

ПРАВО, ВЫСОКИЕ ТЕХНОЛОГИИ, НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ¹

© 2018 г. М. В. Демьянец^{1,*}, Е. В. Понизова^{2,**}, В. А. Михайловская^{3,***}

¹Российская академия народного хозяйства и государственной службы
при Президенте РФ, Москва;

Московский государственный педагогический университет;
Информационно-правовой центр “Правоинформ”, Москва

²Российская академия наук, Москва

³Институт государства и права РАН, Москва

*E-mail: mvd@cpinf.ru

**E-mail: evp@cpinf.ru

***E-mail: varvaramih91@bk.ru

Поступила в редакцию 26.12.2017 г.

В статье рассматриваются роль права в регулировании высоких технологий, проблемы, возникающие в процессе их создания, внедрения и использования, а также тенденции развития экономики и государственного управления в условиях цифровизации и информатизации.

Ключевые слова: правовое регулирование, информационные технологии, робототехника, автоматизация, искусственный интеллект, идентификация, информационные системы, информационные сети, информационная безопасность, национальная безопасность, средства защиты информации, конкуренция.

DOI: 10.7868/S0132076918060124

18–20 декабря 2017 г. состоялся Международный форум “Право, высокие технологии, национальная безопасность” (*International Law & Technology Forum 2017/ILTF 2017*)² (далее – Форум). Мероприятие было организовано Информационно-правовым центром “Правоинформ” при поддержке Института права и национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте РФ (РАНХиГС).

Партнеры ILTF 2017: *стратегические партнеры* – Ассоциация российских банков (АРБ), Ассоциация юристов России (АЮР); Юридическая фирма “ЮСТ”; *информационные партнеры* – информационно-аналитический телеканал “Царьград”, Moscow Business School, Центр исследований киберпространства НИУ ВШЭ, информационный портал sobytiye.ru, интернет-журнал про образовательную робототехнику и роботов Robotoved.ru; *рекламно-информационный партнер* – Contrast Group; *партнер форсайт-проектов* – Некоммерческое партнерство по поддержке инновационных исследований “Неправительственный инновационный центр” (НП НИЦ).

Форум проходил впервые, но по результатам многодневной работы участниками и партнерами было принято решение о необходимости ежегодного его проведения для развития технологий и информации в России в условиях их активного использования и появления новых; формулирования предложений по гармонизации законодательства,

регулирующего создание, внедрение и использование технологий настоящего и будущего, защиты информации, обеспечения национальной и информационной безопасности; демонстрации разработок бизнеса и государства в сфере технологий и защиты информации; обмена опытом о существующих проблемах в сфере информационных технологий и способов их преодоления.

Основной задачей, поставленной при организации ILTF 2017, стало формирование открытой площадки с привлечением специалистов различных областей знаний для обсуждения будущего правового регулирования высоких технологий, включая робототехнику, искусственный интеллект, нейронные сети и др.; эффективного и безопасного их использования; защиты интересов общества, государства и бизнеса с учетом появления новых вызовов и угроз; обеспечения конкурентоспособности последних в процессе развития цифровой экономики и глобализации социальных, экономических и политических процессов.

В работе Форума приняли участие представители органов государственной власти различных уровней; крупных корпораций; юридических компаний и адвокатских образований; финансовых организаций; производители и интеграторы программного обеспечения, техники и информационных систем; экспертных, научных и общественных организаций.

Докладчиками в рамках пленарного заседания и профильных секций выступили представители сферы информационных технологий, финансового сектора, юристы и другие заинтересованные лица.

¹ Статья подготовлена при поддержке РГНФ. Проект № 16-03-00679.

² См.: Официальный сайт ILTF 2017: URL: <http://iltf.ru>

На пленарном заседании выступили ведущие российские эксперты, имеющие опыт построения инновационных центров и наукоградов, экспертизы информационного законодательства, судебной практики, а также участвующие в формировании системы правовых гарантий, стратегическом планировании государственных и бизнес-процессов. Они поделились уникальными знаниями и навыками о перспективах развития высоких технологий с учетом национальных и мировых тенденций; новых подходах к обеспечению национальной и информационной безопасности; перспективах и последствиях внедрения искусственного интеллекта, робототехники, сетей связи нового поколения и других высоких технологий.

Модератором пленарного заседания выступил **начальник Научно-организационного управления РАН, д-р юрид. наук, проф., заслуженный юрист РФ Н.И. Михайлов**, который отметил, что необходимость рассмотрения многих вопросов, обозначенных в программе ILTF 2017, связана не только с состоянием сегодняшнего правового регулирования современных технологий, в том числе электронных, информационных, но и с перспективами их внедрения. В условиях активного развития технологий, использования новых достижений науки и техники в различных сферах экономики огромное значение имеет как грамотное, эффективное законодательство, так и практика его применения, формирующаяся в России и за рубежом и еще требующая совершенствования с учетом потребностей общества, бизнеса и государства.

От *организаторов* выступили: **заместитель директора Института права и национальной безопасности РАНХиГС по научной работе, зав. кафедрой государственного управления и национальной безопасности, доктор полит. наук, проф. А.В. Шевченко** и **директор Информационно-правового центра “Правоинформ”, канд. юрид. наук, доц. М.В. Демьянец**.

В рамках приветствия участникам ILTF 2017 **А.В. Шевченко** отметила, что тематическая повестка мероприятия охватывает обширную область сверхактуальных проблем, с которыми столкнулось государство в сфере экономики, финансов, в социальной, политической, духовной жизни, несмотря на серьезные позитивные перемены по многим важнейшим направлениям общественного и государственного развития. Высокотехнологичные страны за один год проживают 5–7 российских лет, что показывает анализ позиций России по основным направлениям производственной революции. Так, согласно данным международной Федерации робототехники, по состоянию на конец 2016 г. плотность роботизации в России составила всего два робота на 10 тыс. работающих, что также подтверждается Национальной ассоциацией участников рынка робототехники (Россия). Для сравнения: на 10 тыс. занятых в промышленности работников в Южной Корее приходится 478, Японии — 314, Германии — 292, США — 164 робота. Аналогичная ситуация складывается в области искусственного интеллекта. 50 лидирующих компаний контролируют 90% мирового рынка информационных технологий. 39 компаний приходится на Соединенные Штаты Америки, по три — на Великобританию,

Китай, Израиль. При этом только три государства: США, Великобритания и отчасти Китай, — лидируют в разработках карт для искусственного интеллекта будущего.

А.В. Шевченко также полагает, что недооцененной в России остается технология дополненной реальности, которая, по мнению специалистов, превзойдет эффекты Интернета через Интернет вещей. Первые серьезные продукты в этой сфере ожидаются уже в конце нынешнего — начале следующего года.

М.В. Демьянец в продолжение сказанного добавил, что развитие высоких технологий требует не только увеличения количества разработок, но и совершенствования их правового регулирования. Данный тезис был основан на принимаемых в Российской Федерации концептуальных и доктринальных документах, в которых среди приоритетных направлений развития российских информационных и коммуникационных технологий названы: искусственный интеллект, робототехника, биотехнологии, сети связи нового поколения, обработка больших данных, Интернет вещей, индустриальный интернет и др.³

Было подчеркнуто, что экспертным сообществом неоднократно акцентировалось внимание на необходимости развития и стимулирования обозначенных направлений, в том числе посредством совершенствования действующего законодательства. Например, с участием специалистов в области информационных технологий и российских юристов в 2016 г. был разработан проект федерального закона “О внесении изменений в Гражданский кодекс Российской Федерации в части совершенствования правового регулирования отношений в области робототехники”⁴. На уровне Европейского Союза значимость обсуждения и необходимость установления надлежащего правового регулирования достижений в сфере кибернетики, робототехники и других высоких технологий находит свое отражение не только в ежегодных форумах по робототехнике, проводимых с 2010 г. (*EU Robotics Forum*), но и в законодательных инициативах Европарламента. Россия как государство с высокоразвитой экономикой, определяющее среди своих основных приоритетов создание, внедрение и использование высоких технологий, по мнению **М.В. Демьянца**, не может игнорировать такие инициативы, а должна осуществлять поиск собственных форматов для обсуждения вопросов в сфере высоких технологий, представляющих особый интерес для общества и государства.

Заместитель Президента РАН, д-р экон. наук, канд. тех. наук, чл.-корр. РАН В.В. Иванов в своем докладе осветил важнейшие проблемы законодательного обеспечения научно-технологического развития Российской Федерации. Принятие Стратегии национальной безопасности (декабрь 2015 г.) и Стратегии научно-технологического

³ См.: Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20, ст. 2901.

⁴ Россия может первой узаконить роботов. URL: <http://www.vedomosti.ru/technology/articles/2016/12/15/669703-rossiya-uzakonit-robotov> (дата обращения: 07.06.2017).

развития Российской Федерации до 2035 года (декабрь 2016 г.) задало новый вектор развития научно-технологического сектора экономики. При этом переход к новой политике развития объективно требует пересмотра научного законодательства, основу которого составляет Федеральный закон “О науке и государственной научно-технической политике”, принятый в 1996 г.

Современное законодательство в сфере науки не соответствует требованиям принятых стратегических документов и является тормозом научно-технологического развития России. Законодательная система науки нуждается в существенной корректировке в плане обеспечения развития научно-технологического потенциала страны. Необходимо разработать и принять свод законов, регламентирующих все аспекты развития научно-инновационного комплекса.

Этому должна предшествовать разработка и принятие новой доктрины развития российской науки как системы взглядов на роль и значение науки в обеспечении как развития страны, так и национальной безопасности, а также принципов государственного регулирования научной деятельности. На основе доктрины должна быть сформирована новая государственная научно-инновационная политика, ориентированная на достижение в долгосрочной перспективе мирового технологического лидерства. В мировой практике подобная постановка задачи не нова — именно так ставили задачу развития Евросоюз, Финляндия, Китай и многие другие страны, совершившие в конце XX — начале XXI в. качественный технологический рывок.

Политические документы должны составить основу для выработки нового научного законодательства. При этом следует отказаться от сложившейся практики монополизма органов исполнительной власти в сфере формирования научной политики и управления наукой. Представляется, что политическая функция, т.е. определение научно-инновационной политики, должна стать прерогативой Президента РФ, при котором целесообразно создать специальный совещательный орган. Собственно выработкой научно-инновационной политики должна заниматься Российская академия наук как структура, объединяющая наиболее квалифицированных ученых и специалистов из различных секторов экономики, а также ориентированная на решение стратегических задач развития государства.

Советник министра Министерства имущественных отношений Московской области, канд. юрид. наук М.Н. Шувалов в приветственном слове участникам ILTF 2017 отметил, что совершенствование правового регулирования кибернетики, робототехники и высоких технологий представляет для юридического сообщества особый интерес. Более того, в условиях активного развития нейронных сетей и использования робототехники в различных сферах экономики открытое их обсуждение профессиональным юридическим сообществом (с позиции науки и практики) может иметь особую значимость для развития гражданского, предпринимательского, энергетического и других отраслей права.

Старший партнер юридической фирмы “ЮСТ”, д-р юрид. наук, проф., акад. РАН А.Г. Лисицын-Светланов в докладе *“Новые вызовы и угрозы национальной безопасности в сфере экономики: правовой аспект”* обратил особое внимание на стремительное развитие технологий вообще и цифровых технологий, в частности, что активно усиливает конкуренцию между государствами, совпавшую с политической фазой кризиса однополярного мира, т.е. в конфликтной ситуации. Значит, технология по своей природе, тем более цифровая, не может быть национальной, она возникает вне границ.

Докладчик также выделил вопросы создания и внедрения технологий в различных сферах противодействия угрозам безопасности, включая использование высокотехнологичного оружия и новых видов вооружений, информационную безопасность и международное сотрудничество в области высоких технологий. При этом среди основных задач в обозначенных сферах были названы развитие конкуренции на международных и национальных рынках, защита интеллектуальной собственности, а также затронута роль государства в обеспечении информационной безопасности. С учетом специфики информационных отношений и их экстерриториальности, по мнению А.Г. Лисицына-Светланова, решение существующих проблем возможно не только посредством национального, но в первую очередь международного права.

Заместитель председателя Правления АЮР Д.И. Паньшин уделил внимание направлениям деятельности Ассоциации юристов России в части совершенствования правового регулирования высоких технологий и необходимости развития законодательства в сфере робототехники, искусственного интеллекта, информационных и информационно-коммуникационных технологий, в том числе в контексте реализации Программы “Цифровая экономика Российской Федерации”. Д.И. Паньшин отдельно остановился на проблемах правового регулирования криптовалют и подходах стран БРИКС к их решению, а также вопросах противоправного использования информационных технологий в целях легализации доходов, полученных преступным путем.

В завершение работы пленарного заседания по проблемам правового регулирования высоких технологий выступила **зав. сектором информационного права Института государства и права РАН, д-р юрид. наук, заслуженный юрист РФ Т.А. Полякова**, остановившись на деятельности Союзного государства по формированию единого научно-технологического пространства, а также развитию робототехники как одной из приоритетных высокотехнологичных сфер. В частности, были рассмотрены одобренная 16 февраля 2017 г. Европарламентом резолюция и работа по формированию Европейского агентства по роботизации и искусственному интеллекту.

В рамках дискуссии на пленарном заседании отмечалась роль научных фундаментальных и прикладных исследований, которые (как и в зарубежных странах) должны составлять основу для надлежащего функционирования государства, бизнеса, обеспечения их конкурентоспособности, а также прогнозирования их

развития в краткосрочной, среднесрочной и долгосрочной перспективах.

Тенденции эволюции робототехники, искусственного интеллекта, других высоких технологий и проблемы законодательного регулирования и юридической практики были обсуждены в рамках **профильных секций**: *“Робототехника, роботизация и автоматизация государственных и бизнес процессов”*, *“Информационные сети и системы, нейронные сети (проблемы создания и эксплуатации, перспективы государственного и правового регулирования)”*. Модераторами выступили: директор Центра исследований киберпространства НИУ ВШЭ, канд. юрид. наук **А.К. Жарова**, заместитель зав. кафедрой информационной безопасности факультета бизнеса и менеджмента НИУ ВШЭ **В.М. Елин**, директор Информационно-правового центра “Правоинформ”, канд. юрид. наук **М.В. Демьянец**.

В рамках указанных секций было отмечено, что роботизация и автоматизация процессов на производстве, в управлении происходят не первый год, активное внедрение автоматизированных систем управления осуществлялось еще со времен СССР. Только всестороннее изучение имеющегося опыта производства, внедрения и эксплуатации роботизированной и автоматизированной технологий позволяет тщательно проработать существующие правила и сформулировать предложения по совершенствованию законодательства с учетом национальных потребностей и мировых тенденций. Человек использует технологии, информационные сети и системы для локального и удаленного хранения информации и данных, их передачи и обработки. Сегодня уже сложно представить организацию труда, производства, управления без применения технологий. В зависимости от количества пользователей, задач, стоящих перед ними, вида профессиональной деятельности, в которой применяются технологии, появляются новые направления и сферы их использования.

Исполнительный директор “Право.ру” **А.Я. Сарапин** посвятил свое выступление специфическому направлению, которое в последние годы вызывает особый интерес. Речь идет о *Legal Tech* – сфере, основанной на использовании информационных и информационно-коммуникационных технологий при оказании юридических услуг, а также автоматизации юридического бизнеса. Он отметил, что “Право.ру” с 2008 г. ведет активную деятельность по внедрению в юридическую сферу технологий, которая началась с создания собственных сервисов справочно-правовой системы и интеграции разработок компании в деятельность арбитражных судов. К 2010 г. была создана и запущена в эксплуатацию картотека арбитражных дел, объединявшая на тот момент 112 арбитражных судов, в 2012 г. запущена система “Мой арбитр”. Названные продукты, созданные “Право.ру”, направлены на автоматизацию юридических процессов совершенствования порядка обмена электронными документами посредством информационных сетей и систем, используемых участниками судебного процесса и судом. Были рассмотрены вопросы придания юридической силы электронным документам,

использования биометрических данных, идентификации пользователей и взаимодействия частных и государственных информационных систем (например, ГАС “Правосудие”) для целей обеспечения интересов участников производства и судебной системы.

Продолжая тему использования информационных сетей и систем в обеспечении автоматизации и роботизации государственных и бизнес-процессов, **А.К. Жарова** отметила, что согласно Распоряжению Правительства РФ от 1 ноября 2013 г. № 2036-р “Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года” значительное влияние на большинство сегментов отрасли окажет тенденция перехода к “облачным” вычислениям. С учетом этого необходимо совершенствование нормативно-правовых актов, позволяющих бизнесу развиваться наиболее эффективно.

Опираясь на исследования перспектив развития облачных вычислений Института инженеров по электротехнике и электронике (IEEE) **А.К. Жарова** привела сформулированное названной организацией понятие облачной обработки данных, под которой понимается информация, постоянно хранящаяся на серверах в Интернете и временно кэшируемая на клиентской стороне, например на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т.д.

В обеспечении надежности работы “облачного сервиса” огромное значение, по ее мнению, имеют центры обработки данных облачных вычислений, которые часто распространяются по разным географическим регионам как на национальном, так и на глобальном уровне. Функционирование таких центров позволяет гарантировать устойчивость к региональным проблемам и локальным чрезвычайным ситуациям, таким как штормы, землетрясения или кабельные сокращения, а также может использоваться для уменьшения количества определенных вида сетевых атак типа “отказ в обслуживании” (DoS-атаки), позволяя клиентам получать доступ в других местах; способствовать снижению латентности Сети, поскольку услуги предоставляются с сайтов, расположенных в непосредственной географической близости к клиенту; улучшить общую доступность и эффективность обслуживания.

При анализе положения действующих нормативных актов и других официальных документов органов государственной власти, устанавливающих обязательные для соблюдения требования и рекомендации по защите информации в “облаках”, обеспечению прав пользователей, высказано предложение о необходимости разработки для облачного сервиса стандарта, определяющего требования к его функционированию, устойчивости, безопасности и др. Отдельное внимание было уделено роли международных стандартов и сложившейся в иностранных государствах практики обеспечения надежности работы облачного сервиса, а также значению российского гражданского законодательства в решении поставленных проблем.

В.М. Елин рассмотрел вопросы обеспечения информационной безопасности при использовании облачных технологий, рассказал о влиянии российских и международных стандартов, европейского и американского законодательства на данную сферу и высказал предложение о необходимости принятия федерального закона “Об оказании облачных услуг”, создании профильных рабочих групп по обозначенному направлению.

О проблемах развития информационных систем и сетей в контексте использования данных в Интернете вещей высказался **консультант международно-правовой практики O2 Consulting Р. Нуруллаев**. Было отмечено, что внедрение Интернета вещей создает вызовы, которые могут потребовать совершенствования обеспечения безопасности; установления новых нормативных требований к совместимости устройств и защите конкуренции; правового режима данных и возможности их коммерциализации; принципов информированности и добровольности обработки данных. В контексте поставленных проблем докладчик привел несколько примеров о распространении данных, получаемых в результате использования технологии Интернета вещей без согласия пользователей, и рассмотрел возможную сделку компании Roomba о “продаже” данных о планировках квартир и расстановки мебели в них, полученных роботами-пылесосами IRobot.

Р. Нуруллаевым был проанализирован опыт правового регулирования Европейского Союза и обозначены возможные перспективы законодательного регулирования и создания в России государственного оператора больших данных, уполномоченного в том числе на осуществление государственного контроля и надзора и саморегулируемой организации — Ассоциации больших данных.

В завершение первого дня Международного форума “Право, высокие технологии, национальная безопасность” выступил **руководитель Исследовательского центра проблем регулирования робототехники и искусственного интеллекта (АНО “Робоправо”), канд. юрид. наук А.В. Незнамов**, посвятивший свой доклад не только истории развития регулирования новых технологий на примерах США, Англии, Германии, но и существующим подходам к регулированию искусственного интеллекта и робототехники в Европейском Союзе, Японии, Южной Корее, Китае. Были названы и проанализированы инициативы названных стран, концепции и принятые нормативно-правовые акты.

Исходя из зарубежного опыта регулирования и практики, А.В. Незнамов предположил, что необходима разработка Концепции, определяющей подходы, общие принципы, цели и задачи развития искусственного интеллекта и робототехники, и только после ее принятия можно говорить о формировании внутреннего законодательства. В противном случае поспешное принятие нормативно-правовых актов может причинить вред использованию и внедрению названных технологий или воспрепятствовать их развитию.

Отдельное внимание было уделено Модельной конвенции о робототехнике и искусственном интеллекте, планируемой к обсуждению в Государственной Думе и направленной в Организацию Объединенных Наций. Названный документ состоит из нескольких разделов и объединяет все существующие вопросы, требующие регулирования, в частности правила безопасности, создания, использования роботов, разработки искусственного интеллекта, ограничения при использовании военных роботов, развитие правил робототехники и искусственного интеллекта.

Второй день Форума начался с **секции “Обеспечение защиты информации, информационная безопасность государства, бизнеса, общества, личности”**. Модератор — Председатель Совета НП НИЦ С.И. Бочков.

Открыл секцию **президент АРБ, д-р юрид. наук, канд. физ.-матем. наук, проф., чл.-корр. РАН, заслуженный деятель науки РФ Г.А. Тосунян**, подчеркнувший, что изменения, происходящие в экономике, выражаются в переходе от производства, оборота материальных товаров и услуг к производству и обороту так называемых цифровых товаров и услуг, и прежде всего самой информации.

В цифровом пространстве территория обращения информации, как отметил Г.А. Тосунян, определяется не столько наличием инфраструктуры для Интернета или его доступностью, сколько уверенностью контрагентов в достоверности существования этой информации и прав друг друга, т.е. при нахождении в определенном информационном пространстве необходимо понять, каков “периметр доверия” — насколько этой информации можно доверять.

В мире финансовых услуг при переходе в цифровое пространство построение “периметра доверия” определяется не только вопросами идентификации и аутентификации, но и противодействием отмыванию доходов и финансированию терроризма. В этом направлении на законодательном уровне осуществляется ужесточение государственного контроля, а также установление для субъектов правоотношений дополнительных правовых гарантий, способствующих надлежащему удаленному использованию данных, в том числе в банковской сфере.

Инфраструктура Интернета предоставляет возможность почти моментально передавать любые объемы информации. Для вовлечения их в обращение необходимо, по мнению Г.А. Тосуняна, построение интерфейсов между хранилищем данных и инфраструктурой Интернета. Огромное значение для эволюции названной сферы имеет система стандартизации, развитие которой может осуществляться с участием Центрального банка РФ и других финансовых регуляторов.

Среди других важнейших вопросов, требующих особого внимания законодателя и правоприменителя, были выделены: приобретение и реализация прав на цифровые товары и услуги, их защита, информационная безопасность и ответственность, предусмотренная за неправомерное использование данных.

Проблемы применения, использования технологий и защиты информации в автоматизированных информационных системах были рассмотрены в докладе **руководителя российского представительства мирового лидера антивирусного программного обеспечения компании Bitdefender Д.Н. Елисеева**. Согласно приведенным примерам о хищении денежных средств посредством хакерских атак на различные банковские информационные системы, а также совершении мошеннических действий во время ICO одной из существующих проблем в сфере информационной безопасности является отсутствие “цифровой гигиены”. Меры по защите информации и данных должны принимать как владельцы, так и пользователи информационных систем. В частности, речь шла о необходимости систематичной смены паролей; обновления программного обеспечения; использования сертифицированного антивирусного программного обеспечения.

Результат любой автоматизации — работа человека уменьшается за счет функционирования различных информационных систем и программ, что может привести к новым вызовам в областях использования облачных технологий (уязвимости в бессерверных приложениях — сторонние сервисы, нерегулируемый контроль администрирования, неограниченный доступ); автоматизации инструментов маркетинга (CRM-системы, системы автоматизации рекламы и проч.); развития технологий межмашинного взаимодействия (зарождающиеся тенденции M2M — Machine to Machine — минимальное участие, IoT — огромный ботнет и источник мощнейших DDoS-атак); применения инструментов Big data (алгоритмы в Big data тоже уязвимы); анализа данных в режиме реального времени (системы автоматизации бизнеса будут эволюционировать в направлении обработки транзакций real-time, что приведет к полностью синхронизированным операциям).

Д.Н. Елисеев рассказал о возможных мерах, принимаемых интеграторами и производителями программного обеспечения, информационных систем в целях обеспечения их стабильности и информационной безопасности.

Председатель Совета НП НИЦ **С.И. Бочков** в контексте рассматриваемых проблем отметил, что с того времени как началась эпоха защиты информации, в нашем обществе был принят ряд нормативно-правовых актов, появилось множество заблуждений в среде разработчиков при создании различного вида автоматизированных систем в интересах органов государственной власти.

Как правило, опыт и соответствующие навыки предприятий-исполнителей подтверждаются лицензиями и сертификатами (Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, Министерства обороны РФ), при этом соблюдение ГОСТов — обязательное условие. Основная проблема заключается в том, что заказчик считает излишним выставлять соответствующие требования, так как информация, обрабатываемая в автоматизированной системе, не содержит сведений, составляющих государственную тайну. (*Первое заблуждение:*

государственные стандарты (ГОСТы) “отменили”, поэтому можно воспользоваться личным “опытом” и “знаниями” для того, чтобы “убедить” заказчика в собственной компетенции при создании автоматизированных систем любой сложности.)

На сегодняшний день существует нормативная база, определяющая необходимость соблюдения принципов и правил защиты информации в зависимости от ее ценности — стоимости. (*Второе заблуждение: если информация, обрабатываемая в автоматизированной системе, не содержит сведений, составляющих государственную тайну, то можно использовать самые “передовые” зарубежные интернет-технологии (продукты), не обращая внимания на необходимость защиты информации.*)

Качество системы в целом определяется качеством работ на этапах формирования “правильных” требований, получения адекватного требованиям проекта, изготовления, эксплуатации. (*Третье заблуждение: “простота” решения задач по автоматизации (в крайнем случае “перепишем” программное обеспечение) вызывает у заказчика ощущение необязательности формирования детальных требований к создаваемой автоматизированной системе. При этом “не возбраняется пропускать” начальные этапы жизненного цикла системы и приступать сразу к программированию.*)

Качество программного обеспечения автоматизированной системы определяется прежде всего качеством документации — “дорогие” профессионалы не хотят тратить время на “никому не нужную документацию”. Качественная документация — залог качества автоматизированных систем на этапах изготовления и эксплуатации. (*Четвертое заблуждение: существует мнение, согласно которому, если привлечь к созданию автоматизированных систем “дорогих” профессионалов, успех неизбежен.*)

Современный Интернет создавался как средство технической разведки США. И остается таковым по сей день со всеми вытекающими из этого последствиями. (*Пятое заблуждение: Интернет как средство связи не принадлежит никому конкретно. Поэтому этот вид связи самый надежный для создания государственных систем.*)

По мнению докладчика, существуют и другие менее значительные “заблуждения”, которые также негативно влияют на качество и сроки создания автоматизированных систем. При правильном выполнении работ по созданию автоматизированных систем защита информации составляет не более 25% от стоимости системы. В случае внедрения средств защиты в работающую систему конечная стоимость может возрасти многократно.

Существующие проблемы использования и распространения информации были рассмотрены **советником юридической фирмы “ЮСТ”, канд. юрид. наук Д.И. Серегиним** в контексте защиты конкуренции с учётом специфики информационных технологий. Как полагает выступающий, в настоящее время основным средством ведения конкурентной борьбы становятся информационные технологии. С точки зрения антимонопольного законодательства специфика организаций,

осуществляющих свою деятельность в сфере информационных технологий, состоит в том, что они находятся во взаимосвязи практически со всеми другими отраслями экономики; от них зависят большое количество и новизна моделей рынка, а множество вариантов интерпретации поведения хозяйствующих субъектов затрудняет оценку эффектов для конкуренции; идентификация товара осложняется относительной новизной отрасли, отсутствием устоявшихся моделей бизнеса; факторы доминирования на рынке чаще всего прямо не поименованы в законе, а находятся эмпирическим путем.

Организации, занятые в сфере информационных технологий, укрупняются, растут и получают возможность оказывать влияние на рынок. При этом, переходя в эпоху цифровой экономики, непонятна правовая природа самого главного актива — информации. Информационное законодательство в полной мере не регулирует вопросы использования, передачи и распространения информации, а исключение информации из объектов гражданских прав создало ситуацию, при которой субъектам правоотношений не предоставляется возможность надлежащей реализации их прав и интересов в отношении такого объекта, как информация.

Оценка влияния поведения компании на конкуренцию зависит от модели рынка: организация может влиять на рынок, где она занимает доминирующее положение, или на смежный с ним. Выделено несколько моделей рынков: “основной — производный товар”; “двусторонние рынки”; модель рынка с “ключевыми мощностями” (*essential facilities*).

В этой связи Д.И. Серегин назвал некоторые вызовы антимонопольного законодательства. В частности, речь шла о том, что монополизация информационной “биосферы” может создать барьеры для прямой коммуникации между производителем и потребителем; укрупнение (и слияние) массовых социальных сетей в силу сетевого эффекта создает возможность манипулирования потребителями и влияния на рынок.

Секция была завершена докладом **главного специалиста-эксперта отдела защиты от недобросовестной конкуренции управления контроля рекламы и недобросовестной конкуренции ФАС России И.Н. Кожевникова**, которым в первую очередь были выделены основные виды нарушений в Интернете, в том числе недобросовестная конкуренция, путем дискредитации, введения в заблуждение, некорректного сравнения, связанные с созданием смешения, а также приобретением и использованием исключительного права на средства индивидуализации юридического лица, средства индивидуализации товаров, работ или услуг и др. В ходе выступления были подробно проанализированы каждый из названных правонарушений на примере дел, рассмотренных Федеральной антимонопольной службой, в частности дела АО “Лаборатория Касперского” против Microsoft Corporation; Black Friday.

В рамках второго дня Форума состоялась **секция “Криптовалюты как инструмент привлечения средств для финансирования венчурных проектов”**. Модератор — юрист

с международной практикой в инвестиционной сфере, член Эдвайзори групп Plus Ultra, советник Европейского банка Е. Аккуш (Лимассол, Кипр).

Обозначая основные тенденции развития криптовалют, **Председатель Комитета ТПП России по финансовым рынкам и кредитным организациям, Управляющий партнер Группы компаний “Аудит Групп” и “Финансовый интегратор”, канд. экон. наук, канд. юрид. наук, проф., член Международной академии экономики, финансов и права В.А. Гамза** подчеркнул, что сегодня криптовалюта — это технология (блокчейн) и финансовый актив (собственная цифровая валюта). Блокчейн используется не только для совершения действий с криптовалютами, но и для операции с другими активами.

Однако криптовалюта помимо положительных имеет и негативные последствия. Например, с точки зрения национальной безопасности она может быть использована в целях отмывания доходов, полученных преступным путем, финансирования терроризма, уклонения от уплаты налогов. Более того, ее использование может быть направлено на формирование различных пирамид.

В ходе выступления было высказано мнение, согласно которому криптовалюта складывается из базовой криптовалюты (биткоин и т.д.) и токена. Базовые криптовалюты рассматривались в качестве долговых обязательств, а токен как электронные акции. В.А. Гамза рассказал о существующих в Российской Федерации законодательных инициативах и обратил внимание, что формирование нормативной основы необходимо осуществлять с учетом позиции Банка международных расчетов, издающего рекомендации для участников банковских, финансовых правоотношений.

Партнер Plus Ultra Partners Е. Архипов посвятил выступление ICO (*Initial Co in Offering*) как инструменту для финансирования только создаваемых, развивающихся компаний. Были не только названы крупнейшие ICO 2017 г. (*Filecoin, Tezos, EOS, Bancor, Status*), но и рассмотрен порядок его проведения, состоящий из нескольких стадий: эмитент токенов продает токены инвесторам через смарт-контракт; документы по продаже токенов (договор купли-продажи/проспект по частному размещению/иное) заключаются от лица эмитента; собранные средства эмитент передает операционной компании в виде криптовалюты или в виде фиатных валют; инвесторы покупают токены и имеют возможность продажи вторичным инвесторам на крипто-биржах.

Как было отмечено, в практике сформировалось деление токенов на две основные категории: продуктовые токены и ценные бумаги. Раскрывая порядок создания и размещения токенов, были приведены особенности регулирования в некоторых странах: США, Канаде, Китае, Южной Корее, Сингапуре, Швейцарии. При этом, по мнению Е. Архипова, в сложившихся условиях требуется не только унифицированное международное регулирование, но и разъяснения по вопросам криптовалют.

Партнер Baker Boots Е. Степаненко, руководствуясь практикой представляемой ей организации, также

подчеркнула, что в России отсутствует правовое регулирование криптовалют и ICO. Среди основных проблем, требующих решения в рассматриваемой сфере, были названы: отсутствие юридической квалификации предмета сделки, вида заключаемого договора; применимо ли существующее регулирование к сделкам, где стороны не влияют на их исполнение (*smart contract*); соблюдение требований о защите персональных данных; валютный контроль; налогообложение; противодействие отмыванию доходов, полученных преступным путем, и финансированию терроризма; контроль за участниками и площадкой/биржей на IPO/ICO.

Один из основных затронутых вопросов — необходимость определения существующей договорной конструкции, применимой для такой разновидности сделок, что приобретает особую актуальность в условиях использования смарт-контрактов, представляющих собой автоматизированный процесс взаимодействия.

Е. Степаненко были не только обозначены существующие проблемы, но и проанализированы формирующаяся практика, российские законодательные инициативы, а также перспективы их принятия для развития и становления правового регулирования рынка криптовалют.

О практических аспектах проведения ICO рассказал партнер, соруководитель глобальной практики **Растущие компании и венчурный капитал DLA Piper Л. Баталов**. Был поставлен ряд вопросов, возникающих при проведении ICO, в частности выбор юрисдикции совершения операций, который обусловлен нахождением в ней преобладающего большинства инвесторов, т.е. США, Азия, Россия, Украина и Европа; а также эмитента токенов.

Л. Баталов подробно остановился на существующих практических аспектах решения обозначенных им вопросов с учетом правоприменительной практики и нормативного, государственного регулирования, складывающегося в названных юрисдикциях.

Модератор секции **Е. Аккуш** в своем выступлении отметила, что деньги — это технология, прошедшая свою эволюцию через инновации. Биткоин, по ее мнению, — первая форма денег, основанная на протоколе и квалификация криптовалюты посредством существующей терминологии, это попытка построить новое явление финансового мира в старый понятийный аппарат и уже имеющееся регулирование. Дан анализ опыта Европейского Союза в части становления правового и государственного регулирования криптовалют, перечислены преимущества и риски, определенные European Banking Authority (EBA). Источники рисков были представлены в рамках нескольких групп: криптовалюту может создать кто угодно, для чего угодно, изменение в протокол криптовалюты может сделать кто угодно; плательщик и покупатель анонимные; глобальное присутствие криптовалюты (вне национальных границ); отсутствие профессиональных стандартов участников оборота; неясный порядок формирования цены на биржах; отсутствие гарантий платежа или возврата;

отсутствие нормативных определений и стандартов отрасли; информационный дефицит, ненадежность источников; отсутствие стабилизирующего отрасль элемента (обменный курс, рассмотрение споров).

Е. Аккуш подчеркнула, что традиционные методы регулирования не могут применяться, поскольку законодатель не понимает природы криптовалюты — нет определяющего законодательства, а регулятор квалифицирует криптовалюты в первую очередь как финансовые инструменты и предпринимает попытку применить инвестиционное регулирование, а к ICO — краудфандинг. Выделены основные направления, требующие регулирования: выпуск и оборот криптовалюты (определение криптовалюты, требования к эмитентам и правила оборота); требования к приобретателям (AML/CTF/KYC); конвертация криптовалюты в фиатные деньги.

В контексте анализа формирования регулирования криптовалют в Европейском Союзе были рассмотрены европейская система надзора, задачи составляющих ее органов; направления возможного регулирования; а также деятельность и позиции European Banking Authority (EBA) и European Securities and Markets Authority (ESMA) в сфере регулирования криптовалют и ICO.

Руководитель блокчейн направления Группы компаний “Инженеринговые технологии” С. Отелли рассказал о видах хакерских атак и об обеспечении информационной безопасности при совершении операций с криптовалютами и проведении ICO, предложив классификацию хакерских атак по объектам, сервисам или отдельным приложениям, целям атак. Широкое распространение в рассматриваемой сфере сейчас получают “тройные” программы, вирусы, шифрующие файловые системы компьютеров, фишинг. Докладчик обратил внимание на необходимость выбора тех кошельков, которые позволят обеспечить сохранность данных, а также использование других средств.

В результате работы, проведенной на пленарном заседании, профильных секциях, а также в формате дискуссий, участниками ILTF 2017 принято решение о формировании отчета о состоянии высокотехнологичной сферы по рассмотренным направлениям, тенденциях ее эволюции, существующих проблемах и возможных подходах к их решению с учетом не только технического, организационного, но и правового инструментария. Определено, что становление надлежащего правового регулирования является одним из важнейших факторов, стимулирующих развитие высоких технологий в России и за рубежом, способных обеспечить конкурентоспособность бизнеса и государства, а также направленных на удовлетворение их прав и интересов.

Участники ILTF 2017 пришли к выводу о необходимости дальнейшего обсуждения поставленных актуальных проблем при проведении следующего Международного форума “Право, высокие технологии, национальная безопасность” (*International Law & Technology Forum/ILTF*), запланированного на осень 2018 г.

LAW, HIGH TECHNOLOGY, NATIONAL SECURITY: PROBLEMS OF THEORY AND PRACTICE

© 2018 M. V. Demyanets^{1, *}, E. V. Ponizova^{2, **}, V. A. Mikhailovskaya^{3, ***}

¹*Russian Academy of national economy and public administration
the President of the Russian Federation, Moscow;*

*Moscow state pedagogical University;
Information and Legal Center "Pravoinform", Moscow;*

²*Russian Academy of Sciences, Moscow*

³*Institute of State and Law of the Russian Academy of Sciences, Moscow*

**E-mail: mvd@cpinf.ru*

***E-mail: evp@cpinf.ru*

****E-mail: varvaramih91@bk.ru*

Received 26.12.2017

The article examines the role of law in the regulation of high technologies, the problems that arise in the process of their creation, implementation and use, the trends in the development of the economy and public administration in the conditions of digitalization and informatization.

Key words: legal regulation, information technology, robotics, automation, artificial intelligence, identification, information systems, information networks, information security, national security, competition.