-

циальное явление отличается динамизмом, изменчивостью, способностью приобрести в общественном движении различные уровни и виды.

Как отмечал академик А. И. Берг, имеются три основные области сферы управления:

- › управление системами машин, технологическими процессами и вообще процессами, имеющими место при целенаправленном воздействии человека на природу;
- › управление деятельностью человеческих коллективов, решающих ту или иную задачу;
- › управление процессами, происходящими в живых организмах [4, с. 24].

Социальное управление является публичным управлением, которое включает в себя: а) государственное управление, то есть управление в сфере функционирования государственных органов;

б) негосударственное управление, которое в свою очередь, делится на местное самоуправление, осуществляемое органами местного самоуправления; общественное управление осуществляется в объединениях граждан; коммерческое управление.

Под социальным управлением (имеется в виду сознательное управление) понимается воздействие на общество в целом или его отдельные звенья (производство, социально-политическая и духовная жизнь, отрасли экономики, предприятия и т. п.), с тем чтобы обеспечить сохранение их качественной специфики, их нормальное функционирование, совершенствование и развитие, успешное движение к заданной цели [5, с. 58–59].

Один из видов социального управления – государственное управление – выступает предметом исследования различных наук: философия изучает его как один из видов управления обществом, специфическое выражение самоуправляющих свойств последних; социологов интересует главным образом социальная функция государственного управления, ее реальное и конкретное отражение в общественной жизни; экономисты исследуют преимущественно роль государства в экономике, в управлении экономическими процессами, а также само государственное управление в качестве специфического вида труда. Государственное управление представляет большое поле деятельности для психологов. Государственное управление также привлекает внимание представителей математики, кибернетики и других наук. Охват экономической, социальной, правовой и других сфер общества является основным признаком, отличающим государственное управление от управления вообще.

Поэтому понятие государственного управления требуется рассматривать как междисциплинарное, общенаучное.

В литературе сущность, содержание и значение государственного управления характеризуются так: в системе социальных отношений оно занимает главенствующее место и служит укреплению государства, стабилизации общественных отношений, надежной защите государственных интересов как внутри, так и за его пределами; государственное управление – это эффективное средство проведения в жизнь внутренней, внешней, экономической и оборонной политики. Государственное управление представляет собой главный регулятор в борьбе за поддержание законности, правопорядка, обеспечение социальной справедливости и социально-правовой защиты прав и интересов граждан, юридических лиц и общественных объединений. Государственное управление в целях бесперебойности и эффективности действия требует наличие подготовленного кадрового состава, а также неукоснительного соблюдения государственными служащими предписаний.

Государственному управлению присущи следующие характерные черты: управление имеет место всегда там, где осуществляется совместная деятельность людей; управление обеспечивает сознательную, целенаправленную, совместную деятельность людей; управление достигает своих целей путем организации, т. е. объединения, согласования и координирования поведения и действий людей, выполняя тем самым общие для совместной деятельности людей функции и обеспечивая согласованность между индивидуальными действиями; управление осуществляется на началах подчинения участников совместной деятельности единой воле, чем достигается единообразие и соответствие поставленным задачам этой деятельности; управление осуществляется в организационных отношениях.

Понятие государственного управления.

Исследование понятия управления как социально-юридического института в различных направлениях происходит наряду с раскрытием сущности государственного управления, однако некоторые проблемы до сих пор остаются нерешенными.

В административно-правовой науке нет единого понятия государственного управления. Одни его трактуют с точки зрения сути, реального содержания, другие – форм, в которых оно выступает и в которых функционирует. Наиболее часто оно определяется путем отграничения одних ви-

дов государственной деятельности от других. То есть государственное управление – это вовсе не законодательная и не судебная деятельность. Наиболее распространенным является такое определение: государственное управление – это самостоятельный вид государственной деятельности, которая носит подзаконный, исполнительно-распорядительный характер, органов (должностных лиц) относительно практической реализации функций и задач государства в процессе регулирования экономической, социально-культурной и административно-политической сфер.

Существуют различные взгляды на понятие управления. Оно рассматривается:

- › во-первых, как деятельность; считается, что управление есть особая, своеобразная деятельность, осуществляемая в так называемых управляющих структурах, и направлена на выработку, принятие и реализацию управленческих решений, а также на совершение управленческих действий;
- › во-вторых, как определенный вид влияния в различных природных системах (биологическая, социальная, технологическая и т. д.). Это в известной мере универалистская трактовка управления, связанная с кибернетикой, которая характеризует прямые и обратные связи между различными элементами либо объектами мироздания;
- › в-третьих, как вертикальные – «командно-подчиненные» отношения. Главное здесь видят в том, чтобы любая команда была исполнена. В определенных пределах отношения «команда – подчинение» проявляются в управлении, без них оно невозможно, но такое суждение не раскрывает еще сущности управления и его огромной роли в жизнедеятельности людей;
- › в-четвертых, как целенаправленное воздействие, направленное на управляемый объект [4, с. 109–110].

В процессе развития общества государственное управление проходит путь от простой деятельности к сложной, от одноступенчатого управления к многоступенчатой системе. Во многих научных работах с терминами «воздействие», «влияние», «реальное преобразование» происходят ощутимые изменения. К термину «воздействие» добавляется прилагательное «целесообразное», «целенаправленное», «сознательное», что связывает «управление» с человеком и обществом.

Г.В. Атаманчук считает, что данный подход обладает обширными исследователь-

скими возможностями и создает простор для действительного познания управления, причем путем не игнорирования или исключения других (названных выше) подходов, а их сочетания, интеграции в тех пределах, в которых они характеризуют отдельные стороны, элементы либо свойства управления. Управление в жизни людей и общества проявляется тогда, когда в каких-либо взаимодействиях, отношениях, процессах и т. д. и т. п. присутствует сознательное начало, интерес и знание, цели и воля, энергия и действие человека. Г. В. Атаманчук понятие «государственное управление» рассматривает как способ практического, организационного, сознательного управляющего воздействия на регулирование, поддержание, изменение различных структур общества и жизнедеятельности людей путем применения властных полномочий государством [3, с. 17–20].

Системность государственного управления. Государственное управление как сущность и явление, содержание и форма, воздействие и деятельность, в других своих многогранных выражениях существует реально в единстве и взаимосвязи в качестве сложной, целостной системы [6, с. 15–16].

Идеи системного анализа представляют собой одно из плодотворных средств более глубокого теоретического исследования вопросов управления. Системность придает государственному управлению необходимую мобильность, координацию, субординацию, определенную целеустремленность и эффективность.

Для начала мы можем определить систему как нечто целое, абстрактное или реальное, состоящее из взаимосвязанных, взаимодействующих или взаимозависимых компонентов и элементов. Изменение одного из них с необходимостью вызывает то или иное изменение других, а нередко и системы в целом. От состава, внутренней природы частей и зависит, прежде всего, природа целого, его особенность. В качестве компонента рассматривается одушевленная, социальная, активная единица система государственного управления – человек, коллектив и т. п., сознательно действующая в качестве как субъекта, так и объекта управления.

Взаимодействие элементов (в их структуре) придает управлению особое качество целостного общественного явления. Целое же есть не просто сумма составных частей, а их закономерная структурная связь. С другой стороны, отдельные элементы управления хоть и сохраняют относительно самостоятельность, но,

объективно находясь в закономерной структурной связи, также приобретают новое качество – качество частей, элементов единого целого.

Структура составляет одну из фундаментальных характеристик целостной системы. Структура является внутренней организацией – «топологией» системы. Специфика структуры целостной системы зависит прежде всего от природы частей. Структура системы может быть простой или сложной, устойчивой или неустойчивой, разнообразной или единообразной, определенной или неопределенной.

В управлении одна из подсистем, независимо от ее биологической, социальной или иной природы, называется управляющим устройством, а другая, тоже независимо от ее природы – управляемым устройством. Управляющую систему принято называть субъектом, а управляемую – объектом управления. Соответственно, управление может быть выражено через мнимое действие между субъектом и объектом; оно представляет собой процесс связи управляющей и управляемой подсистем.

Системный анализ предполагает вычленение основных элементов и структуры управления. К первым относятся объект, субъект, цель, принципы и методы управления. Элементы, составляющие систему, могут, в свою очередь, рассматриваться как система более низкого порядка.

Прежде всего, при анализе системы государственного управления особо актуальным является вопрос **о субъекте государственного управления** – центральном, ведущем ее элементе. Он выступает в управлении наиболее активной, творческой, деятельной силой. Сущность субъекта, его природа и характер, целевое назначение и структура, другие качества и проявления определяют особенности соответствующего вида социального управления, придают ему определенные свойства и параметры, т. е. фактически устанавливают его.

Важное место в системе государственного управления принадлежит **управляемым объектам**. Разграничение субъекта и объектов управления и их четкая структурно-функциональная характеристика имеют принципиальный методологический смысл. Непосредственным объектом управления признаются такие волевые проявления, как действия, поступки, поведение людей. Таким образом, субъект управления целенаправленно воздействует, в конечном счете, на волю и сознание людей – участников подлежащих упорядочению общественных отношений.

Человек, коллектив и объединение людей сосредотачивают, конечно, в себе качество компонентов и субъекта и объекта государственного управления. Но также очевидно, что в один и тот же момент они могут сразу выполнять различные функциональные роли: в производственном процессе их главная задача состоит в производстве материальных и духовных благ; при осуществлении управления – в подготовке и реализации государственно-управляющих воздействий. В аппарате государственных органов государственные служащие по иерархии должностей одновременно являются для вышестоящих кадров объектами, а для нижестоящих – субъектами управления.

Связь между субъектом и объектом управления бывает прямой и обратной. **Прямая связь** идет от субъекта – управляющего к объекту – управляемому. Основным показателем достижения – влияние субъекта на объект управления – человека, воздействие на их поведение и деятельность, а также эффективная работа механизма управления. Если действие между частями динамической системы имеет круговой характер, то в ней имеется обратная связь [7, с. 82].

Принцип обратной связи – один из самых важных фундаментальных принципов управления. В отличие от прямой связи, обратная связь является регулирующей связью, которая вместе с тем имеет обслуживающую защитную функцию. Прямая связь, по крайней мере в явно выраженной форме, этой функцией не обладает. По существу, обратная связь реализуется в любом устройстве, с помощью которого выходные характеристики какого-либо процесса или ситуации измеряются и сравниваются с заранее установленным стандартом; в том случае, если значения на выходе отклоняются от стандарта, производится необходимая корректировка. В системах без обратной связи управление осуществляется без контроля исполнения: команды исполнительному звену системы выдаются непрерывно по заданной программе. Если прямая и обратная связи между субъектом и объектом управления нарушаются, то отдельные части объекта и элементы управления распадаются, не выдерживают конкуренции и конфликтной ситуации, возникает разбросанность и противоречивая деятельность. Обратная связь означает обратный поток информации в системы управления, т. е. получение управляющим элементом системы информации об управляемом элементе. Это используется для коррекции процесса управления, для

изменения состояния управляемого элемента в нужном направлении.

Под информацией обычно понимаются сведения об окружающем мире, о внутреннем состоянии системы и внешних условиях, которые управляющая система использует в осуществлении управленческих процессов. Наличие информации необходимо для полноценного целенаправленного управления, для обеспечения принятия оптимальных решений. Без полноценной информации, т. е. без качественных сведений, своевременных, непротиворечивых, точных, идущих по разным каналам и дополняющих друг друга, невозможно ориентироваться и принимать разумные решения, нельзя целенаправленно управлять, без полноценной информации нельзя обеспечить процесс.

Таким образом, любая система управления может быть охарактеризована тремя следующими условиями:

- а) прямой связью между управляющей и управляемой частями системы, по которой поступают сигналы управления;
- б) обратной связью управляемой и управляющей частей;
- в) переработкой информации текущего состояния управляемой системы, идущей по каналам обратной связи, в команды управления.

Взаимосвязи управления и регулирования. В литературе принято различать системы управления и процесс управления. Анализ управления с точки зрения его формы или «структуры» имеет отношение к системе управления, в то время как рассмотрение его содержания или функции относится главным образом к процессам управления.

Имея дело с комплексами взаимодействующих элементов, приходится пользоваться такими заведомо абстрактными понятиями, как регулирование, саморегулирование. Регулирование, присущее процессу управления, является внутренне противоречивым вследствие своей неразрывной связи с процессом регулирования, который в определенном отношении выступает как противоположность управлению. По причине этой неразрывной связи понятия «управление» и «регулирование» обычно употребляются как синонимы. Управление и регулирование не синонимы, хотя явления, составляющие эти понятия, органически взаимосвязаны между собой [8, с. 14]. На практике широко используют три вида управления:

- 1) стратегическое;
- 2) тактическое;

3) стабилизирующее (регулирующее).

Стратегическое управление – динамическое и предназначено для распределения определенных ресурсов по времени рассматриваемого периода. Такое управление в экономической литературе нередко называют долгосрочным управлением. Решение такой задачи требует прогнозирования на период управления контролируемых возмущающих факторов.

Тактическое управление – статическое и предназначено для реализации решений стратегического управления вышестоящего уровня в реальном масштабе времени, т. е. на оперативных интервалах вышестоящего стратегического управления. В экономической литературе такое управление нередко называют краткосрочным управлением.

Стабилизирующее – регулирующее управление предназначено для реализации решений тактического управления вышестоящего уровня на интервалах оперативного управления.

Таким образом, в управлении и регулировании выражаются как бы тактика и стратегия системы в процесс ее взаимодействия с окружающей средой. Регулирование – это как бы тактическое, стабилизирующее средство, а управление – стратегическое средство системы; чем более развито управление, тем ярче и наглядно проявляется диалектика взаимосвязи управления и регулирования [8, с. 93–94]. Регулирование – это основное управление, основа которого в процессе осуществления управления в высокоорганизованных системах как бы циклически возвращается к самой себе, но всякий раз на новой основе. В действительности регулирование, говоря философским языком, это инобытие управления. Управление существует благодаря регулированию. Управление содержит регулирование в качестве своего момента и вместе с тем исходит из него и имеет его своей целью [8, с. 87].

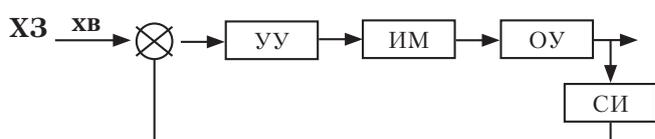
Во всех видах управления, как указано выше, используется принцип обратной связи. Система, реализующая такой принцип управления, в основном состоит из следующих типовых элементов:

- 1) объекта управления (ОУ);
- 2) устройства управления (УУ);
- 3) сравнивающего устройства действительного (реального) и желаемого состояния объекта (СУ);
- 4) средств измерения входных и выходных переменных объекта (СИ);

5) исполнительного механизма (ИМ), реализующего задания УУ.

Структурная схема такой системы представлена на рисунке.

СУ



Источником первичной информации является физические объекты, которые находятся на нижнем (первом) уровне. Информация, используемая на верхних уровнях, формируется на основе информации, полученной на нижнем (первом) уровне путем последовательного ее обобщения.

Система управления в живом организме. Живой организм представляет собой своеобразно устроенную машину, вся работа которой направлена, в конце концов, к тому, чтобы поддерживать индивидуальную жизнь, т. е. сохранять, наперекор разрушающим влияниям, анатомическую и физиологическую целостность тела в течение более или менее долгого времени.

Каждый индивид является классической кибернетической системой. Она состоит из управляющего блока – мозга и объекта управления – тела, эти два блока связаны между собой каналами прямой и обратной связи – нервы, кровеносные сосуды и т. д. В управляющем блоке есть программа – знания, опыт, приобретенные в процессе обучения и воспитания и полученные по наследству. Согласно этой программе и работает система. Авторегуляция в большинстве случаев передается по наследству, начинает работать при строго определенных условиях и совершается автоматически и абсолютно независимо от последующего изменения этих условий.

В отличие от систем управления обществом и процессами технических объектов, данная система является более сложной, так как она осуществляется на атомном и молекулярном уровне. При этом с целью моделирования процессов, происходящих в организме и в каждой клетке, непосредственное измерение первичных параметров не представляется возможным. Сложность также заключается в том, что управление осуществляется нервной системой, состоящей более чем из 100 млрд нейронов. Причем все эти нейроны взаимосвязаны, и каждый нейрон имеет информацию об остальных нейронах. Управление строено по принципу системной иерархичности: элементарные процессы жизне-

деятельности подчинены сложным системным зависимостям (по принципу соподчинения низших отделов высшим). Низшие уровни управления обеспечиваются автоматическими системами регулирования, поддерживающими заданный режим жизнедеятельности.

Среди многочисленных тайн природы, над раскрытием которых работает современная наука, пожалуй, самой грандиозной является высший управляющий аппарат – головной мозг. Начиная с середины XIX века, наука вплотную подошла к исследованию деятельности головного мозга как главного центра управления в живых организмах [9, с. 115].

Одной из особенностей управления в живом организме является то, что «управляющее устройство» в живой авторегуляционной системе одновременно является потенциальным «управляемым устройством» и наоборот. В биологической и социальной системах управления во многих случаях нет такого жесткого разделения на «управляемые» органы, к которым мы привыкли в технике. Так, механизмы управления внутри клетки обладают переменной функцией, они сами управляются и регулируются [9, с. 204]. Можно заметить, что регулирование (особенно авторегуляция) в живых организмах играет несравнимо более важную и необходимую роль, чем в технических устройствах.

Деятельность живого организма можно рассматривать как авторегуляционный процесс, тождественный по своей структуре управлению обратной связи. Если человеческий организм представляет собой в определенном отношении систему управления, сходную с системой управления с обратной связью, то она в связи с высочайшим уровнем организации и сложности человеческого существа должна представлять собой наиболее сложную и разнообразную систему управления многочисленными обратными связями. В живом организме, как правило, все процессы происходят на основе обратной связи. Управляющие системы живых организмов многоуровневые и настройка низших уровней определяется состоянием высших. Эволюция высших уровней приводит к повышению устойчивости за счет передачи соответствующих функций низшим уровням.

В отношении мышц и многих желез как рабочих органов нервная система представляет собрание разнообразных регуляторов их деятельности, при этом действие регуляторов должно быть согласовано с интересами организма, в смысле обеспечения анатомической и физиоло-

гической сохранности тела. Центральная нервная система координирует физиологические функции (адаптации, рефлекторные реакции, гомеостаз и др.), определяя их ритм и общую направленность. В свою очередь, частные формы физиологических функций оказывают влияние на высший управляющий аппарат (головной и спинной мозг). Такая форма контроля и взаимного влияния физиологических функций является главным содержанием принципа системного управления в организме человека.

Создатель кибернетики Н. Винер указывает, что центральная нервная система уже не представляется автономным, независимым органом, получающим раздражения от органов чувств и передающим их в мышцы. Наоборот, некоторые характерные виды деятельности центральной нервной системы объяснимы только как круговые процессы, идущие от нервной системы в мышцы и снова возвращающиеся в нервную систему через органы чувств. При этом не важно, являются ли эти органы чувств проприоцепторами или внешними органами чувств. Нам казалось, что такой подход означает новый шаг в изучении того раздела нейрофизиологии, который затрагивает не только элементарные процессы в нервах и синапсах, но и деятельность нервной системы как единого целого [10, с. 19].

Отдельные элементы организма и его структуры являются целесообразными, потому что это отражает общие задачи управления в своих особенностях, и все вместе взаимно дополняют друг друга, образуя хорошо сыгранный оркестр, где каждый является одновременно и дирижером и исполнителем, и каждая часть организма является не только частью организма, но и частью управления.

Сосуды органа являются исполнительным звеном системы регулирования, реализация регулирующих влияний определяется исходными биофизическими свойствами сосудов.

В человеческом теле заложены бесчисленные регулирующие приспособления, основанные на принципе обратной связи, которые автоматически подстраиваются к изменяющимся условиям окружающей среды. Одной из важных физиологических функций организма является ритмичность; при этом процессы жизнедеятельности организма периодически усиливаются или ослабляются под влиянием экзогенных и эндогенных факторов (биологическая ритмичность). Эти ритмы классифицируются как проявления физической, эмоциональной и интеллектуальной активности.

Это специфическая форма обратной связи, проявляющаяся в поддержании физиологического равновесия, уже давно была известна биологам под названием «гомеостазис». Основная идея гомеостазиса состоит в том, что организм так изменяет свои внутренние и внешние связи, чтобы сохранить постоянство ряда существенных для него показателей внутренней среды [9, с. 58]. Гомеостазис наблюдается во всех без исключения системах управления. Клетке свойственно явление, сходное с гомеостазисом. Клетка способна защитить себя от сил окружающей среды, которые стремятся ее разрушить. Любая клетка тела человека обладает авторегуляцией по принципу обратной связи. Гомеостазис охватывает вегетативную систему, гуморальную систему и физико-климатическую систему организма [9, с. 73]. Соотношение поведения, функций, размеров и форм организма является одновременно и результатом саморегулирования.

Системный подход в физиологии выступает в качестве того связующего элемента, который позволяет рассматривать функции живого организма как единство структуры и функции, осуществляемое в пространственно-временных параметрах. Этот принцип вытекает из основных законов диалектики и может служить методологическим фундаментом для раскрытия физиологических закономерностей.

Таким образом, управление представляет собой универсальное социальное явление, которое аналогично принципам, осуществляемым в машине, живом организме и обществе.

Литература

1. Маркс К., Энгельс Ф. Полное собрание сочинений. 2-е изд., т. 23.
2. Рзаев А. Г. Государственная служба: организационно-правовые аспекты. – Баку : Элм, 2013, – 560 с.
3. Атаманчук Г. В. Управление в жизнедеятельности людей. – М. : РАГС, 2008. – 400 с.
4. Афанасьев В. Г. Научное управление обществом (опыт системного исследования). 2-е изд. – М. : Политиздат, 1973. – 392 с.
5. Афанасьев В. Г. Человек и управление обществом. – М. : Политиздат, 1977. – 382 с.
6. Атаманчук Г. В. Сущность государственного управления. – М. : Юридическая литература, 1980. – 256 с.
7. У. Росс Эшби. Введение в кибернетику. – М. : Иностранная литература, 1959. – 432 с.
8. Петрушенко Л. А. Принцип обратной связи. – М. : Мысль, 1967. – 277 с.
9. Парин В. В., Баевский Р. М. Введение в медицинскую кибернетику. – М. : Медицина, 1966. – 145 с.
10. Ноберт Винер. Кибернетика, или Управление и связь в животном и машине. – М. : Советское радио, 1958. – 215 с.





**Цирлов
Валентин
Леонидович**
кандидат технических
наук, доцент



Никулин Михаил Юрьевич

Правовые основы сертификации средств защиты информации

Аннотация: в статье приведен обзор основных законодательных актов и нормативных документов, лежащих в основе сертификации средств защиты информации по требованиям безопасности информации. Рассматривается структура основных систем обязательной сертификации. Проводится сравнительный анализ правовых аспектов организации каждой из систем сертификации.

Ключевые слова: техническое регулирование, обязательная сертификация, защита тайн.

Задача сертификации средств защиты информации по требованиям безопасности информации возникает при построении автоматизированных систем различного уровня во многих отраслях экономики [1]. Несмотря на то, что наиболее сложными при планировании и реализации сертификационных испытаний остаются технические аспекты, правовые особенности данного вида работ также имеют ряд нюансов и заслуживают отдельного рассмотрения.

В основе любого рода деятельности по оценке соответствия, и, в частности, сертификации средств защиты информации лежит Федеральный закон от 27.12.2002 г. №184-ФЗ «О техническом регулировании». В данном законе под подтверждением соответствия понимается документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров. В свою очередь, одной из форм подтверждения соответствия является сертификация. В области информационной безопасности под сертификацией понимают деятельность третьей стороны по подтверждению характеристик средств защиты информации требованиям нормативных документов по защите информации [10].

При этом Статья 5 названного ранее Закона №184-ФЗ ставит особняком вопросы технического регулирования в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну.

Тем самым различные виды сведений, отнесенных к категории ограниченного доступа (см. Таблицу 1), предполагают наличие различных нормативных требований для соответствующих средств защиты информации [3,4]. Впрочем, на практике большая часть перечисленных в Таблице 1 видов тайн рассматривается просто как конфиденциальная

информация, особняком стоят вопросы организации сертификационных испытаний средств защиты информации, предназначенных для защиты государственной тайны, персональных

данных, а также ряда более специфических видов защищаемой информации [14].

Так, например закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной

Таблица 1

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Статья 5 Закона РФ от 21.07.1993 N 5485-1 «О государственной тайне»
	Указ Президента РФ от 30.11.1995 N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»
Коммерческая тайна	Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»
	Статья 12 Федерального закона от 28.11.2011 № 335-ФЗ «Об инвестиционном товариществе»
Персональные данные	Статья 7 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»
Прочие виды тайн	Соответствующие законы РФ

тайне» определяет именно сертификацию как единственную форму оценки соответствия таких средств защиты. Статья 28 Закона № 5485-1 гласит, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. При этом организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Тем самым, детализация требований по организации соответствующих систем сертификации возложена, соответственно, на ФСТЭК России, ФСБ России и Минобороны России. Все системы сертификации имеют схожую организационную структуру, указанную на рис. 1.

В ряде случаев федеральный орган выполняет роль органа по сертификации. Как правило, схема проведения сертификации выглядит следующим образом:

Заявитель (это либо разработчик, либо другая компания, заинтересованная в проведении сертификации) подает в федеральный орган по сертификации заявку на проведение сертификационных испытаний некоторого продукта.

Федеральный орган определяет испытательную лабораторию и орган по сертификации.

Испытательная лаборатория, находясь в постоянном контакте с заявителем, проводит сертификационные испытания. Если в процессе испытаний выявляются те или иные несоответствия заявленным требованиям, то они могут быть устранены заявителем в рабочем порядке – что происходит в большинстве случаев, или

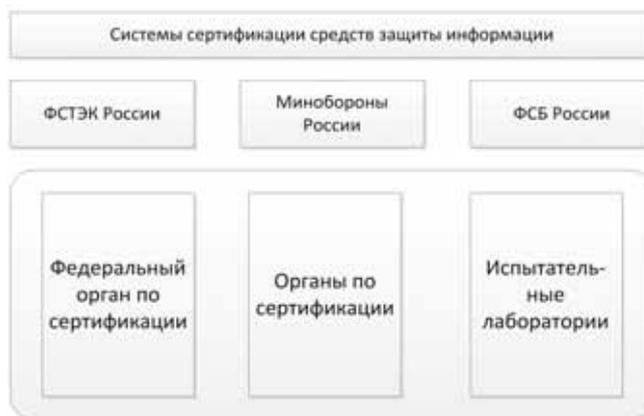


Рис.1. Обобщенная структура основных систем сертификации

же может быть принято решение об изменении требований к продукту – например, о снижении класса защищенности. Безусловно, возможен вариант, когда сертификационные испытания завершаются с отрицательным результатом.

Детальные протоколы испытаний передаются в орган по сертификации, который проводит их независимую экспертизу. Как правило, в данной экспертизе участвуют не менее двух экспертов, которые независимо друг от друга должны подтвердить, что испытания проведены корректно и в полном объеме [10].

Федеральный орган по сертификации на основании заключения органа по сертификации оформляет сертификат соответствия.

Следует сказать, что заявитель на сертификацию должен иметь лицензию на право работы в области создания средств защиты информации, а испытательная лаборатория и орган по сертификации – соответственные аттестаты аккредитации [15].

Что касается документов, на соответствие которым проводятся сертификационные испытания, то они практически идентичны во всех системах сертификации. Существуют два основных подхода к сертификации – и, соответственно, два типа нормативных документов [11].

Функциональное тестирование средств защиты информации, позволяющее убедиться в том, что продукт действительно реализует заявленные функции. Такое тестирование чаще всего проводится на соответствие конкретному нормативному документу – например, одному из руководящих документов Гостехкомиссии России. Такие документы существуют, например, для межсетевых экранов, для средств защиты от несанкционированного доступа. Если же не существует документа, которому сертифицируемый продукт соответствовал бы в полной мере, то функциональные требования могут быть сформулированы в явном виде – например, в Технических условиях, или в виде Задания по безопасности (в соответствии с положениями стандарта ГОСТ Р 15408). В системе сертификации ФСТЭК России для ряда классов СЗИ (в частности, для систем обнаружения вторжений и антивирусов) разработаны современные нормативные документы на базе «Общих критериев» [2–5].

Тестирование программного кода на отсутствие недекларированных возможностей – т.е. возможностей, не описанных или не соответствующих описанным в документации [8]. Классическим примером недекларированных

возможностей являются программные закладки - внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию [7,9,13]. Выявление недекларированных возможностей предполагает проведение определенных тестов в отношении исходных текстов программного обеспечения – соответственно, предоставление исходных текстов является необходимым условием для возможности проведения сертификационных испытаний [6].

В большинстве случаев средство защиты информации должно быть сертифицировано как в части основного функционала, так и на предмет отсутствия недекларированных возможностей.

Важным моментом сертификации является выбор схемы сертификации, а именно: партии (одного или нескольких изделий) или серии (типового образца). В случае серии организация-заявитель должна дополнительно пройти спецэкспертизу по проверке возможности осуществлять производство средств защиты информации. В настоящее время Техническим комитетом по стандартизации ТК-362 «Защита информации» проводятся изыскания по формированию требований к системам менеджмента информационной безопасности в части управления безопасным производством программных СЗИ [1,16].

В заключение необходимо отметить, что на сегодняшний день фактически не существует процедуры взаимного признания сертификатов соответствия между различными системами сертификации средств защиты информации – существуют лишь единичные случаи, когда решение о возможности использования материалов испытаний, полученных в рамках работ в другой системе, принимается федеральным органом по сертификации в индивидуальном порядке. На наш взгляд, разработка системы унификации требований могла бы стать интересным направлением нормотворческой деятельности.

Литература

1. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). – С.37–41.
2. Барабанов А.В., Марков А.С., Фадин А.А. Сертификация программ без исходных тек-

- стов // Открытые системы. СУБД. 2011. № 4. – С.38–41.
3. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. – С.31–33.
4. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. Спецвыпуск №5 «Информатика и системы управления». – С.272–278.
5. Барабанов В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. – С. 48–52.
6. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1(2). – С. 40–48.
7. Клянчин А.И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). – С. 60–65.
8. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Южного федерального университета. Технические науки. 2006. Т. 62. № 7. – С. 82–87.
9. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1(1). – С.42–48.
10. Марков А.С., Цирлов В.Л. Сертификация программ: мифы и реальность // Открытые системы. СУБД. 2011. № 6. – С.26–29.
11. Марков А.С., Цирлов В.Л., Маслов В.Г., Олексенко И.А. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики. 2009. Т.2, №12. – С.2–6.
12. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). – С.61–64.
13. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1(2). – С. 36–39.
14. Федичев А.В., Артамошин С.А. Систематизация видов отношений и ответственности при получении доступа к информации // Вопросы кибербезопасности. 2014. № 2 (3). – С. 51–59.
15. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации // Вопросы кибербезопасности. 2013. № 1(1). – С.49–54.
16. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. – С. 4–14.





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

Электронные денежные переводы в современном банковском законодательстве

***Аннотация:** работа посвящена вопросам развития правового регулирования электронных денежных переводов в современном банковском законодательстве Российской Федерации.*

***Ключевые слова:** электронные деньги, электронные средства платежа, национальная платежная система, коммерческие банки, небанковские кредитные организации.*

Банковские услуги в условиях рыночной экономики становятся важнейшим источником увеличения банковских доходов и удовлетворения потребностей корпоративных клиентов и частных лиц в качественных банковских услугах.

С начала XXI века резко возрос оборот платежной системы как в отношении числа электронных переводов денежных средств, так и в отношении объема переводимых электронных денежных средств. Это отразило в первую очередь быстрый рост активности финансового рынка.

Национальная платежная система играет ключевую роль в экономике страны, обеспечивая перевод денежных средств, в том числе при реализации единой государственной денежно-кредитной политики.

С учетом анализа текущего состояния национальной платежной системы и оказывающих влияние на ее развитие факторов Банк России определил следующие направления ее развития [1]:

- › совершенствование регулирования и правоприменения в национальной платежной системе;
- › развитие платежных услуг;
- › развитие платежных систем и платежной инфраструктуры;
- › повышение консультативной и координирующей роли Банка России в национальной платежной системе;
- › развитие национальной и международной интеграции.

При этом формирование задач в рамках каждого из указанных направлений и их реализация будут осуществляться при следовании Банком России следующим принципам:

- › позиционирование банковской системы Российской Федерации в качестве институциональной основы рынка платежных услуг;
- › соразмерность регулирования, надзора и наблюдения в национальной платежной системе рискам, присущим деятельности ее субъектов и связанным с нарушением бесперебойности функционирования платежных систем, ухудшением качества, снижением безопасности оказания платежных услуг, легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма;
- › открытость процесса развития национальной платежной системы на основе взаимодействия Банка России, заинтересованных органов государственной власти Российской Федерации, профессио-

нальных объединений участников рынка платежных услуг;

- применение в национальной платежной системе национальных стандартов, разработанных с учетом международных стандартов;
- поддержка добросовестной конкуренции на рынке платежных услуг.

Кредитные организации стали стремиться к наибольшей прозрачности, открытости перед клиентами: в них внедряются передовые бизнес-модели и новые банковские технологии (клиент-банк, системы электронных денежных переводов, дебетовые и кредитные карты и т. д.).

Появилась возможность использования передовых современных технологий, при внедрении которых средства могут перемещаться в рамках платежной системы значительно быстрее, что привело к появлению большого количества разнообразных электронных платежных систем и электронных денежных переводов.

Новые банковские технологии позволяют разрабатывать технологические решения, которые обеспечивают сокращение сроков прохождения электронных платежей и совершенствовать расчеты электронными денежными средствами¹.

В соответствии с Федеральным законом от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» [2] до заключения договора с клиентом кредитная организация предоставляет ему информацию:

- о мерах безопасного использования электронных денежных переводов;
- о возможных дополнительных требованиях и ограничениях при использовании электронных денежных переводов в зависимости от оценки риска;
- о способах и сроках уведомления о совершении каждой операции с использованием электронных средств платежа;
- кредитная организация может страховать собственные риски, связанные с совершением операций с использованием электронного средства платежа, без согласия клиента, а также может обеспечивать возможность

страхования клиентом рисков, связанных с совершением операций с использованием электронных средств платежа;

- кредитная организация в зависимости от условий заключенного договора об использовании электронных средств платежа и с учетом оценки риска, правил платежной системы, участником которой является кредитная организация, может выбирать любые доступные способы уведомления клиента в электронном виде и (или) на бумажном носителе.

При заключении с клиентом договора об использовании электронного средства платежа кредитная организация на основе предоставленной клиентом и иной доступной информации оценивает степень риска, связанного с предоставлением клиенту конкретного вида электронных денежных переводов, и предоставляет клиенту соответствующее электронное средство платежа с учетом результатов оценки риска [3].

На сегодняшний день основной неразрешенной проблемой на пути развития электронных денежных переводов следует признать несовершенство правового регулирования электронных денежных переводов в современном банковском законодательстве Российской Федерации.

Цель правового регулирования формирующихся в электронном виде платежных отношений – выработка правил осуществления электронных денежных переводов. Остается актуальным рассмотрение путей регулирования таких отношений, в том числе на основе механизмов обеспечения переводов электронными денежными средствами. При этом необходимость осуществления такого правового регулирования данной сферы банковской деятельности находится в интересах устойчивого развития российской банковской системы и всего российского общества.

Таким образом, на наш взгляд, особое внимание в современном банковском законодательстве Российской Федерации должно быть уделено развитию правового регулирования электронных денежных переводов.

Большинство банковских операций сегодня выполняется при помощи электронных денежных средств и пластиковых карточек, которые вышли на передовые позиции в организации платежного оборота Российской Федерации. Осуществление электронных денежных платежей объективно является основной операцией многих российских банков, а внесение изменений и дополнений в современное банковское законодательство будет способствовать

¹ Федеральный закон от 27.06.11 № 161-ФЗ «О национальной платежной системе» содержит определение электронных денежных средств как денежных средств, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

развитию правового регулирования электронных денежных переводов в банковском законодательстве Российской Федерации.

На наш взгляд, целесообразно будет

1. ввести в ГК РФ новый вид гражданско-правового договора – договор на предоставление электронных средств платежа;
2. внести в Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» следующие изменения и дополнения:
 - › определить перечень существующих видов электронных средств платежа и их признаки;
 - › добавить норму о необходимости двойного уведомления клиента с помощью телекоммуникационных средств, обеспечивающих обратную связь, после совершения операции по списанию и в виде выписок со счета;
 - › расширить способы пополнения клиентами остатка электронных денежных средств путем внесения юридическим лицом наличных денежных средств, перевода без открытия счета, совершения перевода электронных денежных средств со счета на счет;
3. внести изменения в Федеральный закон от 23 декабря 2003 г. № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации» и страховать электронные денежные средства физических лиц, находящихся на персональных электронных счетах, а операторам электронных денежных средств разрешить вступать в систему страхования вкладов;

4. разработать правовой механизм возврата списанных мошенническим путем электронных денежных средств, включая предоставление операторам электронных денежных средств права временно блокировать отправленные электронные денежные средства;
5. разработать регламент действий операторов электронных денежных средств и телекоммуникационных компаний при временном разрыве связи между моментом доступа к информации о платеже банка-получателя и банка-отправителя и самой системы управления рисками.

Перед российским банковским правом сегодня открывается, быть может, уникальная возможность не только установить правовые основы уже сформированных общественных отношений, но и усовершенствовать правила осуществления электронных денежных переводов.

Литература

1. Стратегия развития национальной платежной системы (одобрена Советом директоров Банка России 15.03.2013, протокол № 4).
1. Федеральный закон от 27.06.11 № 161-ФЗ «О национальной платежной системе». // Собрание законодательства Российской Федерации, выпуск № 27, 2011 г., ст. 3872.
2. <Письмо> Банка России от 14.12.2012 № 172-Т «О Рекомендациях по вопросам применения статьи 9 Федерального закона „О национальной платежной системе“».





**Ерохина
Юлия
Владимировна**
кандидат юридических
наук, доцент

Проблемы информационного обеспечения противодействия коррупции

***Аннотация:** выявлены новые тенденции по противодействию коррупционной деятельности, связанные с развитием информационных составляющих. На основе использования приемлемых методов противодействия коррупции в Российской Федерации и Республике Беларусь разработаны предложения по улучшению антикоррупционной деятельности. Информационную базу статьи составляют документы официальной статистики, научно-аналитические материалы и доклады, данные международной статистики, документы и аналитические разработки социально-экономического развития России и Беларуси, статьи научной и периодической печати и прочие источники..*

***Ключевые слова:** противодействие коррупции, информационная безопасность, информация, антикоррупционная политика.*

Современное общество называют информационным, так как информация образует важнейший элемент его жизнедеятельности. Информатизация, как процесс перехода к информационному обществу коснулась всех сфер человеческой жизни. Успешное решение задач, стоящих перед органами государственной власти, сегодня невозможно без использования информационных технологий.

По справедливому замечанию Т.Т. Гапоева, «Информация – это образование, коммерция, творчество, независимость от коррупционера и бюрократа. Она стимулирует внутренний спрос, помогает стартапам, без нее немыслимы инновационные прорывы, привлечение иностранных инвестиций. В итоге информация способствует повышению конкурентоспособности нашей экономики. Для того чтобы россиянин получал необходимую информацию в любом месте и в требуемом объеме, нужны новые технологии, инфраструктура, грамотное экономическое регулирование, образование. Для решения этих задач предусмотрено несколько основных направлений работы: снижение технических ограничений и снятие экономических порогов доступа к информации, а также преодоление бюрократических, ведомственных, давно устаревших нормативных барьеров доступа к информации»[1.].

Проблема противодействия коррупции является одним из ключевых направлений обеспечения национальной безопасности наряду с общими проблемами противодействия организованной преступности и построения информационного общества.

Противодействие коррупции – это мера защиты общества, государства, основных прав и свобод человека от одного из наиболее опасных видов правонарушения, все более приобретающего транснациональный и организованный характер и требующего для борьбы с ним консолидации всех институтов государства и гражданского общества (Модельный закон «О противодействии коррупции», принятый на тридцать первом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (Постановление от 25 ноября 2008 г. № 31-20)).

В целях сбора, хранения, анализа и обобщения информации о фактах, свидетельствующих о коррупции, в том числе о физических

и юридических лицах, причастных к коррупции, в специальных подразделениях по противодействию коррупции создаются и ведутся оперативные учеты и централизованные банки данных.

В современных условиях глобализации негативное влияние коррупции на развитие экономики и государства в целом очевидно и носит не только национальный, но и международный характер, при этом развивающаяся информационная сфера является для этого благоприятной средой.

Конвенция ООН против коррупции, равно как и Конвенция Совета Европы об уголовной ответственности за коррупцию, ратифицированные Российской Федерацией в 2006 г., содержат рекомендации по разработке национальной антикоррупционной стратегии. Согласно ст. 5 Конвенции ООН «каждое государство-участник в соответствии с основополагающими принципами своей правовой системы разрабатывает и проводит эффективную и скоординированную политику противодействия коррупции, способствующую участию общества и отражающую принципы правопорядка, надлежащего управления публичными делами и публичным имуществом, честности и неподкупности, прозрачности и ответственности».

Антикоррупционная политика, проводимая Россией, заключается в разработке и осуществлении разносторонних и последовательных мер государства и общества по устранению причин и условий, порождающих и питающих коррупцию в разных сферах жизни, в том числе и информационной сфере.

Среди мер по предупреждению коррупции, закрепленных в Конвенции ООН против коррупции 2003 г. и представленных в международных антикоррупционных программах, таких как Глобальная программа ООН против коррупции, Программа Группы государств против коррупции (GRECO), приоритетное значение придается мерам, направленным на обеспечение прозрачности и доступа к информации.

Важнейшую основу для государственного управления представляют базовые системы подотчетности применительно к размещению и использованию государственных средств. Бюджет любой страны должен прежде всего отражать все направления деятельности государства, в связи с чем «прозрачность и доступность информации» об управлении государственными расходами является одним из основных факторов обеспечения контроля и надзора за деятельностью государственных органов.

В Российской Федерации обязанность органов государственной власти и органов местного самоуправления, их должностных лиц обеспечивать каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, закреплена в Конституции Российской Федерации (ч. 2 ст. 24). Данный конституционный принцип реализован в ряде законодательных актов, в частности в Федеральном законе «Об информации, информационных технологиях и о защите информации», направленном на регулирование отношений, возникающих при формировании и использовании информационных ресурсов на основе создания, распространения и предоставления потребителю документированной информации, защите информации, прав субъектов, участвующих в информационных процессах.

Были проанализированы электронные порталы органов государственной власти всех субъектов Российской Федерации (в случае отсутствия портала – сайты органов законодательной и исполнительной власти субъекта Российской Федерации) на предмет наличия и объема содержащейся информации о проводимых в субъекте мероприятиях по противодействию коррупции, а также выявления степени доступности к указанной информации. Полнота размещенной информации о деятельности органов государственной власти в области противодействия коррупции в субъектах Российской Федерации различна:

- 1) информация содержится на главной странице официального информационного портала или сайта органа государственной власти субъекта Российской Федерации – 42 (50,6%);
- 2) доступ к информации осуществляется через подразделы главной страницы информационного портала или сайта органа государственной власти субъекта Российской Федерации – 24 (28,9 %);
- 3) доступ к тексту федеральных актов в сфере противодействия коррупции – 48,1%;
- 4) доступ к тексту актов субъектов Российской Федерации в сфере противодействия коррупции – (67,4%);
- 5) перечень федеральных актов в сфере противодействия коррупции – 46,9 %;
- 6) перечень актов субъектов Российской Федерации в сфере противодействия коррупции – (39,7%);
- 7) наличие «горячей линии», «телефона доверия» – 48,1%;

- 8) планы и мероприятия – 39,7 %;
- 9) отчеты, доклады – 40,9%;
- 10) доступ к информации органа, образованного в целях оказания содействия по реализации государственной политики в области противодействия коррупции – 32,5%;
- 11) антикоррупционная экспертиза актов – 46,9%;
- 12) антикоррупционный мониторинг – 1,2% [2.].

Согласно ст. 8 Федерального закона «Об информации, информационных технологиях и о защите информации» «граждане (физические лица) и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами». Доступ к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну) не может быть ограничен.

Право заинтересованных лиц и граждан на доступ к информации также закреплено в Федеральном законе от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», в соответствии с которым пресс-службы федеральных органов государственной власти ведут аудио- и видеозапись всех официальных мероприятий с участием Президента Российской Федерации, заседаний Совета Федерации и Государственной Думы, Правительства Российской Федерации и его Президиума.

Важную роль в формировании общественного мнения, как отмечается в Глобальной программе ООН против коррупции, играют журналисты, что особенно актуально при построении информационного общества. Они создают для потенциальных коррупционеров дополнительный риск быть раскрытыми, поднимают уровень нетерпимости граждан к коррупции, мобилизуют общество на противодействие коррупции. В связи с этим в России на сегодняшний день важной остается задача создания условий для беспристрастности средств массовой информации, при которой журналисты могут честно и правдиво освещать факты коррупции и антикоррупционные инициативы.

Перед Российской Федерацией стоит задача формирования системной антикоррупционной стратегии, приоритетным направлением которой должны стать положения, предотвраща-

ющие коррупционные проявления во всех сферах жизни. Для практической реализации которых необходимо соблюдение принципа верховенства права и реального обеспечения доступа к информации о деятельности государственных органов власти и органов местного самоуправления, являющихся одними из ключевых при построении информационного общества.

В Российской Федерации в структуре МВД создан Департамент информационных технологий, связи и защиты информации, что стало одним из важных этапов масштабного реформирования ведомства. Внедрение информационных технологий – многоаспектный процесс, предполагающий наличие единого организующего центра.

Структура Департамента отражает четыре основных направления его деятельности: совершенствование информационных, телекоммуникационных технологий и систем, координацию работ по обеспечению функционирования систем связи, техническую защиту информации, реализацию государственных и ведомственных программ в области информатизации. Выполнение соответствующих задач возложено на четыре основных управления Департамента.

Первое управление должно вырабатывать общую концепцию, планировать вопросы информатизации, разрабатывать технические документы. Второе управление, к компетенции которого относятся вопросы связи, существовало в структуре МВД России и затем было передано в состав Департамента, созданного в структуре МВД.

На Третье управление возложено решение вопросов, связанных с защитой информации, в том числе конфиденциальной, и персональных данных.

Деятельность Четвертого управления относится к внедрению информационных технологий. Сотрудники управления отвечают за взаимодействие с федеральными органами исполнительной власти по вопросам информатизации, предоставление государственных услуг (исполнение государственных функций) в электронном виде, координацию работы по обеспечению функционирования государственной системы изготовления, оформление и контроль паспортно-визовых документов нового поколения (напомним, что именно МВД России является координатором выполнения указанных работ), системы «112», спутниковой системы ГЛОНАСС и других.

Защита информации – важнейшее направление деятельности. В первую очередь важно

защитить персональные данные, поскольку защищенность личной информации в достаточной степени определяет уровень защищенности личности от противоправных посягательств, и данная взаимообусловленность постоянно возрастает.

Ранее вопросы защиты ведомственных баз данных, а также ведомственных сегментов МВД межведомственных банков данных от утечек информации решали структуры, входившие в состав различных департаментов министерства, что придавало этой работе характер разрозненности и разобщенности. Передача данных функций Департаменту информационных технологий позволит консолидировать эту деятельность, повысить уровень контроля, ответственности конкретных сотрудников за обеспечение защищенности информации и, в конечном счете, минимизировать риск ее неправомерного использования.

Каждое направление работы министерства предполагает определенные программно-технические решения, по сути – наличие отдельных мини-систем. Наиболее актуальные сферы, подлежащие информатизации: деятельность участковых уполномоченных, подразделений ГИБДД, учет вооружения, а также учет лиц, совершивших преступления.

Один из наиболее важных результатов этой работы – максимально облегчить процесс получения населением государственных услуг и исполнения государственных функций. В этих целях, в числе прочего, будут использованы возможности Единого портала государственных и муниципальных услуг (функций). У граждан должна быть возможность получить в любое удобное для них время, даже не выходя из дома, исчерпывающую информацию о предоставлении любой государственной услуги (исполнении государственной функции), входящей в компетенцию МВД России: месте расположения и графике работы соответствующего подразделения, документах, которые необходимо подать (в том числе с возможностью получения в электронном виде формализованных образцов этих документов), а также по иным вопросам.

При этом, помимо наличия специальных знаний в предметной области и опыта работы, важна способность человека в сжатые сроки осознать поставленные перед ним задачи и избирать наиболее эффективные пути их решения.

Однако в этом направлении необходимо изучать, анализировать и внедрять передовой опыт, имеющийся в деятельности иных федеральных органов исполнительной власти

(Минкомсвязи России, ФНС России, ФСБ России, Минтранса России, Минэкономразвития России), органов государственной власти субъектов РФ. Кроме того, не следует забывать о необходимости взаимодействия с экспертным сообществом. Рекомендации со стороны ученых, высказываемые ими при оценке правоприменительной практики, зачастую позволяют находить новые и эффективные пути решения имеющихся проблем. В свою очередь, указанное взаимодействие дает возможность представителям научно-исследовательских учреждений более подробно знакомиться с правоприменительной практикой, проблемами, возникающими в практической сфере.

Взаимодействие с экспертным сообществом по линии работы Департамента информационных технологий, связи и защиты информации МВД России будет осуществляться в формате деятельности научно-технического совета МВД России по науке и передовому опыту.

В связи с этим примечателен передовой опыт и других государств СНГ.

Так, в соответствии со ст. 12 Закона Республики Беларусь «О борьбе с коррупцией» обязанность ведения информационного банка данных для борьбы с коррупцией возложена на прокуратуру.

Основой для первой базы данных в Беларуси является Единый государственный банк данных МВД обо всех уголовных преступлениях и административных правонарушениях, из которого прокуратура собирает сведения о фактах, свидетельствующих о коррупции или создающих условия для совершения коррупционных преступлений. Эти сведения хранятся и обрабатываются в электронном виде на серверах Генеральной прокуратуры Республики Беларусь.

Вторая база данных ведется непосредственно в прокуратуре и формируется на основе результатов прокурорских проверок и информации, предоставляемой из МВД, КГБ и других источников.

Порядок создания и функционирования Единого информационного банка регулируется Законом Республики Беларусь от 9 января 2006 г. «О Единой государственной системе регистрации и учета правонарушений», Постановлением Совета Министров Республики Беларусь от 20 июля 2006 г. № 909 «Об утверждении Положения о порядке функционирования Единой государственной системы регистрации и учета правонарушений»; Постановлением Совета Министров Республики Беларусь от 22 февраля 2008

г. № 251 (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 54, 5/26865), Постановлением Совета Министров Республики Беларусь от 23 декабря 2008 г. № 2010 (Национальный реестр правовых актов Республики Беларусь, 2009 г., № 14, 5/29066), Постановлением Совета Министров Республики Беларусь от 19 мая 2009 г. № 646 (Национальный реестр правовых актов Республики Беларусь, 2009 г., № 131, 5/29780) и т.д.

Регистрацию административных правонарушений осуществляют государственные органы и иные государственные организации (их территориальные структурные подразделения или органы), должностные лица которых в соответствии с законодательством Республики Беларусь наделены полномочиями составлять протоколы об административных правонарушениях либо рассматривать дела об административных правонарушениях, а также суды.

Регистрируют преступления органы предварительного расследования, прокуроры, общие суды, а также органы, осуществляющие исполнение наказаний. Учет правонарушений ведется в информационно-аналитических подразделениях органов внутренних дел.

Сведения об административных правонарушениях, по которым вынесены и вступили в законную силу постановления о наложении административного взыскания или указанные постановления отменены (изменены), помещаются в банк данных регистрационной информации о правонарушениях, по техническим каналам передачи данных либо на магнитных (электронных) носителях информации (далее – по электронным каналам); ежедневно по рабочим дням эти сведения передаются регистрирующими органами в учетное подразделение по месту нахождения регистрирующего органа. Передача же регистрирующими органами сведений об административных правонарушениях на бумажных носителях не допускается.

Сведения о преступлениях, помещенные по электронным каналам в банк данных регистрационной информации о правонарушениях, ежедневно по рабочим дням орган предварительного расследования передает в учетное подразделение по месту нахождения данного органа.

Сведения о преступлениях, зафиксированные прокурором в регистрационных карточках, ежедневно по рабочим дням передаются нарочным или направляются по почте в учетное подразделение по месту нахождения органа предварительного расследования, в производ-

стве которого находилось или находится данное уголовное дело.

Сведения о преступлениях, которые зафиксированы в регистрационных карточках и помещены в банк данных регистрационной информации о правонарушениях, ежедневно по рабочим дням суд передает по электронным каналам в учетное подразделение по месту нахождения суда.

Сведения о преступлениях, помещенные в банк данных регистрационной информации о правонарушениях, следственные изоляторы, исправительные учреждения, исправительные учреждения открытого типа, уголовно-исполнительные инспекции, инспекции по делам несовершеннолетних органов внутренних дел ежедневно по рабочим дням должны передавать по электронным каналам в учетные подразделения по месту нахождения вышеуказанных органов.

Поступившие в учетное подразделение из регистрирующего органа по электронным каналам сведения об административных правонарушениях не позднее чем через сутки после их поступления помещаются в территориальный банк данных о правонарушениях.

В течение суток учетное подразделение, после помещения в территориальный банк данных о правонарушениях сведений об административных правонарушениях, направляет по электронным каналам в регистрирующий орган соответствующее уведомление.

Сведения об административных правонарушениях, переданные в учетное подразделение регистрирующим органом с нарушением порядка присвоения регистрационного номера этому административному правонарушению, фиксации сведений об административном правонарушении и их передачи в органы внутренних дел, учетное подразделение в течение суток со дня их поступления возвращает обратно, т.е. в передавший эти сведения регистрирующий орган. Соответственно регистрирующий орган также в течение суток должен устранить указанные нарушения и повторно передать сведения об административных правонарушениях в учетное подразделение.

Помещенные в региональный банк данных о правонарушениях сведения об административных правонарушениях ежедневно передаются информационно-аналитическими подразделениями ГУВД, УВД, УВДТ по электронным каналам в информационно-аналитическое подразделение МВД.

Сведения об административных правонарушениях, поступившие из информацион-

но-аналитических подразделений ГУВД, УВД, УВДТ, а также из государственных органов, информационно-аналитическое подразделение МВД помещает в единый государственный банк данных о правонарушениях не позднее суток после их поступления.

Сведения о преступлениях, которые поступили по электронным каналам в учетное подразделение из органов предварительного расследования, органов, осуществляющих исполнение наказаний, судов, а также имеются в регистрационных карточках либо в копиях приговоров, постановлений (определений) суда (выписках из приговоров суда), поступивших от прокуроров, из судов, не позднее суток после их поступления должны быть помещены учетным подразделением в территориальный банк данных о правонарушениях.

Сведения о преступлениях, помещенные в территориальный банк данных о правонарушениях, учетное подразделение ежедневно передает по электронным каналам в информационно-аналитические подразделения ГУВД, УВД, УВДТ – соответственно – по подчиненности.

Порядок функционирования оперативно-справочных картотек информационно-аналитических подразделений органов внутренних дел устанавливает Министерство внутренних дел.

В течение трех суток после поступления в информационно-аналитические подразделения ГУВД, УВД из подразделений по гражданству и миграции органов внутренних дел сообщений об изменении физическим лицом фамилии, собственного имени, отчества, изменении и коррекции половой принадлежности, а также о внесении изменений, дополнений и исправлений в записи актов гражданского состояния на лиц, имеющих судимость или несколько фамилий, собственных имен, отчеств (далее – анкетные данные), вышеуказанные информационно-аналитические подразделения помещают в региональные банки данных сведения о правонарушениях на новые анкетные данные физического лица, при необходимости заполняют регистрационные карточки и помещают их в оперативно-справочные картотеки.

Не позднее трех суток после установления информационно-аналитическими подразделениями органов внутренних дел неточностей в анкетных данных физических лиц, сведения о которых помещены в единый государственный банк данных о правонарушениях, в орган уголовного преследования, орган, ведущий административный процесс, или суд, передавший эти сведения, орган внутренних дел направляет уведомление о несоответствии анкетных данных.

В течение пятнадцати суток после поступления из органа внутренних дел в орган уголовного преследования либо орган, ведущий административный процесс, или суд уведомления о несоответствии анкетных данных орган уголовного преследования либо орган, ведущий административный процесс, или суд проводят проверку анкетных данных физического лица. О результатах этой проверки орган уголовного преследования либо орган, ведущий административный процесс, или суд письменно сообщает в орган внутренних дел, направивший уведомление о несоответствии анкетных данных.

Не позднее трех суток после поступления в орган внутренних дел из органа уголовного преследования, органа, ведущего административный процесс, или суда результатов уточнения анкетных данных, информационно-аналитические подразделения органов внутренних дел уточняют анкетные данные в банках данных о правонарушениях соответствующего уровня и регистрационных карточках формы 6, помещенных в оперативно-справочную картотеку (при наличии таковой).

В целях предотвращения утраты (повреждения) сведений о правонарушениях, помещенных в банки данных, осуществляется их резервное копирование на стационарные магнитные (электронные) носители информации, дабы обеспечить их сохранность от несанкционированного доступа

В случаях, предусмотренных законодательными актами Республики Беларусь, МВД предоставляет другим государственным органам доступ по электронным каналам к единому государственному банку данных о правонарушениях.

В случаях, не предусмотренных законодательными актами Республики Беларусь, сведения о правонарушениях, затрагивающие тайну личной жизни физических лиц либо коммерческую или иную охраняемую законом тайну юридических лиц, предоставляются другим государственным органам и иным организациям Республики Беларусь только с согласия указанных лиц.

Таким образом, в целях сбора, хранения, анализа и обобщения информации о фактах, свидетельствующих о коррупции, в том числе о физических и юридических лицах, причастных к коррупции, в специальных подразделениях по борьбе с коррупцией необходимо создать и вести оперативные учеты и централизованные банки данных.

В органах прокуратуры было бы целесообразным вести единые банки данных о состо-

янии противодействия с коррупцией, которые должны формироваться на основании информации, представляемой органами прокуратуры, внутренних дел и национальной безопасности.

Представляется, что в настоящее время в целях обеспечения безопасности предпринимательской деятельности следует законодательно закрепить обязанность опубликования информации о судимости коррупционной направленности и других преступлениях в сфере экономики, а также привлечение лиц к административной ответственности за совершение коррупционных правонарушений. В связи с этим, соответствующие дополнения и изменения необходимо внести в ряд законов и, в первую очередь, в Федеральный закон от 8 августа 2001 г. «О государственной регистрации юридических лиц и индивидуальных предпринимателей». В частности предусмотреть возможность опубликования в реестрах информации о потенциальной опасности хозяйствующих субъектов, выступающих в качестве контрагентов.

Литература

1. ИТ-технологии на службе в органах внутренних дел // Режим доступа: <http://www.sonnest.ru> (дата обращения 19.09.2014)
2. Анализ практики реализации программ противодействия коррупции в субъектах Российской Федерации // Аналитический доклад, науч. руководитель Т.Я. Хабриева. – М., 2012. – 256 с. Режим доступа: <http://www.https://prav.tatar.ru>
3. Анализ практики реализации программ противодействия коррупции в субъектах Российской Федерации // Аналитический доклад / науч. руководитель Т.Я. Хабриева. – М., 2012. – 256 с. Режим доступа: <http://www.https://prav.tatar.ru>
4. Г.А. Василевич. Основные задачи и направления повышения эффективности прокурорского надзора в сфере борьбы с коррупционными правонарушениями // Законность и правопорядок. 2011. № 1 (17). – С. 2–9.
5. А.А. Васин. Модели организации государственных инспекций и борьбы с коррупцией / А.А. Васин, П.А. Картунова, А.С. Уразов // Мат. моделирование. Т. 22. – 2010. № 4. – С. 67–89.
6. Григорьев, Л. Коррупция как препятствие модернизации (институциональный подход) / Л. Григорьев, М. Овчинников // Вопр. экономики. 2008. № 2.
7. Ищенко Н. С. Беларусь и мировой опыт противодействия коррупции. – Гомель : ГГТУ им. П. О. Сухого, 2011. – 250 с.
8. Ю.В. Кузовков. Мировая история коррупции. М. : Анима-Пресс, 2010. – 787 с.
9. Г.А. Сатаров. Диагностика российской коррупции: социологический анализ : краткое резюме докл. – М. : Фонд ИНДЕМ, 2002. – 35 с.





**Добрякова
Галина Эдуардовна**
кандидат юридических наук,
доцент

Проблемы идентификации в информационных системах

***Аннотация:** в статье рассмотрены существующие способы идентификации физических и юридических лиц в информационных системах, их проблемы и перспективы. Дана характеристика единому Российскому стандарту идентификации УЭК и перспективам его развития.*

***Ключевые слова:** идентификация, информационные системы, УЭК (универсальная электронная карта).*

В самом общем случае идентификация представляет собой установление тождества объекта другому [1]. В словаре иностранных слов под идентификацией понимается отождествление, приравнение, уподобление, установление совпадения чего-либо с чем-либо [2]. По «Толковому словарю русского языка» С.И. Ожегова и Н.Ю. Шведовой идентифицировать означает установить совпадение, идентичность [3].

«Одним из наиболее существенных правовых ограничений для использования банковских агентов в настоящее время является наличие жестких требований к идентификации банковских клиентов. Правило «знай своего клиента», применяемое к финансовым организациям ставится во главу угла правительствам в их инициативах по противодействию отмыванию денег и финансированию терроризма. Регулирование в этой сфере вводит обязательное требование к «прозрачности» владельцев счетов, плательщиков и получателей, включая, по меньшей мере, установление личности клиента. Это представляет собой особо сложную проблему при оказании внеофисных банковских услуг» [4, с.4].

Идентификация осуществляется программно-аппаратными методами и в качестве результата присваивает усиленной квалифицированной электронной подписи человеку и юридическому лицу для осуществления юридически значимых действий в системе.

Информационные системы на текущем этапе развития реализуют следующие способы идентификации гражданина.

1. Заполнение гражданином электронной формы с последующим подтверждением факта заполнения электронной формы в удостоверяющем центре либо его представительстве.
2. Заполнение гражданином электронной формы с последующим подтверждением факта заполнения путем оплаты банковской картой.
3. Заполнение гражданином электронной формы с последующим подтверждением факта заполнения путем идентификации по сотовому телефону через оператора мобильной связи (для Москвы и Московской области).
4. Идентификация через портал государственных услуг.
5. Идентификация через персональный аттестат вебмани.
6. Идентификация через УЭК.
7. Биометрическая идентификация посредством сканера стандарта Bio-Link.

Форма запроса, предлагаемая пользователю к заполнению, содержит как общедоступные – фамилия, имя и отчество, пол; так и персональные данные – серия и номер паспорта, дата и место рождения, дата и учреждение, выдавшее паспорт, место регистрации гражданина и место его фактического проживания для получения корреспонденции в физической форме, запись актов гражданского состояния, если лицо состоит в браке, наличие ограничений на совершение действий (полная или частичная дееспособность).

Пользователь заполняет эти данные лично и предупреждается об ответственности за предоставление заведомо ложной информации удостоверяющему центру.

По общему правилу, информационная система может ввести временное ограничение либо полностью удалить пользователя из системы за предоставление заведомо ложной информации, но данные действия вряд ли будут справедливы по отношению к добросовестным пользователям, которые таким образом лишаются защиты от недобросовестных.

В этом случае система по умолчанию будет считать полученные в результате аутентификации данные достоверными, а данные, предоставленные пользователем ошибочными, в связи с чем пользователю будет необходимо привести их в соответствие.

В том или ином виде модуль идентификации пользователя присутствует во всех информационных системах, так как он делает возможным фиксацию действий пользователя в системе, сбор статистики о поведении пользователя и получение результата, так как любое действие пользователя в информационной системе направлено на результат.

Модули идентификации информационных систем дают возможность проведения идентификации как по заполняемой пользователем форме, так и посредством интеграции с базами данных, о чем пользователь дает согласие.

Основная задача идентификации – выделить одного пользователя из неопределенного круга пользователей и присвоить ему параметры доступа. Для этого необходимо взять информацию у юридического лица и идентификационные данные у физического лица, кроме того, у физического лица необходимо запросить согласие на обработку и хранение персональных данных.

Идентификация физических и юридических лиц проходит по разным сценариям, так, для физического лица основным документом является паспорт гражданина Российской Федерации.

Идентификация физических лиц в настоящее время проводится информационными системами следующими путями.

1. Идентификация путем заполнения формы (в том числе нотариально удостоверенной)
2. Идентификация по профилю пользователя в операционной системе (как правило, привязанного к банковской карте пользователя).
3. Идентификация по банковской карте (банковскому переводу).
4. Идентификация по УЭК (для оказания государственных услуг).

Наиболее развита система идентификации в АСУ, рассчитанных на удаленное проведение платежей, такие как клиент-банки, электронные кошельки, поэтому в целях рассмотрения модуля идентификации, остановимся подробно на RBK-money, Qiwi, клиент-банке Сбербанк,

Идентификация путем заполнения формы. Так система RBK-money предусматривает идентификацию путем заполнения формы, система указывает пользователю, что идентификация – это процедура, которая позволяет установить, что именно вы (реальный человек с именем, фамилией и паспортом) являетесь владельцем конкретного счета в системе RBK-Money.

Для прохождения идентификации путем отправки письма с нотариально заверенной подписью пользователь скачивает форму заявления, которая является соглашением на обработку и хранение персональных данных, подпись пользователя заверяется нотариально в соответствии со ст. 80 «Основ законодательства РФ о нотариате» нотариус свидетельствует подлинность подписи на документе, содержание которого не противоречит законодательным актам Российской Федерации. Нотариус, свидетельствуя подлинность подписи, не удостоверяет факты, изложенные в документе, а лишь подтверждает, что подпись сделана определенным лицом. В случае если пользователь младше 18 лет, заявление должно содержать нотариально заверенное согласие одного из родителей.

Далее пользователю надлежит отправить письмо почтой России в офис компании, где оно будет обработано вручную.

Идентификация посредством банковского платежа/перевода. В данном случае цель проведения идентификации достигается за счет использования системой переводов алгоритма проверки личности пользователя, которая делает невозможным отправку анонимных переводов.

Идентификация через систему Contact/банковский перевод. Идентификацию в этом случае проводит кассир-операционист.

Существующая система идентификации работает, что, бесспорно, является ее плюсом. Минусами же являются ручная подготовка и обработка заявок, длительное ожидание идентификации в системе, использование посредников (почта России) не всегда гарантирующих доставку и не гарантирующих целостность.

В текущих системах все сводится к тому, что кто-то проверяет личность человека – либо нотариус, когда удостоверяет форму, либо оператор платежной системы/системы переводов, когда проводит платеж, либо в офисе компании, когда человек приходит лично. Полностью удаленных, дающих человеку возможность идентификации для совершения сделок систем сейчас нет.

Даже получение УЕК требует визита в офис банка-партнера при изготовлении УЕК. Идентификация удаленно не производится ни одной удостоверяющей системой.

Идентификация юридических лиц проходит с учетом приказа Федеральной службы по финансовому мониторингу (Росфинмониторинг) от 17 февраля 2011 г. №59.

Организации в соответствии с подпунктом 1 пункта 1 статьи 7 Федерального закона обязаны идентифицировать клиента, представителя клиента и (или) выгодоприобретателя, за исключением случаев, установленных пунктами 1.1 и 1.2 статьи 7 Федерального закона.

Организации обязаны идентифицировать как лиц (клиентов), которым оказываются услуги либо с которыми заключаются сделки (совершаются операции) разового характера (не предполагающие дальнейшего обслуживания клиента в организации, поскольку при их совершении обязательства сторон выполняются одновременно) (далее – «разовые» операции), вне зависимости от вида, характера и размера оказываемых услуг либо заключаемых сделок (совершаемых операций), так и лиц (клиентов), которые принимаются на обслуживание, предполагающее длящийся характер отношений.

Если от имени юридического или физического лица действует его представитель, организация обязана идентифицировать представителя, проверить его полномочия, а также идентифицировать и изучить представляемого клиента.

При проведении идентификации клиента, представителя клиента, выгодоприобретателя, обновлении информации о них организация вправе на основании пункта 5.4 статьи 7 Федерального закона требовать представления клиентом, представителем клиента и получать от клиента, представителя клиента документы,

удостоверяющие личность, учредительные документы, документы о государственной регистрации юридического лица (индивидуального предпринимателя).

Организация при проведении идентификации клиента, представителя клиента, выгодоприобретателя использует сведения, содержащиеся в едином государственном реестре юридических лиц, сводном государственном реестре аккредитованных на территории Российской Федерации представительств иностранных компаний, а также сведения об утерянных, недействительных паспортах, о паспортах умерших физических лиц, об утерянных бланках паспортов, получаемые в соответствии с абзацем 5 статьи 9 Федерального закона от соответствующих федеральных органов исполнительной власти в установленном порядке.

Организация также может использовать иные дополнительные (вспомогательные) источники информации, доступные организации на законных основаниях.

Способы удаленной идентификации юридических лиц используются, в основном сейчас не для совершения сделок, для этого есть электронная подпись, а для открытия счетов.

В настоящее время удаленное открытие расчетного счета проводит только один банк – «Банк 24.ру», который позволяет открыть счет без физического присутствия в банке (сервис ДОРС). Клиенту для открытия счета нужно заполнить электронную заявку и сделать копии необходимых документов.

«Представителю предприятия необходимо заполнить на сайте стандартную форму электронной заявки. Она содержит ряд вопросов, таких как наименование организации, данные руководителя, то есть информацию, необходимую для идентификации клиента. Эта заявка обрабатывается специалистами банка, после чего клиенту почтой высылаются уже заполненные документы. Клиенту остается только подписать их и по почте переслать обратно в банк вместе с дополнительным пакетом документов по предприятию.

Более того, в случае необходимости к клиенту может выехать наш специалист, который поможет оформить все необходимые для открытия счета документы. В день поступления документов клиента в банк специалисты осуществляют их проверку на соответствие действующему законодательству и открывают клиенту расчетный счет.

Следует отметить, что, согласно действующему в России законодательству, открыть счет

дистанционно (без личного присутствия в банке) пока могут только юридические лица».

Подзаконные акты Банка России описывают идентификацию клиента как некоторую процедуру, основу которой составляет сбор и анализ документов, имеющих к нему отношение. Эти документы выдаются гражданину различными органами государственной власти или уполномоченными учреждениями.

В настоящее время органы загса, ФНС, налоговые органы, ФМС, МВД, ведут персональный учет граждан, организаций, объектов недвижимости и иных объектов, права на которые возникают в результате соблюдения регистрационных процедур.

В науке административного права ставится вопрос о необходимости исследования идентификации различных лиц, как и других объектов материального мира в целях повышения эффективности государственного управления. Только идентификация человека, определение его социального и правового положения позволяют государственным служащим и иным должностным лицам предпринять все необходимые меры по защите его прав и интересов, определяемых его статусом. Наличие прав в свою очередь, влечет за собой и обязанность предоставить идентификатор для подтверждения своего социального статуса.

«С операционной точки зрения можно считать, что «первичную» идентификацию граждан осуществляют уполномоченные органы государственной власти и государственные учреждения. Они же выдают гражданину документ, удостоверяющий личность. Это документ выступает идентификатором физического лица, несущим информацию о его уникальных признаках.

Личная фотография в документе, удостоверяющем личность, иные биометрические данные дают возможность другим лицами и организациям проводить «вторичную» идентификацию, сверяя фотографию в паспорте с внешностью его предъявителя можно установить, принадлежит ли паспорт предъявителю. В случае положительного ответа личные данные отождествляются» [4, с. 52].

Таким образом, к существующим проблемам идентификации в информационных системах относятся:

- › ручная подготовка заявок
- › ручная обработка заявок
- › длительный период ожидания
- › личное присутствие в месте идентификации.

Будущее стандарта идентификации в информационных системах мы видим в машинном

формировании и обработке заявок и удаленной идентификации посредством использования уже имеющихся у пользователей идентификаторов и проверки сведений пользователя самой информационной системой через запросы в соответствующие базы данных.

В настоящее время наиболее масштабным проектом по автоматизации в сфере государственного и муниципального управления является выпуск универсальных электронных карт (УЭК).

Основной задачей универсальной электронной карты является идентификация пользователя и удостоверение его прав на получение государственных и муниципальных услуг, а также иных услуг, оказание которых осуществляется с учетом положений настоящей главы. Закон предполагает, в частности, использование универсальной электронной карты как средства аутентификации для совершения юридически значимых действий в электронной форме в случаях, предусмотренных законодательством РФ.

Федеральная уполномоченная организация открытое акционерное общество «Универсальная электронная карта» – координатор и оператор проекта по внедрению универсальной электронной карты, предусмотренной Федеральным законом №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», принятым в июле 2010 года.

Пока проект находится в стадии реализации, но на сайте проекта заявлено, что географией УЭК является вся территория Российской Федерации. Дополнительно на УЭК могут быть размещены региональные и муниципальные электронные приложения, которые обеспечивают получение услуг, специфичных для конкретного региона (транспортные услуги, кампусы и другие).

Согласно требованиям, установленными Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платёжной системе», ОАО УЭК зарегистрировано Центральным банком Российской Федерации в качестве оператора платёжной системы «Универсальная электронная карта» (далее – Оператор). Запись об Операторе внесена в реестр операторов платёжных систем 29.12.2012 за регистрационным номером – 0019. Функции Расчетного центра в ПС УЭК ПРО100 осуществляет ОАО «Сбербанк России».

Задачей ПС УЭК ПРО100 является осуществление переводов денежных средств с использованием универсальной электронной карты (УЭК).

Огромные перспективы в сфере развития УЭК мы видим в том, что эта программа, в отличие от ранее запущенных, не сфокусирована только для государственных услуг – она открыта для коммерческих компаний, которые могут использовать ее при продаже товаров и услуг своим клиентам, в том числе посредством интернет-магазинов.

Это, несомненно, огромный шаг на пути к аппаратной идентификации человека. Полагаем, что по мере распространения стандарта УЭК большее количество частных компаний начнет использовать его для идентификации своих клиентов и повышения скорости обработки заказов и доставки товаров.

Литература

1. Попандопуло Д.В. Идентификация как объект административного права, административное право и процесс. – 2007, №3.
2. Словарь иностранных слов/ под ред. И.В. Лехина и проф. Ф.Н. Петрова. 5-е издание стереотип. – М. : Государственное издательство иностранных и национальных словарей, 1955, – С.265.
3. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений. 4-е изд, дополненное. М. : Азбуковник, 1999, – с. 236.
4. Иванов О.М., Данилин К.В. «Банковские платежные агенты». М., 2012.





**Леонтьева
Валерия Борисовна**

Технико-правовые основы стоимостиобразования

Аннотация: в статье обосновываются основные междисциплинарные факторы стоимостиобразования товаров и бизнеса – интеллектуальная собственность и потребительная стоимость товаров и услуг. Потребительная стоимость как полезность товара всегда индивидуальна для каждого потребителя. Её превращение в рыночную стоимость происходит, благодаря её спросу и предложению на рынке. Источником потребительной стоимости является интеллектуальная собственность как важнейший стоимостиобразующий фактор. Вся современная экономика постепенно трансформируется в экономику интеллектуальной собственности. Экономико-правовой институт интеллектуальной собственности, развивающийся последние пятьсот лет, медленно расширяясь, остается самым устойчивым знанием и самой стабильной правовой системой.

Ключевые слова: бизнес, государство, инновации, интеллектуальная собственность, образование стоимости, потребительная стоимость, товары, услуги, управление, фактор, ценообразование, экономика.

Экономика интеллектуальной собственности, похоже, в ближайшее время коренным образом изменит представление об экономике в целом и о её связи с юриспруденцией.

Наши исследования показывают, что экономическая наука в целом ориентирована на исследовательскую деятельность и на создание различных теорий, базирующихся на стоимости. Категория стоимости в экономике является фундаментальной, основополагающей. Но когда речь заходит об источниках возникновения стоимости, то выясняется, что у большинства авторов причиной являются спрос и предложение на рынке, то есть интересы покупателя и продавца относительно того, чтобы одному приобрести то, что он ищет, а другому продать то, что он имеет и производит. Цена продажи и цена покупки объединяются в цене сделки, и отсюда возник всем известный термин «ценообразование». Но где же здесь стоимость? Почему никто не исследует источник и процесс образования стоимости?

Классики экономики о потребительной стоимости

Одним из интереснейших парадоксов современной экономики является тот факт, что современных экономистов, как выясняется, истинный фактор стоимостиобразования традиционно не интересует. Хотя именно в нем сокрыта истина. Если же обратиться к создателям науки «экономика» Уильяму Петти (1623–1687), Адаму Смиту (1723–1790) Давиду Рикардо (1772–1823), взгляды которых впоследствии развил К.Маркс, то выясняется, что как истинных классиков их этот вопрос волновал достаточно основательно. На то они и классики, чтобы системно охватить всю область знаний и проблемных отношений с ними связанных.

В экономической науке о закономерностях стоимости впервые заговорил У.Петти. В своем «Трактате о налогах и сборах» [1] он рассуждал о стоимости, ренте, зарплате, разделении труда и деньгах. Он одним из первых высказал идею о существовании в экономике объективных закономерностей, которые называл *естественными за-*

конами. Он фактически сформулировал закон стоимости, близко подошел к понятиям прибавочной стоимости и прибавочного продукта, проанализировал некоторые ценообразующие факторы, изложил соображения об эффективности разделения труда [2].

Однако основоположником классической политической экономии считается Адам Смит. Он первым среди экономистов дал обоснование и определение многим экономическим категориям, включая понятия «стоимость» и его содержание.

«Надо заметить, что слово *стоимость* имеет два различных значения: иногда оно обозначает полезность какого-нибудь предмета, а иногда возможность приобретения других предметов, которую дает обладание данным предметом. Первую можно назвать *потребительной стоимостью*, а вторую – *меновой стоимостью*. Предметы, обладающие весьма большой потребительной стоимостью, часто имеют совсем небольшую меновую стоимость или даже совсем ее не имеют; напротив, предметы, имеющие очень большую меновую стоимость, часто имеют совсем небольшую потребительную или совсем ее не имеют. Нет ничего полезнее воды, но на нее почти ничего нельзя купить, почти ничего нельзя получить в обмен на нее. Напротив, алмаз почти не имеет никакой потребительной стоимости, но часто в обмен на него можно получить очень большое количество других товаров» [3]. Объясняя сущность потребительной стоимости, А.Смит отмечает, что она всегда индивидуальна и зависит от потребностей пользователя в данном товаре на данный момент. Эта стоимость не измеряется в денежном выражении и не сопоставима для разных покупателей.

Другим классиком экономики, уделившим стоимости товаров особое внимание, был Д.Рикардо, который в согласии с А.Смитом, по сути, подтверждает его формулировку этого понятия, делая на него ссылку в своем фундаментальном труде «Начала политической экономии и налогового обложения». «Слово стоимость, – замечает Адам Смит, – имеет два различных значения: иногда оно обозначает полезность какого-нибудь предмета, а иногда возможность приобретения других предметов, которую дает обладание данным предметом. Первую можно назвать *потребительной стоимостью*, вторую – *меновой стоимостью*» [4].

Также как и А.Смит, он отмечает уникальный характер и несопоставимость потребительных стоимостей друг с другом, которые

важны и нужны их потребителям по-разному: кому-то больше, кому-то меньше. Потребительная стоимость определяется мерой потребности в данном товаре конкретного потребителя, у которого со временем данная потребность также меняется.

Среди отечественных экономистов-классиков о потребительной стоимости примерно в тот же период писал Андрей Карлович Шторх (1766–1835) в своем фундаментальном произведении «Курс политической экономии, или Изложение начал, обуславливающих народное благоденствие. Размышления о природе национального дохода» (1815). Стоимость он называет *ценностью товара* и исходит преимущественной из меновой стоимости. «Когда мена введена, полезные предметы или ценности, находящиеся в нашей власти, могут служить двояко: во-первых, *прямо*, когда мы их употребляем для нашей собственной пользы; во-вторых, *непрямо*, когда мы их назначаем в обмен на другие ценности. Отсюда годность предметов и их ценность бывает прямая и непрямая. Предмет получает *прямую ценность* в глазах его владельца, когда он назначает его для собственной пользы или потребления. До сих пор мы рассматривали только этот вид ценности. Предмет получает *непрямую ценность*, когда владелец назначает его для мены. Этот вид ценности всегда пропорционален прямой ценности, признаваемой собственником в тех предметах, которые он хочет приобрести меной» [5].

Здесь важно отметить, что А.К.Шторх ценность предмета как стоимость обмена ставит на второе место, а стоимость потребления – на первое. Таким образом мы убеждаемся, что потребительная стоимость первична. Она вытекает из той прямой пользы, которую товар дает потребителю. Исследования показывают, что под потребительной стоимостью понимается технико-художественное качество товара, удовлетворяющее потребности конкретного потребителя в исполнении для него некой ценной функции. Функциональное соответствие товара тому назначению, которое необходимо его потребителю, определяется преимущественно той интеллектуальной собственностью, которую он содержит в виде патентов, ноу-хау, авторских разработок. Интеллектуальная собственность фиксирует и отличает качество товара от других продуктов других производителей.

Стоимость в марксистской науке

Исследование и определение категории стоимости в марксистской науке в течение дли-

тельного времени строились на тех высказываниях К.Маркса и Ф.Энгельса, которые были опубликованы в их полных собраниях сочинений. Однако, если сравнивать первоисточник и его интерпретацию в советской экономической литературе, то можно отметить, что классики здесь были глубже, нежели их интерпретаторы, у которых стоимость была эквивалентом цены, и потому они оперировали в основном категориями цены как более конкретными и понятными им параметрами.

Знакомя своего друга Фридриха Энгельса с планом произведения «Капитал», Маркс в своем письме ему из Лондона от 02.04.1858 года пишет, что контур первой части включает разделы о капитале, земельной ренте, наемном труде, государстве, международной торговле и мировом рынке. Ключевым разделом здесь является «Капитала», который К.Маркс начинает описывать с уточнения категории «стоимость». Вот, что он пишет: «*Стоимость*. Начисто сводится к количеству труда; время как мера труда. Потребительная стоимость – рассматривать ли её субъективно, как полезность труда, или объективно, как полезность продукта, – выступает здесь лишь как вещественная предпосылка стоимости, предпосылка, которая временно совершенно устраняется их экономического определения формы. Стоимость, как таковая, не имеет иного «вещества», кроме самого труда. Это определение стоимости, впервые только намеченное у Петти и вполне разработанное у Рикардо, есть лишь самая абстрактная форма буржуазного богатства; она сама по себе уже предполагает исчезновение 1) первобытного коммунизма (Индия и т.д.), 2) всех неразвитых, добуржуазных способов производства, в которых обмен еще не господствует полностью. Хотя это и абстракция, но абстракция историческая, которая могла возникнуть только на основе определенного экономического развития общества» [6].

Здесь Маркс потребительную стоимость называет предпосылкой, «которая временно совершенно устраняется из экономического определения формы». И это понятно, поскольку потребительная стоимость не измеряется деньгами, а отражает лишь индивидуальную потребность в ней конкретного потребителя, у которого данная потребность существенно меняется со временем. Именно субъективизм восприятия потребительной стоимости не позволяет её исследовать более глубоко и системно. В целом же категорию «стоимость» Маркс называет «абстракцией исторической, которая могла возникнуть только

на основе определенного исторического развития». И с этим трудно спорить, понимая то, что данной формулировкой Маркс допускает более глубокое понимание этой фундаментальной категории в будущем.

«Все возражения против этого определения стоимости либо вытекают из неразвитости производственных отношений, либо основываются на путанице: более конкретные экономические определения, от которых стоимость абстрагирована и которые поэтому, с другой стороны, могут рассматриваться так же, как дальнейшее развитие стоимости, противопоставляются последней в этой ее абстрактной неразвитой форме. При отсутствии ясности у самих господ экономистов насчет отношения этой абстракции к более поздним конкретным формам буржуазного богатства, возражения эти имели в большей или меньшей мере своё оправдание. Из противоречия между всеобщим характером стоимости и её вещественным бытием в определенной товаре и т.д. – это тот же всеобщий характер, который затем выступает в деньгах, – вытекает категория денег» [6].

Далее, говоря о деньгах, Маркс отмечает связь стоимости товара, цены и количества общественного труда. «Стоимость товара, переведенная на деньги, есть его цена, которая пока выступает только в этом чисто формальном отличии от стоимости. Согласно общему закону стоимости, определенное количество денег выражает лишь определенное количество овеществленного труда. Поскольку деньги являются мерой, изменчивость их собственной стоимости безразлична» [6].

Рассматривая деньги как средство обмена, Маркс на основе двух категорий «товар» и «деньги» рассматривает их кругооборот в двух вариантах: «Т – Д – Д – Т» как товарообращение и «Д – Т – Т – Д» как денежное обращение на товарном рынке [6].

Однако, если с современных позиций поновому и более глубоко посмотреть на данный кругооборот важнейших экономических ценностей на рынке, то применительно к удовлетворению конкретной потребности можно обосновать более полный и системно обоснованный кругооборот: «И – ПС – Т – Д», где И – идея будущего товара, ПС – потребительная стоимость, зафиксированная в данной идее, Т – товар, реализованный на основе идеи и потребительной стоимости, в ней зафиксированной, Д – деньги как выражение стоимости и цены. Таким образом можно построить исходную матрицу, где

идею отобразим в виде идеи объекта интеллектуальной собственности. Это важно, поскольку любая идея фиксируется лишь как объект интеллектуальной собственности, имеющий своих авторов и правообладателей. В таком варианте изобразим матрицу кругооборота потребительской стоимости, которая в исходном виде объекта интеллектуальной собственности фиксируется как планируемая и ожидаемая на рынке, а в виде товара она рассматривается как овеществленная. При этом деньги отображают оценку потребительской стоимости в диалогах «продавец – покупатель», или «производитель – потребитель».

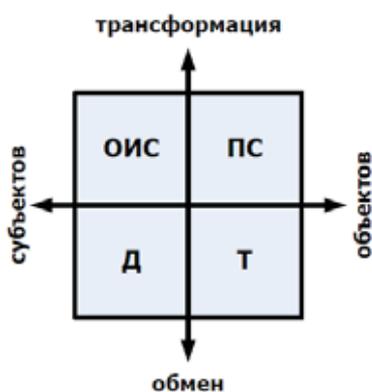


Рис. 1. Матрица кругооборота потребительских стоимостей

Здесь дана матрица кругооборота потребительских стоимостей, которая относительно конкретной потребительской стоимости может достаточно точно фиксировать прогресс в обществе. Для этого необходимо относительно любой важной потребности фиксировать данные кругообороты потребительских стоимостей с периодичностью 5–10–15–20 лет. Если провести такие исследования, то можно отметить на рынке продуктов питания то, что разнообразие потребительских стоимостей растет, номенклатура качество, особенно с позиции экологии нашего человеческого организма, не улучшается и, скорее, ухудшается. На рынке фармацевтической продукции, товаров гигиены и медицинских услуг мы наблюдаем очевидный прогресс, когда диагностирование позволяет задолго до первых очевидных признаков и симптомов выявить зарождение заболеваний в организмах людей и своевременно остановить развитие болезни или полностью вылечить человека. На рынке товаров бытовой и производственной техники мы видим очевидный прогресс. Самый большой прогресс наблюдается на рынке транспортных услуг и товаров.

Отношение Ф.Энгельса к теории прибавочной стоимости, разработанной К.Марксом, и к потребительской стоимости весьма сходно с марксовским, что следует из его писем к друзьям и коллегам по научной деятельности. В своем письме в Петербург к Н.Ф.Даниэльсону Энгельс пишет, в частности, следующее: «Самой модной теорией считается здесь в настоящее время теория Стэнли Джевонсона, согласно которой стоимость определяется полезностью, то есть меновая стоимость = потребительской стоимости, а, с другой стороны, пределом предложения (то есть издержками производства), что есть просто запутанный и окольный способ сказать, что стоимость определяется спросом и предложением. Вульгарная политическая экономия везде и всюду» [7].

В данном случае Энгельс свидетельствует, что Стэнли Джевонс, интуитивно понимая, что потребительская стоимость товара первична и именно она определяет в конце концов его рыночную стоимость как меновую, но объясняет это примитивно, непонятно и запутанно. О том, как происходит переход одной стоимости в другую, то есть как полезность превращается в деньги, ни С.Джевонс, ни Ф.Энгельс не знают, что и признает в своем письме к другу сам Энгельс. Однако, спустя полтора столетия, исследуя истоки потребительской стоимости и её преобразования в меновую, эквивалентную рыночной стоимости, мы можем сегодня достаточно обоснованно изложить эту связь в виде следующей схемы:

«потребность – ОИС – потребительская стоимость – рынок – меновая стоимость – потребление – новая потребность»

Потребительская стоимость как индивидуальная для каждого потребителя полезность товара превращается в меновую стоимость, имеющую денежное выражение лишь при наличии рынка. Более того, чем активнее рынок, чем он разнообразнее и чем более открыт с информационной точки зрения, где легко найти любые товары и всё разнообразие цен на них, тем он более совершенен как инструмент превращения конкретных полезностей, потребительских стоимостей в меновую стоимость, денежную оценку этой полезности.

Современный взгляд на проблему

В различных разделах современных учебников по микроэкономике потребительская стоимость трактуется двояко – как полезность и как способность товара. Например, в известном энциклопедическом справочнике потребительская стоимость рассматривается:

во-первых, как способность товара удовлетворять какую-либо потребность человека;

во-вторых, исходя из трактовки в марксистской политэкономии, она характеризует полезность вещи в качестве предмета потребления, наличия у неё свойств и качеств, позволяющих удовлетворять человеческие потребности [8].

Таким образом, мы заключаем, что любой товар и любая услуга имеют свою потребительную стоимость. Однако характер потребностей у товара и услуги бывают самыми разными, также как и способ их удовлетворения. Одни товары имеют возможность удовлетворять потребности людей непосредственно в качестве предметов потребления, например хлеб, одежда, обувь и т. п., другие это делают косвенно, в качестве средств производства, например станки, оборудование, сырье. Большое количество потребительных стоимостей имеют возможность удовлетворять не одну, а несколько общественных потребностей, например, древесина, к примеру может использоваться как химическое сырье для производства веществ, как топливо, как материал для производства мебели. Здесь в качестве товара также выступают и услуги. «Их специфика заключается в следующем:

1. потребительная стоимость услуги не имеет вещественной формы;

2. потребительная стоимость услуги – это полезный эффект деятельности, живого труда;
3. у услуги нет вещной формы, ее нельзя накопить, ее можно употребить только в момент производства» [8].

Важно отметить, что «из потребительных стоимостей состоит содержание богатства любого общества.

Формы проявления потребительной стоимости:

1. количество;
2. натуральная форма;
3. качество – степень полезности какой-либо потребительной стоимости, уровень ее соответствия потребности, уровень ее пригодности удовлетворять потребность в данных условиях потребления» [8].

При этом следует отличать потребительную стоимость товара, как произведенную в производстве, от потребительной стоимости выращенного продукта в натуральном хозяйстве. Сегодня их объединяет то, что и произведенная и выращенная продукция сегодня основывается на патентах, ноу-хау и эксклюзивных технологиях.

Исследования важности факторов влияния на стоимость предприятия, проведенные институтом СОИС среди профессиональных оценщиков со стажем работы более 5 лет, позволили сформулировать модель (см. рис. 2), где каж-



Рис.2. Зависимость факторов от их важности

дому фактору стоимостиобразования присвоен свой вес, оцененный в процентах. Факторы стоимостиобразования предприятия при оценке стоимости бизнеса различными профессиональными оценщиками оцениваются и ранжируются по-разному. Так для многих из них важнейшими

факторами являются цена товара и объем производства. Однако, когда приходится оценивать конкурентоспособность бизнеса, то на первое место поднимается качество товара и его потребительские свойства в сравнении с конкурентами у других производителей.

В условиях натурального хозяйства выращенные продукты труда, как правило, это потребительная стоимость для дальнейшей переработки и самих производителей конечной продукции. Потребительная стоимость выращенного товара передается непосредственному производителю только лишь при обмене, на основе совершаемых сделок. Сочетание выращенной продукции с дальнейшей её переработкой производится также на основе как известных, так и новых технологий, включающих изобретения и ноу-хау, обеспечивающих новые потребительные стоимости, более удобные и выгодные потребителю и производителю. Между производителем и потребителем также существует конфликт интересов, который заключается в том, что далеко не все, что выгодно и необходимо производителю, выгодно и необходимо потребителю. Самая дешевая продукция сегодня, очень часто, самая низкокачественная и, порой, вредная для массового потребления. В такой продукции обычно не содержатся новые изобретения и ноу-хау и она, чаще всего, не сертифицирована относительно её качества.

В заключение мы приходим к весьма важному и новому, с научной точки зрения, опреде-

лению рынка и его главной функции. **Рынок – это инструмент превращения потребительной стоимости в меновую, где огромное многообразие потребительных стоимостей интегрируется в конкретную меновую стоимость за счет сбалансированного спроса и предложения на конкретный вид товара. Рынок – это инструмент трансформации полезности в деньги и инструмент балансировки цен спроса и предложения, определяющий истинную рыночную стоимость товара, которую последнее время всё чаще называют справедливой стоимостью.**

Данную формулировку сравним с общеизвестными сегодня. «Рынок – экономическая форма обмена продуктами, которые выступают в качестве товаров, при этом производители и потребители выступают в качестве продавцов и покупателей» [9]. Или другое общеизвестное определение для специалистов всех сфер науки и интеллектуальной деятельности: «Рынок – это сфера товарного обмена» [10].

Модель этой трансформации нами предлагается на рис. 3.

Данная модель демонстрирует, как объекты интеллектуальной собственности конкре-



Рис. 3. Плановая модель бизнес-идеи

тизируют и юридически фиксируют, закрепляют конкретную потребительную стоимость через конкретные технические решения при воспроизводстве технологий и продукции и, в итоге, превращаются в меновую стоимость, в доходы и прибыль данного предприятия. Сегодня это особенно актуально в связи с тем, что вся мировая экономика постепенно превращается в экономику интеллектуальной собственности, в инновационную экономику и в экономику знаний.

Эту тенденцию экономических преобразований предвидел и четко обозначил

Ф.Энгельс: «И хотя экономическая потребность была и с течением времени все более становилась главной пружиной прогресса в познании природы, все же было бы педантизмом, если бы кто-нибудь попытался найти для всех этих первобытных бессмыслиц экономические причины. История наук есть история постепенного устранения этой бессмыслицы или замены её новой, но все же менее нелепой бессмыслицей» [10].

Сегодня мы с полной уверенностью можем подтвердить эту оценку Энгельсом современных экономических преобразований.

Современные экономисты и особенно российские крайне редко упоминают роль правовых факторов как стоимостьобразующих и влияющих на эффективность управления и рентабельность предприятия. В связи с этим они почти не обращают внимания на интеллектуальную собственность, относя её к юридической категории. В результате стоимость российских предприятий почти вдвое занижена, а их инвестиционная привлекательность незначительна. Классики отличаются от обычных экономистов тем, что они обладают междисциплинарным мышлением и видением проблем. Так, Ф.Энгельс писал своему коллеге: «Ход «правового развития» состоит по большей части только в том, что сначала пытаются устранить противоречия, вытекающие из непосредственного перевода экономических отношений в юридические принципы, и установить гармоническую правовую систему, а затем влияние и принудительная сила дальнейшего экономического развития опять постоянно ломают эту систему и втягивают ее в новые противоречия (я здесь говорю пока только о гражданском праве» [7].

Действительно, циклическое взаимодействие экономической реальности и правовых систем, которые всегда слегка запаздывают, но с введением новых норм дают новые стимулы развитию экономики, происходит всюду в мировой практике, и там, где есть этот баланс и своевременно происходит актуализация правовых систем, там самые высокие темпы развития экономики и там самые высокие темпы роста стоимости всех экономических субъектов и самые низкие цены на самые высококачественные товары повышенного спроса. Примером тому являются США, Китай, Германия, Южная Корея.

Заключение

1. Потребительная стоимость как важнейшая экономическая категория определяет дальнейшие разнообразные стоимостные, ценовые параметры и прочие экономические показатели предприятия.
2. Источником высококачественной потребительной стоимости являются преимущественно технические решения, заложенные в технологию производства и качество выпускаемой продукции.
3. Качество технических решений фиксируется в объектах интеллектуальной собственности, обладающих новизной и юридической монополией, принадлежащей правообладателям.

4. Технико-правовые основы интеллектуальной собственности определяют стоимостную состоятельность технологий, товаров и бизнеса и являются основой для ценообразования.
5. Стоимостьобразование как процесс самопроизвольного формирования стоимости во всех товарах и услугах, торгуемых на рынке, всегда предшествует ценообразованию и определяет его по сути.
6. Основной функцией рынка, помимо обмена товарами между продавцами и покупателями, является превращение огромного многообразия потребительных стоимостей в меновую и рыночную стоимость, измеряемую в денежном эквиваленте.
7. Рынки с неопределенной и нечетко выраженной потребительной стоимостью (полезностью товара) всегда несостоятельны и обычно изобилуют мошенниками.
8. Без четко обозначенной интеллектуальной собственности крайне сложно расширять рынки сбыта и, тем более, предъявлять претензии к незаконным и нелегальным производителям российской техники, как это произошло, например, с автоматом Калашникова.
9. Без управления стоимостью интеллектуальной собственности крайне сложно стабильно и системно наращивать качество продукции, снижать себестоимости, обеспечивать рост производительности труда.
10. Быстрый рост экономики без фактора интеллектуальной собственности практически невозможен, особенно в экономически слабых отраслях и государствах, что мы наблюдаем во всем мире и в России, в частности.

Литература

1. William Petty. A Treatise of Taxes and Contributions, 1662.
2. Румянцева Е.Е. Новая экономическая энциклопедия. 2-е изд. – М. : Изд. «ИНФРА-М», 2006.
3. Смит А. Исследование о природе и причинах богатства народов/А.Смит; [пер. с англ.; предисл. В.С.Афанасьева] – М. : Изд. «ЭКСМО», 2009. – 960 с. (Антология экономической мысли).
4. Риккардо Д. Начала политической экономии и налогового обложения. Избранное/Д.Риккардо; [пер. с англ.; предисл. П.Н.Клюкина]. – М. : Изд. «ЭКСМО», 2008. – 960 с. (Антология экономической мысли).
5. Шторх А.К. Курс политической экономии, или Изложение начал, обуславливающих

- народное благоденствие/Пер. с франц. Ю.В.Якутин, общ.ред. и вступ.статья. – М. : Изд.Дом «Экономическая газета», 2008.
6. Маркс, К. и Энгельс Ф. Сочинения/К. Маркс и Ф. Энгельс; Ин-т марксизма-ленинизма при ЦК КПСС. – 2-е изд. – Москва : Госполитиздат. Т. 29 : Переписка между К. Марксом и Ф. Энгельсом. Письма К. Маркса и Ф. Энгельса к разным лицам. 1962.
 7. Маркс, К. и Энгельс Ф. Сочинения/. К. Маркс, Ф. Энгельс; Ин-т марксизма-ленинизма при ЦК КПСС. – 2-е изд. – Москва : Госполитиздат. Т. 37. 1962.
 8. Большая экономическая энциклопедия. – М. : Изд. «ЭКСМО», 2008.
 9. Экономическая теория / под ред. А.И.Добрынина, Л.С.Тарасевича : учебник для вузов. – СПб : Изд. СПб ГУЭФ, Изд. «Интер Пабблишинг», 1997.
 10. Большая Российская Энциклопедия. Энциклопедический словарь. Науч. ред. Ю.С.Осипов. – М. : Изд. Большая Российская Энциклопедия, 2011.





**Савичев
Алексей
Аркадьевич**

Сравнительный анализ обеспечения доступа к информации в системе городского самоуправления: история и современность

***Аннотация:** статья посвящена вопросам осуществления права на доступ к информации в России на уровне городского самоуправления в XIX–XX веках и на современном этапе. Сравнивается реализация данного права в прошлом и в современных условиях.*

***Ключевые слова:** местное самоуправление, городское самоуправление, право на доступ к информации, федеральный регистр.*

Право на доступ к информации относится к числу общественно-политических прав. Особое значение имеет реализация данного права на уровне местного самоуправления. Это обусловлено тем, что местное самоуправление представляет собой один из наиболее важнейших институтов демократического государства. Именно органы местного самоуправления представляют собой такие публично-правовые образования, которые максимально приближены к жителям отдельных административно-территориальных образований (этими органами решаются вопросы дорожного хозяйства соответствующего муниципального образования, муниципального жилищного фонда, общего благоустройства территории, где непосредственно проживают граждане).

Гласность как принцип деятельности органов местного самоуправления имеет особое значение для реализации прав, свобод, и законных интересов, в том числе, права на местное самоуправление. Органы местного самоуправления обязаны уделять внимание осуществлению данного принципа, который носит комплексный характер и выражается в праве на информацию через свободу печати и слова, собраний, доступ к материалам и документам, отсутствие цензуры в деятельности средств массовой информации, отчеты должностных лиц местного самоуправления перед населением. Недостаточный уровень информированности граждан о деятельности органов местного самоуправления предопределяет возникновение на практике препятствий для эффективной реализации норм муниципального права, вступает в противоречие с демократической сущностью местного самоуправления.

Итак, рассмотрим некоторые вопросы реализации права на доступ к информации в России на уровне местного самоуправления в отдельные исторические периоды.

Данный вопрос имел актуальность еще во второй половине XIX столетия, ознаменовавшейся достаточно бурным развитием местного управления и самоуправления в России.

В данный исторический период принцип гласности деятельности органов местного самоуправления, в некоторой степени, имел воплощение на практике. В частности, можно говорить об определенной степени открытости органов городского самоуправления для населения. Так, например, в Москве информация о деятельности ор-

ганов городского самоуправления довольно подробно публиковалась в Известиях Московской Городской Думы. Отдельные номера данного журнала свидетельствуют, что жители Москвы имели возможность получить сведения о приговорах Московской Городской Думы; о состоянии городского хозяйства (из отдельных обзоров и статей); о персональном составе гласных Думы; о функционировавших при Думе комиссиях и вопросах, находившихся в их производстве; об отчетах о деятельности Городской Управы; о доходах и расходах города по сметам на отдельные месяцы [1]. То есть уже тогда горожане могли получать информацию не только о результатах правотворческой деятельности органов городского самоуправления, но и конкретные сведения об их правоприменительной деятельности из соответствующих источников официального опубликования правовых актов. Однако, с учетом того, что в выборах в силу барьеров в виде имущественных цензов [2] участвовала совсем незначительная часть населения, данная информация вряд ли могла представлять серьезный интерес для большего числа жителей Москвы. Ведь это были органы, которые, по сути, представляли интересы той небольшой части жителей, которая принимала участие в голосовании. То есть, если функционирование городского самоуправления осуществлялось в большей степени в интересах наиболее состоятельных слоев городского населения, то и право на доступ к информации о муниципальных правовых актах в действительности позволяло учитывать потребности именно таких горожан.

Однако, даже несмотря на наличие формальной возможности доступа к данной информации у всех горожан, у населения не было достаточных рычагов влияния на деятельность органов местного самоуправления (кроме возможности участия в выборах у отдельных социальных слоев). Это обуславливалось тем, что местное самоуправление находилось в серьезной зависимости от органов административно-полицейского управления, т.е. от органов государства (в том числе, в лице губернатора). В таких условиях речь шла об ответственности самоуправления не перед населением, а перед государством. В этой связи говорить о том, что на данном этапе право на доступ к информации о деятельности органов местного самоуправления выступало серьезным условием осуществления населением контроля за их деятельностью не приходится.

В эпоху существования СССР принцип открытости и гласности в деятельности местных

органов власти также сохраняется. Здесь особое внимание заслуживает реализация гражданами права на доступ к информации о деятельности местных властных структур в рамках осуществления так называемого принципа императивного мандата в отношении народных депутатов местных Советов. Императивный мандат противопоставлялся в советской науке «свободному» мандату депутата буржуазных представительных органов. Императивный мандат предполагал, что избиратели дают своему представителю, работающему в Совете безвозмездно и на непостоянной основе обязательные для выполнения наказы, а он обязуется периодически отчитываться о своей работе и о деятельности представительного органа в целом. При этом избиратели могут в любой момент отозвать народного избранника при неисполнении им данных ему наказов. При применении так называемого «свободного» мандата такой возможности у избирателей нет. То есть императивный мандат подразумевает: 1) наказы избирателей; 2) обязательные отчеты депутата перед избирателями; 3) отзыв народного избранника по инициативе избирателей [3]. Соответственно предоставление обязательных отчетов депутата о своей деятельности выступало важнейшей составляющей реализации права граждан на доступ к информации о деятельности местных органов власти. При этом, здесь, в отличие от дореволюционного периода, ответственность местной власти имела место напрямую перед населением хотя бы в силу того, что избиратели могли отозвать депутата при неисполнении им наказов местных жителей.

На современном этапе в России первостепенное значение в вопросе обеспечения гласности местного самоуправления и доступа граждан к информации имеет Конституция Российской Федерации. Так, ч. 3 ст. 15 Основного закона устанавливает, что любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения. Ч. 2 ст. 24 Конституции закрепляет: «Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

В современных условиях в Российской Федерации существует немало возможностей распространения информации о деятельности органов местного самоуправления. Наряду с

электронными и печатными средствами массовой информации, публичными слушаниями (при обсуждении проектов муниципальных правовых актов), собраниями и конференциями граждан и иными возможностями получения информации о деятельности местного самоуправления особую роль стал играть федеральный регистр муниципальных нормативных правовых актов. Муниципальные нормативные правовые акты, в частности, правовые акты, принятые на местном референдуме (сходе граждан), включаются в регистр муниципальных нормативных правовых актов субъекта Российской Федерации, организация и ведение которого осуществляются органами государственной власти субъекта Российской Федерации [4]. Принципами ведения регистра являются актуальность, общедоступность и достоверность сведений, содержащихся в регистре. Регистр ведется в электронном виде на русском языке. Общее руководство деятельностью по ведению федерального регистра муниципальных правовых актов осуществляет Министерство юстиции Российской Федерации [5]. Доступность правовой информации о деятельности органов местного самоуправления выражается в том, что необходимые сведения могут быть получены не только по реквизитам соответствующих документов, но и также при помощи поиска информации по теме правового акта. С этой целью работа по ведению регистра подразумевает не только непосредственный сбор и внесение информации в регистр, но и также ведение классификаторов, словарей и справочников регистра [6]. Предоставление данных сведений осуществляется Научным центром правовой информации при Минюсте России.

Министерство юстиции Российской Федерации анализирует деятельность по ведению регистра муниципальных нормативных правовых актов, составляет обзоры практики его ведения. Наиболее распространенными нарушениями в работе по ведению регистра, как это вытекает из обзоров, являются отсутствие текста или реквизитов муниципального акта, неправильно указанная информация о статусе соответствия или действия муниципального акта, отсутствие актуальной редакции акта, неправильная классификация муниципального акта, а также отсутствие информации об опубликовании [7].

На современном этапе фактически государство в лице Министерства юстиции Российской Федерации, во многом, выступает гарантом обеспечения реализации права на доступ к информации о деятельности органов местного

самоуправления конкретных муниципальных образований.

Если говорить непосредственно об информации из федерального регистра муниципальных актов о деятельности органов городского самоуправления, то на текущем этапе уже действуют соответствующие региональные законы, в том числе, в Москве. Так, на основании ч. 3 ст. 2 Закона г. Москвы «О порядке ведения регистра муниципальных нормативных правовых актов города Москвы» [8] ведение регистра муниципальных актов осуществляется органом исполнительной власти города Москвы, уполномоченным Правительством Москвы на ведение регистра. На сегодняшний день таким органом выступает Департамент территориальных органов исполнительной власти города Москвы [9]. Этот же орган оказывает государственную услугу по предоставлению сведений о муниципальных правовых актах из федерального регистра. Общий срок предоставления данной государственной услуги не может превышать 3 рабочих дней [10]. На сегодняшний день Департаментом осуществляется работа по совершенствованию формирования регистра муниципальных правовых актов города Москвы. Наиболее распространенными ошибками являются: несоответствие документа в электронном виде его бумажной копии; отсутствие приложений к актам как на бумажном носителе, так и в электронных документах; отсутствие сведений об официальном опубликовании нормативных правовых актов и др. [11].

Ведение регистра муниципальных правовых актов позволяет так или иначе решать следующие задачи:

- реализация конституционного права граждан на получение полной и достоверной информации о муниципальных актах;
- обеспечение принципа гласности деятельности органов местного самоуправления;
- создание условий для получения информации о муниципальных актах органами государственной власти, органами местного самоуправления, должностными лицами и организациями;
- информатизация и автоматизация процесса учета муниципальных правовых актов;
- воплощение в действительности принципа демократизма;
- повышение уровня правовой культуры России в целом;
- построение основ правового государства на началах взаимной ответственности личности и государства;

› развитие гражданского общества в России.

Обеспечение максимально широких возможностей получения информации в рассматриваемой сфере представляется особенно важным для формирования и развития гражданского общества в России на современном этапе. По сути, при обеспечении доступа граждан к информации о деятельности местного самоуправления соединяются воедино два важных условия формирования гражданского общества: обеспечение прав и свобод человека и гражданина (как политико-правовая предпосылка) и реализация права человека на информацию (как культурный фактор).

Таким образом, в отличие от периода второй половины XIX века, в условиях современности на фоне развития информационных технологий право на доступ к информации о деятельности органов местного (в том числе, городского) самоуправления позволяет учитывать интересы абсолютного большинства населения. Это подтверждается следующими фактами. Во-первых, на сегодняшний день законом не предусмотрено имущественных цензов для участия в выборах и информация о деятельности местного самоуправления предоставляется для открытого доступа в интересах всего населения, а не в интересах отдельных социальных слоев, выдерживающих соответствующие цензы. Во-вторых, право на доступ к данной информации есть у каждого. В-третьих, в современных условиях возможностей для получения данной информации существует намного больше: печатные и электронные средства массовой информации; публичные слушания; федеральный регистр муниципальных нормативных правовых актов и др.

Литература

1. Известия Московской Городской Думы 1877 г., выпуск 1, 1 июля. – М. : Типо-литография С.П. Архипова и К°, Большая Кисловка, собственный дом, 1877.
2. См.: например, История Москвы с древнейших времен до наших дней : В 3 т. – Т. 2 : XIX век. – М. : Издательство объединения «Мос-

горархив», АО «Московские учебники и картолитография», 1997.

3. Писарев А.Н. История становления и развития правового института депутата Москвы //Труды МГУУ Правительства Москвы, вып. 3. – М., 2005.
4. Федеральный закон от 08.11.2007 № 260-ФЗ (в ред. от 25.12.2008) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с организацией и ведением регистра муниципальных нормативных правовых актов».
5. Постановление Правительства РФ от 10.09.2008 № 657 «О ведении федерального регистра муниципальных нормативных правовых актов».
6. Приказ Минюста РФ от 19.12.2008 № «Об организации работы по ведению федерального регистра муниципальных нормативных правовых актов» (Зарегистрировано в Минюсте РФ 29.12.2008 № 13032).
7. Иванова А. Ю. Проблемы нормотворчества органов местного самоуправления и возможности современных информационных технологий // Правовая информатика. Выпуск 2–2012. – М. : ФБУ НЦПИ при Минюсте России, 2012.
8. Закон г. Москвы от 22 октября 2008 г. «О порядке ведения регистра муниципальных нормативных правовых актов города Москвы».
9. Постановление Правительства Москвы от 31 марта 2009 г. «О мерах по реализации Закона города Москвы от 22 октября 2008 г. № 49 “О порядке ведения Федерального регистра муниципальных нормативных правовых актов города Москвы”».
10. Постановление Правительства Москвы от 15 мая 2012 г. № 200-ПП «Об утверждении административного регламента предоставления государственной услуги города Москвы “Предоставление сведений из регистра муниципальных нормативных правовых актов города Москвы”».
11. http://dtoiv.mos.ru/registr_mnpa/ПОМ/Mistakes_mpa.php.





**Горбачева
Елена Викторовна**

Информатика как теория, определяющая оптимальную организацию информационной работы

***Аннотация:** статья повествует о необходимости компетентности в сфере информатики, правовой информации, информатизации.*

***Ключевые слова:** информатика, информация, правовая информация, информатизация, информациология, информационная система, текст, лингвистическое обеспечение.*

Для успешной деятельности в области правовой информатики необходимы специалисты, точно так же, как и в математике, физике. Однако кажущаяся простота предмета (в медицине, педагогике, а теперь и в вопросах информации, как известно, разбираются все) приводит к решениям, непозволительным для юриспруденции – области, связанной с жизненно важными проблемами общества, где ошибка иногда бывает непоправимой. Некомпетентность в информационной области, к сожалению, наблюдается достаточно часто. В связи с многоаспектностью данной сферы зачастую не находится специалистов, которые могут грамотно определить сам предмет правовой информации, оценить уровень исследований и практических разработок, положенных в основу правовых информационных систем.

Информатика, или теория научной информации, это, по определению, – отрасль знания, изучающая закономерности сбора, обработки, хранения, поиска и распространения документальной научной информации и определяющая оптимальную организацию информационной работы на базе современных технических средств. (Терминологический словарь по научной информации). Информатика – это серьезная наука, основывающаяся на устоявшихся, сложных предметах – семантике, семиотике, теории групп, теории множеств, комбинаторике, структурной лингвистике и т.п., однако в настоящее время зачастую считают, что информатика – прикладная сфера, к которой можно подходить с элементарными знаниями. Поэтому появляется множество научных работ и практических разработок (классификаторов и т.п.), не отвечающих основным научным положениям и здравому смыслу. Надо постоянно помнить о серьезном отношении к информатике как к настоящей науке, которой необходимо специально учиться.

Кроме того, как ко всякой дисциплине, к данному предмету надо иметь и способности. Очень заметно, что информация предпочитает одних людей и не любит других – вплоть до того, что они не могут толком дозвониться по телефону.

Отсутствием «информационного чутья» можно объяснить пассажи из современных книг (примеры даются из солидных трудов известных авторов без их упоминания, так как подобными шедеврами пестрят очень многие труды по проблемам информации).

Очень часты некорректные определения, как, например, это, смешивающее в одно общетеоретические соображения, их неправо-

мерное сужение и привязку к практике: «Под юридической понимается классификация нормативного правового материала, т.е. актов системы законодательства России на примерах отечественной правовой жизни».

Или определение информатизации в труде, который автор считает открытием нового научного направления, – при всей наукообразности оно нарушает основные требования к дефинициям: «информатизация – это естественный социально-космический процесс повышения уровня жизни и создания единого мирового информационно-сотового сообщества». Ведь еще вопрос, повышается ли уровень жизни при воздействии информатизации – общества еще может быть, а для отдельного человека, возможно, самый высокий уровень жизни – сидеть в цветущем саду и не подвергаться никакой информатизации: меньше знаешь – лучше спишь.

Далее, в той же книге объясняется, что информатиология занимается, в основном, естественной информацией, а объект информатики – информация искусственная (данные, показатели...). И как же это может быть, если по данному в том же разделе определению «информатика – важный раздел информатиологии, одна из основных составляющих ее структур». То есть получается, что целое занимается одним, а основная его часть – другим предметом?

Другой автор (программист) в своей работе уверенно выделил в словах юридических текстов «500 приставок». Когда было замечено, что приставок в русском языке не больше двух десятков, автор сказал, что это ему без разницы.

К слову, ощущение информации как самоценной сущности вообще не свойственно многим авторитетам в данной области. Об этом говорит, например, постоянное упоминание в одном контексте слов «информация» и «связь» – вплоть до бывшего названия «Министерство связи и информации». Конечно, это близкие отрасли, техническая связь это одно из средств передачи информации. Однако тогда отрасль информации должна включать и изучение устройства основного передатчика информации – человеческого языка, либо руки, позволяющей фиксировать сведения на различных носителях путем письма. И это гораздо более приоритетные и важные средства передачи информации, чем технические средства связи. И вообще, как передаются сведения – это одно, это способ, а информация – собственно объект, достойный особого изучения.

Особым видом информации является правовая информация. Она лежит в основе нор-

мального функционирования общества, в фундаменте его экономической и политической жизни.

Специфика правовой информации предполагает удовлетворение самых высоких требований к ее полноте и точности, к качеству ее обработки, хранения и передачи: законодательство регулирует все стороны жизни общества и прямо влияет на него. Отсутствие, неполнота или неточность правовой информации влекут моральные и материальные потери, несопоставимые с затратами на ее обработку и услуги при ее предоставлении пользователю. Абонент какой-то справочной системы, не получивший, скажем, полного списка необходимых ему магазинов или видов изделий вполне может обойтись предоставленными сведениями. Потребитель же правовой информации, обеспеченный пакетом нормативных актов, содержащих безупречную информацию на заданную тему, но без единственного акта, отменяющего действие их всех, – рискует очень многим – деньгами, а то и свободой. Незнание закона, как известно, не освобождает от ответственности. Недостаточная правовая информированность деформирует правосознание граждан, существенно осложняет переход к правовому государству.

Правовая информатика, занимающаяся вопросами организации правовой информации, – относительно новая область информационной деятельности, имеющая ярко выраженную специфику, связанную с особенностями предмета правовой информации, которые необходимо учитывать при работе с ней. Повторим, что полнота и точность правового информирования не желательное, а обязательное условие. Поэтому правовая информатика, интегрирующая знания из различных областей, должна быть сферой приложения самых квалифицированных научных сил, разработок высокого уровня. Непонимание основных понятий правовой информатики отзывается недочетами в практических воплощениях ее идей: правовых информационных системах, классификаторах, рубрикаторах.

Создание правовых информационных систем должно быть основано на научном подходе. Без участия специалистов различных отраслей невозможно создать корректное обеспечение работы этих систем. Результаты, полученные усилиями, например, одних прикладных математиков без привлечения юристов и лингвистов демонстрировали свою несостоятельность, отмечаемую специалистами и замечаемую клиентами.

Как ни странно, некоторую отрицательную роль в процессе интеллектуализации ин-

формационных систем сыграл бурный прогресс в области вычислительной техники. Новые потрясающие технические возможности создают впечатление, что компьютеры способны самостоятельно решить проблемы обработки, хранения и поиска правовой информации. Однако необходимо понимать, что при работе с текстом ничто не заменит человека – только специалист может провести предмашинную обработку, выявив закономерности в организации текста, создав необходимые словари и классификаторы, сделав эксплицитными скрытые в тексте связи, выявив выходящие за пределы текста отношения, в общем, выделив инвариант сообщений, что, собственно, по К.Шеннону, и является информацией. Особенно, снова подчеркнем, проблемы интеллектуальной обработки текстов касаются правового материала, предъявляющего особые требования к полноте и точности информации. Так, выделение нормы права (собственно правовой информации) до сих пор является предметом спора высокопрофессиональных ученых-юристов, куда уж тут компьютеру (этот вопрос можно было бы решить путем выделения норм из текста самими законодателями, но в настоящий период им не до таких тонкостей). В режиме реального поиска без предварительной обработки текстов невозможно учесть все способы выражения одного смысла в текстах. Никакой компьютер сам по себе не узнает, что поиск по слову «самолет» должен привести к отбору текстов и со словом «аэроплан», что, если вы ищите документы о правах композиторов, необходимо добавить в запрос слово «автор», а если желаете узнать все о мебели, надо не забыть в запросе отдельно упомянуть и каждый ее вид, так как имеются документы, особо посвященные, скажем, школьным партам. Иначе вашей юридической информации грош цена – она имеет значимость только будучи абсолютно точной и полной.

Помочь в решении указанных проблем могут только специально разработанные средства, такие как различные словари, тезаурусы, в явном виде представляющие синонимичные и родовидовые отношения, средства морфологического анализа и т.п. А сами тексты до ввода в машину должны подвергаться профессиональному членению на нормативные предписания, индексированию и рубрицированию.

Только такая формализованная информация может быть объектом работы вычислительной техники. Только предварительно «образованный» компьютер может выдавать действительно качественный продукт. Его дело – прогон

больших массивов текстов через сито закономерностей, правил и требований, установленных специалистами. Это он делает непревзойденно, результаты порой выглядят фантастически.

Правда, обывательская точка зрения на компьютеризацию существует порой и в самых передовых отрядах информационной технологии – среди создателей правовых систем. Например, очень показательны заявления типа: «Если классификатор на бумажном носителе иногда подвергался изменениям, то в условиях автоматизированного режима это уже связано со значительными трудностями и материальными затратами». И еще: «В новых условиях при смене законодательной материи и иной компьютерной технике выполнить эти условия оказалось невозможным». Это напоминает ситуацию в ЖЭКе, когда на претензии посетителей к долгому обслуживанию важная начальница гордо заявила: «А чего же вы хотите – у нас же компьютеры!».

В настоящее время, правда, поставщики правовой информации поняли, что правовое и лингвистическое обеспечение информационных систем – не роскошь, а средство продвижения к душам и деньгам клиентов. На информационном рынке имеются словари юридических терминов, в системах задействуются механизмы автоматического анализа текстов и т.п.

Недостатки в понимании основных положений теории информации проявляются в качественном уровне продуктов информационной деятельности. Конечно, новейшие технологии, Интернет снимают многие проблемы организации правовой информации, но они не отменяют многие средства и методы, разработанные в прошлые эпохи, исследования в области систематизации и кодификации законодательства и т.л.

Замечено, что многие работники в области правовой информации пребывают в полной уверенности, что до их прихода в эту сферу здесь было сплошное белое пятно. Много сил и средств тратится на то, что давно известно и даже было воплощено в жизнь. Отсюда заявления типа «создание классификатора способствует переходу (!) к этапу систематизации (законодательства)». Однако вопросом систематизации постоянно занимались лучшие юридические силы страны (и в уважаемое дореволюционное время, и в советское, далеко не примитивное в плане классификации юридического материала).

В работе с лингвистическими средствами есть особенность: довольно просто предложить прозрачную, стройную и логичную теорию (концепцию) их создания, однако при ее прак-

тическом воплощении проблемы нарастают, как снежный ком. Столкновение концепции с действительностью – сложной системой связей между элементами, которые к тому же четко не определяются, да еще выраженной на русском языке с его грамматикой, синонимами и т.п. – всегда приводит к сложной, запутанной, долгой работе по согласованию всех элементов.

Специалистам, занимающимся вопросами информационных систем, часто никак не дается понимание идеи тезауруса. Они оправдывают его отсутствие «развитием системы полнотекстового поиска в электронном виде». Однако никакой полнотекстовый поиск не дает возможности поставить в соответствие ключевому слову синонимы, которыми так богат русский язык, или расширить запрос родовыми или видовыми понятиями. А только это обеспечивает полноту по-

иска, что является необходимейшим, первейшим условием именно для правовой информации.

При разработке классификаторов совсем не обязательна линейность. Например, можно сделать нечто вроде тезауруса органов, где синонимичными являются названия органов, употреблявшиеся в разные годы, и ввести родовидовые отношения. Можно сделать красивую многомерную картинку на экране компьютера.

В заключение хотелось подчеркнуть главную мысль: проблемы правовой информатики не уходят в связи с появлением новых технологий; эти технологии только предоставляют неограниченные возможности для более глубоких научных и практических разработок в сложной, важной и очень интересной области правовой информатики.





**Барабанов
Александр
Владимирович**
старший преподаватель
МГТУ им. Н.Э.Баумана

Нормативные вопросы безопасного производства программ

Аннотация: рассмотрены вопросы стандартизации процесса разработки безопасных программных средств. Проанализированы основные положения проекта ГОСТ «Защита информации. Разработка безопасных программных средств. Требования». Показана возможность гармонизации указанного стандарта с стандартами серии.

Ключевые слова: безопасное программное средство, уязвимости программных средств, дефекты безопасности программных средства.

На протяжении последних лет наблюдается устойчивый рост количества нарушений ИБ, приводящих к снижению уровня целостности, доступности и конфиденциальности информационных ресурсов автоматизированных систем [1, 8]. Опыт работы аккредитованной испытательной лаборатории [2, 6], проводящей сертификационные испытания ПО в различных системах сертификации, показывает, что даже в продуктах, представляемых разработчиками на сертификацию, содержатся уязвимости и дефекты безопасности. Наиболее распространенными типами уязвимостей, выявляемых в ПО, подаваемом сертификацию, являются: аутентификационные данные в исходном коде ПО, межсайтовый скрптинг, внедрение SQL-кода [1].

Проведенные исследования позволили определить три основных причины наличия уязвимостей в ПО [2].

1. Недостаток мотивации разработчиков. Потребители в первую очередь приобретают ПО, которое является первым на рынке или обладает уникальными функциональными возможностями. В связи с этим разработчики ПО заинтересованы в скорейшем выпуске ПО или его обновлений на рынок, что влечет за собой отсутствие должного внимания к вопросам обеспечения безопасности.
2. Отсутствие у разработчиков необходимых знаний. Методы построения безопасного ПО еще находятся в стадии изучения и формирования. В связи с этим современный разработчик ПО не всегда полностью понимает, как правильно проектировать и разрабатывать программу именно с точки зрения безопасности, что ведет к наличию большого

числа уязвимостей в ПО, выпускаемом на рынок.

3. Отсутствие у разработчиков необходимых технологий. Современные инструментальные средства обеспечения безопасности разработки (статические анализаторы, сканеры уязвимостей и т.д.) еще не вышли на необходимый уровень развития и не еще могут в полной мере помочь разработчикам решить вопросы безопасности их ПО.

Угрозы безопасности ПО могут быть классифицированы по стадии жизненного цикла разработки ПО (стадии разработки, поставки, установки и эксплуатации), для которой они характерны [5, 9, 10].

Источником угроз безопасности ПО на стадии разработки ПО являются внутренние разрушители, в первую очередь недобросовестные разработчики, которые пытаются повлиять на штатный режим функционирования ПО путем внесения несанкционированных изменений в следующие объекты:

- требования к ПО, проектная документация ПО;
- исходные тексты ПО или исполняемые модули;
- тестовая документация или результаты тестирования ПО [3];
- эксплуатационная документация;
- инструментальные средства, используемые при разработке ПО.

Недобросовестные разработчики могут как входить в штат компании-разработчика ПО или привлекаться временно, так и являться разработчиком ПО с открытым исходным текстом, которое используется при реализации ПО.

Источником угроз безопасности ПО на стадии поставки ПО могут являться организа-

ции, осуществляющие поставку ПО конечному пользователю. В ходе этой процедуры в ПО могут быть несанкционированно внедрены вредоносные модули или выполнена замена стандартных модулей ПО на модули с недеklarированными возможностями [4]. Если поставка ПО осуществляется с использованием сетевых протоколов передачи данных (например, путем получения дистрибутива ПО с сервера организации-разработчика), то источником угрозы может выступать внешний нарушитель, который может заменить файлы дистрибутива ПО в

процессе их передачи или перенаправить пользователя на вредоносный сайт для скачивания дистрибутива ПО с использованием атак типа «межсайтовый скриптинг».

Источником угроз безопасности ПО на стадии эксплуатации ПО являются внутренние или внешние нарушители, которые могут выполнять локальные или удаленные (с использованием сетевых протоколов) атаки на ПО с целью эксплуатации уязвимостей.

Основные категории угроз безопасности ПО и их описания приведены в таблице 1.

Таблица 1.
Основные категории угроз безопасности ПО

Категория угроз безопасности ПО	Краткое описание	Нарушаемое свойство информационной безопасности	Последствия от реализации угрозы
Саботаж	Нарушение штатного режима функционирования ПО, удаление исполняемых модулей ПО.	Доступность	Реализация атаки типа «отказ в обслуживании»
Внедрение программных закладок	Несанкционированная модификация исполняемых модулей ПО, внедрение в ПО вредоносных модулей или программных закладок	Целостность	Нарушение штатного режима функционирования ПО, выполнение ПО команд атакующего
Получение несанкционированного доступа	Несанкционированный доступ к функциональным возможностям ПО	Нарушение политик разграничения доступа	Несанкционированное выполнение команд или копирование/кража исполняемых файлов
Раскрытие архитектуры ПО	Раскрытие архитектуры и принципов работы ПО с использованием механизмов декомпиляции или дизасемблирования	Конфиденциальность	Получение предварительной информации об атакуемом ПО, получение информации об архитектуре и принципах работы ПО, что является интеллектуальной собственностью разработчика

Таким образом, на сегодняшний день важным направлением развития, нацеленным на повышение качества ПО и уменьшение числа уязвимостей и дефектов безопасности, является внедрение цикла разработки безопасного ПО. Опыт компании Microsoft показал, что внедрение цикла разработки безопасного ПО позволяет сократить число уязвимостей в ПО компании в среднем на 80%. В настоящее время известны методологии проектирования безопасного ПО, которые успешно используются предприятиями-разработчиками. В таблице 2 представлены результаты сравнитель-

ного анализа следующих методологий проектирования безопасного ПО:

- › «Общие критерии» (ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»);
- › методология OWASP CLASP (Complex Lightweight Application Security Process);
- › методология Microsoft Security Development Life Cycle;
- › методология Cisco SDL;
- › методология OpenSAMM.

Таблица 2.

Результаты сравнительного анализа методологий проектирования безопасного ПО

Характеристика	Методология				
	«Общие критерии»	Microsoft SDL	Open SAMM	Cisco SDL	OWASP CLASP
Обучение специалистов	-	+	+	+	-
Обеспечение физической и логической безопасности при разработке ПО	+	-	-	-	-
Управление конфигурацией	+	-	-	-	-
Моделирование угроз	+	+	+	+	+
Определение требований безопасности к разрабатываемому ПО	+	+	+	+	+
Использование принципов безопасного проектирования	+	+	+	+	+
Анализ исходных кодов ПО	-	+	+	+	+
Анализ уязвимостей	+	+	+	+	+
Использование методов проектирования безопасного ПО	-	+	+	+	+
Обеспечение безопасности поставки	+	-	+	+	-

В настоящее время ФСТЭК России ведется работа над государственным стандартом «Защита информации. Требования по обеспечению безопасности разработки программного обеспечения». Кроме этого, в соответствии с нормативным правовым актом ФСТЭК России «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», использование в информационной системе системного и (или) прикладного ПО, разработанного с использованием методов защищенного программирования, является дополнительной мерой по обеспечению безопасности информации в случае определения в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов. В тоже время документ, определяющий содержание и порядок выполнения работ по созданию ПО с использованием методов защищенного программирования, отсутствует. Эти положения и определяют актуальность разработки ГОСТ.

При разработке первой редакции проекта ГОСТ учитывались следующие особенности:

1. Поскольку известно, что стоимость устранения уязвимостей и дефектов безопасности

ПО выше на поздних стадиях проектирования, ГОСТ должен обеспечить внедрение необходимых процедур на самых ранних стадиях проектирования ПО.

2. ГОСТ должен учитывать современные тенденции разработки безопасных ПО, учитывать положения «лучших практик» (например, Microsoft SDL, Cisco SDL) [12-14].
3. ГОСТ должен быть полностью совместим с методологией разработки и сертификации ПО, используемой в настоящее время ФСТЭК России («Общие критерии») [9].
4. Разрабатываемый ГОСТ должен обеспечить возможность интеграции процедур разработки безопасного ПО с существующей на предприятии системой управления ИБ (например, построенной в соответствии с ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования») [11].

Анализ современных методологий проектирования безопасного ПО позволил сформулировать следующий перечень процедур, которые должны быть реализованы разработчиком для успешного противостояния угрозам безопасности ПО:

- процедуры управления конфигурацией;

- › процедуры определения модели жизненного цикла;
- › процедуры проектирования и реализации безопасных ПО;
- › процедуры использования инструментальных средств и методов разработки;
- › процедуры обеспечения безопасности разработки;
- › процедуры поставки;
- › процедуры обновления и устранения уязвимостей и дефектов безопасности ПО.

Следует отметить, что требования к реализации большинства процедур согласованы с требованиями доверия, предъявляемыми ГОСТ Р ИСО/МЭК 15408-3 (табл. 3) [1].

Таблица 3. Соответствие требованиям ИСО 15408

Требование разрабатываемого стандарта	Требование ГОСТ Р ИСО/МЭК 15408-3
Требования к функциональным возможностям системы управления конфигурацией	ACM_CAP.1, ACM_CAP.2, ACM_CAP.3, ACM_CAP.4, ACM_CAP.5
Требования к области действия системы управления конфигурацией	ACM_SCP.1, ACM_SCP.2, ACM_SCP.3
Требования к средствам автоматизации процесса управления конфигурацией	ACM_AUT.1, ACM_AUT.2
Требования к процедурам определения модели жизненного цикла	ALC_LCD.1, ALC_LCD.2, ALC_LCD.3
Требования к процедурам проектирования и реализации безопасных ПО	ATE_FUN.1, ATE_FUN.2, AVA_VLA, ADV_FSP, ADV_HLD, ADV_LLD, ADV_RCR
Требования к процедурам использования инструментальных средств и методов разработки	ALC_TAT.1, ALC_TAT.2, ALC_TAT.3
Требования к обеспечению безопасности разработки	ALC_DVS.1, ALC_DVS.2
Требования к процедуре поставки	ADO_DEL.1, ADO_DEL.2, ADO_DEL.3, ADO_ISG, AGD_ADM, AGD_USR
Требования к реализации процедур обновления и устранения недостатков	ALC_FLR.1, ALC_FLR.2, ALC_FLR.3

Отдельно рассмотрим перечень основных требований к процедурам проектирования и реализации безопасных ПО, сформулированные по результатам анализа «лучших практик» и обобщения опыта работы аккредитованных испытательных лабораторий систем сертификации средств защиты информации.

1. Должно проводиться периодическое обучение разработчиков ПО с целью повышения их осведомленности в области разработки безопасного ПО. Выполнение данного требования позволяет обеспечить повышение осведомленности в области безопасной разработки ПО сотрудников, связанных с разработкой ПО и, как следствие, повышение уровня безопасности разрабатываемого ПО. В программу обучения сотрудников могут входить курсы безопасного программирования, инспекции кода, тестирования на проникновение, статического анализа, динамического анализа, функционального тестирования и другие [7].
2. Разработчиком ПО должны быть определены и документированы требования безопасности к разрабатываемому ПО. Например, могут быть определены следующие классы требований: требования к обеспечению конфиденциальности, требования к обеспечению идентификации и аутентификации, требования к реализации разграничения доступа, требования к обработке ошибок и исключений ПО.
3. Проектирование ПО должно выполняться с использованием принципов проектирования безопасных ПО. При выполнении проектирования разработчиком могут, например, использоваться следующие принципы: принцип эшелонированной защиты, принцип минимальных привилегий, принцип модульного проектирования, принцип разделения обязанностей.
4. При проектировании ПО разработчиком должно выполняться моделирование угроз с целью выявления уязвимостей ПО этапа проектирования, результаты моделирования угроз должны документироваться.
5. Разработка ПО должна выполняться с использованием методов защищенного про-

граммирования. Например, в ходе разработки ПО разработчик должен избегать использования скомпрометированных (небезопасных) функций в исходных кодах ПО. В качестве источника небезопасных функций могут использоваться, например, списки «Security Development Lifecycle Banned Function Calls» компании Microsoft.

6. Должен проводиться периодический статический анализ исходных кодов ПО с целью выявления уязвимостей и дефектов кода, результаты анализа должны документироваться.
7. Должна проводиться периодическая инспекция кода с целью выявления уязвимостей и дефектов кода, результаты инспекции должны документироваться.
8. Должно проводиться и документироваться тестирование (функциональное, нагрузочное) ПО.
9. Должен проводиться динамический анализ исходных кодов ПО с целью выявления уязвимостей и дефектов кода, результаты анализа должны документироваться.
10. Должно проводиться тестирование на проникновение с целью выявления уязвимостей ПО, результаты тестирования должны документироваться.
11. Должны быть разработаны функциональная спецификация ПО, проектная документация (проект верхнего уровня, проект нижнего уровня) и документация, демонстрирующая соответствие между всеми смежными параметрами имеющихся представлений ПО.

Планируется, что будет введена некоторая градация, которая позволит предъявлять требования к организациям-разработчикам в зависимости от критичности создаваемого ПО.

Внедрение подобных процедур в российские организации-разработчики ПО, на наш взгляд, повысит уровень защищенности создаваемого ПО и, как следствие, значительно уменьшит число инцидентов ИБ.

Литература

1. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). С.37-41.
2. Костокрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996. 280 с.
3. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № СПЕС. С. 90–103.
4. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1(1). С.28–36.
5. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. №3. С. 56–61.
6. Марков А.С., Цирлов В.Л. Сертификация программ: мифы и реальность // Открытые системы. СУБД. 2011. № 6. С. 26–29.
7. Марков А.С., Цирлов В.Л., Маслов В.Г., Олексенко И.А. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики. 2009. Т. 2. № 12. С. 2–6.
8. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61–64.
9. 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.
10. Правовое обеспечение информационной безопасности / Минаев В.А., Фисун А.П., Скрыль С.В., Дворянкин С.В., Никитин М.М. – М.: Маросейка, 2008 г. 368 с.
11. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4-14.
12. Howard M., Lipner S. The Security Development Lifecycle: A Process for Developing Demonstrably More Secure Software. Microsoft Press. 2006. 352 p.
13. Cisco Secure Development Lifecycle. Cisco White Paper. 2013. 4 p.
14. Software Assurance Maturity Model: A guide to building security into software development. Ver. 1.0. OWASP. 2013. 96 p.



Цирлов

Валентин Леонидович

кандидат технических наук

Правовые основы кибербезопасности Российской Федерации

***Аннотация:** работа посвящена основным нормативно-правовым актам, лежащим в основе зарождающейся тематики обеспечения кибербезопасности. Дан краткий обзор проекта Концепции стратегии кибербезопасности Российской Федерации, а также анализ международного стандарта ISO/IEC 2703. Проведен анализ потенциальных путей развития соответствующей нормативной базы.*

***Ключевые слова:** кибербезопасность, информационная безопасность, руководящие принципы, стандарты, нормативный документ.*

Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации является органичным компонентом государственной политики развития национального сектора применения информационных технологий [7]. Среди основных документов, определяющих на сегодняшний день фундаментальные подходы к обеспечению информационной безопасности в Российской Федерации, можно выделить, в первую очередь, следующие:

- › Закон Российской Федерации 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- › Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года;
- › Доктрина информационной безопасности Российской Федерации;
- › Стратегия развития информационного общества в Российской Федерации.

Указанные, а также сопутствующие им ведомственные нормативные документы (в первую очередь это документы ФСТЭК России) на сегодняшний день формируют комплексную систему требований по обеспечению информационной безопасности для информационных систем различного уровня. В то же время вопрос уточнения специфики киберпространства, а также соответствующих угроз и механизмов защиты, безусловно, заслуживает отдельного рассмотрения.

Из современных правовых документов в области безопасности киберпространства следует особо отметить следующие:

- › Концептуальные взгляды на деятельность Вооруженных сил РФ в информационном пространстве;
- › Проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [8];
- › Указ Президента России 2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Однако, на сегодняшний день в Российской Федерации документом, определяющим наиболее фундаментальные подходы к обеспечению кибербезопасности, является Концепция стратегии кибербезопасности Российской Федерации. Документ определяет киберпространство как сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а кибербезопасность, в свою очередь, как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Тем самым, понятие «кибербезопасность» является по определению более узким, чем понятие «информационная безопасность». Следует обратить внимание, что указанное определение отличается и от общепринятых в отдельных отраслях определенных понятия «кибербезопасности» [1-5].

Общая структура направлений деятельности, предложенная в названном документе, приведена на рис. 1.

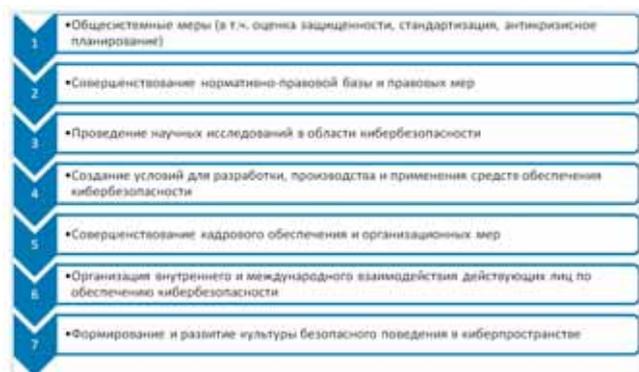


Рис. 1. Общая структура деятельности по обеспечению кибербезопасности Российской Федерации

Нетрудно видеть, что предложенные механизмы должны сформировать логичную и целостную систему, однако для практической их реализации необходима колоссальная работа по подготовке нормативных документов, регламентирующих отдельные аспекты соответствующей деятельности.

На этом этапе может быть полезен международный стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности» (ISO/IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity), разработанный подкомитетом SC 27 «Информационные методы обеспечения безопасности» технического комитета ISO/TC «Информационные технологии». Понятие киберпространства в данном документе носит более прикладной характер: оно рассматривается как комплексная среда, возникающая в результате взаимодействия людей, программного обеспечения и удаленных сервисов с использованием информационных и телекоммуникационных технологий. Принципиально важным при этом является вопрос взаимодействия между различными организациями, обеспечивающими существование киберпространства как единого целого: по мнению разработчиков стандарта тот факт, что каждая из организаций решает вопросы обеспечения информационной безопасности самостоятельно, создает предпосылки для реализации принципиально новых угроз информационной безопасности.

Тем самым, кибербезопасность (cybersecurity) реализуется на стыке следующих

трех компонентов системы обеспечения информационной безопасности (рис. 2):

- › безопасность приложений;
- › сетевая безопасность;
- › безопасность сети интернет.

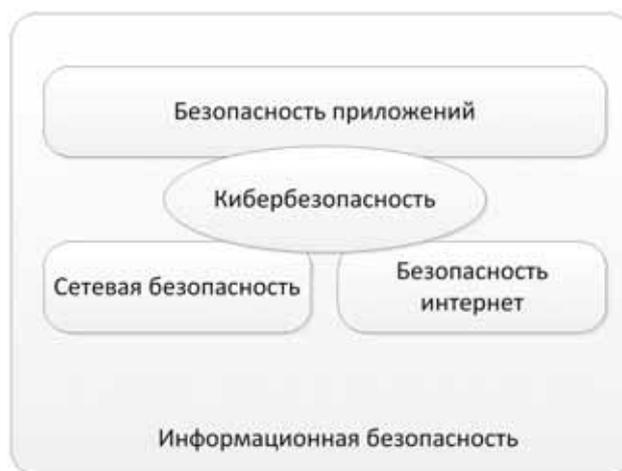


Рис. 2. Место понятия кибербезопасность

Выделяются две основных категории участников информационного взаимодействия (рис. 3): провайдеры и потребители.



Рис. 3. Участники информационного взаимодействия

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

По сути, в содержательной части стандарт представляет собой набор рекомендаций для провайдеров и потребителей по обеспечению кибербезопасности. Если для физических лиц рекомендации сводятся в основном к выполнению рекомендаций провайдеров, то про-

вайдеры должны реализовывать полноценную систему управления информационной безопасности в соответствии с требованиями стандарта ISO/IEC 27001 [9]. Подчеркивается важность анализа рисков и управления рисками согласно ISO/IEC 27005 [6].

Категории механизмов безопасности, предлагаемые для киберпространства, включают следующие аспекты:

- › Безопасность приложений
- › Защиту серверов
- › Защиту конечных пользователей
- › Защита от атак, связанных с использованием методов социальной инженерии.

На наш взгляд, акцент на организацию межсистемного взаимодействия, характерный для стандарта, нельзя назвать в полной мере обоснованным – тем самым, принятие аутентичного перевода ISO/IEC 27032 в качестве стандарта ГОСТ Р вряд ли целесообразно. В то же время, отдельные положения стандарта вполне могут быть задействованы при разработке аналогичного отечественного нормативного документа (например, в статусе документа Минобороны или ФСТЭК России).

Литература

1. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
2. Гольчевский Ю.В., Некрасов А.Н. К вопросу о кибербезопасности Интернет – пользователей // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 235-261.
3. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Информационное право. 2013. № 5. С. 10-13.
4. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С. 10-16.
5. Капто А.С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. № 7. С. 616.
6. Марков А.С., Цирлов В.Л. Управление рисками – нормативный вакуум информационной безопасности//Открытые системы. СУБД. 2007. № 8. С. 63-67.
7. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61-64.
8. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1(1). С.17-27.
9. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4-14.
10. Карцхия А.А. Развитие законодательства о промышленной собственности и реформа гражданского законодательства Российской Федерации // Мониторинг правоприменения. 2013. № 1. С.14-21.





**Родина
Валерия
Владимировна**
кандидат
политических наук

Особенности формирования законодательной базы промышленной политики на примере России и Германии

***Аннотация:** В статье рассматриваются особенности формирования законодательной базы промышленной политики, сравнивается опыт России и Германии. Выявляются принципы и закономерности реализации промышленной политики на региональном и наднациональном уровнях. Исследуется влияние обязательств, принятых Российской Федерацией в рамках вступления в ВТО, на развитие российской промышленности. Анализируются различные примеры легальных дефиниций промышленной политики в рамках имеющихся проектов федеральных законов. Сравняются цели и задачи, стоящие перед государственной промышленной политикой в России и Германии. Приводятся новые механизмы интеграции в условиях общей промышленной политики стран-участниц Евразийского экономического союза, которые также сравниваются с основными принципами промышленной политики Европейского союза. В своей статье автор приходит к выводу о целесообразности совершенствования законодательства для проведения эффективной промышленной политики.*

***Ключевые слова:** промышленная политика, региональный кластер, Евразийский экономический Союз, Европейский Союз, штандортная политика.*

В условиях внешнеполитических рисков, угрозы санкций, роста барьеров для трансфера технологий перед Россией стоит первоочередная задача – модернизация национальной промышленности.

Проводимая государственная политика в сфере развития промышленности способна повлиять не только на экономику, но и на все общественные институты, поскольку она признана определить наиболее значимые, стратегические направления развития страны, реализация которых способствует процветанию нации и обеспечению ее суверенитета.

Тем не менее, в настоящее время применение инструментов поддержки промышленности ограничено правилами ВТО. Выполнение обязательных соглашений ВТО потребовало пересмотра ряда мер государственной поддержки отечественных предприятий, однако в новых условиях Российской Федерации стали доступны такие инструменты поддержки, которые уже не первый год применяются во многих развитых странах, участницах торгового Союза.

В целом новая линия Правительства Российской Федерации по модернизации промыш-

ленного сектора лежит в общем тренде Таможенного Союза и Евразийского экономического союза, ее характеризует изменение парадигмы в реализации промышленной политики, которая с начала российских реформ не поддерживалась ведущими либеральными экономистами.

Логика либерального подхода заключается в том, что основа возможных экономических выгод от производства и торговли лежит, прежде всего, в импорте: чем импорт дешевле, тем лучше, даже если получается дефицит торгового баланса. Несколько иное мнение по вопросам промышленной политики было сформулировано в рамках неоклассицизма, когда, с одной стороны, предполагается создание конкурентоспособной промышленности, с другой – отставляется конкурентная среда, стимулирующая процессы международной специализации и научно-технический прогресс.

В современных условиях важными задачами государства в реализации промышленной политики, характерных как для России, так и для ряда западных стран являются:

➤ нормативное правовое регулирование промышленной деятельности;

- › создание новых инструментов поддержки и развития промышленной инфраструктуры, а также модернизация уже действующих;
- › создание промышленного сектора, конкурентного с иностранными предприятиями;
- › развитие ресурсосберегающих, безопасных и экологически чистых производств.

Перечисленные задачи в России уже частично реализуются по средствам проводимой государственной политики путем принятия федеральных целевых программ, отраслевых стратегий, государственных программ.

Правительством РФ были утверждены 5 государственных программ. Из них 4 отраслевые госпрограммы – авиационная, электронная и радиоэлектронная, фармацевтическая и медицинская, судостроительная – и 1 госпрограмма имеет межотраслевой характер. Также Минпромторгом России администрируется 16 стратегий развития различных отраслей и подотраслей промышленности.

Кроме того, для адаптации российской промышленности к новым условиям работы в рамках ВТО Правительством Российской Федерации был разработан План действий Правительства, направленных на адаптацию отдельных отраслей экономики к условиям членства Российской Федерации во Всемирной торговой организации, и План повышения темпов роста российской экономики, предусматривающие также мероприятия по поддержке секторов обрабатывающей промышленности.

Тем не менее, для систематизации мер развития промышленности, определения полномочий государственных органов и органов местного самоуправления реализуемая государством промышленная политика должна обладать полноценным правовым документом, имеющим фундаментальный характер.

В целях эффективной реализации ключевых инструментов промышленной политики в России необходимо наличие законодательного акта, предметом регулирования которого будут являться отношения, связанные с развитием промышленной деятельности.

Однако анализ выявил, что термин «промышленная политика» на федеральном уровне в законодательстве современной России не определен ни одним нормативно-правовым актом.

Понятие «промышленная политика» впервые упоминается в Указе Президента Российской Федерации «О мерах по реализации промышленной политики при приватизации государственных предприятий» № 1392

от 16.11.1992 г., но Указ не содержит никакого определения промышленной политики.

Существуют либо отклоненные, либо еще не принятые проекты, вводящие на федеральном уровне определение промышленной политики. К ним можно отнести – проект федерального закона №75357-5 «О развитии промышленности» (внесен в Государственную Думу ФС РФ 24.06.2008) и проект федерального закона №98281-5 «О национальной промышленной политике Российской Федерации», (внесен в Государственную Думу ФС РФ 11.09.2008).

В Проекте федерального закона №75357-5 «О развитии промышленности» в статье 3 дано следующее определение: «промышленная политика – система согласованных правовых, социально-экономических, организационных, информационных, научно-технических и иных мер, направленных на поддержку и рост промышленного производства, обеспечение его эффективности и высокой конкурентоспособности, содействие технико-технологическому процессу исходя из приоритетов устойчивого и сбалансированного социально-экономического развития территорий и страны в целом».

В Проекте федерального закона 98281-5 «О национальной промышленной политике Российской Федерации» в статье 3 дано следующее определение: «Национальная промышленная политика – система правовых и экономических мер и действий субъектов промышленной политики, исходящих из приоритетного обеспечения конкурентоспособности национальной экономики, стабильного и инновационного социально-экономического развития Российской Федерации, субъектов Российской Федерации, муниципальных образований».

В Проекте федерального закона «О промышленной политике в Российской Федерации», который был разработан Министерством промышленности и торговли Российской Федерации и внесен в Правительство РФ и Государственную Думу РФ в июне 2014 года, в статье 3 дано следующее определение: «Промышленная политика – комплекс правовых, экономических, организационных и иных мер государственного воздействия на промышленную деятельность, направленных на развитие промышленного потенциала Российской Федерации, обеспечение производства конкурентоспособной качественной продукции, повышение производительности труда, сбалансированное и стабильное развитие промышленности в целях социально-эко-

номического развития и обеспечения безопасности Российской Федерации».

Данный проект закона подготовлен в соответствии с Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, которая утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. Проект закона имеет вполне инструментальный характер, и потому проходил длительное общественное обсуждение и согласование в различных ведомствах. Несмотря на рамочный характер, он содержит правовые инструменты реализации промышленной политики.

Приведенные в перечисленных законопроектах формулировки в целом достаточно универсальны и единообразно отражают задачи, которые стоят перед государством, осуществляющим промышленную политику. Они подчеркивают, что к приоритетным задачам относится формирование правовой системы, обеспечивающей эффективную промышленную деятельность, направленную на развитие промышленного потенциала РФ.

Практически каждое определение включает в себя основное целеполагание – необходимость стимулирования промышленного производства, восполнение технологического отставания, снижение зависимости от импорта, низкой эффективности и повышение конкурентоспособности. Также определения содержат акцент на введении экологических и энергосберегающих методов производства.

Отсутствие определения промышленной политики в законодательстве ряда стран, в том числе с развитой промышленностью, а так же отсутствие полноценного закона о промышленной политике достаточно типичное явление в зарубежной юридической практике.

В результате анализа открытых источников было выявлено, что в нормативно-правовых актах Германии определение промышленной политики (*Industriepolitik*) отсутствует. Кроме того, отсутствует и документ, который бы регулировал промышленную политику на федеральном уровне, задавал рамки функционирования промышленной политики.

Также в открытых источниках отсутствует информация о наличии или подготовке федерального законопроекта о промышленной политике в ФРГ.

Расходятся и экспертные мнения относительно формулировки определения «промышленная политика». Так, авторитетная не-

мецкая энциклопедия «*Meuers Lexikon online*» определяет промышленную политику следующим образом: «Промышленная политика это любые действия государства (международные, федеральные, государственные или местные) в региональной и структурной политике, направленные на поддержание, формирование, регулирование и распространение промышленности».

Сайт Федерального агентства гражданского образования (*Bundeszentrale für politische Bildung, bpb*) дает следующее определение: «Сумма всех политических и организационных мероприятий, а также законодательных мер, которые направлены на поддержание промышленной структуры государства, на адаптацию промышленности к новым рыночным условиям (например, путем экспортных субсидий) или к новым экономическим и технологическим задачам (например, путем поощрения научных исследований и разработок)».

Один из основоположников немецкой концепции промышленной политики Гуттманн рассматривал её как «сумму всех мероприятий, как прямых, так и косвенных, по оказанию воздействия на предприятия промышленного сектора экономики», то есть исключал из неё другие сектора, в частности, сектор услуг. Другой немецкий эксперт Гален считал, что промышленная политика есть синоним «секторальной структурной политики», другими словами, использование методов структурной политики применительно к различным секторам, включая сектор услуг [1].

Ряд специалистов настаивает на том, что эта политика всё-таки должна ограничиваться только промышленным сектором экономики. Большинство экспертов сходятся во мнении, что промышленную политику в общем виде можно рассматривать как реакцию на проблемы отдельных секторов и отраслей и как поддержку структурной трансформации, в том числе, в направлении перехода на «инновационные пути развития» [2].

Все эти перечисленные определения свидетельствуют о том, что в научном сообществе Германии до сих пор ведутся дискуссии по формированию единого подхода к проведению промышленной политики.

Несмотря на отсутствие определения промышленной политики в национальном законодательстве и единых подходов к реализации промышленной политики как в России, так и в Германии, законодательное регулирование промышленной сферы можно встретить в ряде

документов регионального законодательства, а также международных соглашениях.

Появление нормативно-правовых актов, определяющих промышленную политику, в регионах России было связано, в первую очередь, с кризисными явлениями в промышленном секторе, которые были наиболее ощутимы на уровне субъектов Федерации. Необходимо было оперативно реагировать на вызовы времени.

Преимущественно механизмы поддержки региональной промышленности определялись не подзаконными актами, а системообразующим для всей правовой базы нормативно-правовым актом – региональным законом. Это указывает на постоянный характер закрепляемых положений и некую преемственность в реализации промышленной политики. Региональные законы, в первую очередь, определили приоритетные направления промышленной деятельности, приоритетные виды продукции, объекты государственного регулирования, способы государственной поддержки субъектов промышленной деятельности и источники финансирования.

На сегодняшний день на территории Российской Федерации Закон о промышленной политике принят в 29 субъектах страны.

Так, в Законе г. Москвы от 16.06.1999 № 21 «О промышленной деятельности в городе Москве». В статье 2 «термины и определения» указано: «Промышленная политика города Москвы – скоординированный комплекс мер (система) органов власти города Москвы, направленных на законодательное, экономическое, информационное, организационно – распорядительное регулирование в области промышленной деятельности, учитывающих промышленную политику федеральных органов государственной власти и интересы субъектов промышленной деятельности» .

В региональных законах обозначаются экономические, правовые и организационные основы промышленной политики. Преимущественно промышленная политика основывается на следующих принципах:

- создание условий для развития и увеличения промышленного и интеллектуального потенциалов, позволяющих субъектам промышленной деятельности активно адаптироваться к динамично изменяющимся требованиям внутреннего и внешнего рынков;
- поэтапное повышение эффективности промышленной деятельности, ориентированной на создание высоких и наукоемких техноло-

гий, обеспечивающих производство конкурентоспособной продукции;

- приоритетное развитие ресурсосберегающих, безопасных и экологически чистых производств;
- улучшение экологической обстановки;
- обеспечение занятости городского населения;
- содействие подготовке и переподготовке кадров;
- содействие развитию кооперационных и интеграционных процессов с другими регионами Российской Федерации, странами СНГ и дальнего зарубежья;
- равенство прав и ответственности всех субъектов промышленной деятельности;
- расширение налогооблагаемой базы.

Тем не менее, региональные законы характеризуются структурной неоднородностью и различными подходами к определению предмета промышленной политики, кроме того, регионы не демонстрируют единого подхода в правовом регулировании.

Помимо законов в регионах разработаны концепции и программы развития промышленности. Такая структура характерна порядка для 20 регионов РФ.

Подобный региональный подход к реализации промышленной политики характерен для многих западных стран: в настоящее время в нормативно-правовых актах Германии государственное регулирование промышленной политики происходит в рамках штандортной (территориальной) политики.

Немецкий экономист Альфред Вебер в своей работе «О штандортах промышленности. Чистая теория штандорта» еще в начале XX века предложил методологическую схему выбора оптимального места размещения предприятий. В ее основу он положил не столько принцип минимизации издержек производства и сбыта, сколько ввел понятие «фактор размещения» как четко выраженное преимущество, возникающее в процессе экономической деятельности. Данная теория позволяет рассматривать регионы (земли) как целостное хозяйственно-политическое и социальное пространство, имеющее свои четко определенные интересы и цели.

Наиболее успешными примерами штандортной политики на уровне регионов являются западные федеральные земли – Бавария, Баден-Вюртенберг, Бремен, Гамбург и восточные – Саксония, Тюрингия, Бранденбург, а также Берлин.

Относительно новым явлением стал процесс кластеризации немецких штандортов. Реги-

ональный кластер – это территориально сгруппированные компании, связанные друг с другом кооперацией и разделением труда, что дает им возможность для усиления своих и получения дополнительных конкурентных преимуществ. На основе таких кластеров в немецких регионах стали создаваться так называемые сети и центры компетенций, которые представляют собой попытки бизнес-сообществ получить дополнительные преимущества от кластеризации конкретных штандортов. Такие сети содействуют превращению региональных кластеров в инновационные центры национального, европейского и даже мирового значения и соответственно росту конкурентоспособности регионов, в которых они расположены [1].

Таким образом, региональный принцип формирования промышленной политики является достаточно распространенным явлением в мировой практике. В России он обусловлен кризисными явлениями в промышленном секторе, необходимостью оперативно реагировать на проблемы, стоящие перед той или иной отраслью, а в ФРГ данный принцип появился в результате приоритетного развития территорий и желания оптимально эффективно развивать промышленный сектор.

Описание целей и задач промышленной политики можно встретить и в международных соглашениях.

Так, в Соглашении между Правительством Российской Федерации и Правительством Республики Беларусь о проведении единой структурной промышленной политики (Минск, 8 сентября 1999 г.) указано, что стороны будут осуществлять меры по проведению единой структурной промышленной политики.

В программе «Структурная перестройка и экономический рост в 1997 – 2000 годах» не дается нормативного определения промышленной политики, тем не менее, определяются цели и методы промышленной политики. «С учетом сегодняшнего состояния промышленности главная цель промышленной политики на современном этапе реформ определяется как повышение эффективности и конкурентоспособности российской промышленности на внешнем и внутреннем рынках и ее подъема. Методы промышленной политики, применяемые в условиях рыночной экономики, достаточно разнообразны. Главными из них являются следующие:

› формирование институциональных и законодательных условий для развития позитивных структурных изменений в промышленности;

› реформирование налоговой системы с целью ее упрощения, обеспечения равномерности и посильности налогового бремени, создания условий для развития эффективного производства на основе самофинансирования;

› меры внешнеэкономической поддержки. В их число входят методы внешнеэкономического регулирования, такие, как ставки импортных тарифов, и меры специального регулирования, применяемые в рамках правил Всемирной торговой организации (ВТО)» .

В Соглашении о сотрудничестве в области промышленности и создании Совета по промышленной политике государств – участников СНГ (Ашхабад, 30 мая 2012 г.) под термином «промышленная политика» понимается следующее: «участие государств – участников настоящего Соглашения в формировании структуры и организации промышленности в целях стимулирования роста промышленного производства (обеспечение его эффективности и конкурентоспособности, содействие технико-технологическому процессу)» .

Кроме того, согласованная промышленная и экономическая политика с недавнего времени зафиксирована между Россией, Казахстаном и Белоруссией Договором о создании Евразийского экономического союза.

Подписание Договора о Евразийском экономическом союзе открывает самые широкие перспективы для трех стран, но уже не только как для торговых партнеров в рамках Таможенного Союза: появляются новые механизмы интеграции в условиях общей промышленной политики. Россия, Белоруссия и Казахстан переходят на принципиально новый уровень взаимодействия, создают общее пространство со свободным перемещением товаров, услуг, капиталов и рабочей силы. Государства «тройки» будут проводить согласованную политику в ключевых отраслях экономики – в энергетике, промышленности, сельском хозяйстве, транспорте.

В «Договоре о Евразийском экономическом союзе» в статье 62 «Промышленная политика и сотрудничество» дается определение целей промышленной политики: «Целями осуществления промышленной политики в рамках Союза являются ускорение и повышение устойчивости промышленного развития, повышение конкурентоспособности промышленных комплексов государств-членов, осуществление эффективного сотрудничества, направленного на повышение инновационной активности, устранение барьеров в промыш-

ленной сфере, в том числе на пути движения промышленных товаров государств-членов».

Особенностью немецкой, как и других европейских промышленных политик, также является необходимость их согласования с соответствующими органами Евросоюза, среди которых особое место занимает Совет по конкурентоспособности.

В тексте Маастрихтского договора есть раздел «Промышленная политика», в котором говорится о необходимости «облегчения» приспособления европейской промышленности к структурным изменениям, что свидетельствует о переходе к активной промышленной политике в ЕС.

В редакции Ниццкого Договора 2001 г. речь идет об обеспечении конкурентоспособности промышленности Сообщества и государств-членов. Согласно Статье 157, действия государств-членов направлены на:

- ускорение адаптации промышленности к структурным сдвигам;
- содействие созданию благоприятной среды развития во всем Сообществе предпринимательства, в особенности мелкого и среднего;
- содействие созданию благоприятных условий для сотрудничества между предприятиями;
- содействие лучшему использованию промышленного потенциала политики инноваций, проведению исследований и технологического развития.

Государства-члены должны консультироваться друг с другом и с Комиссией и, в случае необходимости, согласовывать свои действия.

В Лиссабонском договоре, например, появляются уже взаимные обязательства финансового характера, в частности речь идет о расходах на НИОКР не менее 3% своего ВВП.

В новой стратегии «Европа 2020: стратегия разумного, устойчивого и всеобъемлющего роста», принятой в 2010 году, в разделе «Промышленная политика в условиях глобализации» сформулированы основные принципы промышленной политики Европы. В частности, в стратегии говорится о помощи бизнесу (прежде всего малому и среднему) в преодолении экономического кризиса, его интеграции в мировой рынок, и введении экологических методов производства в промышленность.

Поскольку формирование консолидированной промышленной политики зачастую передано на уровень наднациональных союзов, государства-участники вынуждены согласовывать свою промышленную политику между собой. Можно предположить, что передача части

суверенитета наднациональным союзам объясняет отсутствие единого нормативно-правового акта на государственном уровне, что во многом компенсируется наличием региональных законов по промышленной политике.

Таким образом, можно отметить, что отсутствие понятия «промышленная политика» в законодательстве Российской Федерации – не уникальное явление, в мировой практике подобная ситуация наблюдается, в том числе, в промышленно развитой Германии.

На основании анализа был выявлен региональный принцип законодательного регулирования промышленной политики, который присущ как российскому законодательству, так и германскому. Его появление определяется необходимостью оперативного и точечного реагирования на проблемы, стоящие перед промышленным сектором.

Наднациональный принцип в промышленной политике явление относительно новое, оно связано с быстро развивающимися тенденциями кооперации государств на международном уровне. Очевидно, что в скором времени согласование приоритетов промышленной политики, в том числе, механизмов ее реализации будет передано в наднациональные органы.

Необходимо отметить, что определение «промышленной политики», приведенное в проектах федеральных законов, подчеркивает приоритетность формирования правовой системы для проведения промышленной политики. Определяет способность промышленной политики обеспечить суверенитет государства, которое ее осуществляет.

Таким образом, в сложившихся экономических и политических условиях применение традиционных механизмов промышленной политики требует новых подходов, которые должны быть зафиксированы на уровне федерального закона.

Литература

1. Андрианов К.Н. Промышленная политика Германии: основные аспекты и важнейшие направления // Вестник МГИМО-Университета. М., 2012. [Электронный ресурс] : офиц. текст. — Режим доступа : http://vestnik-old.mgimo.ru/filesserver/26/22_andrianov.pdf
2. Дрожжина Е.В., «Промышленная политика европейских стран», Доклады института Европы № 259, Москва, 2010
3. Анисимов В.Ф. Формирование муниципального уровня промышленной политики (Тео-

- ретические и методические аспекты) : Дис. ... канд. экон. наук : 08.00.05 : Москва, 2002.
4. Афанасьева М.В. Особенности государственной промышленной политики в условиях модернизации технологической среды : Дис. ... канд. экон. наук : 08.00.05 / М.В. Афанасьева ; [Рос. экон. ун-т им. Г.В. Плеханова].— Москва, 2011.
 5. Башкирцев А.С. , Маковкина С.А. Элементы формальных институтов в организации региональной промышленной политики // Вопросы управления, Выпуск №1(22). 2013.
 6. Гринберг Р.Г. О промышленном развитии России // Экономика и управление: Российский научный журнал. 2008. — №5.
 7. Горин Е.А. Организационно-экономические основы реформирования регионального промышленного комплекса. [Текст] : Дис. ... докт. экон. наук : специальность 08.00.05 / Е.А. Горин ; [С.-Петерб. гос. ун-т экон. и фин]. СПб., – 2001.
 8. Романова О.А. Промышленная политика: эволюция механизмов реализации // Современная конкуренция, 2008. — №6.
 9. Соколов А.В. Регулирование деятельности корпораций с участием государства как форма реализации промышленной политики: автореферат дис. ... докт. экон. наук ; 08.00.05 / А. В.Соколов ; [С.-Петерб. гос. ун-т экон. и фин].— СПб., 2011.
 10. Татаркин А.И. Промышленная политика как основа системной модернизации экономики России // Экономика и управление: Российский научный журнал, 2008. — № 2.
 11. Шаккум М. Национальная промышленная политика в свете присоединения к ВТО // Промышленная политика в Российской Федерации, 2007. — №1.
 12. Яньшина М.Н. Совершенствование механизма реализации промышленной политики в России : Дис. ... канд. экон. наук : 08.00.01 /М.Н. Яньшина ; [Место защиты: Волгогр. гос. ун-т].— Волгоград, 2013.
 13. Рыжов К.Б. Инкорпорация международных актов в российское законодательство и конкуренция юрисдикций // Мониторинг правоприменения. 2012. — № 4. С.30-46.





**Кубанков
Александр
Николаевич**
доктор военных наук,
профессор

Уточнение содержания учебной дисциплины «Правовые вопросы доступа к информации»

Аннотация: рассмотрена структура и содержание учебной дисциплины «Правовые вопросы доступа к информации». Обосновано включение в нее раздела «Стандартные политики управления доступом и информационными потоками». Внесено предложение по проведению практических занятий на примерах из финансово-кредитной сферы.

Ключевые слова: магистратура, информационная безопасность страны, информационная безопасность организации, доступ к информации.



**Половникова
Людмила
Сергеевна**

В РПА Минюста России реализуется одна из первых магистерских программ в стране «Правовое обеспечение информатизации и информационной безопасности» [1, 2]. Особую актуальность этот предмет получает в свете всемирного признания серьезной международной проблемы баланса между правом на доступ к информации, правом на тайну и ограничением доступа к потенциально опасному контенту, выразившегося в одобрении Первым комитетом Генеральной Ассамблеи ООН 11 ноября 2013 г. российской резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [3]. Учебный план [4] этой магистерской программы предусматривает изучение в третьем семестре ряда дисциплин [5], в частности, дисциплины «Правовые вопросы доступа к информации».

На данную дисциплину отводятся 2 зачетные единицы учебного времени (72 часа): из них на аудиторные занятия отводятся 24 часа, остальные – на самостоятельную работу. Из 24 часов аудиторных занятий 4 часа отводится на лекции, 8 – на семинары и 12 – на практические занятия. Видами промежуточных аттестаций являются курсовая работа и экзамен. Кроме того, по данной дисциплине разработана рабочая программа, и в течение 3-х лет дисциплина преподавалась в РПА Минюста России.

Целью изучения данной дисциплины является получение выпускником необходимых общекультурных и профессиональных компетенций, позволяющего успешно работать в избранной сфере деятельности [6]. Для достижения данной цели у слушателей формируется как необходимый объем теоретических знаний, так и практические навыки и умения. При выборе содержания дисциплины и методики ее преподавания авторы исходили из базового принципа востребованности тех или иных знаний и умений для должностей, предлагаемых современными работодателями юристам-специалистам в сфере информационной безопасности.

Предметную область дисциплины можно сегментировать на следующие разделы:

1. Право на доступ к информации. Институт правового режима информационных ресурсов.
2. Общедоступная информация.
3. Информация с ограниченным доступом.

4. Ответственность за нарушение правового режима информационных ресурсов.

Трехлетний опыт преподавания этой дисциплины позволяет сделать вывод, что содержание и методика преподавания требуют уточнения.

Во-первых, одобренная Первым комитетом Генеральной Ассамблеи ООН 11 ноября 2013 г. резолюция подтверждает остроту противоречия между основополагающими правами на информацию и на тайну. В связи с этим предлагается при изучении первого раздела провести два занятия (лучше с элементами игры) на темы: «Проблема баланса между правом на информацию и правом на тайну» и «Проблема ограничения доступа к потенциально опасному контенту».

Во-вторых, в рамках реализации распоряжения Правительства Российской Федерации от 29.11.2012 № 2204-р ФГУП «НПП «Гамма» с участием представителей федеральных органов исполнительной власти, научных организаций, бизнес-сообществ, общественных организаций, работодателей и образовательных организаций осуществляет разработку профессионального стандарта под названием «Специалист по информационной безопасности» [7].

В проекте стандарта среди знаний, необходимых для работы в сфере информационной безопасности, указывают знание основных видов политик (корпоративных нормативно-правовых актов) управления доступом и информационными потоками в информационных системах и основных формальных моделей управления доступом. А среди необходимых умений можно выделить разработку частных политик информационной безопасности предприятия, в том числе политики управления доступом и информационными потоками.

Исходя из изложенного, предлагается включить в программу учебной дисциплины «Правовые вопросы доступа к информации» раздел «Стандартные политики управления доступом и информационными потоками».

В-третьих, данная дисциплина предполагает проведение практических занятий. Естественным является обучение на них лучшим корпоративным практикам. Полагаем, что организациями, обладающими лучшей практикой обеспечения информационной безопасности, являются организации финансово-кредитной сферы. В финансовой сфере вопрос защиты информации всегда был одним из важнейших, включая правовую охрану банковской тайны, правовое

обеспечение автоматизированных информационных систем и безопасности клиентских удаленных сервисов. К традиционным сферам ответственности добавились защита персональных данных, увеличив нагрузку подразделений информационной безопасности банков.

С учетом того, что в банковской сфере вопросы защиты информации и доступа к информации решены на самом высоком нормативном и техническом уровне [8], предлагается проводить практические занятия на примерах правового регулирования доступа к информации в организациях финансово-кредитной сферы.

Литература

1. Морозов А.В., Филатова Л.В. О работе кафедры информационного права, информатики и математики РПА Минюста России // Информационное право. – 2013. – № 3. – С. 14–15.
2. Морозов А.В. Структура и содержание магистерской программы «Правовое обеспечение информационной безопасности» // Правовая информатика. – 2012, № 2. – С. 41–46.
3. «России сослужили хорошую спецслужбу» // Газета «Коммерсантъ», № 206, 11.11.2013.
4. Крылов Г.О., Кубанков А.Н. Учебный план магистерской программы «Правовое обеспечение информационной безопасности» // Информационное право, 2013. – № 3. – С. 18–21.
5. Кубанков А.Н. Содержание учебной дисциплины «Система обеспечения информационной безопасности России» // Правовая информатика, 2013. – № 1. – С. 45–47.
6. Кубанков А.Н., Сахнин А.А. Опыт взаимодействия вуза и инновационного предприятия при подготовке специалистов для сферы безопасности радиосвязи // Безопасность информационных технологий, 2012. – № 1. – С. 33–36.
7. Проект Профессионального стандарта «Специалист по информационной безопасности» [Электронный ресурс]. – Режим доступа: http://azi.ru/component/option,com_docman/task,doc_download/gid,37/Itemid,/ свободный (загрузка). – Загл. с экрана.
8. Евстифеева Н.А., Крылов Г.О., Рябков В.Е. Признаковое пространство в задачах анализа репутационных рисков кредитных организаций как субъектов финансовой и информационной безопасности // Правовая информатика, 2012. – № 3. – С. 17–18.

Сведения об авторах

БАРАБАНОВ Александр Владимирович – старший преподаватель МГТУ им.Н.Э.Баумана.
E-mail: ab@сnpo.ru

ГОРБАЧЕВА Елена Викторовна – начальник научно-исследовательской лаборатории юридических техник и лингвистического обеспечения.
E-mail: gorbacheva@scli.ru

ДОБРЯКОВА Галина Эдуардовна – кандидат юридических наук, доцент, Российская государственная академия интеллектуальной собственности, г. Москва.
E-mail: galina@dobriakova.ru

ЕРОХИНА Юлия Владимировна – кандидат юридических наук, доцент кафедры теории права и сравнительного правоведения факультета права, Высшая школа экономики, г. Москва.
E-mail: yerohina@hse.ru

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

ЛЕОНТЬЕВА Валерия Борисовна – аспирант ФГБОУ ВПО «Финансовый университет при Правительстве Российской Федерации», г. Москва.
E-mail: info@sois.ru

НИКУЛИН Михаил Юрьевич – старший преподаватель МГТУ им.Н.Э. Баумана, г. Москва.
E-mail: m.nikulin@сnpo.ru

ПОЛОВНИКОВА Людмила Сергеевна – магистрантка Российской правовой академии Минюста России, г. Москва.
E-mail: sula871@gmail.com

РЗАЕВ Али Гейдар оглы – доктор юридических наук, главный научный сотрудник Института Философии и Права НАН Азербайджана, г. Баку.
E-mail: professorqurbanov@yandex.com

РОДИНА Валерия Владимировна – кандидат политических наук референт заместителя Министра промышленности и торговли Российской Федерации, г. Москва.
E-mail: velnews@mail.ru

САВИЧЕВ Алексей Аркадьевич – ведущий юрисконсульт отделения формирования входного потока ФБУ НЦПИ при Минюсте России, г. Москва.
E-mail: ucx7801@mail.ru

ТОНКОНОГОВ Александр Викторович – доктор философских наук, научный руководитель Российского центра стратегического моделирования г. Москва.
E-mail: alekstonkonogov@yandex.ru

ЦИРЛОВ Валентин Леонидович – кандидат технических наук, исполнительный директор, CISSP, АМВСІ ЗАО НПО «Эшелон», г. Москва.
E-mail:partners@npo-echelon.ru

ЧХУТИАШВИЛИ Лела Васильевна – кандидат экономических наук, доцент – кафедры философских и социально-экономических дисциплин Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва.
E-mail: lela@email.ru

Abstract and keywords

A.V. Tonkonogov

Ensuring Russia's cybersecurity under today's geopolitical conditions

Abstract: The paper is devoted to problems of ensuring the cybersecurity of today's Russia, the author's definitions of such notions as cybersecurity, cyberwar, and cyber revolution are given, legal and organisational measures for counteracting threats in the cybersecurity sphere are propounded.

Keywords: cybersecurity, ensuring national security, cyberwar, cyber revolution, today's Russia, geopolitical rivalry.

A.G.o. Rzaev

The content and nature of public administration

Abstract: In the paper an analysis of the meaning and notion of public administration is presented and its systemicity is studied, as well as such constituent parts of control systems as subject, object, feedforward and feedback connection, information. Also considered are the relation between control and regulation and the control system in a living organism as an example of a classic cybernetic system.

Keywords: public administration, subject and object of control, feedforward and feedback connection, system analysis, cybernetics, information, regulation, living organism, homeostasis.

V.L. Tsirlov, M.Yu. Nikulin

Legal foundations for the certification of data protection solutions

Abstract: An overview of the basic laws and regulations underlying the certification of data protection solutions in accordance with information security requirements is presented. The structure of the main systems of mandatory certification is considered. A comparative analysis of the legal aspects of organisation of each certification system is made.

Keywords: technical regulation, mandatory certification, secrets protection.

L.V. Chkhutiashvili

Electronic money transfers in today's banking laws

Abstract: This paper is devoted to issues of development of legal regulation of electronic money transfers in today's banking laws of the Russian Federation.

Keywords: electronic money, electronic means of payment, the national payment system, commercial banks, non-bank credit organisations.

Yu.V. Erokhina

Problems of information support for combating corruption

Abstract: New trends in combating corruption activities that are related to the development of information components are identified. Proposals for improving anti-corruption activities are worked out on the basis of using acceptable ways of combating corruption in the Russian Federation and the Republic of Belarus. The information basis of the paper comprises official statistical documents, scientific and analytical materials and reports, international statistical data, documents and analytical blueprints of Belarus and Russia's social and economic development, scientific papers and periodical articles, and other sources.

Keywords: combating corruption, information security, information, anti-corruption policy.

G.E. Dobryakova

Problems of identification in information systems

Abstract: Existing ways of identifying natural and juridical persons in information systems as well as related problems and prospects are considered in the paper. A characterisation of the Russia's Unitary Russian Standard for Universal Electronic Cards Identification and the prospects of its development are given.

Keywords: identification, information systems, universal electronic card (UEC).

V.B. Leontyeva

Technical and legal foundations of value formation

Abstract: The main interdisciplinary factors determining the formation of value and business, that is, intellectual property and use value of goods and services are validated in the paper. Use value that reflects the usefulness of goods is always individual for each consumer. Its transformation into market value occurs due to market supply and demand. The source of use value is intellectual property as a most important value forming factor. All modern economy is gradually transforming into the economy of intellectual property.

The economic and legal institution of intellectual property that has been evolving over the last five hundred years, expanding slowly, remains the most stable knowledge and legal system.

Keywords: business, state, innovations, intellectual property, formation of value, use value, goods, services, management, factor, price formation, economy.

A.A. Savichev

A comparative analysis of securing access to information in city self-government system: history and today

Abstract: The paper is devoted to issues of exercising the right to information access in Russia at the municipal government level in the 19–20 centuries and today. The implementations of this right in the past and under today's conditions are compared.

Keywords: local self-government, city self-government, right to information access, federal register.

E.V. Gorbacheva

Informatics as a theory determining an optimal organisation of information work

Abstract: The paper tells about the need for competence in the field of informatics, legal information, and informatisation.

Keywords: informatics, information, legal information, informatisation, informatiology, information system, text, linguistic support.

Aleksandr Barabanov, Ph.D., Senior Lecturer, Bauman MSTU

Regulatory issues of information security software production

Abstract: The problems of standardization process to develop safe software are considered. The main provisions of the draft Standard "Information Security. Developing secure software. Requirements" are analyzed. The possibility of harmonization of this standard with ISO 27000 and ISO 15408 is shown.

Keywords: security software tool, software vulnerability, software bugs.

V.L. Tsirlov

Legal foundations of cybersecurity in Russia

Abstract: Basic cybersecurity standards and guidelines are considered. A brief overview of the Cybersecurity strategy in Russian Federation and of the international standard ISO / IEC 27032 is given. Analysis of possible ways to develop corresponding standards is presented.

Keywords: cybersecurity, information security, guidelines, standards, regulations

V.V. Rodina, Ph.D.

Peculiarities of formation of legislative base of industrial policy on the example of Russia and Germany

Abstract: The features of formation of the legal framework of industrial policy are discussed in this article, also compared to the experience of Russia and Germany. It identifies the principles and laws of industrial policy at the regional and supranational levels. The impact of commitments, which was made by the Russian Federation to the WTO accession on the development of Russian industry are examined in the article. The various examples of industrial policy legal definitions are analyzed in the existing federal bills. The author compares the goals and tasks of the state industrial policy in Russia and Germany. Provides new mechanisms for integration in a common industrial policy of the Eurasian Economic Union member countries, which are also compared with the basic principles of the European Union Industrial Policy. The author concludes that formation of the feasibility of legislative perfection is the priority for effective industrial policy.

Keywords: *Industrial policy, regional cluster, the European Union, the Eurasian Economic Union, Standort policy.*

A. N. Kubankov, L. S. Polovnikova

Elaborating the contents of the academic discipline “Legal Issues of Access to Information”

Abstract: In the paper, the structure and contents of the academic discipline “Legal Issues of Access to Information” are considered. A justification is given for including a new section in it entitled “Standard policies for controlling access and information flows”. It is proposed to hold training workshops using the examples taken from the finance and credit field.

Keywords: Master’s programme, the country’s information security, an organisation’s information security, access to information.

Над номером работали:

Главный редактор
Ответственный секретарь
Ответственный редактор
Литературный редактор
Выпускающий редактор
Компьютерная верстка
Тиражирование (печать)

А.В. Федичев
Э.И. Атагимова
Ю.В. Матвиенко
Е.В. Горбачева, Т.В. Галатонов
И.Г. Колмыкова
А.С. Михеева
Н.Г. Шабанова

Требования, предъявляемые к рукописям, направляемым в редакцию

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